



Simply Better Connections

KG0016 / KG0032

16/32-Port KVM over IP
OmniBus Gateway
User Manual

Compliance Statements

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT

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

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

FCC Caution

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

Warning

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

Achtung

Der Gebrauch dieses Geräts in Wohnumgebung kann Funkstörungen verursachen.

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 .

Industry Canada Statement

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

CAN ICES-003 (A) / NMB-003 (A)

RoHS

This product is RoHS compliant.

Battery Safety Notice

- ◆ There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the relevant instructions.

Batterie avis de sécurité

- ◆ Il existe un risque d'explosion si la batterie est remplacée par un incorrect tapez. Jeter les piles usagées selon la pertinente instructions.

User Information

Online Registration

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

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

Telephone Support

For telephone support, call this number:

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

User Notice

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

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

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

Product Information

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

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

Package Contents

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

The standard KVM over IP OmniBus Gateway package consists of:

- 1 KG0016 / KG0032 16/32-Port KVM over IP OmniBus Gateway
- 1 foot pad set (4 pcs)
- 1 mounting kit
- 2 control terminal blocks
- 2 power cords
- 2 Lok-U-Plugs
- 1 Lok-U-Plug installation tool
- 1 user instructions

Content

Compliance Statements	ii
Battery Safety Notice	iii
Batterie avis de sécurité	iii
User Information	iv
Online Registration	iv
Telephone Support	iv
User Notice	iv
Product Information	v
Package Contents	vi
Content	vii
About This Manual	xiv
Conventions	xvi
Terminology	xvi

Chapter 1. Introduction

Overview	1
Features	3
Hardware	3
Management	3
Easy-to-Use Interface	4
Security	4
Virtual Media	5
Virtual Remote Desktop	5
System Requirements	6
Servers	6
KVM DigiProcessors	7
Operating Systems	7
Browsers	8
Cable Holders	8
Components	9
KG0016 Front View	9
KG0016 Rear View	9
KG0032 Rear View	9

Chapter 2. Hardware Setup

Overview	13
Before You Begin	13
KG0016 / KG0032 Installation	14
Single-Stage Installation Diagram	15
Securing the Cables	16
Connecting the USB KVM DigiProcessor	17
Hot Plugging	20
The Adapter ID Function	20
Powering Off and Restarting	20

Port Selection	20
LCD Operation	21
Home Screen	22
Menu Screen	23
Environment Status Screen	24
Restore to Default	25
Reboot System	25
Shutdown System	26

Chapter 3. Logging In

Overview	27
Browser Login	28
Windows Client AP Login	29
The Windows Client AP Connection Screen	30
Connecting – Windows Client AP	31

Chapter 4. The User Interface

Overview	33
The Web Browser Main Page	33
Page Components	34
Manufacturing Number	34
Tab Bar	35
About	36
User Settings	37
Preferences Settings	38
View Preference	40
Adjust Viewer Preference	40
Change Password	41
The AP GUI Main Page	42
The Control Panel	43
WinClient Control Panel	43
WinClient Control Panel Functions	44
Online Ports	46
Favorite	46
Adding / Removing Port(s)	47
Window Position	48
Start Array	49
The Message Board	50
Message Display Panel	50
Compose Panel	50
User List Panel	50
Video Settings	51
Network Bandwidth Information for KVM Sessions	53
Zoom	54
Mouse DynaSync Mode	55
Automatic Mouse Synchronization (DynaSync)	55
Mac and Linux Considerations	56

Manual Mouse Synchronization	56
Mouse Pointer Type	57
The On-Screen Keyboard	58
Changing Languages	58
Selecting Platforms	59
Expanded Keyboard	59
Macros	60
Hotkeys	60
User Macros	62
System Macros	66
Virtual Media	69
Mounting Virtual Media	69
Mounting Virtual Media - Drag and Drop	71
More Settings	74
Dock Position	74
Customize Control Panel	75
User Preferences	76
Change Password	76
The Web Client Control Panel	77
Functions	77
Web Client Video Settings	78
Web Client On-Screen Keyboard	79
Web Client Mouse Pointer Type	79
Virtual Media	80
Web Client Mouse Sync Mode	81
Automatic Mouse Synchronization (DynaSync)	81
Mac and Linux Considerations	82
Manual Mouse Synchronization	82

Chapter 5. Dashboard

Overview	83
System Status	83
Device Overview	84
Online Status	85
Device Information	85
System Status	86

Chapter 6. Port Access

Overview	87
The Sidebar	88
The Sidebar Tree Structure	88
Filter	89
Favorites	90
Adding a Favorite	90
Modifying a Favorite	91
Port Naming	92
Configuration	93

Port Level	94
Access	96
Device Level Browser GUI Interface	96
Port Level Browser GUI Interface	97

Chapter 7.Port View

Overview	99
----------------	----

Chapter 8.User Accounts

Overview	101
Users	102
Modifying User Accounts	106
Deleting User Accounts	106
Group	107
Creating Groups	107
Modifying Groups	109
Deleting Groups	109
Users and Groups	110
Assigning Users to a Group - User	110
Removing Users from a Group - User	111
Assigning Users to a Group - Group	112
Removing Users from a Group - Group	113
Device Assignment	114
Assigning Device Permissions - User	114
Assigning Device Permissions - Group	116
Account Policy	117
Online User	119

Chapter 9.Device Management

KVM over IP OmniBus Gateway Devices	121
Device Information	122
General	122
System Info. & Settings	123
Settings	123
System Status	124
Operating Mode	125
Network	126
IP Installer	126
Service Ports	126
NIC Settings	127
IPv4 Settings	128
IPv6 Settings	129
ANMS	130
Event Destination	130
SMTP Settings	130
Log Server	131
SNMP Trap	132

Syslog Server	132
Authentication	133
RADIUS Settings	133
AD / LDAP Settings	134
SNMP Agent	136
Security	138
Access Protection	138
Login Failures	139
Filter	140
Encryption	143
Security Level	143
Certificate	144
Private Certificate	144
Certificate Signing Request	146
Date / Time	148
Time Zone	148
Date / Time	148
Network Time	149
Disclaimer	150
Chapter 10.Log	
Overview	151
Log Information	152
Filter	153
Notification Settings	155
Chapter 11.Maintenance	
Overview	157
Firmware Upgrade	158
Firmware Upgrade Recovery	159
EDID Update	160
Update Adapter Display Information	160
Backup / Restore	161
Backup	161
Restore	162
Terminal	163
System Operation	164
Restore Default Values:	164
Chapter 12.Download	
Overview	165
Chapter 13.The Log Server	
Installation	167
Starting Up	168
The Menu Bar	169
Configure	169

Events	170
Search:	170
Maintenance:.....	171
Options	172
Help	172
The Log Server Main Screen	173
Overview.....	173
The List Panel.....	173
The Event Panel	174

Appendix

Safety Instructions	175
Rack Mount	177
Consignes de sécurité	178
Montage sur bâti	181
Technical Support	182
North America	182
Specifications	183
KG0016 / KG0032.....	183
Troubleshooting	185
Mouse Problems	187
Virtual Media	189
Web Browser	189
The WinClient AP	190
Sun Systems.....	190
Mac Systems	191
IP Address Determination	192
IP Installer.....	192
Browser	193
IPv6	194
IPv6 Stateless Autoconfiguration	194
Port Forwarding	195
Keyboard Emulation	196
Sun Keyboard	197
Additional Mouse Synchronization Procedures	198
Windows:.....	198
Sun / Linux	199
Additional Video Resolution Procedures	200
Trusted Certificates	201
Installing the Certificate	202
Certificate Trusted	203
Mismatch Considerations	204
Self-Signed Private Certificates	205
Examples	205
Importing the Files	205
Factory Default Settings	206

Virtual Media Support 207
ATEN Standard Warranty Policy. 208

About This Manual

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

The KVM over IP OmniBus Gateway models covered in this user manual include:

Models	Product Names
KG0016	16-Port KVM over IP OmniBus Gateway
KG0032	32-Port KVM over IP OmniBus Gateway

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

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

Chapter 2, *Hardware Setup*, provides step-by-step instructions for setting up the KVM over IP OmniBus Gateway.

Chapter 3, *Logging In*, describes how to log in to the KVM over IP OmniBus Gateway with each of the available access methods: from an Internet browser, a standalone Windows application (AP) program.

Chapter 4, *The User Interface*, describes the layout and components of the KVM over IP OmniBus Gateway user interface.

Chapter 5, *Dashboard*, shows the **KVM over IP OmniBus Gateway**'s device and system information.

Chapter 6, *Port Access*, describes the Port Access page and how to configure the options it provides regarding port and power outlet management.

Chapter 7, *Port View*, describes the panel array mode and how to configure its settings.

Chapter 8, *User Accounts*, shows super administrators and administrators how to create, modify, and delete users and groups, as well as assign attributes to them.

Chapter 9, *Device Management*, shows super administrators how to configure and control the overall KVM over IP OmniBus Gateway operations.

Chapter 10, *Log*, explains how to view, clear and export event log information, and how to set up event notification for the KVM over IP OmniBus Gateway.

Chapter 11, *Maintenance*, explains how to upgrade the KVM over IP OmniBus Gateway firmware, as well as the firmware of the KVM DigiProcessors used to connect its ports to the installed devices.

Chapter 12, *Download*, describes how to download standalone AP versions of the Win Client and the Log Server programs.

Chapter 13, *The Log Server*, explains how to install and configure the Log Server.


Appendix, Provides technical and troubleshooting information at the end of the manual.

Note:

- ◆ Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit or connected devices.
 - ◆ The product may be updated with features and functions added, improved or removed since the release of this manual. For an up-to-date user manual, visit <http://www.aten.com/global/en/>
-

Conventions

This manual uses the following conventions:

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

Terminology

Throughout the manual, the terms *Local* and *Remote* are used in regard to the operators and equipment deployed in a KVM over IP OmniBus Gateway 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 — Someone who logs in over the net from a location that is *remote from the switch*.
- ◆ User's Point of View
 - ◆ Local client users — Someone who's sitting at his computer performing operations on the servers connected to the switch that is *remote from him*.
 - ◆ Remote servers — Servers that are *remote from the local client user*.

Chapter 1

Introduction

Overview

The KG0016 / KG0032 16/32-Port KVM over IP OmniBus Gateway provides remote over IP access, allowing users to access, monitor, and control up to 16/32 servers over a network. With KG0016 / KG0032's independent remote connections, it ensures higher operation efficiency and optimizes the user experience by eliminating waiting time and bus sharing. This single management platform connects servers through a single secure portal, simplifying access and control for efficient administration. With its all digital KVM over IP architecture, the KG0016 / KG0032 prevents video lagging and freezing, ensuring stable and smooth video display, particularly in long-distance extension application. Equipped with dual on-board 10G NICs for redundancy, this series is built to guarantee reliability and availability of remote access to all servers. The virtual media transmissions are 10 times faster than traditional KVM over IP switches, allowing for the completion of a 1GB file transmission in just one minute. When the KG series works with the KVM DigiProcessor series (KG1900T / KG6900T / KG8900T / KG9900T), it delivers superior video resolutions up to 1920 x 1200 @ 60 Hz, for distances up to 100 meters over a single Cat 5e/6 cable.

The KG series can be remotely accessed via WinClient AP or HTML5 WebClient* at a console from a separate location for management and operation. The WinClient AP comes with complete KVM functions and provides users with continuous, reliable connections. It can help users to simultaneously monitor the status of all connected servers on Array View and control a specific server through Control View. For basic KVM functions, users can directly access and control one of the ports through the HTML5 WebClient by simply launching a client viewer from a browser, without the need for pre-installed software. Additionally, it allows users to easily separate the client viewer from the browser and drag it to a second monitor for control while monitoring the status of all ports on the Port View from Web GUI.

This KVM over IP OmniBus Gateway allows out-of-band access to connected servers from remote consoles via the management network for BIOS-level troubleshooting when the production network is down. It enables IT administrators to manage servers via management networks that are separated from the main / production networks. If there's difficulty in accessing the servers through the production network, administrators can still access servers

via KG series. To provide stringent security, the KG series offers TLS 1.3 and an embedded FIPS 140-2 certified OpenSSL cryptographic module. Security features of the KG series include 256-bit AES encryption for secured data transmissions, as well as RADIUS, LDAP, LDAPS, and MS Active Directory for 3rd-party authentication services.

Additional exclusive features of KG series include a Message Board, Panel Array Mode™ Live+, Mouse DynaSync™, and a front panel LCD display. ATEN KVM over IP OmniBus Gateway saves users time and money by enabling administrators to manage their servers from virtually anywhere – minimizing travel and MTTR (Mean Time to Repair) costs, ensuring the highest availability for data center services.

Note: We recommend using the WinClient app for more robust management and control. Performance and usage may vary depending on the user's hardware configuration. A minimum of 8 GB RAM, dual core CPU, and a graphics card that supports OpenGL are required. Please also make sure that the browser used is up to date.

Features

Hardware

- ◆ High port density – RJ-45 connectors and Cat 5e / 6 cable for up to 16/32 ports in 1U housing (KG0016 / KG0032)
- ◆ All-digital KVM over IP optimum transmission – offers reliable transmission over long distances with noise immunity, signal quality preservation, and efficient compression
- ◆ Extends 1920 x 1200 @ 60 Hz resolutions up to 100m via Cat 5e/6 without signal interference and close-to-zero latency
- ◆ Up to 16/32 independent connections for remote KVM over IP access
- ◆ Dual 10G NICs for redundant LAN or two IP operation
- ◆ LCD display – provides real-time connection status, notifications, and system alert message
- ◆ LED indication of connection and hardware status
- ◆ Multi-platform server environments: Windows, Mac, and Linux
- ◆ All-around ventilation chassis design improves airflow efficiency – induces cold air suction on both sides at the front panel and dissipates heat via ventilation holes on the back panel
- ◆ Dual power supply with power redundancy

Management

- ◆ Simultaneously shares 16/32 independent connections to the attached servers (KG0016 / KG0032)
- ◆ Out-of-Band access
- ◆ Green IT Fan – auto-fan-speed adjustment corresponding to temperature
- ◆ Event logging and Windows-based log server
- ◆ Event notification – supports notification of SMTP email, SNMP Trap, and SMS (with additional mobile devices)
- ◆ Event destination – event logs will be saved to Log server, and Syslog server
- ◆ Firmware upgradeable
- ◆ Port share mode – allows multiple users to gain access to a server simultaneously
- ◆ Supports IPv4, IPv6

Easy-to-Use Interface

- ◆ The intuitive WinClient AP's supports of an Array View and a Control View – enables users to monitor all servers and control a specific server concurrently
- ◆ Panel Array Mode™ Live+ – real-time monitoring of livestreamed video feeds from all ports in a configurable multi-screen layout
- ◆ Browser-based, and AP GUIs offer a unified multi-language interface to minimize user training time and increase productivity
- ◆ Multiplatform client support (Windows, Mac OS X, and Linux) via WebClient
- ◆ Multi-browser support – Edge, Chrome, Firefox, Safari, and Opera
- ◆ Supports web-friendly KVM-over-IP access with HTML5 WebClient viewer – users can remotely access all the connected servers and PCs without Java or browser plug-in installation
- ◆ Full-screen or sizable and scalable virtual remote desktop
- ◆ Keyboard / mouse broadcast – keyboard and mouse signals can be duplicated across all servers simultaneously

Security

- ◆ High-grade security – supports an embedded FIPS 140-2 certified OpenSSL cryptographic module (Certificate #4282)
- ◆ Remote authentication support: RADIUS, LDAP, LDAPS, and MS Active Directory
- ◆ Supports TLS 1.3 data encryption and RSA 2048-bit certificates to secure user logins in from 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 video, and virtual media data encryption
- ◆ Support for IP / MAC filter
- ◆ Configurable user and group permissions for server access and control
- ◆ Automated CSR creation utility and third party CA certificate authentication

Virtual Media

- ◆ Virtual media transmission rate is approximately 10 times faster than traditional KVM, ideally for file transfers, OS patching, software installation, and diagnostic testing
- ◆ Works with USB-enabled servers in operating system and at the BIOS level
- ◆ Supports USB2.0 DVD / CD drives, USB mass storage devices, PC hard drives, and ISO images

Virtual Remote Desktop

- ◆ Video quality such as color depth and bandwidth's increment / decrement can be adjusted for optimizing data transfer speed
- ◆ Mouse DynaSync™ – automatically synchronizes remote mouse movements
- ◆ On-screen keyboard with multi-language support
- ◆ BIOS-level access for troubleshooting

System Requirements

Remote User Computers

Remote user computers (also referred to as client computers) are the ones the users log in to the KVM over IP OmniBus Gateway with from remote locations over the Internet (see *Terminology*, page xvi). The following equipment must be installed on these computers:

- ◆ For best results, we recommend computers with at least a Pentium III 1+ GHz processor, with their screen resolution set to 1024 x 768.
- ◆ IE8 or above web browser.
- ◆ Browsers must support TLS 1.2 encryption.
- ◆ For best results, a network transfer speed of at least 1 Gbps is recommended.
- ◆ For the DirectX 8 must be present, and at least 4 GB of memory must be available after installation.
- ◆ For the Windows Client AP, DirectX 8 must be present, and at least 90 MB of memory must be available after installation.
- ◆ For the *Log Server*, you must have the Microsoft Jet OLEDB 4.0 or higher driver installed.

Servers

Servers are the computers connected to the KVM over IP OmniBus Gateway via KVM DigiProcessors. The following equipment must be installed on these servers:

- ◆ A VGA, SVGA or multisync port.
- ◆ For USB KVM DigiProcessors Cable Connections: a Type A USB port and USB host controller.

KVM DigiProcessors

- ◆ Cat 5e (or higher) cable is required to connect the KVM over IP OmniBus Gateway to the KVM DigiProcessors (see page 17).
- ◆ The following KVM DigiProcessors are required for use with the KVM over IP OmniBus Gateway:

Function	Module
For USB computers – VGA output and Virtual Media support	KG1900T
For USB computers – DVI output and Virtual Media support	KG6900T
For USB computers – HDMI output and Virtual Media support	KG8900T
For USB computers – DisplayPort output and Virtual Media support	KG9900T

Operating Systems

- ◆ Supported operating systems for remote user computers include Windows 2000 or later.
- ◆ Supported operating systems for the servers connected to the KVM over IP OmniBus Gateway’s ports are shown in the table, below:

OS		Version
Windows		2000 or later
Linux	RedHat	7.1 or later
	Fedora	Core 2 or later
	SuSE	9.0 or later
	Mandriva (Mandrake)	9.0 or later
UNIX	AIX	4.3 or later
	FreeBSD	4.2 or later
	Sun	Solaris 8 or later
Novell	Netware	5.0 or later
Mac		OS 9 or later*
DOS		6.2 or later

Browsers

Supported browsers for users that log into the KVM over IP OmniBus Gateway include the following:

Browser		Version
IE		8 or later
Edge		118 or later
Chrome		8.0 or later
Firefox	Windows	3.5 or later
	Linux	3.0 or later
Safari	Windows	4.0 or later
	Mac	3.1 or later
Opera		10.0 or later

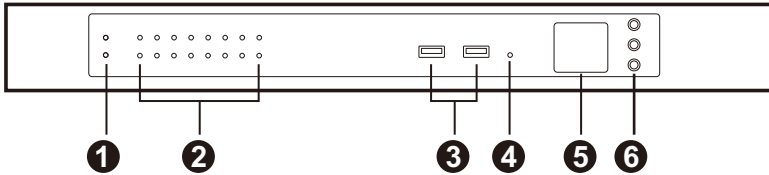
* See *Mac Systems*, page 191, for further information.

Cable Holders

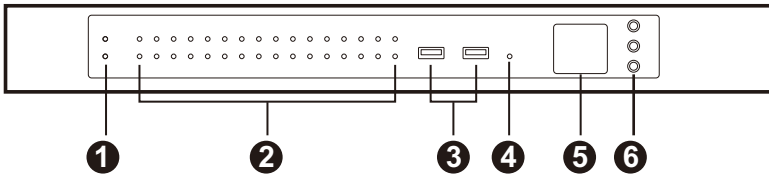
Cable holders are optional accessories. For added safety, use ATEN Lok-U-Plug cable holders to secure the cables in place on the KVM over IP OmniBus Gateway. Only the ATEN Lok-U-Plug cable holders that have been specifically designed to work with the KVM over IP OmniBus Gateway can be used. Using any other kinds of cable securing device could potentially result in irreversible damage or harm to the KVM over IP OmniBus Gateway or users. For a list of compatible cable holders, please refer to the Compatible Products section on the product web page.

Components

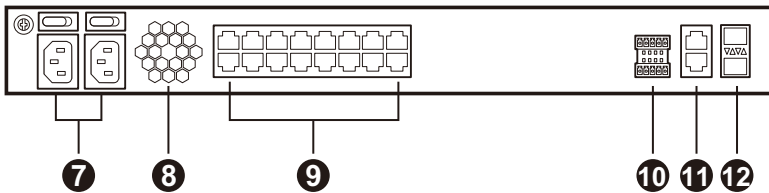
KG0016 Front View



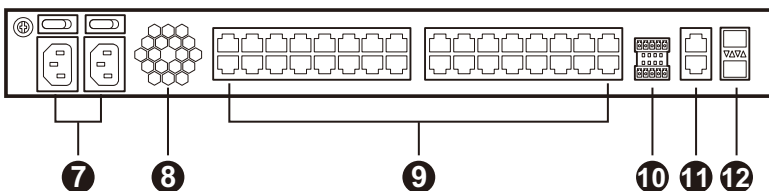
KG0032 Front View



KG0016 Rear View



KG0032 Rear View



No.	Component	Description
-----	-----------	-------------

Front View

No.	Component	Description
1	power LEDs	Lights green when the unit is powered on and indicates which of the two power sources are available.
2	port LEDs	<p>The port LEDs provide status information about their corresponding KVM Ports.</p> <ul style="list-style-type: none"> ◆ GREEN: The computer attached to the port is running 1000 Mbps. ◆ RED: The computer attached to the port is running 10 Mbps. ◆ ORANGE: The computer attached to the port is running 100 Mbps.
3	USB Type-A ports (reserved for future expansion)	Not applicable for now, reserved for future expansion.
4	reset button	<p>Note: This switch is recessed and must be pushed with a small object, such as the end of a paper clip, or a ballpoint pen.</p> <ul style="list-style-type: none"> ◆ Pressing and releasing this switch when the unit is running performs a system reset. ◆ Pressing and holding this switch in for more than three seconds when the unit is running resets its configuration to the factory default settings. <p>Note: This does not clear User Account information. See <i>Factory Default Settings</i>, page 206, for information on clearing user account information.</p> <ul style="list-style-type: none"> ◆ Pressing and holding this switch while powering on the switch returns the unit to its factory default firmware level, rather than the firmware version that the switch has been upgraded to. This allows you to recover from a failed firmware upgrade and gives you the opportunity to try upgrading the firmware again. <p>Note: This operation should only be performed in the event of a firmware upgrade failure that results in the device becoming inoperable.</p>
5	LCD panel	Indicates information of the device, restore the device default, reboot system, and shutdown system. See <i>LCD Operation</i> , page 21.
6	OSD navigation and enter buttons	Controls the LCD screen to see information of the device, restore the device default, reboot system, and shutdown system. See <i>LCD Operation</i> , page 21.

Rear View

No.	Component	Description
7	power sockets and switches	<ul style="list-style-type: none">◆ The power cable(s) plugs in here. The left power socket corresponds to the left power switch, and the right power socket corresponds to the right power switch.◆ These standard slide switches power the unit on and off.
8	fan	Feeds real-time fan speed information to the Device Management page. The speed of each fan in the images above are shown on the <i>Dashboard</i> , See page 83 for details.
9	KVM ports	The Cat 5e cables that link the unit to the KVM DigiProcessors (which connect to the servers), plug in here.
10	digital I/O ports (reserved for future expansion)	Not applicable for now, reserved for future expansion.
11	serial ports (reserved for future expansion)	Not applicable for now, reserved for future expansion.
12	SFP+ slots	The 10 Gbps optical fiber module that connects the unit to the LAN plugs in here.

This Page Intentionally Left Blank

Chapter 2

Hardware Setup

Overview

For convenience and flexibility that allows USB interfaces, as well as multiple platforms, the KVM over IP OmniBus Gateway design utilizes KVM DigiProcessors, that serve as intermediaries between the KVM over IP OmniBus Gateway and the connected devices (see *Connecting the USB KVM DigiProcessor*, page 17 for details).

A separate KVM DigiProcessor is required for each server or device connection. The model numbers are given in the *KVM DigiProcessors* section, page 7.

Before You Begin



1. Important safety information regarding the placement and grounding of this device is provided on page 175 and onwards. 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. Please operate the device with caution when under high environmental temperatures, as the surface of the device may become overheated under such conditions. For instance, the surface temperature of the device may reach 70 °C (158 °F) or higher when the environmental temperature reaches close to 50 °C (122 °F).

KG0016 / KG0032 Installation

Refer to the installation diagrams starting on page 15 (the numbers in the diagram correspond with the numbers of the instruction steps), and do the following:

1. Ground the KG0016 / KG0032 by connecting one end of a grounding wire to the grounding terminal and the other end to a suitable grounded object.

Note: Do not omit this step. Proper grounding helps to prevent damage to the unit from power surges or static electricity.

2. Use a cat 5e/6 cable to connect any available KVM port to a KVM DigiProcessor that is appropriate for the server you are installing and then plug the other end of the KVM DigiProcessor to your server.

Note:

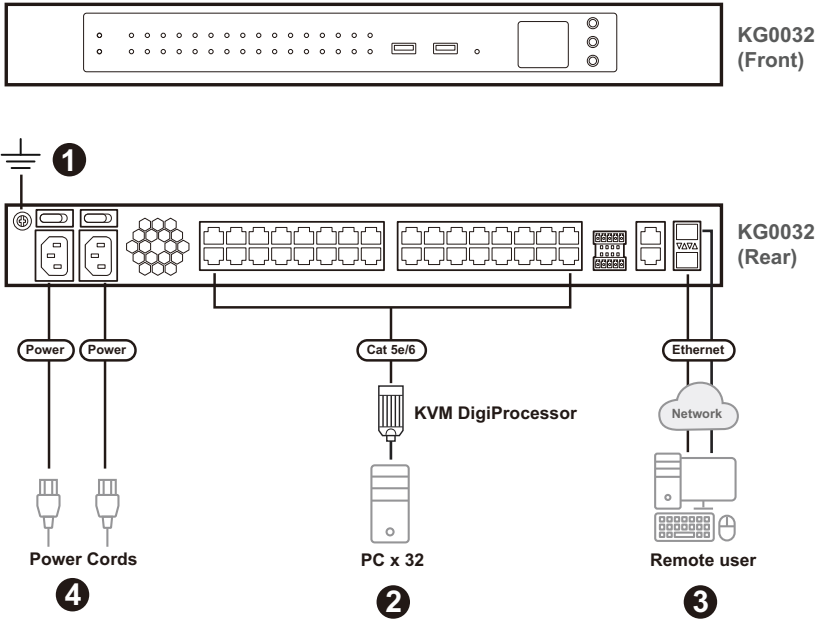
- ◆ The distance between the KVM over IP OmniBus Gateway and the KVM DigiProcessor must not exceed the maximum distance specified for the KVM DigiProcessor you are using.
 - ◆ Make sure the KG0016 / KG0032 and the KVM DigiProcessor are connected directly with each other and there is no network switch in between.
-

3. Connect the fiber module and fiber to the unit's SFP+ slots and connect the other end to a network switch for over IP operation such as WinClient and WebClient.
4. Connect the power cords to one of the unit's power socket and then switch the power switch to ON. Now the KG0016 / KG0032 is powered on.

Note: For power redundancy, connect a second power cord to the unit's second power socket.

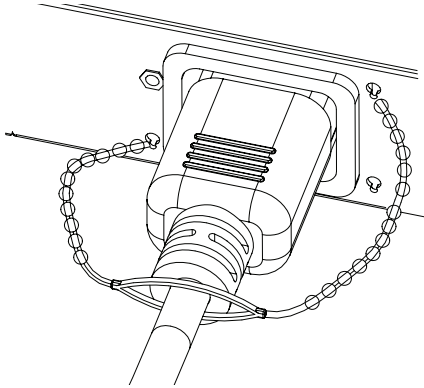
5. Power on the servers and the other connected devices.

Single-Stage Installation Diagram



Securing the Cables

For added safety, use ATEN Lok-U-Plug cable holders to secure the cables of your powered devices in place on the KVM over IP OmniBus Gateway. Secure the cable holders using the specially designed holes around the individual power outlets, as shown below:



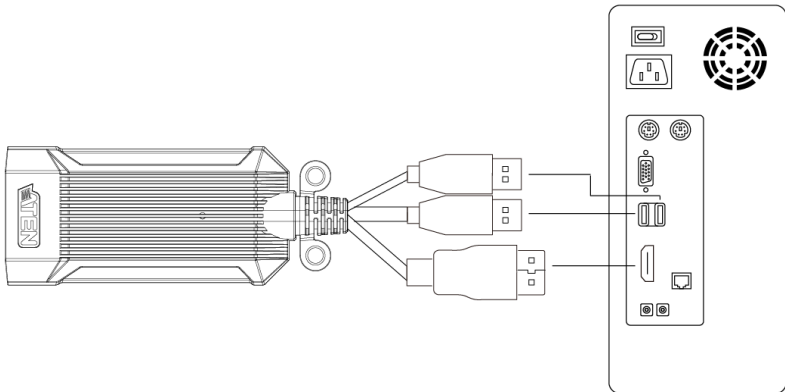
-
- Note:** 1. Cable holders are an optional accessory. See *Cable Holders*, page 8.
2. Only the ATEN Lok-U-Plug cable holders that have been specifically designed to work with the KVM over IP OmniBus Gateway can be used. Using any other kinds of cable securing device could potentially result in irreversible damage or harm to the KVM over IP OmniBus Gateway or users.
-

Connecting the USB KVM DigiProcessor

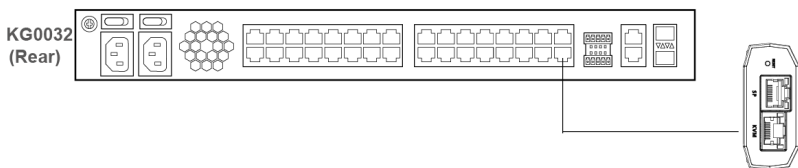
To connect a USB KVM DigiProcessor (KG1900T / KG6900T / KG8900T / KG9900T) to a KVM over IP OmniBus Gateway, follow the steps below.

Note: A KG8900T USB HDMI KVM DigiProcessor is used as an example to illustrate the procedure.

1. Connect the USB and HDMI connectors of the USB KVM DigiProcessor to the corresponding ports on the PC you are installing.



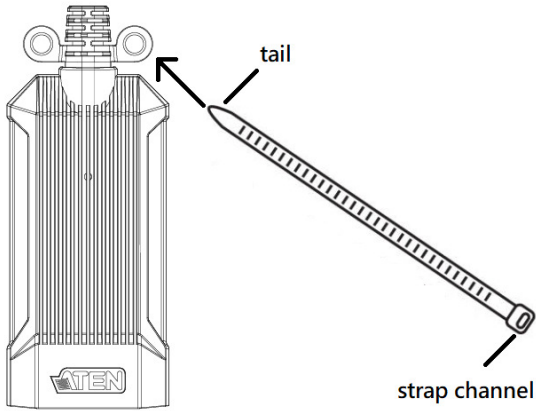
2. Connect the RJ-45 port (KVM port) of the USB KVM DigiProcessor to the KVM over IP OmniBus Gateway's KVM port via a Cat 5e/6 cable.



3. You can secure the USB KVM DigiProcessor to a rack using a cable tie, a screw and a cage nut, or a magic tape.

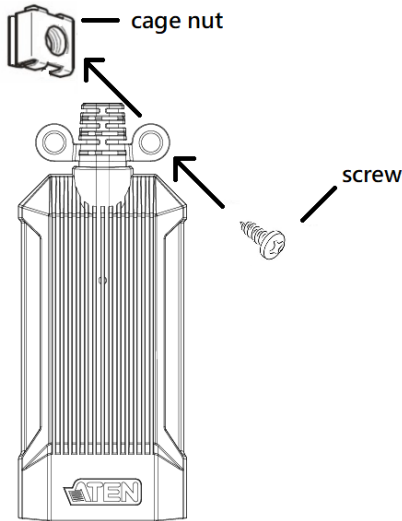
- ◆ **Securing the USB KVM DigiProcessor using a cable tie**

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



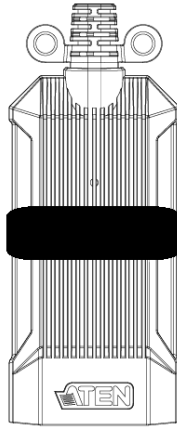
◆ **Securing the USB KVM DigiProcessor using a screw and a cage nut**

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



- ◆ **Securing the USB KVM DigiProcessor using a magic tape**

Use a self-prepared magic tape to hold the USB KVM DigiProcessor to a rack.



Hot Plugging

KVM over IP OmniBus Gateways support hot plugging – components can be removed and added back into the installation by unplugging and replugging cables from the ports without the need to shut the unit down.

Note: If the server's Operating System does not support hot plugging, this function may not work properly.

The Adapter ID Function

KVM DigiProcessor information (the Adapter ID, port name, OS, keyboard language, and access mode) is stored on the KVM DigiProcessor. The KVM over IP OmniBus Gateway's *Adapter ID* function takes this information and stores it along with the KVM DigiProcessor's configuration information (access rights, etc.) in its database. As a result, when you move a server together with its KVM DigiProcessor from one port to another, you do not have to reconfigure its settings. Instead, the Adapter ID function restores them at the new location.

When moving the server and KVM DigiProcessor to another switch, however, only the information that is stored on the KVM DigiProcessor is retained. For the other settings, you must either reconfigure them or use the *Backup/Restore* function (see page 161) to restore them.

Since port settings are stored with the KVM DigiProcessor, if you move a server to a new port without its original KVM DigiProcessor; or if you connect a different server to the KVM DigiProcessor, you must manually reconfigure the port settings for the new server.

Powering Off and Restarting

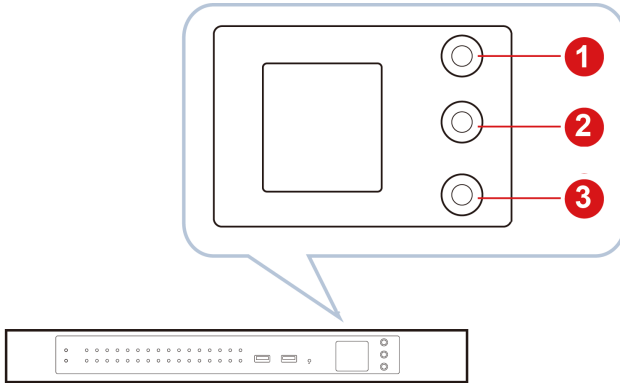
If it becomes necessary to power off the KVM over IP OmniBus Gateway, or if the KVM over IP OmniBus Gateway loses power and needs to be restarted, wait 30 seconds before powering it back on. The servers should not be affected by this, but if any of them should fail, simply restart them.

Port Selection

Port selection is accomplished by means of the GUI. Port selection details are discussed in Chapter 6, *Port Access*.

LCD Operation

The readout section on KVM over IP OmniBus Gateway contains an LCD display for users to check the information of the device, restore the device to default, reboot system, and shutdown system.

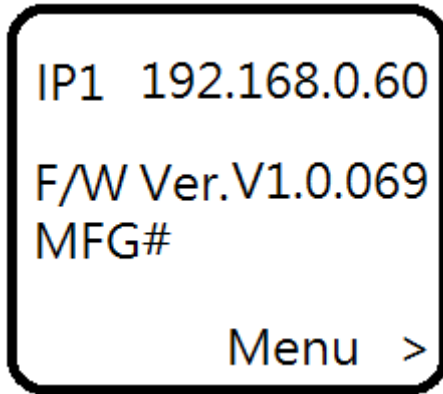


There 3 buttons that deliver the following functions:

No.	Button	Description
1	UP	<ul style="list-style-type: none"> ◆ When you are in the Menu screen, press the button to go up. ◆ Press and hold the button for 3 seconds to lock / unlock the LCD operation.
2	DOWN	<ul style="list-style-type: none"> ◆ When you are in the Menu screen, press the button to go down.
3	Menu / ENTER	<ul style="list-style-type: none"> ◆ Press the button to enter the Menu screen for more information. ◆ Press the button to select.

Home Screen

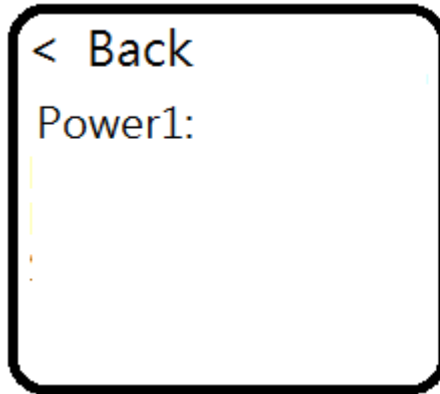
Once the device is connected to an AC power source and turned on, home screen shows on the LCD display.



Item	Description
IP1 / IP2	Indicates the IP address of LAN 1 / LAN 2.
F/W	Indicates the firmware version and MFG number.
Menu >	Press the Menu button to go to the Menu screen.

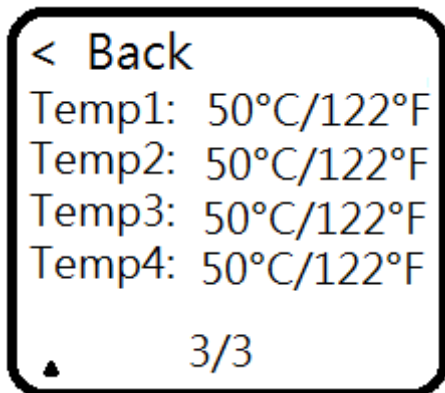
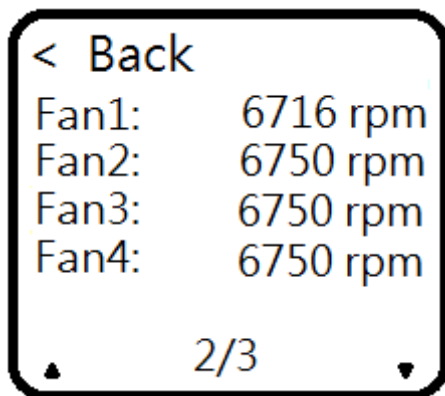
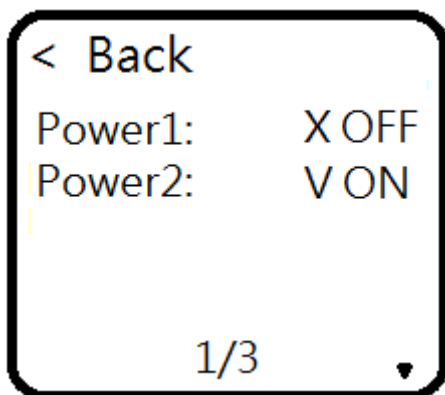
Menu Screen

On main menu screen, you can check the environment status of the KVM over IP OmniBus Gateway, restore the device to default, reboot the system, or shutdown the system.

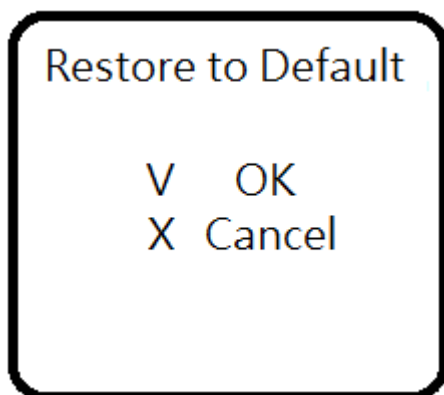


Item	Description
< Back	Press the Enter button to go to the previous screen.
Environment Status	Press the Enter button to go to the Environment Status screen.
Restore to Default	Press the Enter button to restore the device to default.
Reboot System	Press the Enter button to go to reboot the system.
Shutdown System	Press the Enter button to go to shutdown the system. Note: Shutdown System only shutdowns the operating system. To shutdown the device completely, or restart the device, use the power switches located on the unit's rear panel.

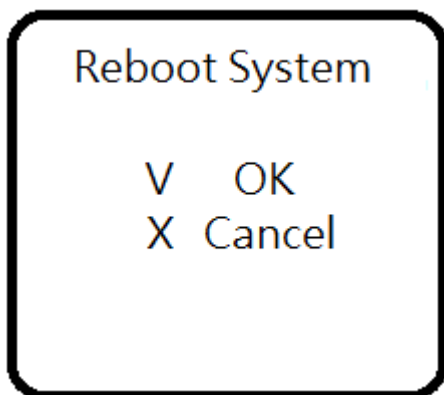
Environment Status Screen



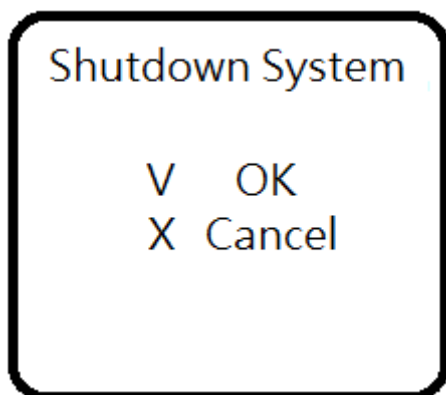
Restore to Default



Reboot System



Shutdown System



Chapter 3

Logging In

Overview

KVM over IP OmniBus Gateway can be accessed from an Internet browser; a Windows application (AP) program.

No matter which access method you choose, the KVM over IP switch's authentication procedure requires you to submit a valid username and password. If you supply invalid login information, the authentication routine will return an *Invalid Username or Password*, or *Login Failed* message. If you see this type of message, log in again with a correct username and password.

Note: If the number of invalid login attempts exceeds a specified amount, a timeout period is invoked. You must wait until the timeout period expires before you can attempt to log in again. See *Login Failures*, page 139 for further details.

Browser Login

KVM over IP OmniBus Gateway can be accessed via an Internet browser running on any platform. To access the KVM over IP OmniBus Gateway, do the following:

1. Open the browser and specify the IP address of the KVM over IP OmniBus Gateway you want to access in the browser's location bar.

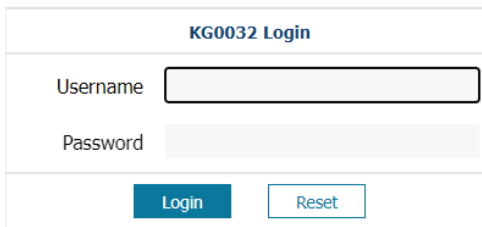
Note: For security purposes, a login string may have been set by the administrator (see page 141 for details). If so, you must include a forward slash and the login string along with the IP address when you log in. For example:

192.168.0.100/kg0032

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

2. When a Security *Alert* dialog box appears, accept the certificate – it can be trusted. (See *Certificate Trusted*, page 203, for details.) If a second certificate appears, accept it as well.

Once you accept the certificate(s), the login page appears:



The screenshot shows a web form titled "KG0032 Login". It contains two input fields: "Username" and "Password". Below the input fields are two buttons: "Login" (a blue button) and "Reset" (a white button with a blue border).

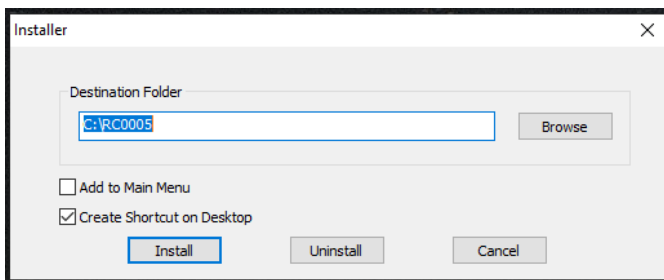
3. Provide your username and password (set by the administrator), then click **Login** to bring up the Web Main Page. For a discussion of the Web Main Page, see page 33.



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

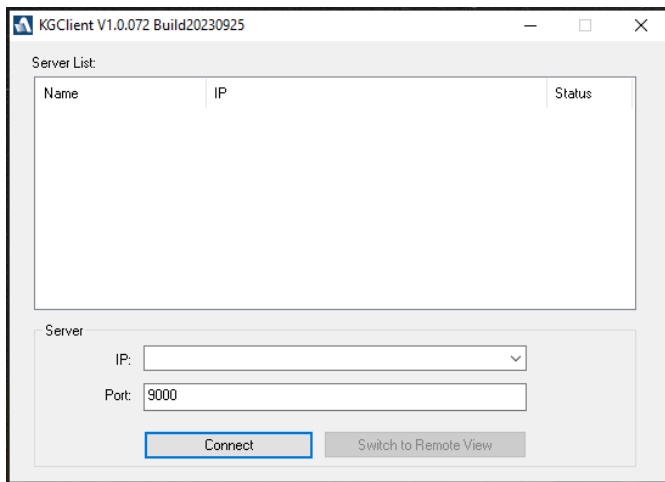
Windows Client AP Login

In some cases, the Administrator may not want the KVM over IP OmniBus Gateway to be available via browser access. The Windows AP Client allows direct remote access to Windows systems users, without having to go through a browser (although you initially download the Windows AP Client program from the browser page – see Chapter 12, *Download*).

To connect to the KVM over IP OmniBus Gateway, go to the location on your hard disk that you downloaded the Windows AP Client program to, and double-click its icon (*WinClient.exe*) to install the WinClient app. The installer page appears.



Click **Install** to install the WinClient app, and you should find an icon that looks like this  on your desktop. Double-click  to bring up the Windows Client Connection Screen:



The Windows Client AP Connection Screen

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

Item	Description
Server List	<p>Each time the WinClient.exe file is run, it searches the user's local LAN segment for KVM over IP OmniBus Gateway, and lists whichever ones it finds in this box. If you want to connect to one of these units, double-click it. (See <i>Connecting – Windows Client AP</i>, page 31 for details.)</p> <p>Note:</p> <ol style="list-style-type: none"> 1. The KVM over IP OmniBus Gateway will not appear in the list unless its <i>Enable Device List</i> configuration parameter has been enabled. See <i>Operating Mode</i>, page 125 for details. 2. Only units whose Access Port settings for <i>Program</i> (see <i>Service Ports</i>, page 126) match the number specified for <i>Port</i> in the Server area of this dialog box appear in the Server List window.
Server	<p>This area is used when you want to connect to a KVM over IP OmniBus Gateway at a remote location. You can drop down the IP list box and select an address from the list. If the address you want isn't listed, you can key in the target IP address in the IP field, and its port number in the Port field. (If you don't know the port number, contact your Administrator.)</p> <ul style="list-style-type: none"> ◆ When the IP address and port number have been specified, click Connect. (See <i>Connecting – Windows Client AP</i>, page 31 for details.) ◆ When you have finished with your session and come back to this dialog box, click Disconnect to end the connection.
Switch to Remote View	<p>Once you have been authenticated (see <i>Connecting – Windows Client AP</i>, page 31 for details), this button becomes active. Click it to switch to the GUI Main Page. The GUI Main Page is described on page 42.</p>

Connecting – Windows Client AP

To connect to a KVM over IP OmniBus Gateway do the following:

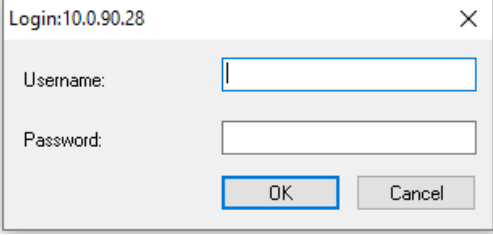
1. From the *Server List* box, **double-click** the device that you wish to connect to.

– Or –

Specify its IP address and port number in the *Server IP* and *Port* input boxes.

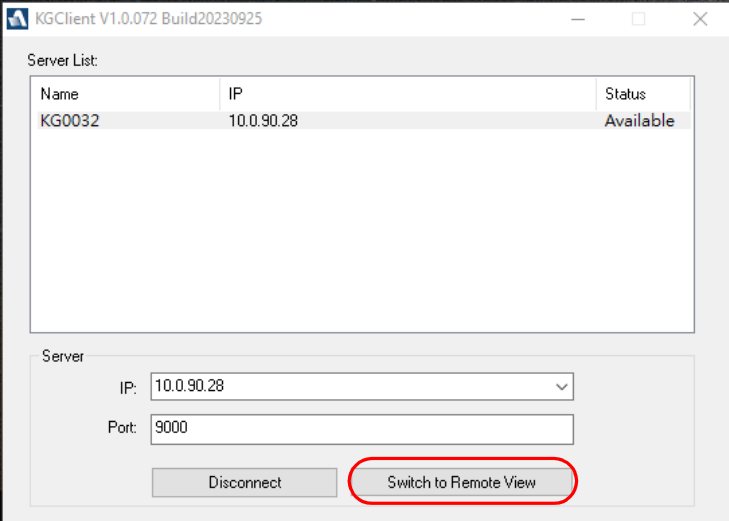
2. Click **Connect**.

The *Login* dialog box appears:



The image shows a 'Login:10.0.90.28' dialog box with a close button (X) in the top right corner. It contains two input fields: 'Username:' and 'Password:'. Below the input fields are two buttons: 'OK' and 'Cancel'.

3. Key in a valid Username and Password, and then click **OK**.
4. Once you have been authenticated, the *Switch to Remote View* button becomes active. Click it to connect to the switch and bring up its GUI Main Page. For a description of the GUI Main Page, see page 48.



The image shows the main window of the KGClient software, titled 'KGClient V1.0.072 Build20230925'. It features a 'Server List' section with a table containing one entry:

Name	IP	Status
KG0032	10.0.90.28	Available

Below the table is a 'Server' section with two input fields: 'IP:' (containing '10.0.90.28') and 'Port:' (containing '9000'). At the bottom of the window are two buttons: 'Disconnect' and 'Switch to Remote View', which is highlighted with a red circle.

This Page Intentionally Left Blank

Chapter 4

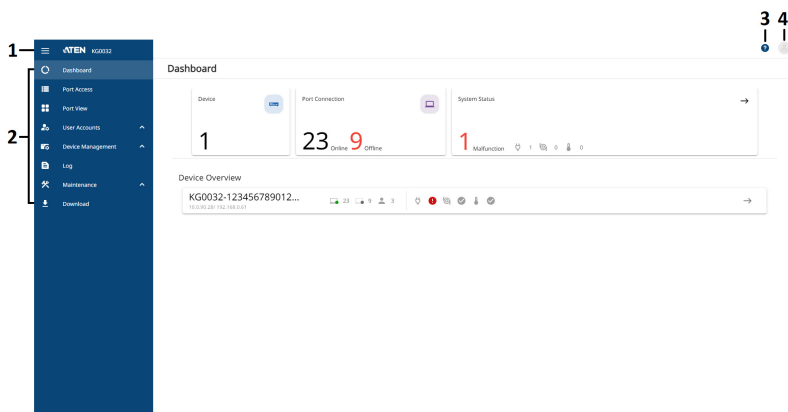
The User Interface

Overview

Once you have successfully logged in, the KVM over IP OmniBus Gateway's user interface Main Page appears. The look of the page varies slightly, depending on which method you used to log in. Each of the interfaces is described in the sections that follow.

The Web Browser Main Page


To ensure multi-platform interoperability, access to the KVM over IP OmniBus Gateway can be accomplished with most standard web browsers. Once users log in and are authenticated (see page 28), the *Web Browser Main Page* comes up, with the Port Access page displayed:



Note: The screen depicts a Super Administrator's page. Depending on a user's type and permissions, not all of these elements appear.

Page Components

The web page screen components are described in the table, below:









No.	Item	Description
1		Click to expand or minimize the Tab Bar.
2	Tab Bar	The tab bar contains the KVM over IP OmniBus Gateway main operation categories. The items that appear in the tab bar are determined by the user's type, and the authorization options that were selected when the user's account was created. See <i>Tab Bar</i> , page 35.
3	About	About provides information regarding the KVM over IP OmniBus Gateway's current firmware version and its online help. See <i>About</i> , page 36.
4	User Settings	Click this button for user information, configure user preferences settings, change password, and logout. See <i>User Settings</i> , page 37.

Manufacturing Number

The “MFG Number” (Manufacturing Number) is an internal serial number used by ATEN’s factory and technical support staff to identify products. This number does not affect products’ warranty. If your product requires after-sales services, you may provide the MFG Number to ATEN’s sales or technical support staff to identify the product and model number.

Tab Bar

The number and type of icons that appear on the Tab Bar at the top of the page are determined by the user's type (Super Administrator, Administrator, User) and the permissions assigned when the user's account was created. The functions associated with each of the icons are explained in the table below:

Icon	Function
	Dashboard: The Dashboard page is used to easily view the device information such port connection, system status, and device overview.
	Port Access: The Port Access page is used to access and control the devices on the KVM over IP OmniBus Gateway installation. This page is available to all users.
	Port View: The Port View page invokes Panel Array Mode. Under this mode, the screen divides into a grid of up to 64 panels.
	User Accounts: The User Accounts page is used to create and manage Users and Groups. It can also be used to assign devices to them. User Management is discussed on page 101. This tab is available to the Super Administrator, as well as administrators and users who have been given User Management permission. The tab doesn't appear for other administrators and users.
	Device Management: The Device Management page is used to configure and control the overall operation of the KVM over IP OmniBus Gateway. This page is available to the Super Administrator, as well as administrators and users who have been given Device Management permission. The tab doesn't appear for other administrators and users.
	Log: The Log page displays the contents of the log file. The Log page is discussed on page 151.
	Maintenance: The Maintenance page is used to install new firmware; backup and restore configuration and account information; ping network devices; and restore default values. The Maintenance page is discussed on page 157. This page is available to the Super Administrator (and Administrators and Users with <i>Maintenance</i> permission). The icon doesn't display on the page of ordinary administrators and users.
	Download: Users can click this icon to download AP versions of the Windows Client; and the Log Server. This page is available to all users. The programs that can be downloaded depend on the user's permissions.

About

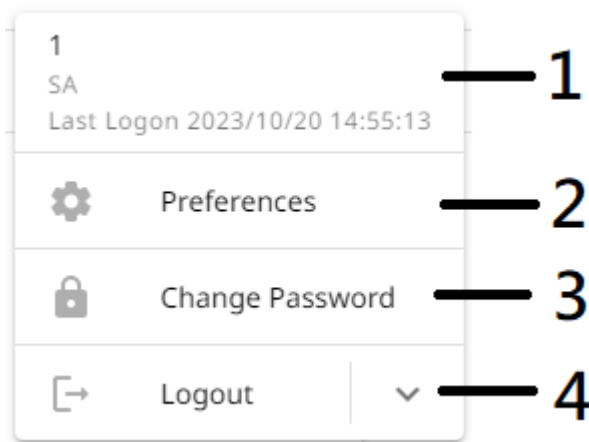
Click to brings up a panel with Online Help and About options.



No.	Item	Description
1	Online Help	Click to access to the KVM over IP OmniBus Gateway webpage for its related information such as QSG and user manual.
2	About	Click to see the information about the KVM over IP OmniBus Gateway's firmware version.

User Settings

Click to bring up a panel with Preferences and Change Password options, or to log out and end your KVM over IP OmniBus Gateway session.



No.	Item	Description
1	User Information	Display the user information and its description.
2	Preferences	Click to configure the user preferences settings such as language, ID display / duration, logout timeout, and viewer settings. See <i>Preferences Settings</i> , page 38.
3	Change Password	Click to change the login password. See <i>Change Password</i> , page 41.
4	Logout	Click to log out and end your KVM over IP OmniBus Gateway session.

Preferences Settings

The *Preferences* page allows users to set up their own, individual, working environments. The KVM over IP OmniBus Gateway stores a separate configuration record for each user profile, and sets up the working configuration according to the *Username* that was keyed into the Login dialog box:

The screenshot shows a 'Preferences' dialog box with the following settings:

- Language:** English
- ID Display:** Port Number + Port Name
- ID Duration:** 3 sec
- Logout Timeout:** 0 min
- Viewer:** #1 Web Client (selected), #2 Win Client

Buttons: Cancel, Save

The page settings are explained in the following table:

Settings	Description
Language	Selects the language that the interface displays in.
ID Display	Selects how the Port ID is displayed: the Port Number alone (PORT NUMBER); the Port Name alone (PORT NAME); or the Port Number plus the Port Name (PORT NUMBER + PORT NAME). The default is PORT NUMBER + PORT NAME.
ID Duration	Determines how long a Port ID displays on the monitor after a port change has taken place. You can choose an amount from 1-255 seconds. The default is 3 seconds. A setting of 0 (zero) means the Port ID is always on.
Logout Timeout	If there is no user input for the amount of time set with this function, the user is automatically logged out. A login is necessary before the KVM over IP OmniBus Gateway can be accessed again.

Settings	Description				
Viewer	<p>In the browser version of this page, a <i>Viewer</i> section is available. You can choose which viewer method is preferred when connecting to a port.</p> <p>Viewer</p> <table border="1" data-bbox="689 240 915 316"><tbody><tr><td data-bbox="689 240 915 276">#1 Web Client</td><td data-bbox="945 252 965 276">↑</td></tr><tr><td data-bbox="689 282 915 316">#2 Win Client</td><td data-bbox="945 290 965 314">↓</td></tr></tbody></table> <p>Refer to <i>Viewer Preference</i> on page 39 (below) for more information.</p>	#1 Web Client	↑	#2 Win Client	↓
#1 Web Client	↑				
#2 Win Client	↓				

View Preference

This section only appears in the browser version of the *User Preferences* page and is mainly concerned with the automatic viewer selection of the system.

To choose a viewer manually, refer to *The Sidebar*, page 88.

Usable viewers are automatically determined by the status of the system at the time of the login and by the type of browser.

When you try to connect to a port (double-click the port or select a port and click the **Connect**), the system will use the viewer according to the viewer list. An example is shown below:

Viewer	#1 Web Client	↑
	#2 Win Client	↓

- ◆ The top-most method is the most preferred method and is listed as #1 (Web Client by default).
- ◆ If the preferred method is supported when connecting to a port, the system will try connecting using the preferred method.
- ◆ If the method is not supported, the system will try connecting using the next method, and try the last method last.

Adjust Viewer Preference

Follow the steps below to adjust the preference.

1. Click to select and highlight the method. The #2 *Win Client* method is shown above as the selected.
2. Click the up ↑ or down ↓ arrow to shift its position around. The up arrow ↑ brings it up (more preferred) while the down arrow ↓ brings it down (less preferred).

Change Password

Change Password
✕

Old Password

New Password

Confirm Password

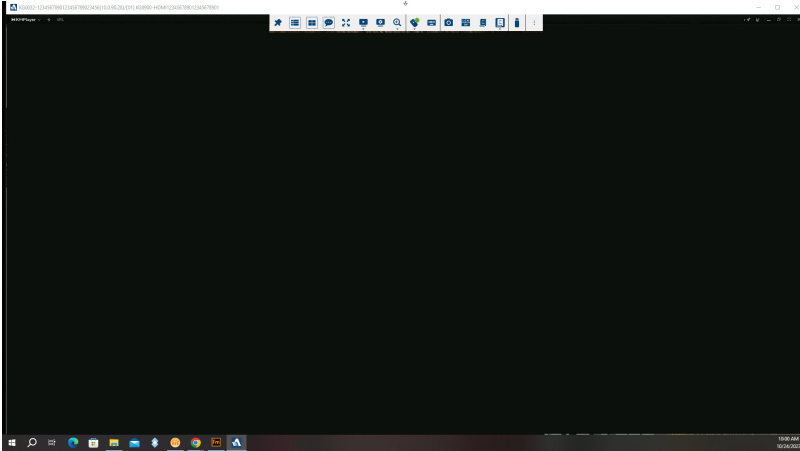
Cancel

Save

Settings	Description
Old Password	Enters the correct old password for the KVM over IP OmniBus Gateway.
New Password	Enters a new password for the KVM over IP OmniBus Gateway.
Confirm Password	Enters to confirm the new password you have entered above for the KVM over IP OmniBus Gateway.

The AP GUI Main Page

With WinClient AP, once users log in (see *Logging In*, page 27), the *GUI Main Page* comes up:



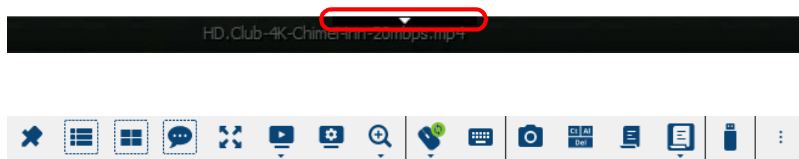
The GUI Main Page is designed for control purpose only. There is a hidden *Control Panel* at the upper or lower center of the screen that becomes visible when you mouse over it. The default is at the upper center of the screen.

The Control Panel

WinClient Control Panel

Since the WinClient Control Panel (for the WinClient AP) contains the most complete functionality, this section describes the WinClient Control Panel. Although the WebClient Control Panel (for the Web Viewer) does not enable all of the features that this one does, the functions that they do share are the same, and you can refer to the information described here when using it.













The Control Panel is hidden at the upper, lower center, right, or left of the screen (the default is at the upper center), and becomes visible when you mouse over it.













Note: The above image shows the complete Control Panel. The icons that appear can be user selected. See *Customize Control Panel*, page 75, for details.

WinClient Control Panel Functions

The Control Panel functions are described in the table below.

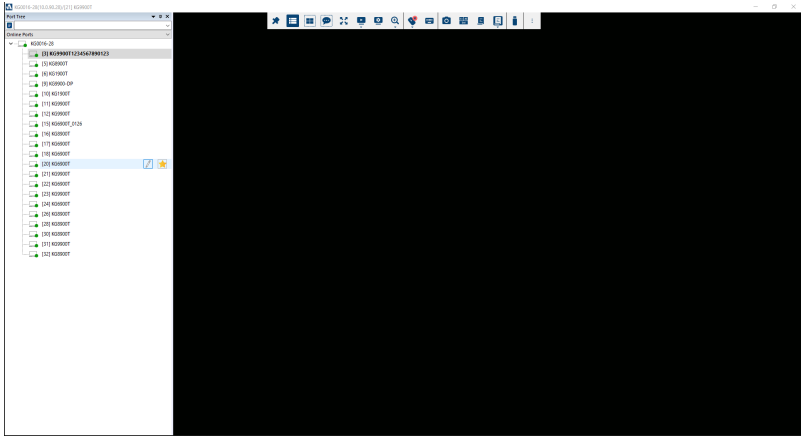
Icon	Function
	This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.
	Click to select the port you wish to connect to.
	Under an accessed port, click to invoke Panel Array Mode (see <i>Port View</i> , page 99).
	Click to bring up the Message Board (see <i>The Message Board</i> , page 50).
	Toggles the display between <i>Full Screen Mode</i> and <i>Windowed Mode</i> .
	Click to select the port you wish to connect to.
	Click to bring up the Video Options dialog box. (see <i>Video Settings</i> , page 51, for details).
	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 54 for details.
	Click to toggle the remote display between color and grayscale views.
	Click to toggle Automatic or Manual mouse sync. <ul style="list-style-type: none"> ◆ 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 55 for a complete explanation of this feature.
	Click to select the mouse pointer type. Note: This icon changes depending on which mouse pointer type is selected (see <i>Mouse Pointer Type</i> , page 57).
	Click to bring up the on-screen keyboard (see <i>The On-Screen Keyboard</i> , page 58).

	Click to take a snapshot (screen capture) of the remote display. See <i>Snapshot</i> , page 75, for details on configuring the Snapshot parameters.
	Click to send a Ctrl+Alt+Del signal to the remote system.
	Click to bring up the Macros dialog box (see page 60 for details).
	Click to display a dropdown list of <i>User</i> macros in order to access and run macros more conveniently than using the Macros dialog box (see the <i>Macros</i> icon in the table above, and the <i>Macros</i> section on page 60).
	Click to bring up the <i>Virtual Media</i> dialog box. The icon changes depending on the status of the virtual media function. See <i>Virtual Media</i> , page 69, for specific details. Note: This icon displays in gray when the function is disabled or not available.
	Click to toggle sound from the remote server to be heard on the client computer's speakers on or off. The "prohibited" symbol (a red circle with a diagonal bar) displays on the icon when the speaker is toggled Off.
	These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. ◆ When the lock state is <i>On</i> , the LED is bright 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. Click on the icon to toggle the status. Note: These icons and your local keyboard icons are in sync.
	Clicking an icon causes the corresponding LED on your keyboard to change accordingly. Likewise, pressing a Lock key on your keyboard causes the icon's color to change accordingly.
	Click to bring up more Control Panel Configuration functions. See <i>More Settings</i> , page 74, for details on configuring the Control Panel.



Online Ports

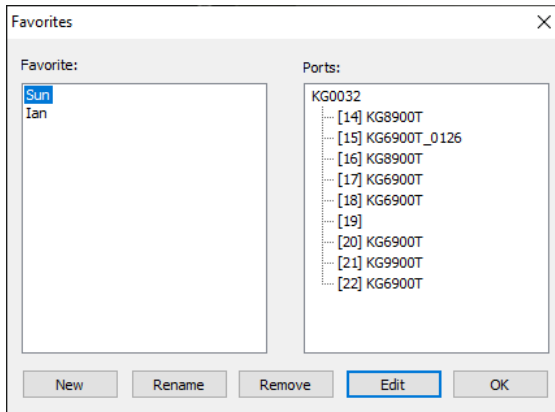
The Online Ports icon shows all the available ports on the KVM over IP OmniBus Gateway. You can access to any of the online port by double-clicking beside it.



Favorite


Click to add a favorite for your online ports.

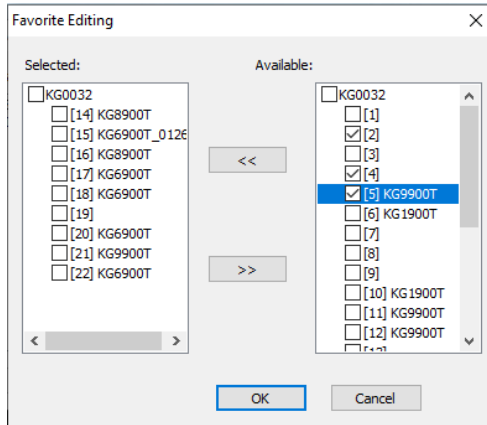
From the pop-up window you can create, rename, remove, or edit a favorite.




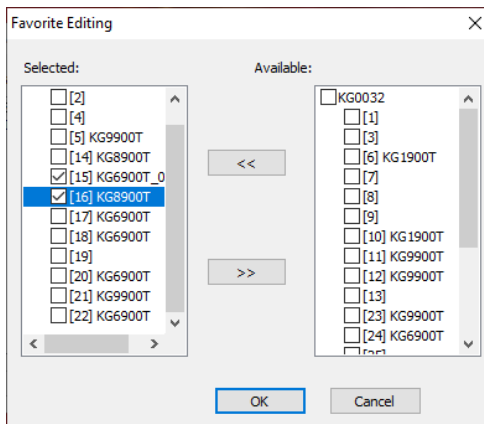
Adding / Removing Port(s)

To add / remove port(s), follow the steps below.


1. From the pop-up window, select the favorite you want to add port(s), and click **Edit**.
2. From the Favorite Editing pop-up window, select the port(s) you want to add by checking the checkbox beside it and click .

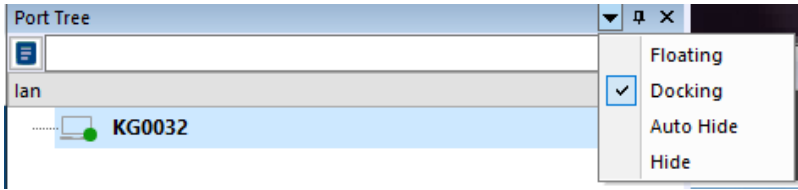


3. From the Favorite Editing pop-up window, select the port(s) you want to remove by checking the checkbox beside it and click .



Window Position

To adjust to window position, click , four options are available.

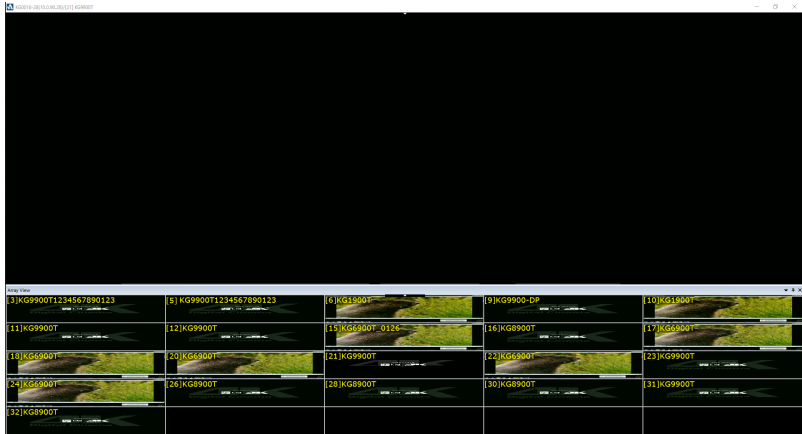


Settings	Description
Floating	The window position is adjustable, you can use a mouse cursor to move the window anywhere you like on the screen.
Docking	The window position is fixed and placed on the left side of the screen.
Auto Hide	The window automatically hides on the left side of the screen, it opens up when you mouse over it.
Hide	The window hides and will not open up.



Start Array

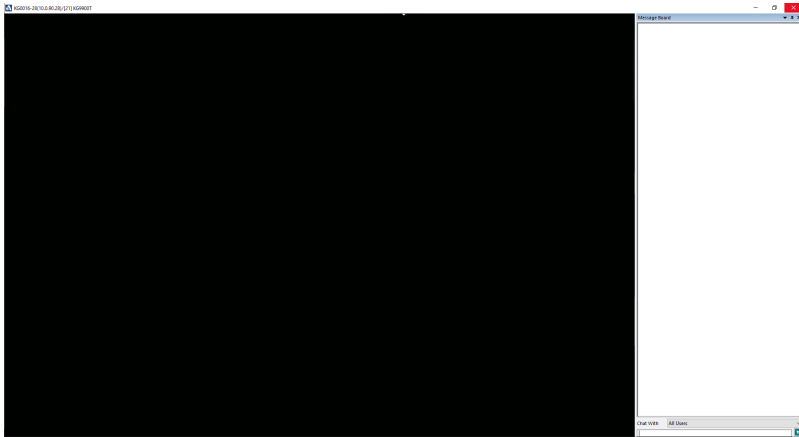
The Start Array icon invokes Panel Array Mode. Under this mode, the screen divides into a grid of up to 64 panels. To invoke the Panel Array Mode, click the **Start Array** icon and select **All Ports**. If there is a favorite created in Port Access, you can invoke a panel array mode showing only the port(s) assigned to the favorite.





The Message Board

The KVM over IP OmniBus Gateway supports multiple user logins, which may cause access conflicts. To alleviate the problem, a message board has been provided, which allows users to communicate with each other:



Message Display Panel

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

Compose Panel

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

User List Panel

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

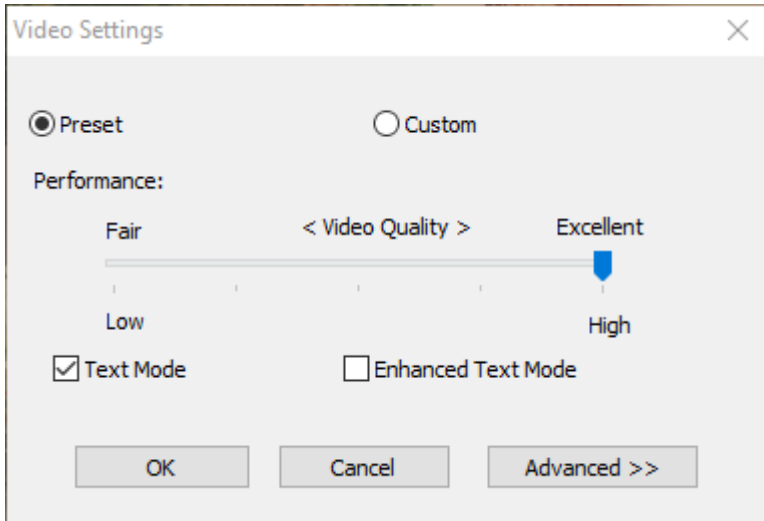
- ◆ Your name appears in blue; other users' names appear in black.
- ◆ By default, messages are posted to all users. To post a message to one individual user, select the user's name before sending your message.
- ◆ If a user's name is selected, and you want to post a message to all users, select All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



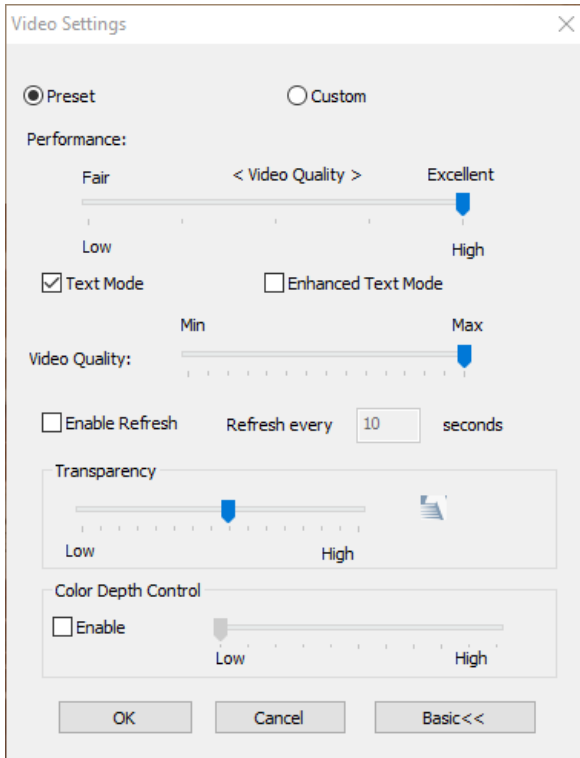
Video Settings

Clicking the *Video Settings* icon on the Control Panel brings up the *Basic Video Settings* dialog box with basic settings. The options in the basic dialog box allow you to slide the Performance bar setting, enable /disable Text Mode and Enhanced Text Mode. Selecting the *Advanced* button opens the *Advanced Video Settings* dialog box, providing more detailed options including Video Quality, Enable Refresh, Transparency and Color Depth Control, as shown below and on the next page:

Basic Video Settings



Advanced Video Settings



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

Options	Usage
Preset / Custom	Using the Preset and Custom buttons allow you to set and save custom video settings, and revert back to default video settings.
Performance	Use the slide bar to select the type of Internet connection that the local client computer uses. The KVM over IP OmniBus Gateway will use that selection to automatically adjust the <i>Video Quality</i> settings to optimize the quality of the video display. Since network conditions vary, if none of the preset choices seem to work well, you can select <i>Advanced</i> and use the Video Quality slide bar to adjust the settings to suit your conditions.
Text Mode	Click to enable / disable the Enhanced Text Mode. See <i>Enhanced Text Mode</i> , page 53.

Options	Usage
Enhanced Text Mode	<p>Check this to solve video display problems related to video screen resolution that affect some interface systems (e.g., Sun Blade 1000 and other servers). This setting can improve the image color on some displays.</p> <p>Default YUV: 4:1:1 Enhanced Text Mode YUV: 4:4:4</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 KVM over IP OmniBus Gateway 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 KVM over IP OmniBus Gateway 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 KVM over IP OmniBus Gateway 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>Adjusts the transparency of the toolbar that comes up when the GUI hotkey ([Scroll Lock][Scroll Lock], for example), is invoked. Slide the bar until the display in the example window is to your liking.</p>
Color Depth Control	<p>This setting determines the richness of the video display by adjusting the amount of color information.</p>

Network Bandwidth Information for KVM Sessions





For network bandwidth management, under ideal circumstances, a KVM session of a full-screen video display at 1920x1200 @60Hz will take up approximately 260Mbps.

However, since the network environment of each station/session varies, the aforementioned information proposes what is ideal but does not warrant the smoothness/quality for each session.



Zoom

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

Setting	Description
200%	Sizes and displays the remote view window at 200%.
175%	Sizes and displays the remote view window at 175%.
150%	Sizes and displays the remote view window at 150%.
125%	Sizes and displays the remote view window at 125%.
110%	Sizes and displays the remote view window at 110%.
100%	Sizes and displays the remote view window at 100%.
90%	Sizes and displays the remote view window at 90%.
80%	Sizes and displays the remote view window at 80%.
75%	Sizes and displays the remote view window at 75%.
67%	Sizes and displays the remote view window at 67%.
50%	Sizes and displays the remote view window at 50%.
33%	Sizes and displays the remote view window at 33%.
25%	Sizes and displays the remote view window at 25%.
	Sizes and displays the remote view window at 100%. The difference between this setting and the 100% setting is that when the remote view window is resized its contents don't resize – they remain at the size they were. To see any objects that are outside of the viewing area move the mouse to the window edge, to have the screen scroll.
	
	
	



Mouse DynaSync Mode

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.

Note: This feature is only available for Windows and Mac systems (G4 or later) whose adapter attribute OS setting is configured for Win or Mac (see *Configuration*, page 93), which are connected to the KVM over IP OmniBus Gateway with one of the following KVM DigiProcessor: KG1900T, KG6900T, KA8900T, or KG9900T.

All other configurations must use manual mouse synchronization (described in the next section).

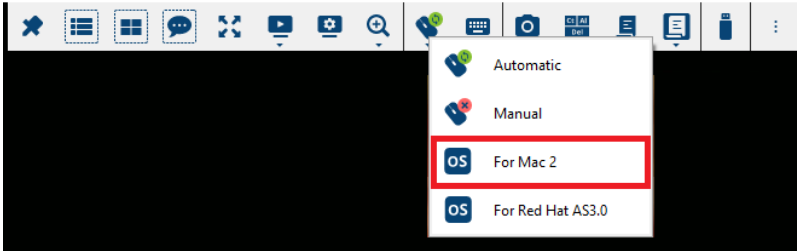
The icon on the Control Panel indicates the synchronization mode status as follows:

Icon	Function
	This icon displays in gray to indicate that Mouse DynaSync is not available – you must use manual synching procedures. This is the default setting for all KVM DigiProcessors other than the KG1900T, KG6900T, KG8900T, and KG9900T.
	The green check mark on this icon indicates that Mouse DynaSync is available and is enabled . This is the default setting when Mouse DynaSync is available (See Note above).
	The red X on 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 under *Manual Mouse Synchronization*, page 56.

Mac and Linux Considerations

- For Mac OS versions 10.4.11 or later, there is a second DynaSync setting to choose from. If the default Mouse DynaSync result is not satisfactory, try the **Mac 2** setting. To select Mac 2, left-click the *Mouse DynaSync Mode* icon from the control panel and select *For Mac 2*:



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

Manual Mouse Synchronization

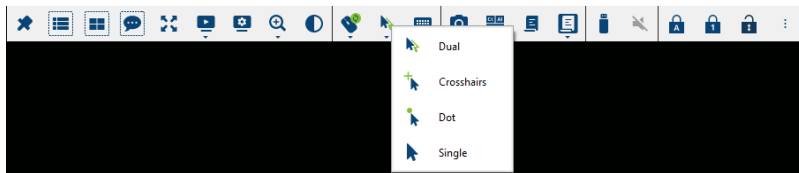
If the local mouse pointer goes out of sync with the remote system's mouse pointer there are a number of methods to bring them back into sync:

1. Perform a video and mouse auto sync by clicking the *Video Settings* icon on the Control Panel (see page 51).
2. Perform an *Auto Sync* with the Video Adjustment function (see *Video Settings*, page 51, for details).
3. Invoke the *Adjust Mouse* function with the *Adjust Mouse* hotkeys (see *Adjust Mouse*, page 61, 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 server attached to the KVM over IP OmniBus Gateway. See *Additional Mouse Synchronization Procedures*, page 198, for instructions.



Mouse Pointer Type

KVM over IP OmniBus Gateway offer a number of mouse pointer options when working in the remote display. Click this icon to select from the available choices:

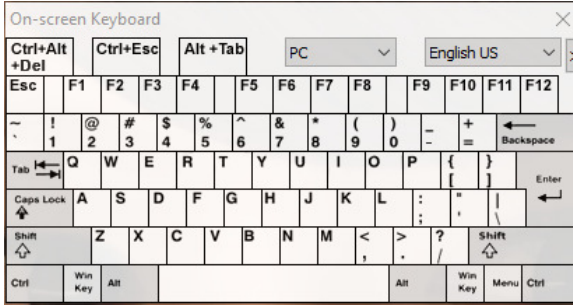


-
- Note:**
1. Before accessing a port, only Dual and Crosshairs are available for the Windows Viewers. Once the port is accessed, three pointers are available.
 2. Selecting the Single pointer has the same effect as the *Toggle mouse display* hotkey function (see *Toggle Mouse Display*, page 61 for details).
 3. The icon on the Control Panel changes to match your choice.
-



The On-Screen Keyboard

The KVM over IP OmniBus Gateway 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:



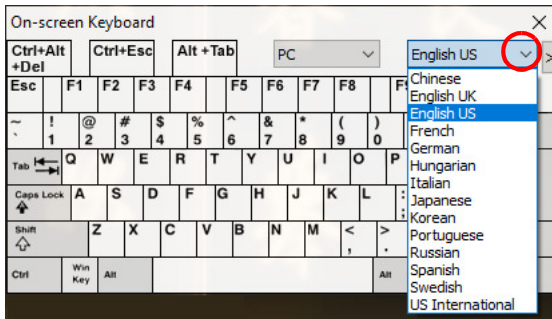
One of the major advantages of the on-screen keyboard is that if the keyboard languages of the remote and local systems aren't the same, you don't have to change the configuration settings for either system. Just bring up the on-screen keyboard; select the language used by the server you are accessing; 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.

Changing Languages

To change languages, do the following:

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

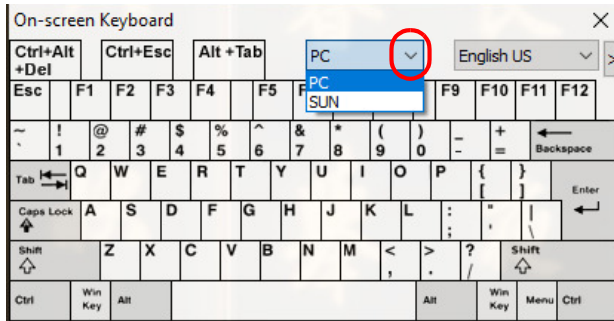


2. Select the new language from the list.

Selecting Platforms

The On-screen Keyboard supports the Sun platform as well as the PC. To select the platform, do the following:

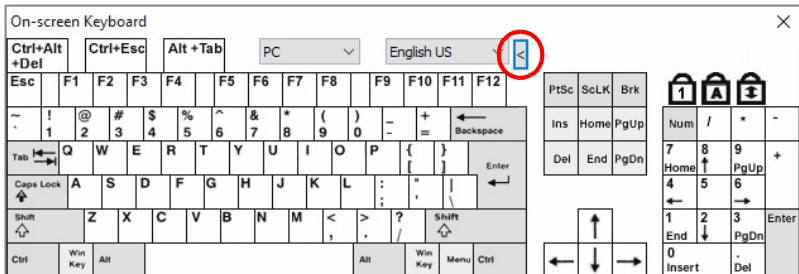
1. Click the down arrow next to the currently selected platform, to drop down the platform list.



2. Select the new platform from the list.

Expanded Keyboard

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





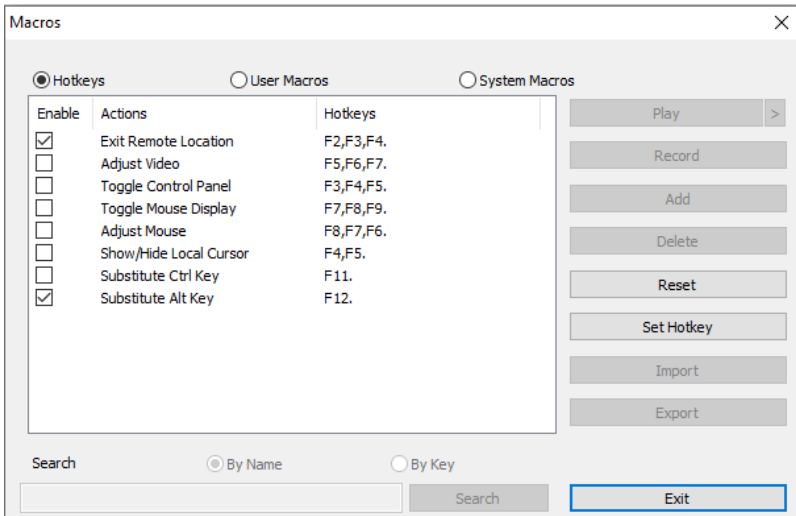
Macros

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. The *Hotkey Setup* utility (accessed by clicking this icon), lets you configure which hotkeys perform the actions.

The hotkeys that invoke an action are shown to the right of its name. Use the checkbox to the left of an action's name to enable or disable its hotkey.



To change the hotkey for an action, do the following:

1. Highlight the *Name*, 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**.

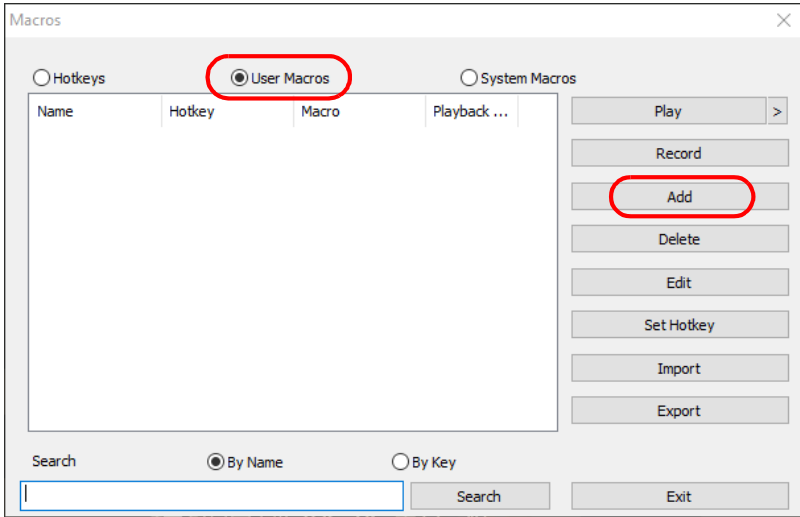
An explanation of the Hotkey actions is given in the table below:

Action	Explanation
Exit Remote Location	Breaks the connection to the KVM over IP OmniBus Gateway and returns you to local client computer operation. This is equivalent to clicking the <i>Exit</i> icon on the Control Panel. The default keys are F2, F3, F4.
Adjust Video	Brings up the <i>Video Settings</i> dialog box. This is equivalent to clicking the <i>Video Settings</i> icon on the Control Panel. The default keys are F5, F6, F7.
Toggle Control Panel	Toggles the Control Panel Off and On. The default keys are F3, F4, F5.
Toggle Mouse Display	If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to shrink the non-functioning pointer down to a barely noticeable tiny circle, which can be ignored. Since this function is a toggle, use the hotkeys again to bring the mouse display back to its original configuration. This is equivalent to selecting the <i>Dot</i> pointer type from the <i>Mouse Pointer</i> icon on the Control Panel. The default keys are F7, F8, F9.
Adjust Mouse	This synchronizes the local and remote mouse movements. The default keys are F8,F7,F6.
Show/Hide Local Cursor	Toggles off and on: hides local cursor and locks the mouse pointer and keyboard use within the Windows Client AP window, plus hides the control panel. This is equivalent to selecting the <i>Single</i> pointer type from the <i>Mouse Pointer</i> icon on the Control Panel. The default keys are F4,F5.
Substitute Ctrl Key	If your local client computer captures Ctrl key combinations, preventing them from being sent to the remote server, you can implement their effects on the remote server 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 server as [Ctrl + 5]. The default key is F11.
Substitute Alt Key	Although all other keyboard input is captured and sent to the KVM over IP OmniBus Gateway, [Alt + Tab] and [Ctrl + Alt + Del] work on your local client computer. In order to implement their effects on the remote server, another key may be substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del]. The default key is F12.

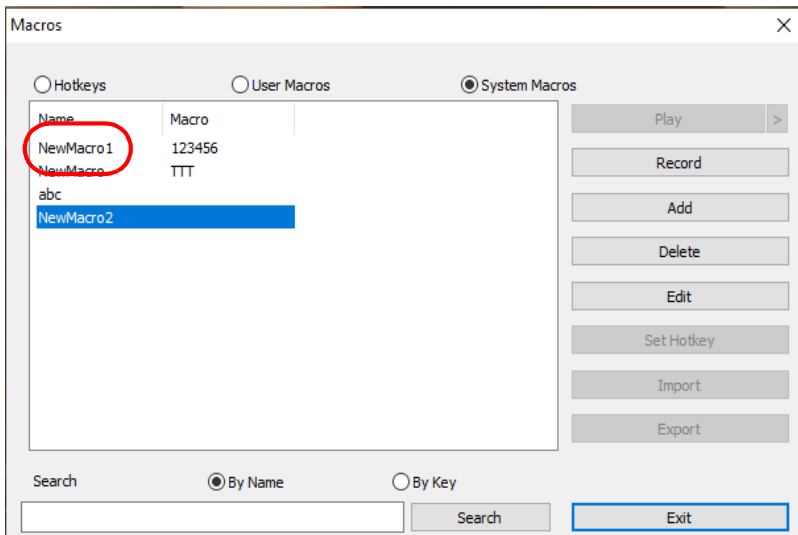
User Macros

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

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

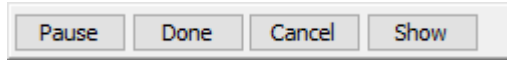


2. In the dialog box that comes up, replace the “New Macro” text with a name of your choice for the macro:



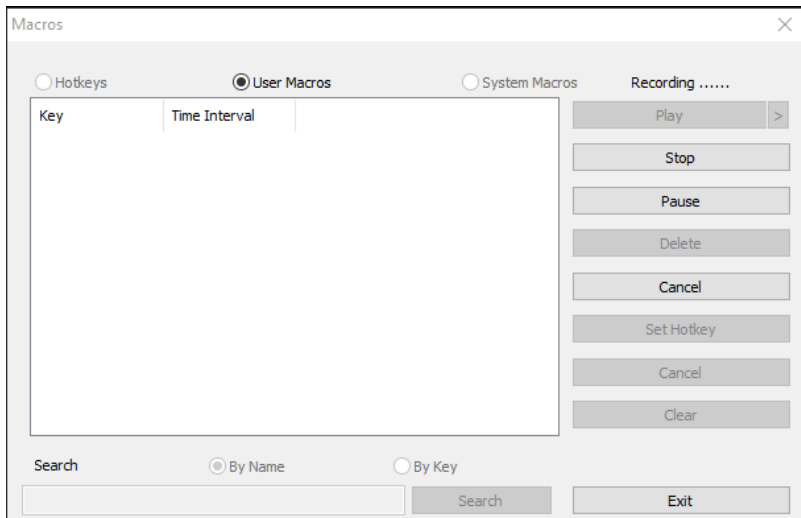
3. Click **Record**.

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



4. Press the keys for the macro.

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

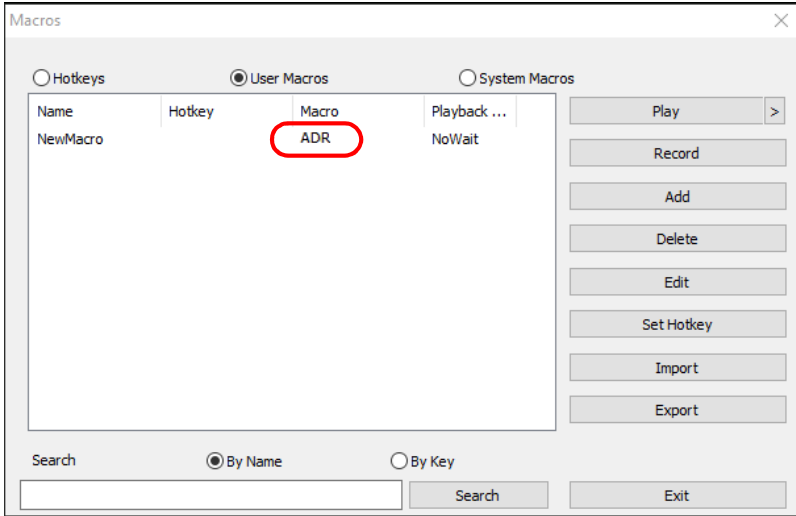


- ◆ Clicking **Cancel** cancels all keystrokes.
- ◆ When you have finished, click **Record**. (This is the equivalent of clicking *Done* in Step 5.)
- ◆ When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.

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

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

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

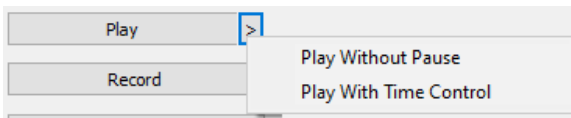


6. If you want to change any of the keystrokes, select the macro and click **Edit**. This brings up a dialog box similar to the one for Show. You can change the content of your keystrokes, change their order, etc.
7. Repeat the procedure for any other macros you wish to create.

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

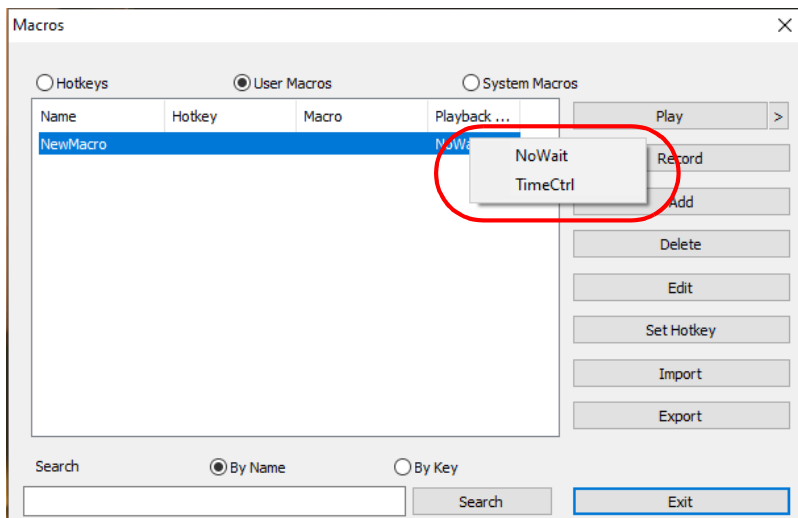
1. By using the hotkey (if one was assigned).
2. By opening the Macro List on the Control Panel and clicking the one you want (see page 45).
3. By opening this (Macros) dialog box and clicking **Play**.

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



- ◆ If you choose *Play Without Pause*, 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 (*NoWait* or *TimeCtrl*), which 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 alternate choice.

-
- Note:** 1. Information about the Search function is given on page 65.
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
-

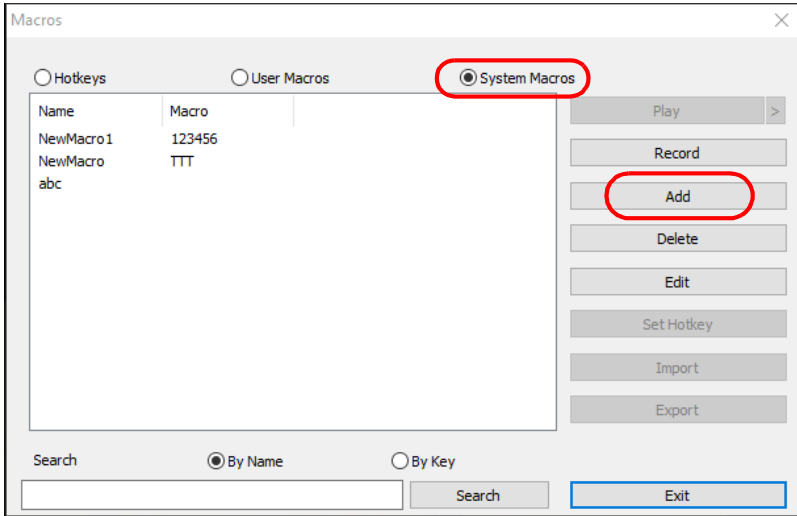
■ Search

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.

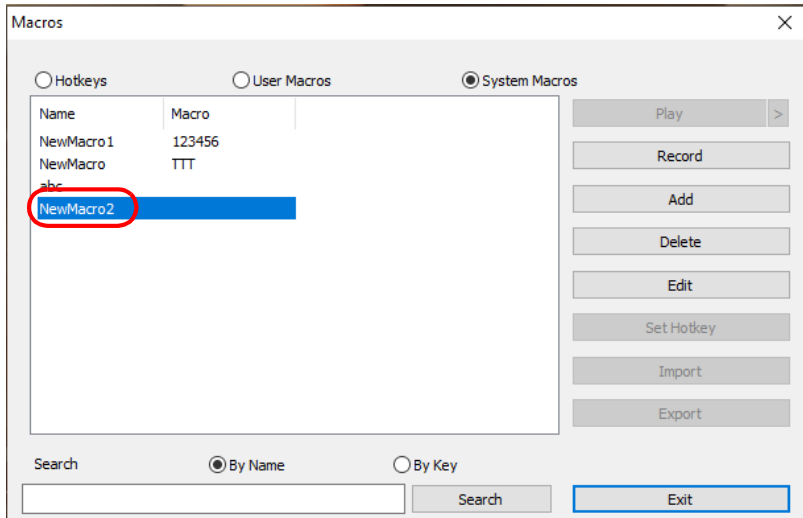
System Macros

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 server'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**.

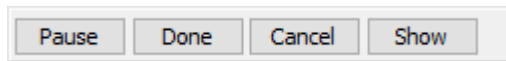


2. In the dialog box that comes up, replace the "New Macro" text with a name of your choice for the macro:



3. Click **Record**.

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



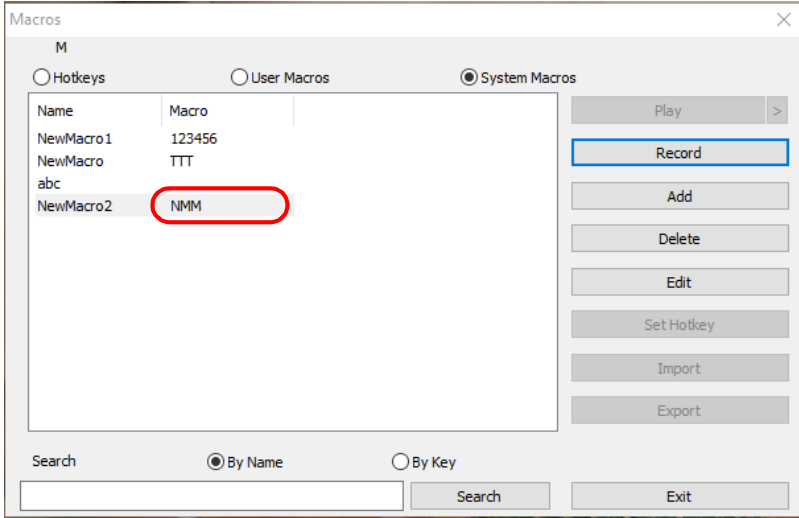
4. Press the keys for the macro.

- ◆ To pause macro recording, click **Pause**. To resume, click **Pause** again.
- ◆ Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes (see page 67).
- ◆ When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.

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

2. 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.
-

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



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

Once the system macros have been created, they are available for use on a port-by-port basis. They get selected on a port's *Port Configuration* (see *Configuration*, page 93 for details).

Note: 1. Information about the Search function is given on page 65.




- You can choose only one system macro per port.
 - Systems macros are stored on the KVM over IP OmniBus Gateway, therefore macro names may not exceed 64 bytes; hotkey combinations may not exceed 256 bytes. (Each key usually takes 3–5 bytes.)
-



Virtual Media

The *Virtual Media* feature allows a drive, folder, image file, removable disk, or smart card reader on a user's system to appear and act as if it were installed on the remote server.

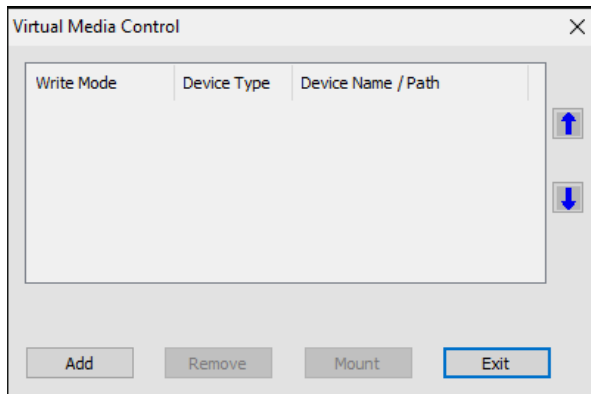
The Virtual Media icon changes depending on the status of the virtual media function, as shown in the table below:

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

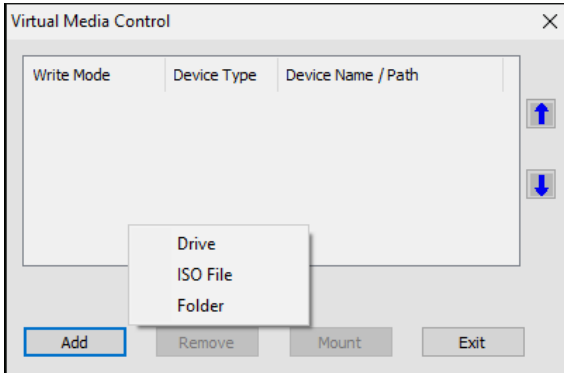
Mounting Virtual Media

To mount a virtual media device, do the following:

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

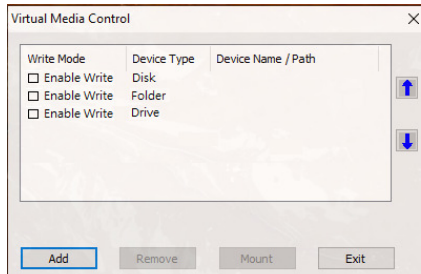


2. Click **Add**; then select the media source.



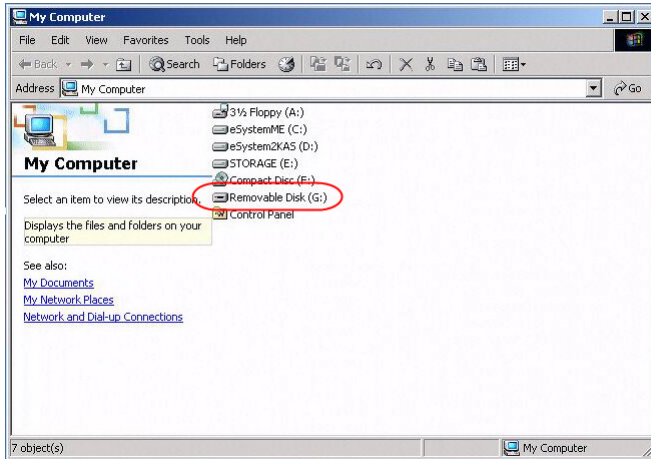
Depending on your selection, additional dialog boxes appear to enable you to select the drive, ISO file, or folder. See *Virtual Media Support*, page 207 for a list of supported virtual media types, and details about mounting them.

3. If your device only supports full speed USB, put a check in the *Disable High Speed USB Operation Mode* checkbox.
4. To add additional media sources, click **Add**, and select the source as many times as you require. Up to three virtual media choices can be mounted. The top three in the list are the ones that are selected. Virtual Media and Smart Card readers can be mounted at the same time. 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.
5. *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. For 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, its checkbox appears in gray.

6. To remove an entry from the list, select it and click **Remove**.
7. 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 server, where they show up as drives, files, folders, etc. on the remote server's file system.



Once mounted, you can treat the virtual media as if they really existed on the remote server – drag and drop files to/from them; open files on the remote server 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 client computer's storage. Files that you drag from the redirected media will actually come from your local client computer's storage.

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

Mounting Virtual Media - Drag and Drop

It will be easier to perform a drag and drop mount if you set the mouse pointer option to *Dual* (see *Mouse Pointer Type*, page 57).

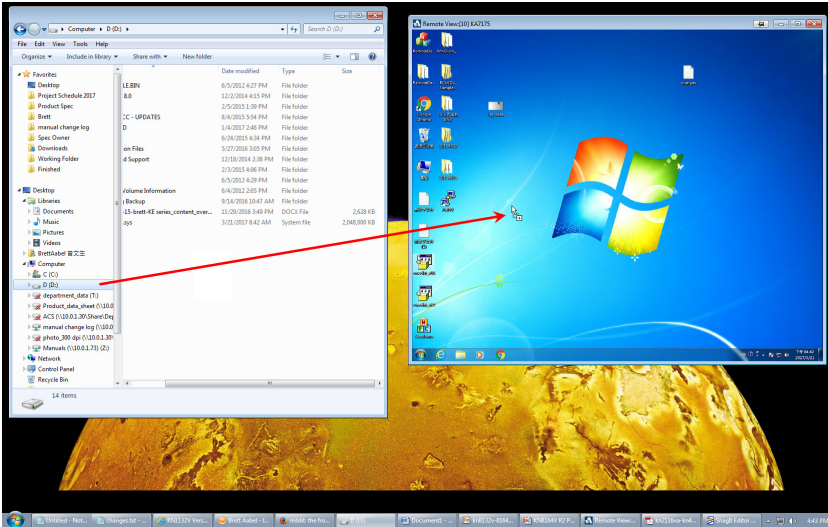
To mount a virtual media device via drag and drop, do the following:

1. Open a session on the remote server and ensure the Virtual Media icon is blue:



2. Open an Explorer window on the local computer and select the media source you want to mount, then hold a left-click with the mouse to drag and drop the virtual media source to the remote view window, as shown below:

- ◆ Drag and Drop = Virtual Media **Read** only
- ◆ Drag and Drop + [Ctrl] = Virtual Media **Read + Write**

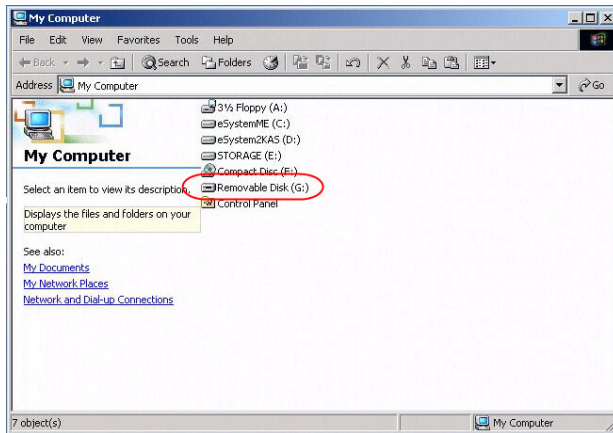


See *Virtual Media Support* on page 207 for a list of supported virtual media types, and details about mounting them.

3. While the virtual media drive mounts a message will appear on the remote view screen, as shown here:



4. The virtual media devices that you have dragged and dropped are redirected to the remote server, where they show up as drives, files, folders, etc. on the remote server's file system.



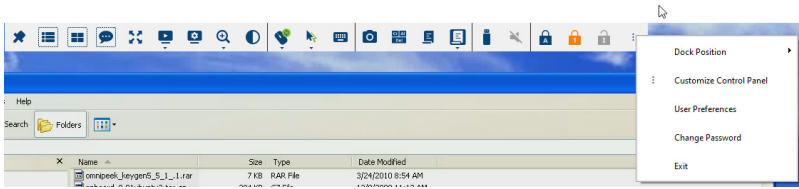
Note: If a redirected device cannot be written to, it appears in gray.

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

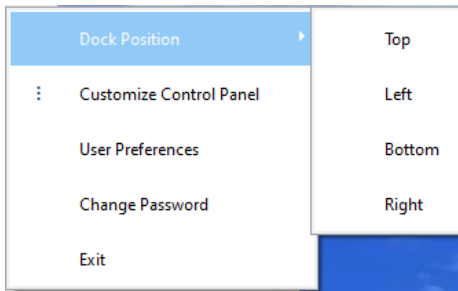
Files that you save to the redirected media will actually be saved on your local client computer's storage. Files that you drag from the redirected media will actually come from your local client computer's storage.

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

More Settings



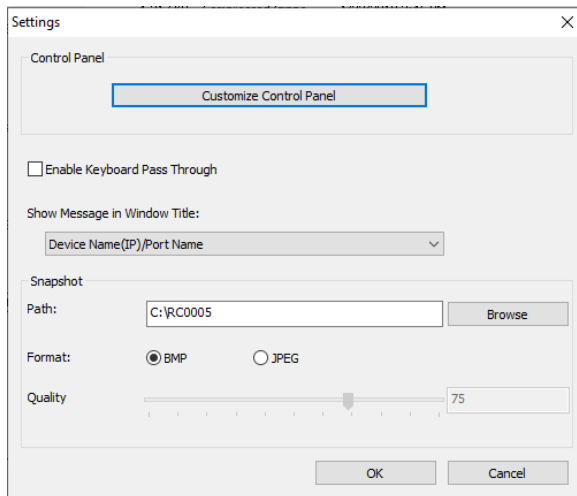
Dock Position



The dock position adjusts the dock position to top, left, bottom, or right of the screen.

Customize Control Panel

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



The organization of the dialog box is described in the table, below:

Item	Description
Customize Control Panel	Allows you to select which icons display in the Control Panel. Check the ones you want to see, uncheck the ones you don't want.
Enable Keyboard Pass Through	When this is enabled, the Alt-Tab key press is passed to the remote server and affects that server. If it is not enabled, Alt-Tab acts on your local client computer.
Show Message in Window Title	Select to show message such as port name, device name, resolution, frame rate, and bandwidth in the window title.
Snapshot	<p>These settings let the user configure the KVM over IP OmniBus Gateway screen capture parameters (see the <i>Snapshot</i> description under <i>The Control Panel</i>, page 43):</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 don't specify a directory here, the snapshot is saved to your desktop. ◆ Click a radio button to choose whether you want the captured screen to be saved as a BMP or a JPEG (JPG) file. ◆ If you choose JPEG, you can select the quality of the captured file with the slider bar. The higher the quality, the better looking the image, but the larger the file size.

User Preferences

Item	Description
Language	Selects the language that the interface displays in.
Logout Timeout	If there is no user input for the amount of time set with this function, the user is automatically logged out. A login is necessary before the KVM over IP OmniBus Gateway can be accessed again.
Toolbar Position	Adjusts the toolbar position to top, left, bottom, or right of the screen.
Startup	<ul style="list-style-type: none"> ◆ Continue Where You Leave Off: The WinClient viewer opens and connects to the port you were on when you close the viewer. ◆ Open Port List: The WinClient viewer opens and shows a port list that you can connect to. ◆ Connect First Port: The WinClient viewer opens and connects to the first port.
Others	<ul style="list-style-type: none"> ◆ Array View Settings: Adjusts the panel array view settings. ◆ Message Board Settings: Adjusts the message board settings.

Change Password









This is the same as changing the password explained in the *User Settings, Change Password*, page 76.



The Web Client Control Panel

The Web Client control panel is a simpler version of the WinClient control panel with fewer functions as shown below:



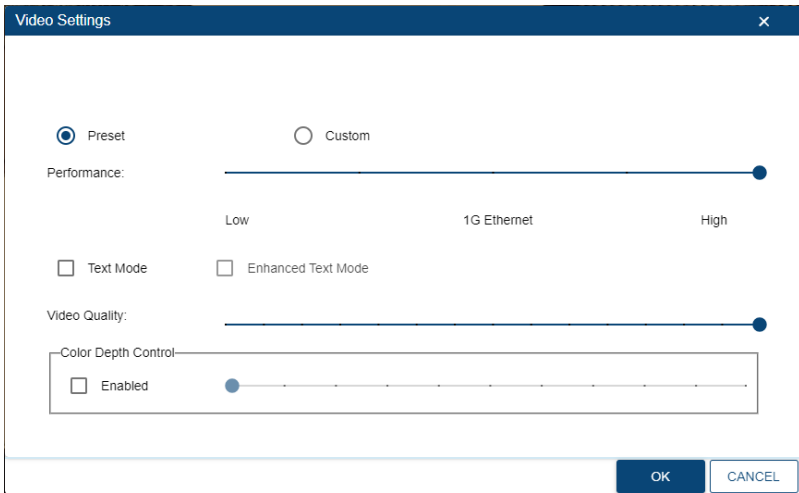
Functions

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.
	Click for the Video Settings window. (Refer to <i>Web Client Video Settings</i> on page 78 for more information).
	Click for a Screen Mode drop-down menu. Choose between <i>Full Screen Mode</i> and <i>Fit to Window</i> .
	Click to toggle the remote display between color and grayscale views.
	Click to toggle Automatic or Manual mouse sync. <ul style="list-style-type: none"> ◆ 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 55 for a complete explanation of this feature.
	Click to select the mouse pointer type. <p>Note: This icon changes depending on which mouse pointer type is selected (see <i>Mouse Pointer Type</i>, page 57).</p>
	Click to bring up the on-screen keyboard (see <i>The On-Screen Keyboard</i> , page 58).
	Click to send a Ctrl+Alt+Del signal to the remote system.

	<p>Click to bring up the <i>Virtual Media</i> dialog box. The icon changes depending on the status of the virtual media function. See <i>Virtual Media</i>, page 69, for specific details.</p> <p>Note: This icon displays in gray when the function is disabled or not available.</p>
	<p>Click to toggle sound from the remote server to be heard on the client computer's speakers on or off. The "prohibited" symbol (a red circle with a diagonal bar) displays on the icon when the speaker is toggled Off.</p>

Web Client Video Settings

Clicking this icon will bring up the web client video settings as shown below:



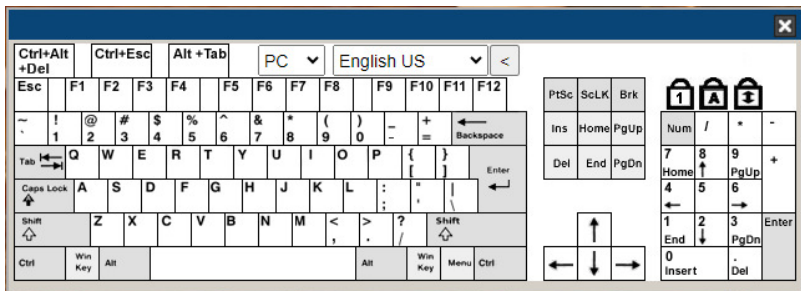
The options are described in the table below:

Options	Usage
Performance	<p>Use the slide bar to select the type of Internet connection that the local client computer uses. The KVM over IP OmniBus Gateway will use that selection to automatically adjust the <i>Video Quality</i> settings to optimize the quality of the video display.</p> <p>Since network conditions vary, if none of the preset choices seem to work well, you can select <i>Advanced</i> and use the Video Quality slide bar to adjust the settings to suit your conditions.</p>

Options	Usage
Enhanced Text Mode	Check this to solve video display problems related to video screen resolution that affect some interface systems (e.g., Sun Blade 1000 and other servers). This setting can improve the image color on some displays. Default YUV: 4:1:1 Enhanced Text Mode YUV: 4:4:4
Video Quality	Drag the slider bar to adjust the overall Video Quality. The larger the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may adversely effect response time.
Color Depth Control	This setting determines the richness of the video display by adjusting the amount of color information.

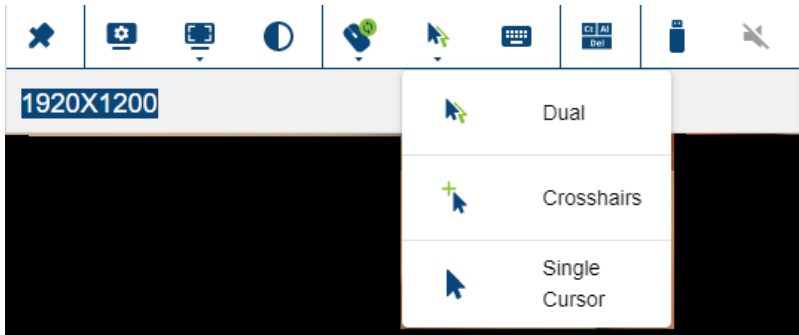
Web Client On-Screen Keyboard

Click this icon to bring up the on-screen English keyboard:



Web Client Mouse Pointer Type

KVM over IP OmniBus Gateway offer a number of mouse pointer options when working in the remote display. Click this icon to select from the available choices:



Note: 1. Available options will depend on the browser. For example, Internet Explorer has Dual and Crosshairs types while Chrome has Dual, Crosshairs and Single Cursor.

2. The icon on the Control Panel changes to match your pointer choice.

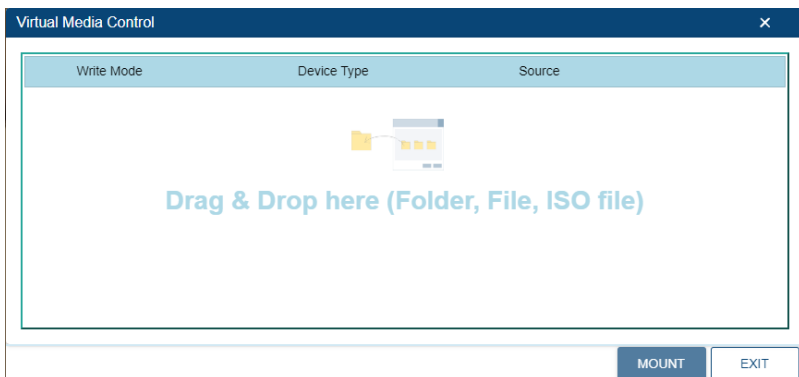
Virtual Media

To set up a Virtual Media device, do the following:

1. Click the **Virtual Media** icon to bring up the *Virtual Media Control*.

Note: 1. For *Internet Explorer* web browser, only ISO file is supported.
For more information see

2. Virtual Media writing is not supported by Web Client.



2. Simply drag and drop the selected file into the *Virtual Media Control* dialog box, and click **Mount**.
3. To end the redirection, click on the Virtual Media icon and all mounted devices are automatically unmounted.

Web Client Mouse Sync Mode

Synchronization of the local and remote mouse pointers is accomplished either automatically or manually.



Automatic Mouse Synchronization (DynaSync)

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

Note: This feature is only available for Windows and Mac systems (G4 or later) whose adapter attribute OS setting is configured for Win or Mac (see *Configuration*, page 93), which are connected to the KVM over IP OmniBus Gateway with one of the following KVM DigiProcessors: KG1900T, KG6900T, KA8900T, or KG9900T.

All other configurations must use manual mouse synchronization (described in the next section).

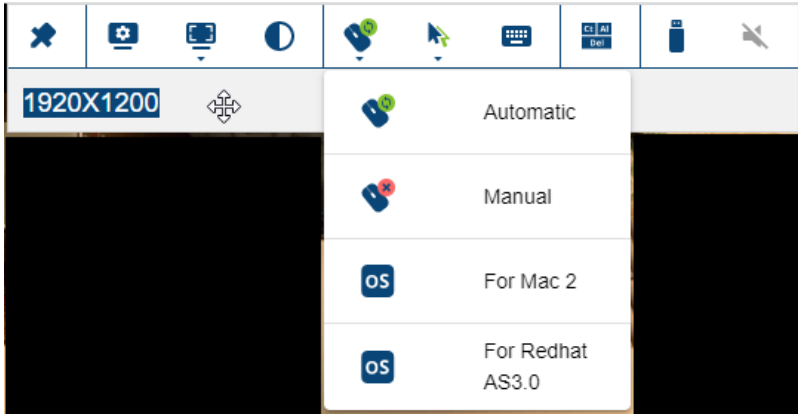
The icon on the Control Panel indicates the synchronization mode status as follows:

Icon	Function
	The green check mark on this icon indicates that Mouse DynaSync is enabled . This is the default setting (See Note above).
	The red X on this icon indicates that Mouse DynaSync is not enabled .

Clicking the icon toggles its status between enabled and disabled. If you choose to disable Mouse DynaSync mode, you must use the manual syncing procedures described below.

Mac and Linux Considerations

- For Mac OS versions 10.4.11 or later, there is a second DynaSync setting to choose from. If the default Mouse DynaSync result is not satisfactory, try the **Mac 2** setting.



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

Manual Mouse Synchronization

If 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 auto sync, refer to page 77.
2. Move the pointer into all 4 corners of the screen (in any order).
3. Drag the Control Panel to a different position on the screen.

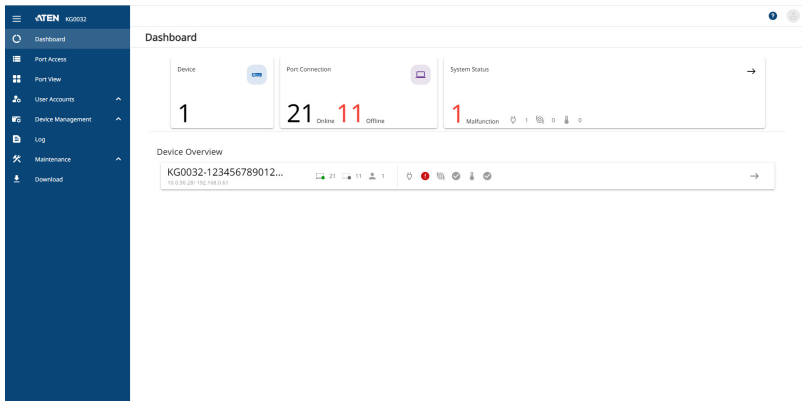
Set the mouse speed and acceleration for each problematic server attached to the KVM over IP OmniBus Gateway. See *Additional Mouse Synchronization Procedures*, page 198, for instructions.

Chapter 5

Dashboard

Overview

When you log in to the KVM over IP OmniBus Gateway, the *Dashboard* page comes up with the KVM over IP OmniBus Gateway's device information page displayed.



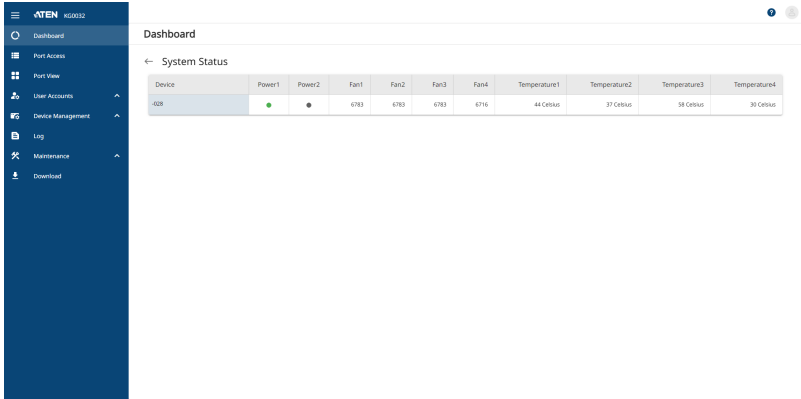
The Dashboard page is designed for users to easily view the device information such port connection, system status, and device overview.

System Status

To check the system status, from the *Dashboard* page, go to *System Status* and click → .



The *System Status* page appears.



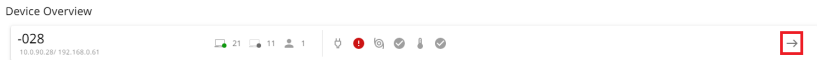
Dashboard

← System Status

Device	Power1	Power2	Fan1	Fan2	Fan3	Fan4	Temperature1	Temperature2	Temperature3	Temperature4
-028	●	●	6783	6783	6783	6716	44 Celsius	37 Celsius	58 Celsius	39 Celsius

Device Overview

To go to device overview, from the *Dashboard* page, go to *Device Overview* and click →.

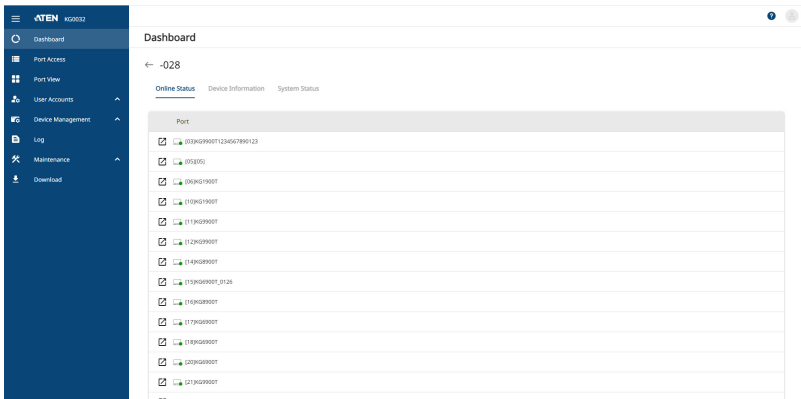


Device Overview

-028
10.0.90.28/192.168.0.61

→

The *Device Overview* page appears.




Dashboard

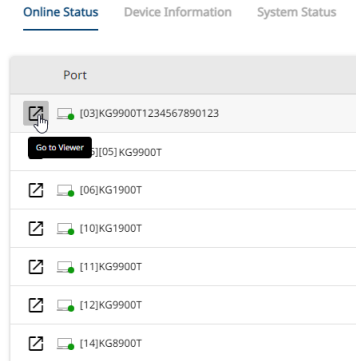
← -028

Online Status Device Information System Status

Port
00302999001324567890123
001000
00002190001
110002190001
111002999001
112002999001
114002999001
115008999001_0128
116002999001
117002999001
118002999001
120002999001
121002999001

Online Status

The Online Status page shows all the available ports connected to the KVM over IP OmniBus Gateway. You can quick access to any available port's WebClient panel by clicking  beside it.





Device Information

The Device Information page shows device information such as device name, MAC address, firmware version, and etc.

Online Status	Device Information	System Status
Device Name:	-028	
MAC1 Address:	00-10-74-03-00-44	
MAC2 Address:	00-10-74-03-00-45	
Firmware Version:	V1.0.080 Build20231027	
IP Address1:	10.0.90.28	
Subnet Mask 1:	255.255.252.0	
Gateway 1:	10.0.90.254	
Preferred DNS Server 1:	10.0.1.6	
Alternate DNS Server 1:	10.0.1.7	
IPv6 Address 1:	fd90::fa6e:46e8:afc1:5484	
IPv6 Subnet Prefix Length 1:	64	
IPv6 Gateway 1:	fe80::ae71:2eff:fe70:c072	
IPv6 Preferred DNS Server 1:	fd00::6	
IP Address 2:	192.168.0.61	
Subnet Mask 2:	255.255.255.0	
IPv6 Subnet Prefix Length 2:	64	

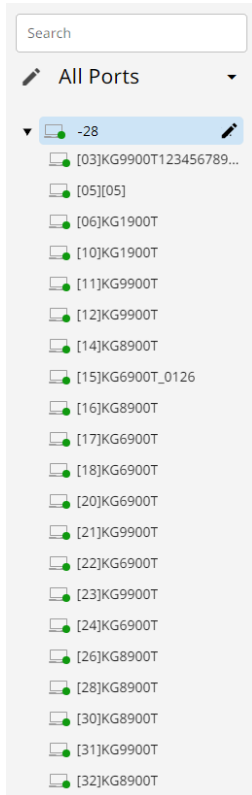
System Status

The System Status page shows the system status that are identical to the *System Status* (page 83) but only in a different layout.

Online Status	Device Information	System Status
Power1		On
Power2		Off
Fan1		6750 rpm
Fan2		6750 rpm
Fan3		6783 rpm
Fan4		6683 rpm
Temperature1		44 Celsius
Temperature2		37 Celsius
Temperature3		58 Celsius
Temperature4		30 Celsius

The Sidebar

All KVM switches – including their ports and outlets – are listed in a tree structure in the Sidebar at the left of the screen:




The Sidebar Tree Structure

The characteristics of the Sidebar tree structure are the following:

- ◆ Users are only allowed to see the devices and ports/outlets that they have access permission for.
- ◆ Ports and child devices can be nested under their parent devices.

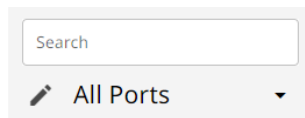
Click ► in front of a device to expand the tree and see the ports/outlets nested underneath it. Click ▼ to collapse the tree and hide the nested ports/outlets.

- ◆ A port's ID number is displayed in brackets next to its icon. The ports/outlets but can also be named (see *Port Naming*, page 92, for details).
- ◆ Switches and ports that are on line have their monitor screen with a dot in Green; the monitor screens with a dot in Grey for devices and ports that are offline.
- ◆ To access and operate a port with WebClient panel, double-click  beside it. Port operation details are discussed in Chapter 4, *The Web Client Control Panel*.

Note: You can only access one port at a time. To see two different ports, you would have to log in two separate times.

Filter

Filter allows you to control the number and type of ports that display in the Sidebar.



The meanings of the choices are explained in the following table:


Choices	Explanation
Search	<p>If you key in a search string and click Search, only port names that match the search string display in the tree. Wildcards (? for single characters; * for multiple characters) and the keyword or are supported, so that more than one port can show up in the list.</p> <p>For example:</p> <ol style="list-style-type: none"> 1. If you key in Web*, both Web Server 1 and Web Server 2 show up in the list. 2. If you key in W*1 or M*2, both Web Server 1 and Mail Server 2 show up in the list.
All Ports (default setting)	<p>This is the default view. With no other filter options selected, all of the ports that are accessible to the user are listed in the Sidebar.</p> <p>If any <i>Favorites</i> have been specified (see page 90), you can drop down the list box and select Favorites instead of All. If you select Favorites, only the items you have selected as Favorites display in the tree.</p>

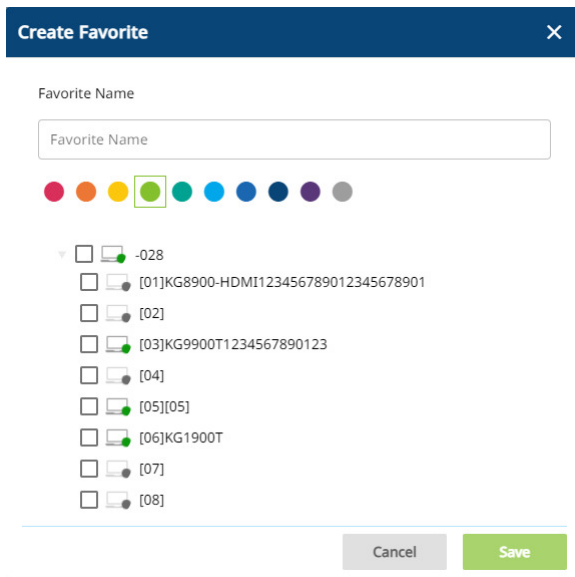
Favorites

Ports that you frequently access can be saved in a favorite list. Simply open the list and select a group of ports – rather than hunting for it in the Sidebar. This feature is especially handy on large, crowded installations.

Adding a Favorite

To add a port to the favorites, do the following:










1. From the Filter section, click  and select **+ Create Favorite**.
2. The Create Favorite pop-up window appears.





Create Favorite ✕


Favorite Name


Favorite Name


        


 -028


 [01]KG8900-HDMI123456789012345678901


 [02]


 [03]KG9900T1234567890123

 [04]

 [05][05]

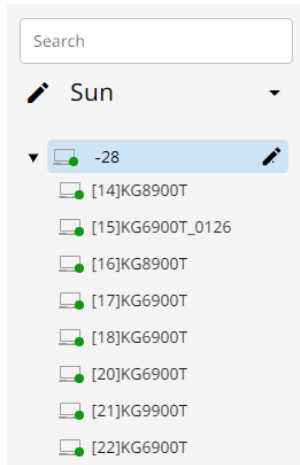
 [06]KG1900T

 [07]

 [08]


3. Define a name and color coding for your Favorite and select the ports you want to add to this favorite.
4. Click **Save**.

5. Once saved, the Favorite created should be listed automatically.




Note: Favorites can be selected for filtering in the Sidebar. See *Filter*, page 89 for details

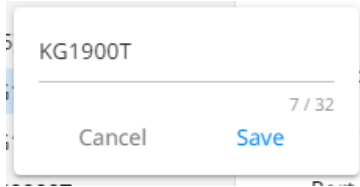
Modifying a Favorite

- ◆ To modify a Favorite, or one of the items contained in it, edit a Favorite Name, or delete a Favorite, click  beside the selected favorite, then the Modify Favorite pop-up window appears.
- ◆ Click Save when the configuration is done.

Port Naming

For convenience – especially in large installations with many devices and ports – administrators and users with port configuration permission, can give each port a name. To assign, modify or delete a name, do the following:

1. Click once on the item you want to edit and then click  beside it.
2. A pop-up window appears.

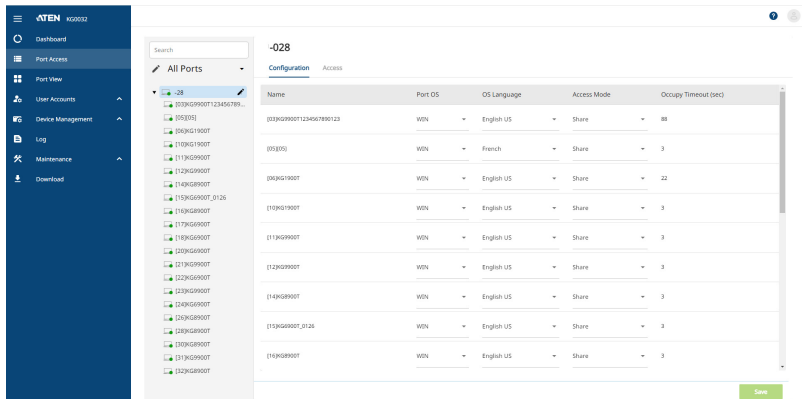


3. Key in a name for the item (or change/delete a previous one).
 - ◆ You can use any combination of letters, numbers, and symbols on the keys of keyboards with a PC US English layout. In this case, the maximum number of characters allowed is 20.
 - ◆ You can also activate your local IME to input non-English characters. For languages that use 2-byte encoding, the maximum number of characters allowed is 9.
4. When you have finished editing the name, click **Save**.

Configuration

Device Level

When a device is selected in the Sidebar, there are three items available under Configuration page: *Port OS*, *OS Language*, *Access Mode*, and *Occupancy Timeout*.



Select a port in the list to configure *Port OS*, *OS Language*, *Access Mode*, and *Occupancy Timeout*. Choose one of the options described in the table:

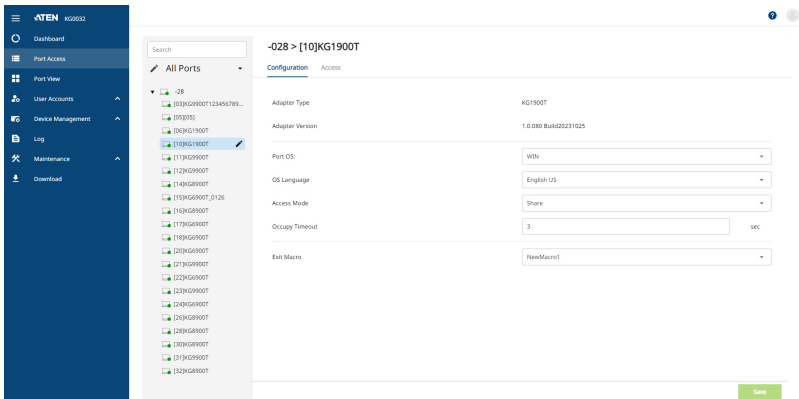
Column	Description
Port OS	Specifies the operating system that the server on the connected port is using. Choices are Win, Mac, Sun, and Other. The default is Win.
OS Language	Specifies the OS language being used by the server on the connected port. Drop down the list to see the available choices. The default is English US.

Column	Description	
Access Mode	Defines how the port is to be accessed when multiple users have logged on, as follows:	
	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 users to communicate with each other regarding control of the keyboard and mouse or keyboard, mouse, and video of a Share 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. If the user who controls the port is inactive for longer than the time set in the Timeout box, port control is transferred to the first user to move the mouse or strike the keyboard.
	Exclusive	The first user to switch to the port has exclusive control over the port. No other users can view the port. The Timeout function does not apply to ports which have this setting.
Occupy Timeout	<p>The Occupy Timeout field sets a time threshold for users on ports whose Access Mode has been set to Occupy (see <i>Access Mode</i>, page 94). If there is no activity from the user occupying the port for the amount of time set here, the user is timed out and the port is released. The first user to send keyboard or mouse input after the port has been released gets to occupy the port.</p> <p>Input a value from 0 to 255 seconds. The default is 3 seconds. A setting of 0 causes the port to be released the instant there is no input.</p>	

When you have finished configuring, click **Save**.

Port Level

When a port is selected in the Sidebar, the Configuration page looks similar to the one below. There are five items available under Configuration page: *Port OS*, *OS Language*, *Access Mode*, *Occupy Timeout*, and *Exit Macro*.



Select a port in the sidebar to configure *Port OS*, *OS Language*, *Access Mode*, *Occupy Timeout*, and *Exit Macro*. Choose one of the options described in the table:

Column	Description	
Port 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.	
OS 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.	
Access Mode	Defines how the port is to be accessed when multiple users have logged on, as follows:	
	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 users to communicate with each other regarding control of the keyboard and mouse or keyboard, mouse, and video of a Share 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. If the user who controls the port is inactive for longer than the time set in the Timeout box, port control is transferred to the first user to move the mouse or strike the keyboard.
	Exclusive	The first user to switch to the port has exclusive control over the port. No other users can view the port. The Timeout function does not apply to ports which have this setting.
Occupy Timeout	The Occupy Timeout field sets a time threshold for users on ports whose Access Mode has been set to Occupy (see <i>Access Mode</i> , page 94). If there is no activity from the user occupying the port for the amount of time set here, the user is timed out and the port is released. The first user to send keyboard or mouse input after the port has been released gets to occupy the port. Input a value from 0 to 255 seconds. The default is 3 seconds. A setting of 0 causes the port to be released the instant there is no input.	
Exit Macro	The Exit Macro panel contains a drop-down listbox of user created System macros. You can select a macro from the list that will execute when exiting the remote server. See <i>System Macros</i> , page 66 for details on creating exit macros.	

When you have finished configuring, click **Save**.

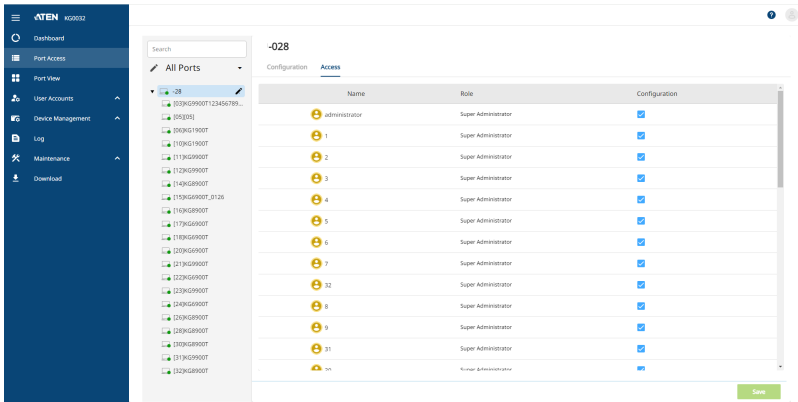
Access

Administrators use the *Access* page to set user and group access and configuration rights for switches and ports.

Note: The Access page only appears for those users with User Management permissions. It isn't available for other users.

Device Level Browser GUI Interface

If a KVM over IP OmniBus Gateway is chosen in the Sidebar, the Main panel looks similar to the one shown below:

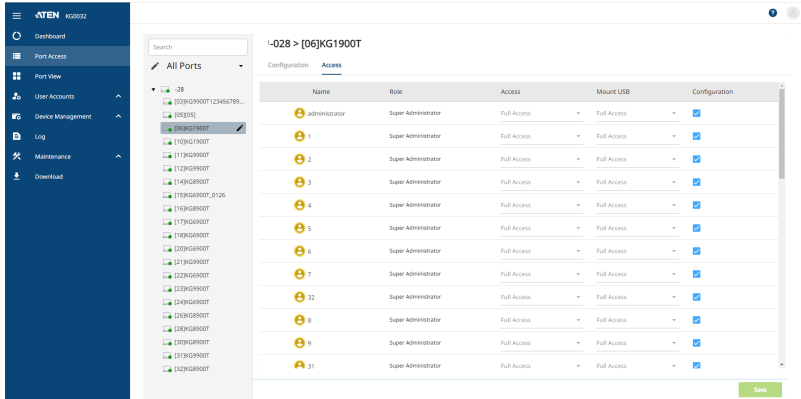


The main panel consists of two columns: *Name*, and *Config*:

- ◆ *Name* lists all the users and groups that have been created.
- ◆ *Role* indicates its role between Super Administrator and Normal User.
- ◆ *Configuration* indicates the users who have Configuration privileges. A check mark (✓) indicates that the user has permission to make changes to the KVM over IP OmniBus Gateway configuration settings (see Chapter 9, *Device Management*); an empty checkbox means that the user is denied permission to make configuration changes.
- ◆ When you have finished configuring, click **Save**.

Port Level Browser GUI Interface

If a port is chosen in the Sidebar, the Main panel looks similar to the one shown below:



The port access settings are explained in the following table:

Name	Each port accessible to the user is listed under the <i>Names</i> column.	
Role	The Role column is where you choose a role between Super Administrator or Normal User for a user.	
Access	The Access column is where device access rights are set. To cycle through the choices, click the icon in the row that corresponds to the user you want to configure. The meanings of the icons are as follows	
	No Access	No access rights - the Port will not show up on the User's list on the Main Screen.
	View Only	The user can only view the remote screen; he cannot perform any operations on it.
	Full Access	The user can view the remote screen and can perform operations on the remote server from his keyboard and monitor.

Mount USB	<p>The Mount USB column is where permission to mount Virtual Media devices on remote servers is configured. To cycle through the choices, click the icon in the row that corresponds to the user you want to configure. The icons are the same as the ones in the <i>Access</i> column.</p> <ul style="list-style-type: none">◆ With a <i>No Access</i> setting, the user will not see the virtual media even if it has been configured on the remote system.◆ With a <i>Read Only</i> setting, the user can only view the contents of the virtual media (read only), he can not perform any operations on it.◆ With a <i>Full Access</i> setting, the user can mount, read, and write to the virtual media. <p>Note: This entry does not appear for KVM over IP OmniBus Gateway that do not support the USB Virtual Media function.</p>
Configuration	<p>Sets or denies permission for the user to make changes to a port's configuration settings. A check mark (<input checked="" type="checkbox"/>) indicates that the user has permission; an empty checkbox means that the user does not have permission.</p>

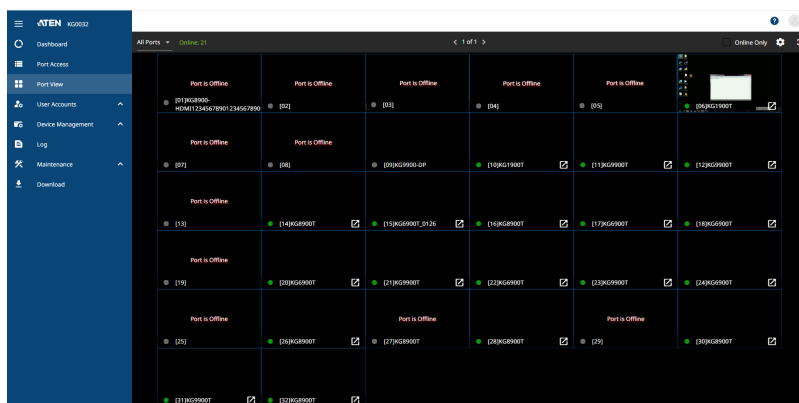
When you have finished configuring, click **Save**.

Chapter 7

Port View

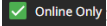
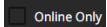


Overview

When you select the *Port View* tab the screen comes up with the *Port View* page displayed.



The Port View page invokes Panel Array Mode. Under this mode, the screen divides into a grid of up to 64 panels. To access and operate a port with WebClient, double-click the port panel. Port operation details are discussed in Chapter 4, *The Web Client Control Panel*.

Function	Description
All Ports (default setting)	This is the default view. With no other filter options selected, all of the ports that are accessible to the user are listed in the Panel Array Mode. If any <i>Favorites</i> have been specified (see page 90), you can drop down the list box and select Favorites instead of All. If you select Favorites, only the items you have selected as Favorites display in the Panel Array Mode.
Online: (n)	The n stands for an amount of online ports (up to 16/32) available on the KVM over IP OmniBus Gateway.

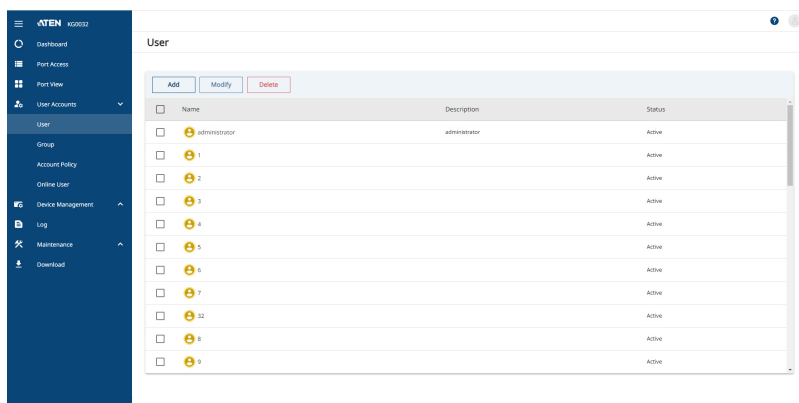
Function	Description
Online Only	<p>Click to toggle the Online Only on and off.</p> <ul style="list-style-type: none"> ◆  Online Only : when enabled, only the online ports available on the KVM over IP OmniBus Gateway are displayed. ◆  Online Only : when disabled, all the ports on the KVM over IP OmniBus Gateway are displayed.
	<p>Click to configure the <i>Layout</i> and <i>Mode</i> settings.</p> <div data-bbox="574 394 705 509" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p>< Layout 6*6</p> <p>< Mode 16:9</p> </div> <ul style="list-style-type: none"> ◆ Layout: chooses a layout between 1*1, 2*2, 3*3, 4*4, 5*5, 6*6, 7*7, and 8*8. ◆ Mode: chooses a mode between 16:9, 4:3 aspects ratios, or Fit Screen.
	<p>Click to toggle the Full Screen function on or off.</p>

Chapter 8

User Accounts

Overview

When the User Accounts is selected, the tab opens up for a list of options including *User*, *Group*, *Account Policy*, and *Online User*. Each options are explained fully in the following pages, please see below for reference.



- ◆ User: modifies the user settings, see *Users*, page 102.
- ◆ Group: modifies the group settings, see *Group*, page 107.
- ◆ Account Policy: configures the account policy settings, see *Account Policy*, page 117.
- ◆ Online User: disconnects the online user(s) from accessing the KVM over IP OmniBus Gateway, see *Online User*, page 119.

Users

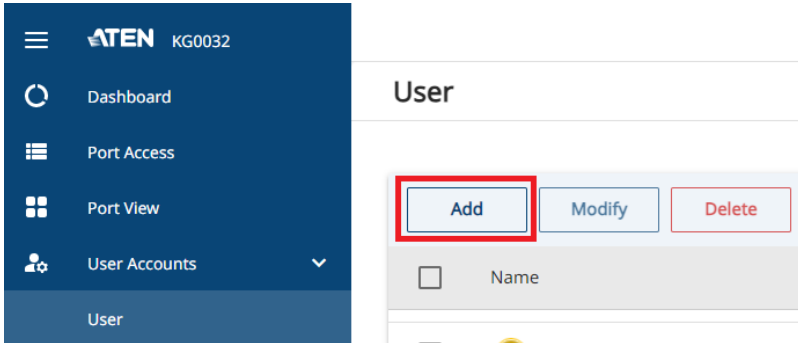
The KVM over IP OmniBus Gateway supports three types of user, as shown in the table, below:

User Type	Role
Super Administrator	Access and manage ports and devices. Manage Users, and Groups. Configure the overall installation. Configure personal working environment.
Administrator	Access and manage authorized ports and devices. Manage Users and Groups. Configure personal working environment.
User	Access authorized ports and devices. Manage authorized ports and devices; configure personal working environment. Note: Users who have been given permission to do so, may also manage other users.

Adding Users

To add a user, and assign user permissions, do the following:

1. Click **Add** from the *User* page.



- The Add pop-up window appears.

- Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Username	From 1 to 20 characters are allowed depending on the Account Policy settings. See <i>Encryption</i> , page 143.
Password	From 0 to 32 characters are allowed depending on the Account Policy settings. See <i>Encryption</i> , page 143.
Confirm Password	To be sure there is no mistake in the password, you are asked to enter it again. The two entries must match.
Description	Additional information about the user that you may wish to include.

Field	Description
User Type	<p>There are three categories: Super Administrator, Administrator and User. There is no limitation on the number of accounts that can be created in each category.</p> <ul style="list-style-type: none"> ◆ The Super Administrator is responsible for the overall installation configuration and maintenance; user management; and device and port assignments. The Super Administrator's permissions (see page 104) are automatically assigned by the system and cannot be altered. ◆ The default permissions for Administrators include everything except <i>View Only</i>, but the permissions can be altered for each Administrator by checking or unchecking any of the permissions checkboxes. ◆ The default permissions for Users include the Win and web clients, but the permissions can be altered for each User by checking or unchecking any of the permissions checkboxes. <p>Note: Users who have been given User Management privileges cannot access or configure Groups.</p>
<p>Permissions</p> <p>Note: For ordinary users, in addition to enabling <i>Device Management</i>, <i>Port Configuration</i>, and <i>Maintenance</i> permissions, the user must also be given those rights for each device and port that he will be allowed to manage. See <i>Device Assignment</i>, page 114 for details.</p>	<ul style="list-style-type: none"> ◆ Enabling <i>Device Management</i> allows a user to configure and control the settings for overall KVM over IP OmniBus Gateway operations (see <i>Device Management</i>, page 121). ◆ Enabling <i>Port Configuration</i> allows a user to configure and control the settings for individual ports (see <i>Configuration</i>, page 93). ◆ Enabling <i>User Management</i> allows a user to create, modify, and delete user and group accounts. ◆ Enabling <i>Maintenance</i> allows a user to perform all the Maintenance operations available under the Maintenance tab (see <i>Maintenance</i>, page 157). ◆ Enabling <i>System Log</i> allows a user to access the system log (see <i>Log</i>, page 151). ◆ Enabling <i>View Only</i> limits users to only being able to view the display of connected devices. They cannot control port access, nor can they input any keyboard or mouse signals to the devices they view. ◆ Enabling <i>Windows Client</i> allows a user to download the Windows Client AP software, and access the KVM over IP OmniBus Gateway with it, in addition to (or instead of) the browser access method. ◆ Enabling <i>Web Client</i> allows a user to access the KVM over IP OmniBus Gateway via a web browser.

Field	Description
Status	<p>Status allows you to control the user's account and access to the installation, as follows:</p> <ul style="list-style-type: none"> ◆ <i>Disable Account</i> lets you suspend a user's account without actually deleting it, so that it can be easily reinstated in the future. ◆ If you don't want to limit the time scope of the account, select <i>Account Never Expires</i>; if you do want to limit the amount of time that the account remains in effect, select <i>Account Expires On</i>, and key in the expiration date. ◆ To require a user to change his password at the next logon, select <i>The user is required to change the password upon the next login</i>. This can be used by the administrator to give the user a temporary password to log in for the first time, and then let the user set the password of his choice for future logins. ◆ To make a password permanent, so that the user cannot change it to something else, select <i>The user cannot change the account password</i>. ◆ For security purposes, administrators may want users to change their passwords from time to time. <ul style="list-style-type: none"> ◆ If not, select <i>Password Never Expires</i>. This allows users to keep their current passwords for as long as they like. ◆ If so, select <i>Password Expires After</i>, and key in the number of days allowed before the password expires. Once the time is up, a new password must be set.

4. At this point you can assign the new user to a group by selecting the *Groups* tab – the Groups page is discussed on page 110. You can also assign the user's port access rights by selecting the *Devices* tab – the Devices page is discussed on page 114.

Note: Optionally, you can skip this step now to add more users and create groups, and come back to it later.

5. When your selections have been made click **Save**.

6. The new user appears in the list.

Repeat the above procedure to add additional users.

Modifying User Accounts

To modify a user account, do the following:

1. Select the user's name by checking the checkbox beside it and click **Modify**.
2. In the Modify pop-up window that comes up, make your changes, then click **Save**.

Note: The *User* page is discussed on page 102; the *Groups* page is discussed on page 110, the *Devices* page is discussed on page 114.

Deleting User Accounts

To delete a user account do the following:

1. Select the user's name by checking the checkbox beside it.
2. Click **Delete** and click **Delete**.
3. Click **OK**.

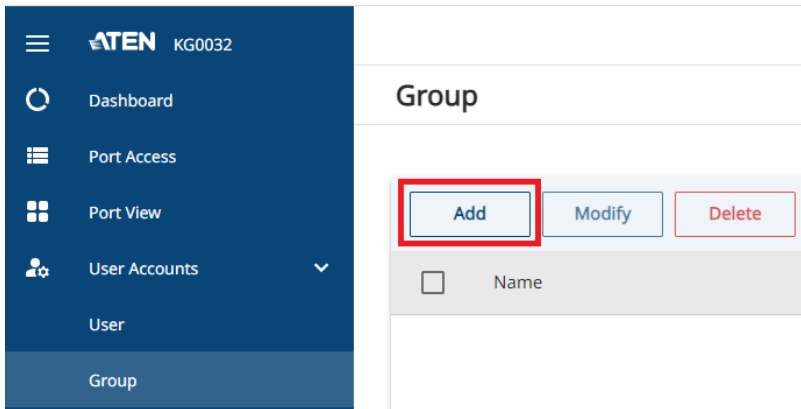
Group

Groups allow administrators to easily and efficiently manage users and devices. Since device access rights apply to anyone who is a member of the group, administrators need only set them once for the group, instead of having to set them for each user individually. Multiple groups can be defined to allow some users access to specific devices, while restricting other users from accessing them.

Creating Groups

To create a group, do the following:

1. Click **Add** from the *Group* page.



2. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Group Name	A maximum of 16 characters is allowed.
Description	Additional information about the user that you may wish to include. A maximum of 63 characters is allowed.
Permissions	Permissions and restrictions for groups are set by checking the appropriate boxes. These are the same permissions as the ones specified for Users. See <i>Permissions</i> , page 104 for details

3. At this point you can assign users to the group by selecting the *Members* tab – the Members page is discussed on page 112. You can also assign the group’s port access rights by selecting the *Devices* tab – the Devices page is discussed on page 114.

Note: Optionally, you can skip this step now to add more groups and assign users to them, and come back to it later.

4. When your selections have been made click **Save**.
5. The new group appears in the list.

Repeat the above procedure to add additional groups.

Modifying Groups

To modify a group, do the following:

1. Select the group's name by checking the checkbox beside it and click **Modify**.
2. In the Modify pop-up window that comes up, make your changes, then click **Save**.

Note: The *Group* page is discussed on page 107; the *Members* page is discussed on page 112, The *Devices* page is discussed on page 114.

Deleting Groups

To delete a group do the following:

1. Select the user's name by checking the checkbox beside it.
2. Click **Delete** and click **Delete**.
3. Click **OK**.

Users and Groups

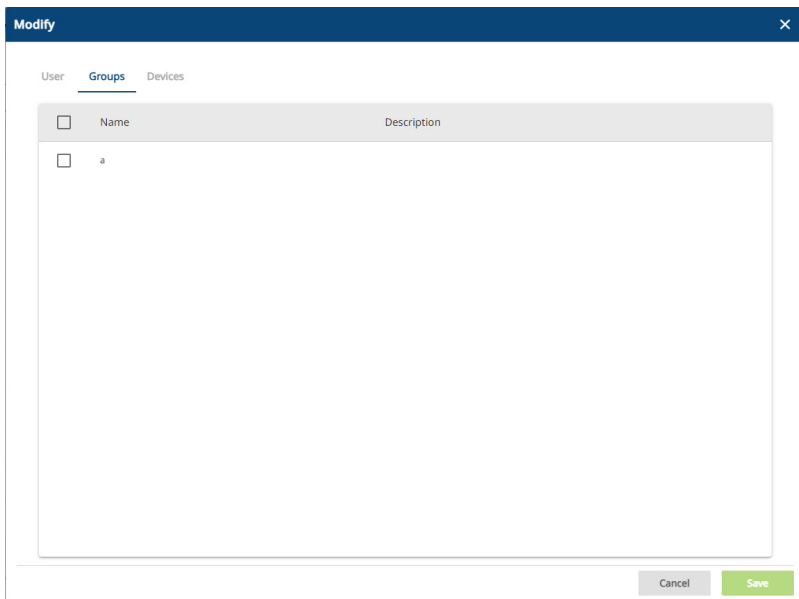
There are two ways to manage users and groups: from the Users's Modify pop-up; and from the Group's Modify pop-up windows.

Note: Before you can assign users to groups, you must first create them. See *Adding Users*, page 102 for details.

Assigning Users to a Group - User

To assign a user to a group from the User's Modify pop-up window, do the following:

1. Select the user's name by checking the checkbox beside it and click **Modify**.
2. In the Modify pop-up window that comes up, select the *Groups* tab. A screen, similar to the one below, appears:



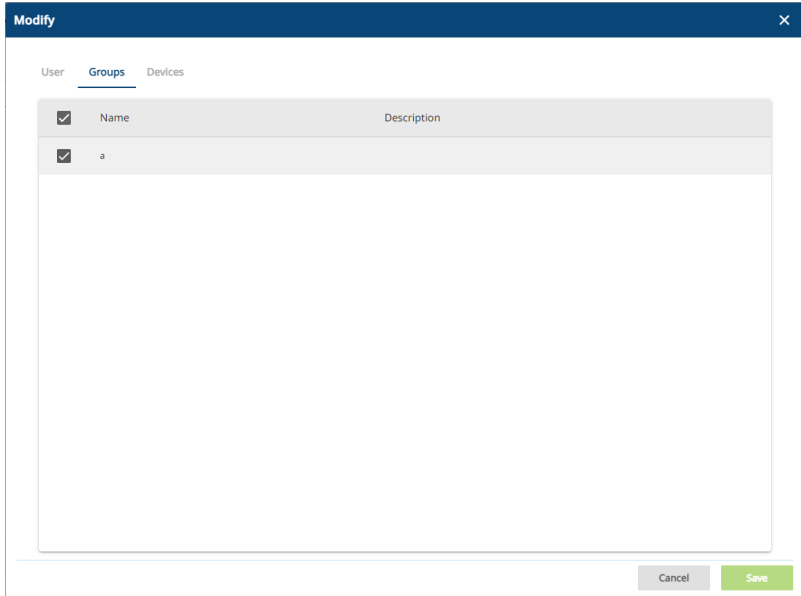
3. Select the group(s) that you want the user to be in.
4. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users from a Group - User

To remove a user from a group from the User's Modify pop-up window, do the following:

1. Select the user's name by checking the checkbox beside it and click **Modify**.
2. In the Modify pop-up window that comes up, select the *Groups* tab. A screen, similar to the one below, appears:

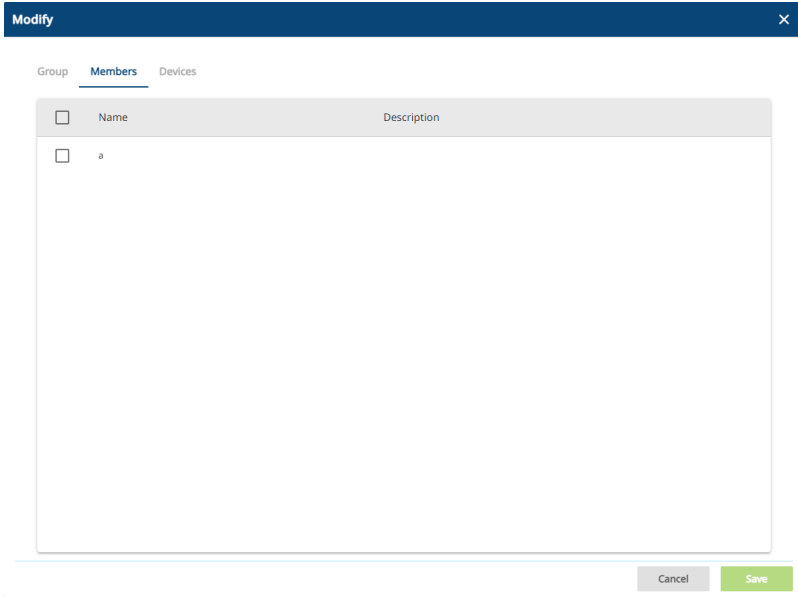


3. Select the group(s) that you want to remove the user from.
4. Click **Save** when you are done.

Assigning Users to a Group - Group

To assign a user to a group from the Group's Modify pop-up window, do the following:

1. Select the group's name by checking the checkbox beside it and click **Modify**.
2. In the Modify pop-up window that comes up, select the *Members* tab. A screen, similar to the one below, appears:



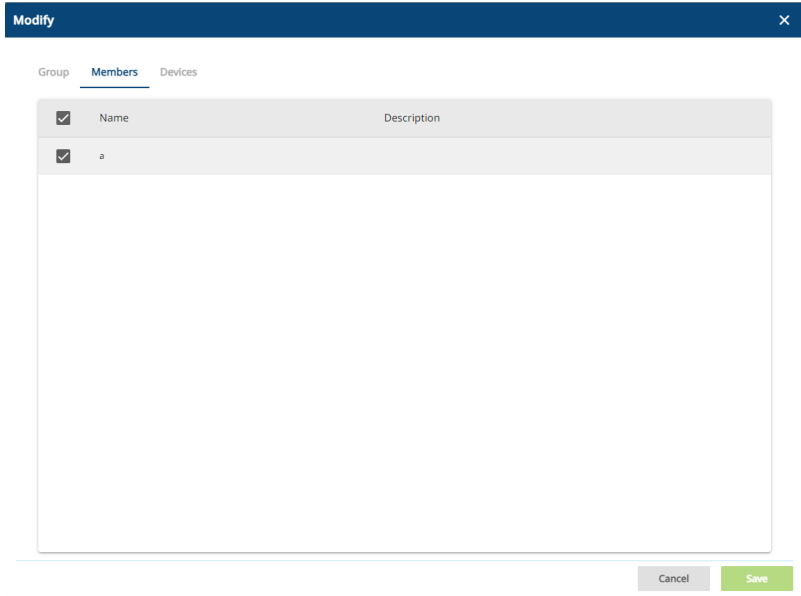
3. Select the user(s) that you want to be a member of the group.
4. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users from a Group - Group

To remove a user from a group from the Group's Modify pop-up window, do the following:

1. Select the group's name by checking the checkbox beside it and click **Modify**.
2. In the Modify pop-up window that comes up, select the *Members* tab. A screen, similar to the one below, appears:



3. Select the user(s) that you want to remove from the group.
4. Click **Save** when you are done.

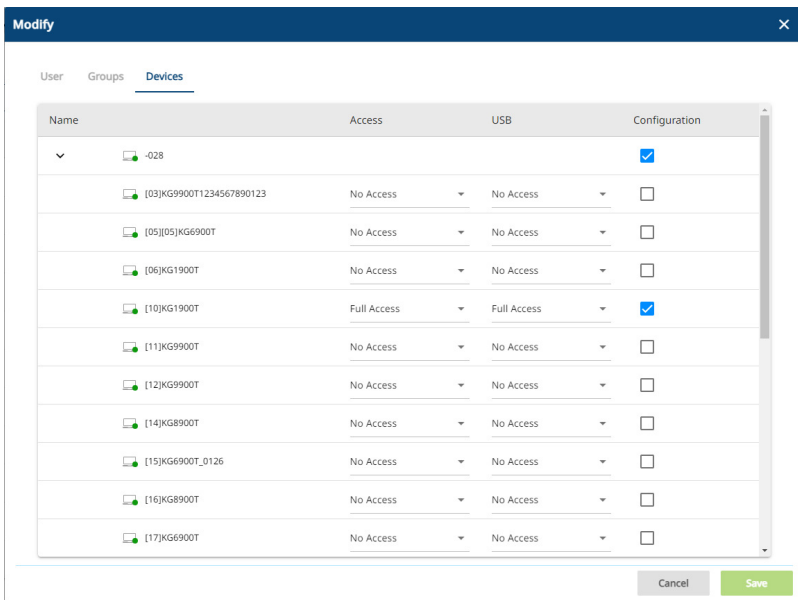
Device Assignment

When a user logs in to the KVM over IP OmniBus Gateway, the interface comes up with the Port Access page displayed. All the ports that the user is permitted to access are listed in the Sidebar at the left of the page. Access permissions for those ports and the devices connected to them are assigned on a port-by-port basis from the *User* or *Group* list of the User Accounts page.

Assigning Device Permissions - User

To assign a device permissions to a user from the User's Modify pop-up window, do the following:

1. Select the user's name by checking the checkbox beside it and click **Modify**.
2. In the Modify pop-up window that comes up, select the *Devices* tab. A screen, similar to the one below, appears:



3. Make your permission settings for each port according to the information provided below:

Name: Each port accessible to the user is listed under the *Names* column.

Access: The *Access* column is where device access rights are set. Click the icon in the row that corresponds to the port you want to configure to cycle through the choices. The meanings of the icons are described in the table below:

No Access	No access rights - the Port will not show up on the User's list on the Main Screen.
View Only	The user can only view the remote screen; he cannot perform any operations on it.
Full Access	The user can view the remote screen and can perform operations on the remote server from his keyboard and monitor.

USB: The *USB* column is where USB Virtual Media device access rights are listed. This entry does not appear for KVM over IP OmniBus Gateway that do not support the USB Virtual Media function. Click the icon in the row that corresponds to the port you want to configure to cycle through the choices.

No Access means that the User cannot mount, read, and write the virtual media; *View Only* means that the user can only read already mounted virtual media data; *Full Access* means that the User can mount, read, and write the virtual media.

Config: The *Config* column is where a user's permission to make changes to a port's configuration settings are permitted/restricted. Click the icon in the row that corresponds to the port you want to configure to cycle through the choices.

A check mark (✓) indicates that the user has permission to make changes to the port's configuration settings; an empty checkbox means that the user is denied permission to make configuration changes.

4. When you have finished making your choices, click **Save**.

Assigning Device Permissions - Group

To assign a device permissions to a Group of users, do the following:

1. Select the group's name by checking the checkbox beside it and click **Modify**.
2. In the Modify pop-up window that comes up, select the *Devices* tab.
3. The screen that comes up is the same one that appears in the User's Modify pop-up window. The only difference is that whatever settings you make apply to all members of the group instead of just one individual member.

Make your device assignments according to the information described under *Assigning Device Permissions - User*, page 114.

Account Policy

In the Account Policy sub-tab, system administrators can set policies governing usernames and passwords.

Account Policy

Minimum Username Length	<input style="width: 95%;" type="text" value="1"/>
Minimum Password Length	<input style="width: 95%;" type="text" value="0"/>
Password Must Contain At Least	<input type="checkbox"/> One Upper Case <input type="checkbox"/> One Lower Case <input type="checkbox"/> One Number <input type="checkbox"/> One Special ?
<input type="checkbox"/> Minimum Number(%) of Characters Changed from Previous Password	<input style="width: 95%;" type="text" value="50"/>
<input type="checkbox"/> Disable Duplicate Login	
<input type="checkbox"/> Enforce Password History	<input style="width: 95%;" type="text" value="3"/>

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

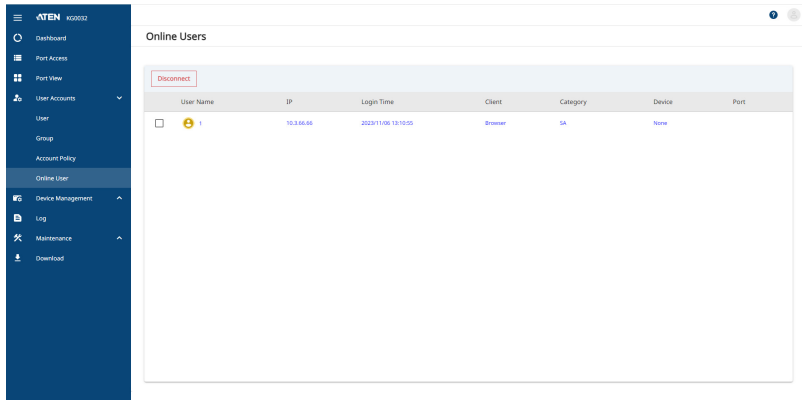
Entry	Explanation
Minimum Username Length	Sets the minimum number of characters required for a username. Acceptable values are from 1–16. The default is 6.
Minimum Password Length	Sets the minimum number of characters required for a password. Acceptable values are from 0–32. A setting of 0 means that no password is required. Users can login with only a Username. The default is 6.
Password Must Contain At Least	Checking any of these items requires users to include at least one uppercase letter, one lowercase letter or one number in their password. Note: This policy only affects user accounts created after this policy has been enabled, and password changes to existing user accounts. Users accounts created before this policy was enabled, and there is no change to the existing passwords, are not affected.

Entry	Explanation
Minimum Number(%) of Characters Changed from Previous Password	Sets the minimum number in percentage of characters required to be changed from the previous password.
Disable Duplicate Login	Check this to prevent users from logging in with the same account at the same time.
Enforce Password History	This prevents users from using the same password when they are required to recreate their password. Enter the number of password changes that must occur before a previous password can be used a second time.

When you have finished configuring, click **Save**.

Online User

In the Online User sub-tab, users with device management permission can disconnect online users from accessing the KVM over IP OmniBus Gateway.



To disconnect a user from accessing the KVM over IP OmniBus Gateway, do the following:

1. Select the user's name by checking the checkbox beside it and click **Disconnect**.
2. Click **Confirm**.

This Page Intentionally Left Blank

Chapter 9

Device Management

KVM over IP OmniBus Gateway Devices

When the Device Management is selected, the tab opens up for a list of options with the KVM over IP OmniBus Gateway including *Device Information*, *Operating Mode*, *Network*, *ANMS*, *Security*, *Date / Time*, and *Disclaimer*. Each option is explained fully in the following pages, please see below for reference.

Device Information	
General	
Device Name:	-028
MAC1 Address:	00-10-74-03-00-44
MAC2 Address:	00-10-74-03-00-45
Firmware Version:	V1.0.000-84R0231-1027
IP Address 1:	10.0.10.28
Subnet Mask 1:	255.255.252.0
Gateway 1:	10.0.10.254
Preferred DNS Server 1:	10.0.1.6
Alternate DNS Server 1:	10.0.1.7
IPv6 Address 1:	fe80::f56c:46e8:af:c1:5484
IPv6 Subnet Prefix Length 1:	64
IPv6 Gateway 1:	fe80::ae71:2eff:60:70:c072
IPv6 Preferred DNS Server 1:	6000:6
IP Address 2:	192.168.0.51
Subnet Mask 2:	255.255.255.0
IPv6 Subnet Prefix Length 2:	64

- ◆ **Device Information:** shows the general device and system information of the KVM over IP OmniBus Gateway, and configures its system settings, see *Device Information*, page 122.
- ◆ **Operating Mode:** configures the operating mode, see *Operating Mode*, page 125.
- ◆ **Network:** configures the network settings, see *Network*, page 126.
- ◆ **ANMS:** configures the ANMS settings such as event destination, authentication, and SNMP agent, see *ANMS*, page 130.
- ◆ **Security:** configures the security settings such as access protection and certificate, see *Security*, page 138.
- ◆ **Date / Time:** configures the date and time settings, see *Date / Time*, page 148.
- ◆ **Disclaimer:** configures the disclaimer, see *Disclaimer*, page 150.

Device Information

There are two sections in the Device Information page, *General* and *System Info. & Settings*.

General

The *General* section of the Device Information page displays the name of the selected device, its firmware version, the FPGA (Field-Programmable-Gate-Array) and information about its network configuration.

Device Information	
General	System Info. & Settings
Device Name:	中文中文中文中文中文-028
MAC1 Address:	00-10-74-03-00-44
MAC2 Address:	00-10-74-03-00-45
Firmware Version:	V1.0.080 Build20231027
IP Address 1:	10.0.90.28
Subnet Mask 1:	255.255.252.0
Gateway 1:	10.0.90.254
Preferred DNS Server 1:	10.0.1.6
Alternate DNS Server 1:	10.0.1.7
IPv6 Address 1:	fd90::fa6e:46e8:afc1:5484
IPv6 Subnet Prefix Length 1:	64
IPv6 Gateway 1:	fe80::ae71:2eff:fe70:c072
IPv6 Preferred DNS Server 1:	fd00::6
IP Address 2:	192.168.0.61
Subnet Mask 2:	255.255.255.0
IPv6 Subnet Prefix Length 2:	64

System Info. & Settings

The *System Info. Settings* section of the Device Information page presents information concerning the device's environment, and configures the Power Supply Detection, Fan Warning Message, and Temperature Warning Message settings.

Device Information

General System Info. & Settings

Settings

Power Supply Detection

Fan Warning Message

Temperature Warning Message

Temperature Threshold - Celsius Fahrenheit

System Status

Power1	● On
Power2	● Off
Fan1	6818 rpm
Fan2	6783 rpm
Fan3	6818 rpm
Fan4	6716 rpm
Temperature1	42 Celsius

Settings

The meanings of the Settings entries are explained in the table below:

Item	Description
Power Supply Detection	<p>When this function is enabled (there is a check in the checkbox), if there is only one source of power, the KVM over IP OmniBus Gateway will beep constantly to warn you of the problem.</p> <p>You will see a message asking you to confirm that your intention is to only have one power source. If your intention is to only have one source of power, there are two ways to stop the beeping: 1) You can disable power supply warnings by unchecking the checkbox. Do this if you want to disable this function on a permanent basis.</p> <p>Or, 2) you can confirm your intention in the dialog box. Do this if you only want to disable the warning temporarily. With this method, the warning function will be back in effect after the next system reset.</p> <p>The default for this function is enabled.</p>

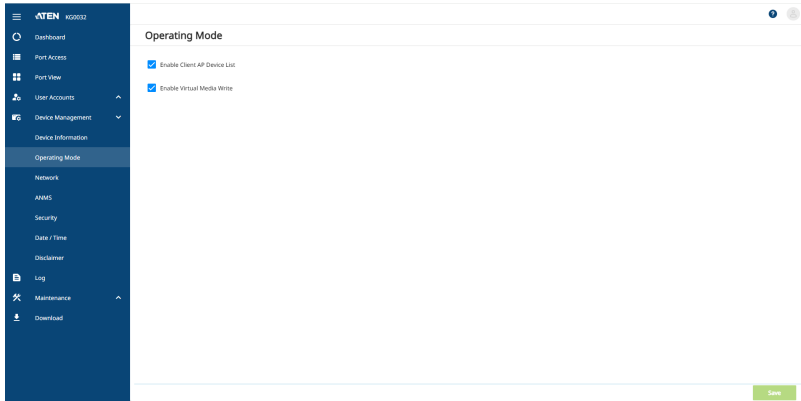
Item	Description
Fan Warning Message	<p>Place a check in the checkbox to enable a fan warning message. If this function is enabled, when any fan stops spinning the system records the event in the system log. If it is not enabled, the event will not be recorded.</p> <p>Note: The warning doesn't necessarily mean that the fan has failed, since the fan will stop spinning (as desired) when the temperature drops below its lower setting.</p> <p>The default for this function is enabled.</p>
Temperature Warning Message	<p>Place a check in the checkbox to enable a temperature warning message. If this function is enabled, when the device's temperature drops below the Low threshold setting, or exceeds the High threshold setting, the system records the event in the system log. If it is not enabled, the event will not be recorded.</p> <p>The default for this function is enabled.</p>
Temperature Threshold	<ul style="list-style-type: none">◆ Sets the temperature threshold for the Temperature Warning Message.◆ Temperature readings from the KVM over IP OmniBus Gateway's built-in sensors are indicated here and can be displayed in degrees Celsius or Fahrenheit.

When you have finished configuring, click **Save**.

System Status

The System Status displays information of the device's environment. The icons for Power 1 and Power 2 display in gray when there is no power to the power supply – they display in green when power is present.

Operating Mode



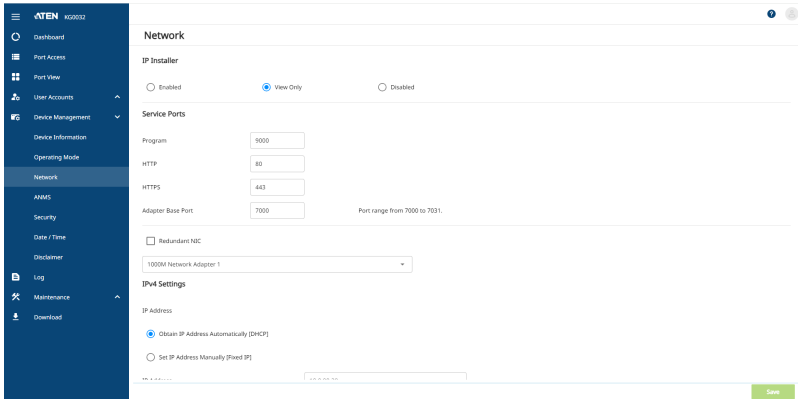
The Operating Mode page is used to set working parameters, as described below:

- ◆ If *Enable Client AP Device List* is enabled, the KVM over IP OmniBus Gateway appears in the Server List when using the WinClient AP (see *Windows Client AP Login*, page 29). If this option is not enabled, the KVM over IP OmniBus Gateway can still be connected to, but its name will not appear in the Server List.
- ◆ If *Enable Virtual Media Write* is enabled, the KVM over IP OmniBus Gateway 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.

When you have finished configuring, click **Save**.

Network

The Network page is used to specify the network environment.



Each of the elements on this page is described in the sections that follow.

IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the KVM over IP OmniBus Gateway.

Click one of the radio buttons to select *Enable*, *View Only*, or *Disable* for the IP Installer utility. See *IP Installer*, page 192, for IP Installer details.

Note: 1. If you select *View Only*, you will be able to see the KVM over IP OmniBus Gateway 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 *Disable* after each use.

Service Ports

As a security measure, if a firewall is being used, the Administrator can specify the port numbers that the firewall will allow. If a port other than the default is used, users must specify the port number as part of the IP address when they log in. If an invalid port number (or no port number) is specified, the KVM over IP OmniBus Gateway will not be found. An explanation of the fields is given in the table below:

Field	Explanation
Program	This is the port number for connecting with the WinClient AP, WebClient viewer, or via Virtual Media. 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.
Adapter Base Port	The port for Adapter access. The default is 7000.

-
- Note:** 1. Valid entries for all of the Service Ports are from 1–65535.
2. 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 doesn't matter what these numbers are set to, since they have no effect.
-

NIC Settings

- ◆ Redundant NIC

The KVM over IP OmniBus Gateway is designed with two network interfaces. If *Redundant NIC* is enabled (the default), both interfaces make use of the IP address of Network Adapter 1.

Under this configuration, the second interface is usually inactive. If there is a network failure on the first interface, the KVM over IP OmniBus Gateway automatically switches to the second interface.

- ◆ Redundant NIC Enabled – Single IP Address for Both Interfaces

To enable the Redundant NIC function, do the following:

1. Click to put a check in the *Redundant NIC* checkbox.
2. *Network Adapter 1* is selected in the network adapter listbox, and the listbox is disabled – you cannot configure Network Adapter 2.
3. Configure the IP and DNS server addresses for Network Adapter 1 (see the sections below).

- ◆ Redundant NIC Not Enabled – Two IP Addresses

If you choose not to enable the Redundant NIC function, the two NICs can be configured with separate interfaces. Users can log into the KVM over IP OmniBus Gateway with either IP address. To set up the KVM over IP OmniBus Gateway with this configuration, do the following:

1. If there is a check in the *Redundant NIC* checkbox, click to remove it.
2. In the network adapter listbox; select Network Adapter 1.
3. Configure the IP and DNS server addresses for Network Adapter 1 (see the sections below).
4. Drop down the network adapter listbox; select Network Adapter 2.
5. Configure the IP and DNS server addresses for Network Adapter 2.

IPv4 Settings

- ◆ IP Address:

IPv4 is the traditional method of specifying IP addresses. The KVM over IP OmniBus Gateway can either have its IP address assigned dynamically (DHCP), or it can be given a fixed IP address.

- ◆ For dynamic IP address assignment, select the *Obtain IP Address Automatically [DHCP]* radio button. (This is the default setting.)
- ◆ To specify a fixed IP address, select the *Set IP Address Manually [Fixed IP]* radio button and fill in the fields with values appropriate for your network.

Note: 1. If you choose *Obtain IP Address Automatically [DHCP]*, when the KVM over IP OmniBus Gateway starts up it waits to get its IP address from the DHCP server. If it hasn't obtained the address after one minute, it automatically reverts to its factory default IP address (192.168.0.60.)

2. If the KVM over IP OmniBus Gateway is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see *IP Address Determination*, page 192, for information./

-
- ◆ DNS Server
 - ◆ For automatic DNS Server address assignment, select the *Obtain DNS Address Automatically* radio button.
 - ◆ To specify the DNS Server address manually, select the *Set DNS Address Manually* radio button, and fill in the addresses for the Preferred and Alternate DNS servers with values appropriate for your network.

Note: Specifying the Alternate DNS Server address is optional.

IPv6 Settings

- ◆ IP Address:

IPv6 is the new (128-bit) format for specifying IP addresses. (See *IPv6*, page 194 for further information.) The KVM over IP OmniBus Gateway can either have its IPv6 address assigned dynamically (DHCP), or it can be given a fixed IP address.

- ◆ For dynamic IP address assignment, select the *Obtain IPv6 Address Automatically [DHCP]* radio button. (This is the default setting.)
- ◆ To specify a fixed IP address, select the *Set IPv6 Address Manually [Fixed IP]* radio button and fill in the fields with values appropriate for your network.
- ◆ DNS Server
 - ◆ For automatic DNS Server address assignment, select the *Obtain DNS Address Automatically* radio button.
 - ◆ To specify the DNS Server address manually, select the *Set DNS Address Manually* radio button, and fill in the addresses for the Preferred and Alternate DNS servers with values appropriate for your network.

Note: Specifying the Alternate DNS Server address is optional.

When you have finished configuring, click **Save**.

ANMS

The ANMS (Advanced Network Management Settings) page is used to set up login authentication and authorization management from external sources. It is organized into three sections – each with a series of related panels, as described, below:

Event Destination

ANMS

[Event Destination](#) [Authentication](#) [SNMP Agent](#)

SMTP Settings

Enable Report from the Following SMTP Server

SMTP Server

Service Port

My Server Requires Secured Connection (SSL)

My Server Requires Authentication

Account Name

Password

From

To

Log Server

Enable

SMTP Settings

To have the KVM over IP OmniBus Gateway email reports from the SMTP server to you, do the following:

1. Enable the *Enable Report from the Following SMTP Server*, and key in either the IPv4 address, IPv6 address, or domain name of the SMTP server.

2. If your server requires a secure SSL connection, put a check in the *My Server Requires Secure Connection (SSL)* checkbox.
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: 1. Only one email address is allowed in the *From* field, and it cannot exceed 64 Bytes.

2. 1 Byte = 1 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 Bytes.

Log Server

Important transactions that occur on the KVM over IP OmniBus Gateway, such as logins and internal status messages, are kept in an automatically generated log file.

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

Note: The port number must be different than the one used for the *Program* port (see *Program*, page 127).

See Chapter 13, *The Log Server*, for details on setting up the log server. The Log File is discussed on page 151.

SNMP Trap

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

1. Check *Enable*.
2. Key in either the IPv4 address, IPv6 address, or domain name of the computer to be notified of SNMP trap events.
3. Key in the port number. The valid port range is 1–65535.

Note: The logs that are notified of SNMP trap events are configured on the Notification Settings page under the Log tab. See *Notification Settings*, page 155 for details.

Syslog Server

To record all the events that take place on KVM over IP OmniBus Gateways and write them to a Syslog server, do the following:

1. Check *Enable*.
2. Key in either the IPv4 address, IPv6 address, or domain name of the Syslog server.
3. Key in the port number. The valid port range is 1-65535.

When you have finished configuring, click **Save**.

Authentication

ANMS

Event Destination **Authentication** SNMP Agent

Disable Device Authentication

RADIUS Settings

Enable

Preferred RADIUS	<input type="text" value=""/>
Server IP	<input type="text" value="10.0.92.221"/>
Port	<input type="text" value="1645"/>
Authentication Type	<input type="text" value="PAP"/>
Timeout	<input type="text" value="3"/> sec
Retries	<input type="text" value="3"/>
Shared Secret (at least 6 characters)	<input type="text" value="....."/>

AD / LDAP Settings

Enable

◆ Disable Local Authentication

Selecting this option disables login authentication on the KVM over IP OmniBus Gateway. The device can only be accessed using LDAP, LDAPS, MS Active Directory, or RADIUS authentication.

RADIUS Settings

To allow authentication and authorization for the KVM over IP OmniBus Gateway through a RADIUS server, do the following:

1. Check **Enable**.
2. Select Preferred or Alternate RADIUS server.

3. Fill in the IP addresses and service port numbers for the Preferred and Alternate RADIUS servers. You can use the IPv4 address, the IPv6 address or the domain name in the IP fields.
4. Select the *Authentication Type*: PAP or CHAP.
5. In the *Timeout* field, set the time in seconds that the KVM over IP OmniBus Gateway waits for a RADIUS server reply before it times out.
6. In the *Retries* field, set the number of allowed RADIUS retries.
7. In the *Shared Secret* field, key in the character string that you want to use for authentication between the KVM over IP OmniBus Gateway and the RADIUS Server. A minimum of 6 characters is required.
8. On the RADIUS server, Users can be authenticated with any of the following methods:
 - ◆ Set the entry for the user as **su/xxxx**
Where *xxxx* represents the Username given to the user when the account was created on the KVM over IP OmniBus Gateway.
 - ◆ Use the same Username on both the RADIUS server and the KVM over IP OmniBus Gateway.
 - ◆ Use the same Group name on both the RADIUS server and the KVM over IP OmniBus Gateway.
 - ◆ Use the same Username/Group name on both the RADIUS server and the KVM over IP OmniBus Gateway.

In each case, the user's access rights are the ones assigned that were assigned when the User of Group was created on the KVM over IP OmniBus Gateway. (See *Adding Users*, page 102.)

AD / LDAP Settings

To allow authentication and authorization for the KVM over IP OmniBus Gateway via LDAP / LDAPS, refer to the information in the table, below:

Item	Action
Enable	Put a check in the <i>Enable</i> checkbox to allow LDAP / LDAPS authentication and authorization.
LDAP Server IP and Port	<p>Select Preferred or Alternate LDAP Server and fill in the IP address and port number for the LDAP or LDAPS server.</p> <ul style="list-style-type: none"> ◆ You can use the IPv4 address, the IPv6 address or the domain name in the <i>LDAP Server</i> field. ◆ For LDAP, the default port number is 389; for LDAPS, the default port number is 636.

Item	Action
Timeout	Set the time in seconds that the KVM over IP OmniBus Gateway 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: ou=kn8132,dc=aten,dc=com
Admin Name	Key in the LDAP administrator's username.
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.

On the LDAP / LDAPS server, Users can be authenticated with any of the following methods:

- ◆ With MS Active Directory schema.
- ◆ Without schema – Only the Usernames used on the KVM over IP OmniBus Gateway are matched to the names on the LDAP / LDAPS server. User privileges are the same as the ones configured on the KVM over IP OmniBus Gateway.
- ◆ Without schema – Only Groups in AD are matched. User privileges are the ones configured for the groups he belongs to on the KVM over IP OmniBus Gateway.
- ◆ Without schema – Usernames and Groups in AD are matched. User privileges are the ones configured for the User and the Groups he belongs to on the KVM over IP OmniBus Gateway.

Note:

1. LDAP attribute is required for complete setup. LDAP attribute can be retrieved from the GET command using the Terminal interface. Please refer to *Terminal* on page 163 for more details. An unique X500 Object ID (OID) is assigned from your organization or defined by you own (e.g. 1.3.6.1.4.1.21317.1.3.1.3) for the attribute.
2. For more information on configuring LDAP, you can download the full LDAP instructional manual from our website.

When you have finished configuring, click **Save**.

SNMP Agent

The SNMP Agent allows you to configure most Device Management settings with a MIB browser using the MIB file downloaded from our website. The MIB file imports into the MIB browser to configure the following Device Management settings: *Operating Mode*: Mode, COM Settings; *Network*: IP Installer, Service Ports, IPv4 Settings, IPv6 Settings; *ANMS - Event Destination*: Log Server, SNMP Trap.

Download the **KG MIB File** on our website from any KVM over IP OmniBus Gateway product page under *Support and Download*.

To connect to the KVM over IP OmniBus Gateway through an MIB browser, use the instructions below to add an SNMP Agent to allow access from the computer you will use to configure to the KVM over IP OmniBus Gateway settings.

ANMS

Event Destination Authentication **SNMP Agent**

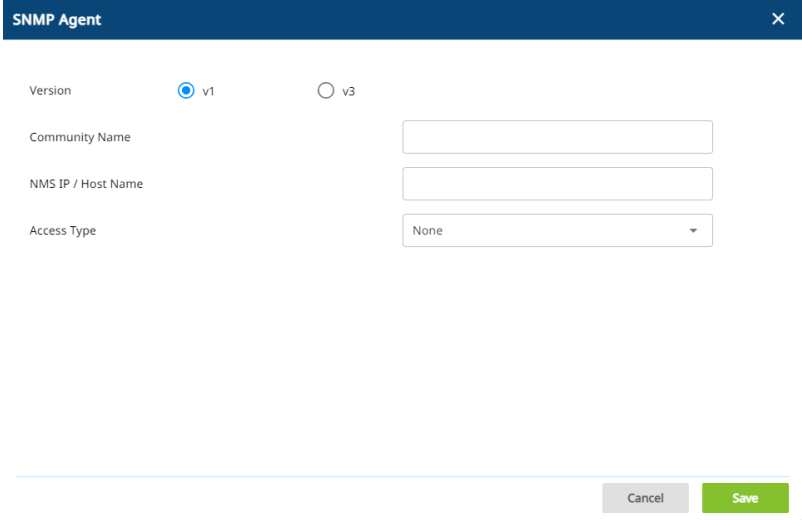
Enable

Add Modify Delete Node

Community / User Name	IP	Version	Access Type
<input type="checkbox"/> 2	2	v1	None

To add an SNMP Agent, do the following:

1. Check **Enable**.
2. Click **Add**. A SNMP Agent pop-up window appears:



The image shows a configuration window titled "SNMP Agent" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Version:** Two radio buttons are present. The first is labeled "v1" and is selected (indicated by a blue dot). The second is labeled "v3" and is unselected.
- Community Name:** A text input field.
- NMS IP / Host Name:** A text input field.
- Access Type:** A dropdown menu with "None" selected.
- Buttons:** At the bottom right, there are two buttons: "Cancel" (grey) and "Save" (green).

3. Select the Version.
4. Enter a Community Name.
5. Key in NMS IP/Host Name. Enter the IP address of a computer that will access the KVM over IP OmniBus Gateway via a MIB browser.
6. Select the Access Type and click **Save**.
7. From a MIB browser, import the MIB file* and then enter the IP address of the KVM over IP OmniBus Gateway.

Note: Download the **KN MIB File** on our website from any KVM over IP OmniBus Gateway product page, under *Support and Download*.

Security

The Security page is organized into two sections – each with a series of related panels, as described, below:

Access Protection

Security

[Access Protection](#) [Certificate](#)

Login Failures

Enable

Allowed

Timeout min

Lock Client PC Lock Account

Filter

Enable IP Filter

Include Exclude

<input type="checkbox"/> 192.168.0.90 - 192.168.0.100	<input type="button" value="Add"/>
<input type="checkbox"/> 192.168.0.90 - 192.168.0.100	<input type="button" value="Modify"/>
<input type="checkbox"/> 192.168.0.90 - 192.168.0.100	<input type="button" value="Delete"/>
<input type="checkbox"/> 192.168.0.90 - 192.168.0.100	

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

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

Entry	Explanation
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 a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.
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. Note: 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.

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

Filter

Filter

Enable IP Filter

Include

Exclude

<input type="checkbox"/>	192.168.0.90 - 192.168.0.100
<input type="checkbox"/>	192.168.0.90 - 192.168.0.100
<input type="checkbox"/>	192.168.0.90 - 192.168.0.100
<input type="checkbox"/>	192.168.0.90 - 192.168.0.100

Add

Modify

Delete

Login String

Enable MAC Filter

Include

Exclude

<input type="checkbox"/>	123456789012
<input type="checkbox"/>	123456789012
<input type="checkbox"/>	123456789012
<input type="checkbox"/>	123456789012

Add

Modify

Delete

◆ IP and MAC Filtering

IP and MAC Filters control access to the KVM over IP OmniBus Gateway based on the IP and/or MAC addresses of the client computers attempting to connect. A maximum of 100 IP filters and 100 MAC filters are allowed. If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.

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

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

- ◆ Adding Filters

To add an IP filter, do the following:

1. Click **Add**. An Add pop-up window similar to the one below appears:

The screenshot shows a dark blue header bar with the word "Add" on the left and a close "X" icon on the right. Below the header, the text "Please enter a specific IP address or IP range." is displayed. There is a checkbox labeled "Single" which is checked. Below the checkbox are two text input fields, both containing "0.0.0.0". At the bottom right of the window are two buttons: "Cancel" (grey) and "Save" (green).

2. Key the address you want to filter in the field on the left.
 - ◆ To filter a single IP address, click to put a check in the *Single IP* checkbox.
 - ◆ To filter a continuous range of addresses, key in the end number of the range in the field on the right.
3. After filling in the address, click **Save**.
4. Repeat these steps for any additional IP addresses you want to filter.

- ◆ Login String

The *Login String* entry field lets the super administrator specify a login string (in addition to the IP address) that users must add to the IP address when they access the KVM over IP OmniBus Gateway with a browser.

For example, if *192.168.0.126* were the IP address, and *abcdefg* were the login string, then the user would have to key in:

192.168.0.126/abcdefg

-
- Note:**
1. Users must place 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 KVM over IP OmniBus Gateway login page using the IP address alone. This makes your installation less secure.
-

The following characters are allowed in the string:

0–9 a–z A–Z ~ ! @ \$ & * () _ - = + [] .

The following characters are not allowed:

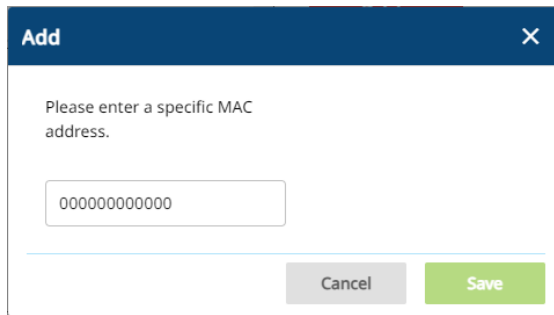
% ^ ” : / ? # \ ‘ { } ; ’ < > [Space]

Compound characters (É Ç ñ ... etc.)

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

To add a MAC filter, do the following:

1. Click **Add**. An Add pop-up window similar to the one below appears:



The image shows a dialog box titled "Add" with a close button (X) in the top right corner. The main text inside the dialog says "Please enter a specific MAC address." Below this text is a text input field containing the MAC address "000000000000". At the bottom of the dialog, there are two buttons: a grey "Cancel" button and a green "Save" button.

2. Specify the MAC address in the dialog box, then click **Save**.
 3. Repeat these steps for any additional MAC addresses you want to filter.
- ◆ **IP Filter / MAC Filter Conflict**

If there is a conflict between an IP filter and a MAC filter – in other words, if a computer’s address is allowed by one filter but blocked by the other – then the blocking filter takes precedence (the computer’s access is blocked).
 - ◆ **Modifying Filters**

To modify a filter, select it in the IP Filter or MAC Filter list boxes and click **Modify**. The Modify pop-up window is similar to the Add pop-up window. 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**.

Encryption

Enabling encryption affects system performance – no encryption offers the best performance. To enable encryption, check the *Enable Video Encryption* and *Enable VM Encryption* checkboxes, and click **Save**.

Security Level

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

The screenshot shows the 'Security' configuration page with the 'Access Protection' tab selected. Under 'Security Level', four radio buttons are visible: 'High', 'Medium High', 'Medium', and 'Custom'. The 'Custom' option is selected. To the right of these radio buttons are four checkboxes: 'Enable ICMP Service' (checked), 'Enable SNMP Service' (unchecked), 'Enable Telnet Service' (unchecked), and 'Enable SSH Service' (checked). Below these is the 'Enable HTTP Service' checkbox (unchecked) and the 'HTTPS Service' dropdown menu, which is currently set to 'Use TLS v1.3'. A note at the bottom left states: 'Note: you can use both HTTP and HTTPS to log in.' Below the note is the 'Enable FIPS' checkbox (unchecked).

1. High (Disable all services except: SSHv2, HTTPS(TLS v1.2))
2. Medium-high (Enables SSHv2, redirect HTTP to HTTPS, HTTPS(TLS v1.2), ICMP)
3. Medium (Enables SSHv2, redirect HTTP to HTTPS, HTTPS(TLS v1.0, 1.1, 1.2), SNMP Agent, ICMP) (**Default**)
4. Custom: Click to check the following security options you wish to apply:
 - ◆ Enable ICMP service
 - ◆ Enable SNMP service
 - ◆ Enable Telnet service
 - ◆ Enable SSH session
 - ◆ Enable HTTP session
 - ◆ Enable HTTPS session (Select between “Use TLS v1.3”, ”Use TLS v1.2, v1.3”, “Use TLSv1.0, v1.1, v1.2, v1.3”.)
5. If you want to enable FIPS security standard, click to check the *Enable FIPS*.

When you have finished configuring, click **Save**.

Certificate

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 +

Upload Restore Default



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

- ◆ **Generating a Self-Signed Certificate**

If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See *Self-Signed Private Certificates*, page 205 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 and private encryption key, save them to a convenient location on your computer.
- ◆ **Importing the Private Certificate**

To import the private certificate, do the following:

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

Note: 1. Clicking **Restore Default** returns the device to using the default ATEN certificate.

2. 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.

Certificate Signing Request

The interface shows a list of certificates with a '+' icon in the top right corner. Below the list are four buttons: 'Add' (blue), 'Get CSR' (blue), 'Upload' (light blue), and 'Remove CSR' (red).

To perform this operation do the following:

1. Click **Add**. The following Certificate Signing Request pop-up window appears:

The pop-up window is titled 'Certificate Signing Request' and contains the following fields:


- Country (2 letter code)
- State or Province
- Locality
- Organization
- Unit
- Common Name
- Email Address

At the bottom right, there are 'Cancel' and 'Save' 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

Information	Example
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Techdoc Department
Common Name	mycompany.com Note: This must be the exact domain name of the site that you want the certificate to be valid for. If the site's domain name is <i>www.mycompany.com</i> , and you only specify <i>mycompany.com</i> , the certificate will not be valid.
Email Address	administrator@yourcompany.com

- After filling in the form (all fields are required), click **Save**.
A self-signed certificate based on the information you just provided is now stored on the KVM over IP OmniBus Gateway.
- 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  to locate the file; then click **Upload** to store it on the KVM over IP OmniBus Gateway.

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

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

Date / Time

The Date / Time page sets the KVM over IP OmniBus Gateway time parameters:

Set the parameters according to the information below.

Time Zone

- ◆ To establish the time zone that the KVM over IP OmniBus Gateway 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.

When you have finished configuring, click **Save**.

Date / Time

- ◆ Click < or > to move backward or forward by one month increments and decrements.
- ◆ Click < or > to move backward or forward by one year increments and decrements.
- ◆ In the calendar, click on the day.
- ◆ To set the time, click and drag the blue dot clockwise or anti-clockwise to set the hour, click and drag the blue dot again to set the minute.
- ◆ Click **Set** to save your settings.

Network Time

To have the time automatically synchronized to a network time server, do the following:

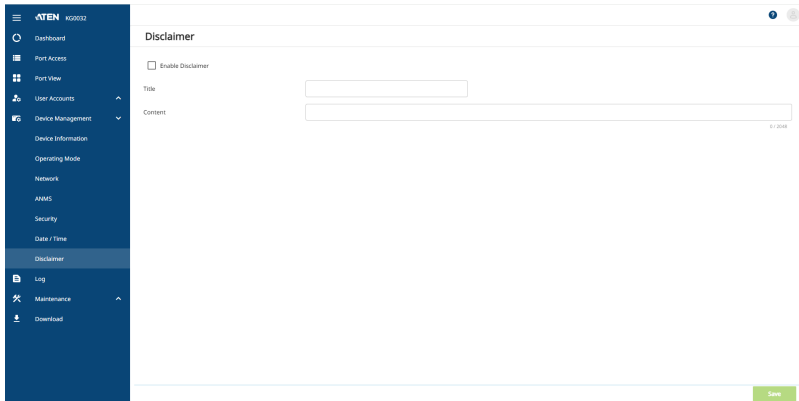
1. Check the *Enable Auto Adjustment* checkbox.
2. Drop down the time server list to select your preferred time server
– or –

Check the *Preferred Custom Server IP* checkbox, and key in either the IPv4 address, IPv6 address, or domain name 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**.

Disclaimer

You may set up disclaimers here as shown in the diagram below:

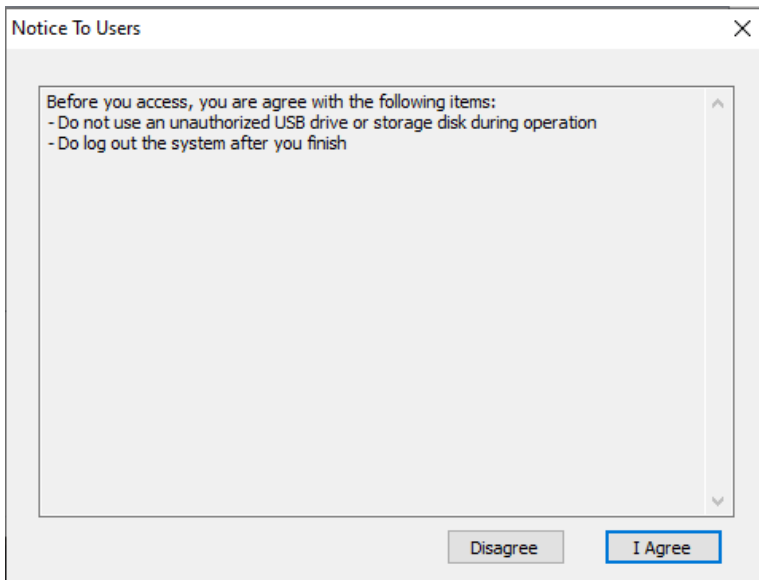


The screenshot shows the WtEN web interface for configuring a disclaimer. The left sidebar contains a navigation menu with the following items: Dashboard, Port Access, Port View, User Accounts, Device Management, Device Information, Operating Mode, Network, APSS, Security, Date / Time, Disclaimer (highlighted), Log, Maintenance, and Download. The main content area is titled "Disclaimer" and includes a checkbox for "Enable Disclaimer", a "Title" input field, and a "Content" text area. A "Save" button is located at the bottom right of the form.

To enable disclaimers upon logging in, check the *Enable Disclaimer* checkbox (Disabled by default).

Enter the title and content of the disclaimer and click **Save** to save the changes.

Disclaimers will be shown upon logging in. An example is shown below for logging in using Windows Client AP:



The screenshot shows a "Notice To Users" dialog box with a close button (X) in the top right corner. The text inside the dialog reads: "Before you access, you are agree with the following items:" followed by a list of two items: "- Do not use an unauthorized USB drive or storage disk during operation" and "- Do log out the system after you finish". At the bottom of the dialog, there are two buttons: "Disagree" and "I Agree".

Chapter 10

Log

Overview

The KVM over IP OmniBus Gateway logs all the events that take place on it. To view the contents of the log, click the *Log* tab. The device's Log Information page, similar to the one below, appears:

The screenshot displays the ATEN KVM032 Log Information page. The left sidebar contains navigation options: Dashboard, Port Access, Port View, User Accounts, Device Management, Device Information, Operating Mode, Network, ANMS, Security, Date / Time, Disclaimer, Log (selected), Maintenance, and Download. The main content area is titled 'Log' and includes 'Log Information' and 'Notification Settings' tabs. Below these are buttons for 'Pause', 'Clear Log' (highlighted with a red box), 'Export Log', and 'Filter'. A table of log entries is shown below:

Time	Severity	User	Log Information
2023/11/06 19:37:22	Least	1	OP User 1 (IP=10.3.66.66) logged out. Online time : 00:00h:00m:30s.
2023/11/06 19:36:56	Least	1	OP User 1 gain full access privilege, and switch to (2023) 海峽一二三四五六七七八九十
2023/11/06 19:36:52	Least	1	OP User 1 logged in.
2023/11/06 19:36:52	Least	System	OP User 1 (IP=10.3.66.66) attempting to login.
2023/11/06 19:36:52	Least	System	SVS Access via remote client IP=10.3.66.66
2023/11/06 19:36:52	Least	System	SVS Connected to 10.3.66.66 (24-62-48-78-CC-00)
2023/11/06 19:36:24	Least	1	DM User 1 modified disclaimer setting.
2023/11/06 15:48:25	Least	1	DM User 1 modified device information setting.
2023/11/06 15:48:18	Least	1	DM User 1 modified device information setting.
2023/11/06 14:29:48	Least	System	SVS User 1 end session of user ian.
2023/11/06 14:29:51	Least	System	OP User ian from 10.9.66.84 (24-62-48-78-CC-00) attempting to login via browser.
2023/11/06 14:28:35	Least	1	UM User 1 create account for user ian

Log Information

The Log Information page displays events that take place on the KVM over IP OmniBus Gateway, and provides a breakdown of the time, the severity, the user, and a description of each one. You can change the sort order of the display by clicking on the column headings.

The screenshot shows the 'Log Information' page with a table of events. The table has four columns: Time, Severity, User, and Log Information. The events listed include user logouts, privilege gains, logins, remote access, system connections, and device settings modifications.

Time	Severity	User	Log Information
2023/11/06 19:37:22	Least	1	OP: User 1 (IP=10.3.66.66) logged out. Online time: 0D:00H:00M:30S.
2023/11/06 19:36:56	Least	1	OP: User 1 gain full access privilege, and switch to [SYS00] 系统—二三四五十六七八九十
2023/11/06 19:36:52	Least	1	OP: User 1 logged in.
2023/11/06 19:36:52	Least	System	OP: User 1 (IP=10.3.66.66) attempting to login.
2023/11/06 19:36:52	Least	System	SYS: Access via remote client (IP=10.3.66.66).
2023/11/06 19:36:52	Least	System	SYS: Connected to 10.3.66.66 (34-62-88-78-CC-DD).
2023/11/06 19:36:24	Least	1	DM: User 1 modified disclaimer setting.
2023/11/06 15:48:25	Least	1	DM: User 1 modified device information setting.
2023/11/06 15:48:18	Least	1	DM: User 1 modified device information setting.
2023/11/06 14:29:48	Least	System	SYS: User 1 end session of user lan.
2023/11/06 14:29:31	Least	System	OP: User lan from 10.3.66.84 (34-62-88-78-CC-DD) attempting to login via browser.
2023/11/06 14:28:35	Least	1	UM: User 1 create account for user lan

The log file tracks a maximum of 512 events. When the limit is reached, the oldest events get discarded as new events come in. The purpose of the buttons at the bottom of the page are described in the following table:

Button	Explanation
Pause	Clicking <i>Pause</i> stops the display of new events. When the display is paused the button changes to <i>Resume</i> . Click Resume to start displaying events again.
Clear Log	Clicking <i>Clear Log</i> clears the log file.
Export Log	Clicking <i>Export Log</i> lets you save the contents of the log to a file on your computer.
Filter	Clicking <i>Filter</i> allows you to search for particular events by date or by specific words or strings, as described in the next section.

Filter





Filter lets you narrow the log event display to ones that occurred at specific times; ones containing specific words or strings; or ones involving specific users. When you access this function, the log filter pop-up window appears:

The screenshot shows a 'Display Options' dialog box with a dark blue header and a close button (X) in the top right. The dialog contains several sections:

- Start Date / Time...:** A checkbox (unchecked) followed by a date/time selection field with a calendar icon and a clock icon.
- End Date / Time...:** A checkbox (unchecked) followed by a date/time selection field with a calendar icon and a clock icon.
- Today Only:** A checkbox (unchecked).
- Device Time:** A checkbox (unchecked).
- Information:** Two empty text input fields.
- User:** A checked checkbox.
- Priority:** A checked checkbox.
- Least:** A checked checkbox.
- Less:** A checked checkbox.
- Most:** A checked checkbox.

At the bottom right, there are three buttons: 'Close' (grey), 'Apply' (green), and 'Reset' (green).

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

Item	Description
Start Date / Time	<p>Filters for events from a specific date and time to the present.</p> <ul style="list-style-type: none"> ◆ Put a check in the checkbox. ◆ Click  to set the date that you want the filtering to start from. ◆ Click  to set the time that you want the filtering to start from. <p>All events from the Start date / time to the present are displayed.</p>
End Date / Time	<p>Filters for events from a specific date and time to a specific date and time. First select the Start Date/Time (described above).</p> <ul style="list-style-type: none"> ◆ Put a check in the checkbox. ◆ Click  to set the ending date. ◆ Click  to set the ending time.
Today Only	<p>Only the events for the current day are displayed.</p>
Device Time	<p>Shows the events according to the time configured on the KVM over IP OmniBus Gateway.</p>

Item	Description
Information	<p>Filters for a particular word or string. Key the word or string into the <i>Information</i> text box. Only events containing that word or string are displayed. Wildcards (? for single characters; * for multiple characters) and the keyword or are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.</p>
User	<p>Filters for specific users. First put a check in the <i>User</i> checkbox; then key in the user's Username; then click Apply. Only events containing that Username are displayed.</p> <p>Note: If the <i>User</i> checkbox is not checked here in the Filter panel, the entire User column does not appear in the main panel.</p>
Priority	<p>Filters based on the severity rating of the event. Least events appear in black; Less events appear in blue; Most events appear in red.</p> <p>First put a check in the <i>Priority</i> checkbox; then check the severity options you want to filter for (you can check more than one item). Only events that match the severity ratings you specified appear in the display.</p> <p>Note: If the <i>Priority</i> checkbox is not checked here in the Filter panel, the entire Priority column does not appear in the main panel.</p>
Apply	Click to apply the filter choices.
Reset	Click this button to clear the entries in the dialog box and start with a clean slate.
Close	Click this button to exit the log filter function.

Notification Settings

The Notification Settings page lets you decide which events trigger a notification, and how the notification are sent out:

Log			
Log Information		Notification Settings	
Event	SNMP	SMTP	Syslog
▼ Authentication Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Login	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Login Fail	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Locked	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IP Address Locked	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Logout	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
End Session	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Browser Viewer started	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Browser Viewer ended	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ KVM Viewer Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Viewer Switch Port	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Notifications can be sent via SNMP trap, SMTP email, written to the SysLog file, or any combination of the three. A check mark (✓) indicates that notification of the event is enabled for the method specified in the column heading; an empty box indicates that notification is not enabled.

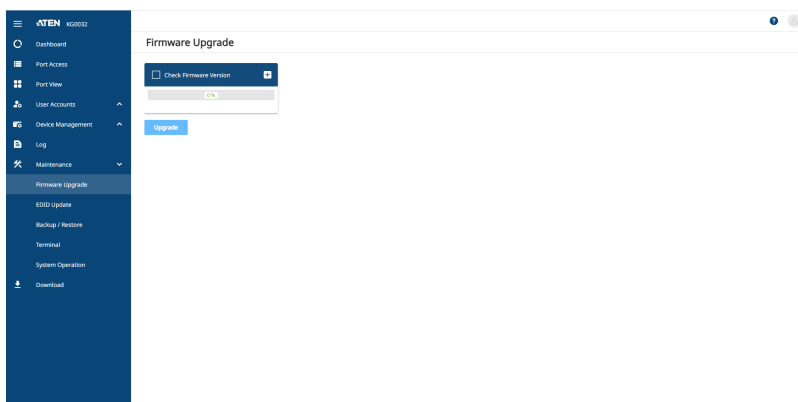
This Page Intentionally Left Blank

Chapter 11

Maintenance

Overview

The *Maintenance* function is used to upgrade firmware; backup and restore configuration and account information; send terminal commands, ping network devices; and restore default values.

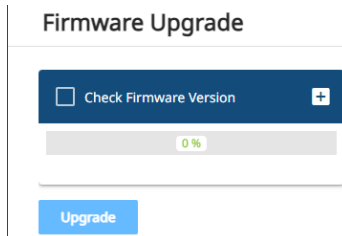


Firmware Upgrade

As new versions of the firmware become available, they can be downloaded from our website. Check the website regularly to find the latest information and packages.

To upgrade the main firmware, do the following:

1. Download the new firmware file (KVM over IP OmniBus Gateway), to your computer.
2. Log in to the KVM over IP OmniBus Gateway; and click the *Maintenance* tab. The Maintenance tab opens to the *Upgrade Firmware* page:



3. Click **+**; navigate to the directory that the new firmware file is in and select the file.
4. Click **Upgrade** to start the upgrade procedure.
 - ◆ If you enabled *Check Firmware Version* the current firmware level is compared with that of the upgrade file. If the current version is equal to or higher than the upgrade version, a popup message appears, to inform you of the situation and stops the upgrade procedure.
 - ◆ If you didn't enable *Check Firmware Version*, the upgrade file is installed without checking what its level is.
 - ◆ As the upgrade proceeds, progress information is shown in the *Progress* bar.
 - ◆ Once the upgrade completes successfully, the KVM over IP OmniBus Gateway resets itself.
5. Log in again, and check the firmware version to be sure it is the new one.

Note:

- ◆ To recover from a “failed upgrade” situation, see *Firmware Upgrade Recovery*, page 159.
 - ◆ The KVM DigiProcessor automatically upgrades its firmware, please do not shut down the KVM over IP OmniBus Gateway or remove the KVM DigiProcessors.
-

Firmware Upgrade Recovery

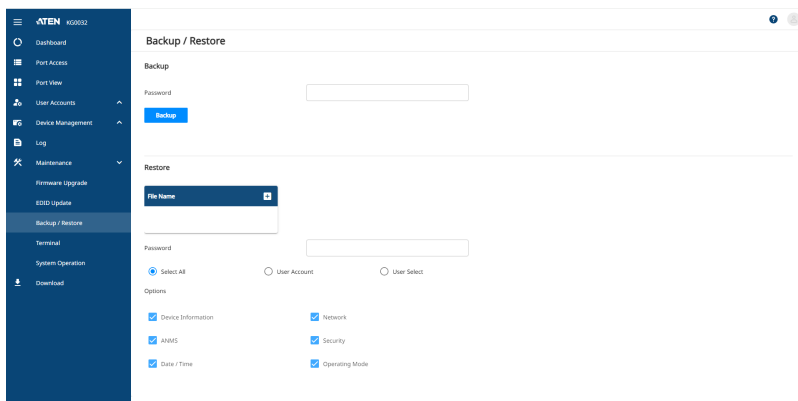
Should the device's main firmware upgrade procedure fail, and the device becomes unusable, the following firmware upgrade recovery procedure will resolve the problem:

1. Power off the device.
2. Press and hold the reset button in (see *reset button*, page 10).
3. While holding the reset button in, power the device back on.

This causes the device to use the original factory installed main firmware version. Once the KVM over IP OmniBus Gateway is operational, you can try upgrading the main firmware again by logging on to the KVM over IP OmniBus Gateway via web browser (see *Firmware Upgrade*, page 158).

Backup / Restore

Selecting the Backup / Restore menu item gives you the ability to back up the KVM over IP OmniBus Gateway's configuration and user profile information:



Backup

To backup the device's settings do the following:

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


Note: 1. Setting a password is optional. If you do not set one, the file can be restored without specifying a password.

2. If you do set a password, make a note of it, since you will need it to be able to restore 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.

Restore

To restore a previous backup, do the following:

1. Click ; navigate to the file and select it.

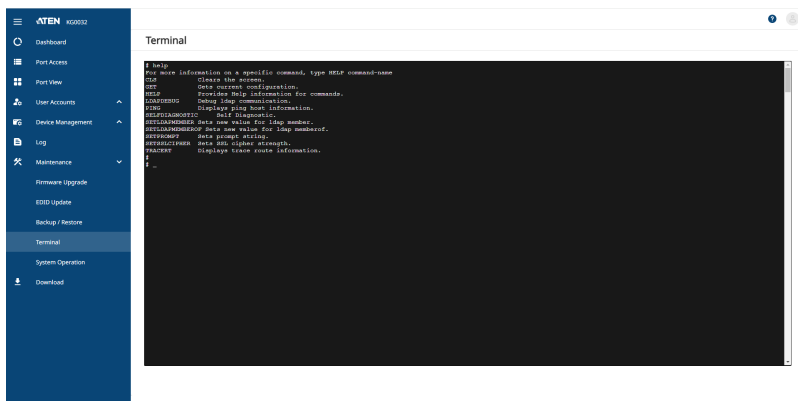
Note: If you renamed the file, you can leave the new name. There is no need to return it to its original name.

2. If you set a password when you created the file, key it in the *Password* field.
3. Select as many of the options that are presented as you wish to restore.
4. Click **Restore**.

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

Terminal

Terminal provides a command line to execute options using a terminal interface. Type a command in the window and hit [Enter] to execute it.

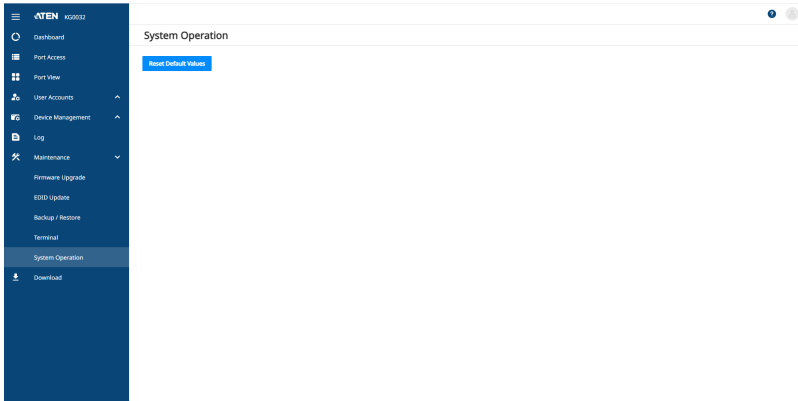


Available commands include:

- ◆ CLS => Clears the screen.
- ◆ GET => Gets current configuration.
- ◆ HELP => Provides Help information for commands.
- ◆ LDAPDEBUG => Debugs ldap communication.
- ◆ PING => Displays ping host information.
- ◆ SELFDIAGNOSTIC => Self diagnostic.
- ◆ SETLDAPMEMBER => Sets new value for ldap member.
- ◆ SETLDAPMEMBEROF => Sets new value for ldap memberof.
- ◆ SETPROMPT => Sets prompt string.
- ◆ SETSSLCIPHER => Sets SSL cipher strength.
- ◆ TRACERT => Displays trace route information.

System Operation

The System Operation page lets you restore certain configuration changes that were made to the KVM over IP OmniBus Gateway back to their original factory default values.



Restore Default Values:

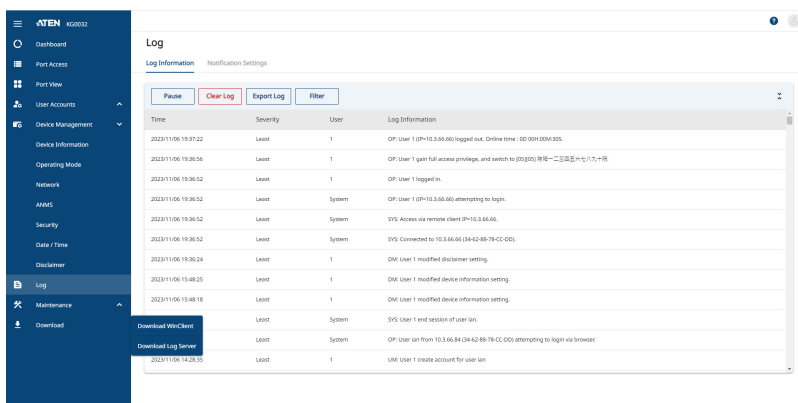
Clicking this button undoes all Customization page changes that have been made to the KVM over IP OmniBus Gateway (except for the Port Names), as well as the Network Transfer Rate (on the Network page), and returns the parameters to the original factory default settings.

Chapter 12

Download

Overview

Download is used to download stand-alone AP versions of the Windows Client and the Log Server:



Click the program you want to download; save it to a convenient location on your hard disk, and run it from there.

This Page Intentionally Left Blank

Chapter 13

The Log Server

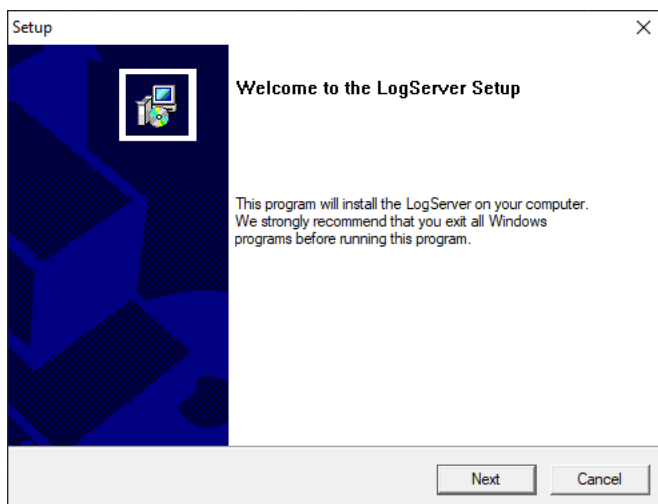
The Windows-based Log Server is an administrative utility that records all the events that take place on selected KVM over IP OmniBus Gateway and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

1. Log into the KVM over IP OmniBus Gateway (see page 27).
2. Click the *Download* tab and download the Log Server AP program.
3. Go to the location on your hard disk that you downloaded the Log Server program to, and double click its icon (*LogSetup.exe*) to bring up the **Setup** screen.

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

The Log Server installation screen appears:



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

Starting Up

To start 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 131.
2. The Log Server requires the Microsoft Jet OLEDB 4.0 driver. See *The Log Server program does not run.*, page 192 if the program doesn't start.
-

The screen is divided into three components:

- ♦ A *Menu Bar* at the top
- ♦ A panel that will contain a list of KVM over IP OmniBus Gateway in the middle (see *The Log Server Main Screen*, page 173).
- ♦ 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 List window to enable it.

Configure

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

- ◆ To add a unit to the list, click **Add**.
- ◆ To edit or delete a listed unit, first select the target in the List window, then open this menu and click **Edit** or **Delete**.

When you choose *Add* or *Edit*, a pop-up window similar to the one below appears:

The screenshot shows a dialog box titled "Add a Server" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Address:** A text box containing "Server Address".
- Port:** A text box containing "9001".
- Description:** A text box containing "Server Description".
- Limit:** A text box containing "100" followed by the label "Days".
- Enable automatic export for every:** A checkbox that is currently unchecked, followed by a text box containing "1" and the label "Days".
- Save to:** A text box with a "Browse..." button to its right.
- 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 KVM over IP OmniBus Gateway is running on, or its DNS name.
Port	The port number that was assigned to the Log Server under <i>Device Management</i> (see <i>Log Server</i> , page 131).
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. Events that exceed the amount of time specified here can be removed with the Maintenance function (see <i>Maintenance.</i> , page 171).
Enable Automatic Export for every / Save to	Check the box and enter the number of days to pass before the system auto exports a log file. Click Browse to select the directory location where the log file will export to.

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

Events

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

Search:

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

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

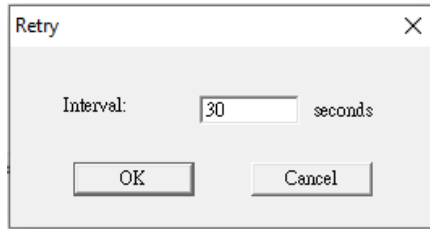
Item	Description
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected unit.
Search last results	This is a secondary search performed on the events that resulted from the previous search.
Search excluding last results	This is a secondary search performed on all the events in the database for the selected unit excluding the events that resulted from the previous search.
Server List	KVM over IP OmniBus Gateway 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	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: 2023/11/04
Start Time	Select the time that you want the search to start from. The format follows the HH:MM:SS convention.
End Date	Select the date that you want the search to end at.
End Time	Select the time that you want the search to end at.
Pattern	Key in the pattern that you are searching for here. The multiple character wildcard (%) is supported. E.g., h%ds would match hands and hoods.
Results	Lists the events that contained matches for the search.
Search	Click this button to start the search.
Print	Click this button to print the search results.
Export	Click this button to save the search results to file.
Exit	Click this button to exit the Log Server.

Maintenance:

This function allows the administrator to perform manual maintenance of the database, such as erasing specified records before their expiration time is up.

Options

Network Retry allows you to set the number of seconds that the Log Server should wait before attempting to connect if its 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 set up, 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 all of the units that have been selected for the Log Server to track (see *Configure*, page 169).
- ◆ The lower (Event) panel displays the tick information for the currently selected unit. (If there are more than one unit, the selected unit is the one that is highlighted).
- ◆ To select a unit in the list, simply click on it.

The List Panel

The List panel contains six fields:

Field	Explanation
ID / State	Shows the ID number of the device and determines whether the Log Server records the ticks for this unit, or not. If the ID checkbox is checked, the State field displays <i>Recording</i> , and the ticks are recorded. If the ID checkbox is not checked, the State field displays <i>Paused</i> , and the ticks are not recorded. Note: Even though a unit is not the currently selected one, if its Recording checkbox is checked, the Log Server will still record its ticks.
Address	This is the IP Address or DNS name that was given to the unit when it was added to the Log Server (see <i>Configure</i> , page 169).
Port	This is the Access Port number assigned to the unit (see <i>Configure</i> , page 169).
Connection	<ul style="list-style-type: none"> ◆ If the Log Server is connected to the unit, this field displays <i>Connected</i>. ◆ If the Log Server is not connected, this field displays <i>Waiting</i>. This means that the Log Server's MAC address has not been set properly. It needs to be set on the <i>Device Management Date / Time</i> page (see page 148).
Days	This field displays the number of days that the unit's log events are to be kept in the Log Server's database before expiration (see <i>Configure</i> , page 169).
Description	This field displays the descriptive information given for the unit when it was added to the Log Server (see <i>Configure</i> , page 169).

The Event Panel

The lower panel displays log events for the currently selected unit. Note that if there are more than one units, even though they aren't currently selected, if their *Recording* checkbox is checked, the Log Server records their log events and keeps them in its database.

Safety Instructions

General

- ◆ This product is for indoor use only.
- ◆ Read all of these instructions. Save them for future reference.
- ◆ Follow all warnings and instructions marked on the device.
- ◆ Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- ◆ Do not use the device near water.
- ◆ Do not place the device near, or over, radiators or heat registers.
- ◆ The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- ◆ The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- ◆ Never spill liquid of any kind on the device.
- ◆ Avoid circuit overloads. Before connecting equipment to a circuit, know the power supply's limit and never exceed it. Always review the electrical specifications of a circuit to ensure that you are not creating a dangerous condition or that one doesn't already exist. Circuit overloads can cause a fire and destroy equipment.
- ◆ Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- ◆ The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- ◆ To prevent damage to your installation it is important that all devices are properly grounded.
- ◆ The device is designed for IT power distribution systems with 230V phase-to-phase voltage.
- ◆ 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.
 - ◆ Additional protection to secure and fix the equipment is needed if the equipment is installed by stacking; by locking it to the rack, screwing it to the frame, or other similar methods.
 - ◆ Keep the Cat 5e/6 cable as far away as possible from potential sources of EMI, such as electrical cables, transformers, and light fixtures. Do not tie the cables to electrical conduits or lay the cables on electrical fixtures.

Rack Mount

- ◆ 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.
- ♦ 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.
- ♦ Débranchez l'unité de la prise murale avant de la nettoyer. N'utilisez pas de produits de nettoyage liquide ou sous forme d'aérosol. Utilisez un chiffon humide pour le nettoyage de l'unité.
- ♦ L'appareil doit être alimenté par le type de source indiqué sur l'étiquette. Si vous n'êtes pas sûr du type d'alimentation disponible, consultez votre revendeur ou le fournisseur local d'électricité.
- ♦ Afin de ne pas endommager votre installation, vérifiez que tous les périphériques sont correctement mis à la terre.

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

- ♦ N'essayez pas de réparer l'unité vous-même. Confiez toute opération de réparation à du personnel qualifié.
- ♦ Si les conditions suivantes se produisent, débranchez l'unité de la prise murale et amenez-la à un technicien qualifié pour la faire réparer:
 - ♦ Le cordon d'alimentation ou la fiche ont été endommagés ou éraillés.
 - ♦ Du liquide a été renversé dans l'unité.
 - ♦ L'unité a été exposée à la pluie ou à l'eau.
 - ♦ L'unité est tombée ou le boîtier a été endommagé.
 - ♦ Les performances de l'unité sont visiblement altérées, ce qui indique la nécessité d'une réparation.
 - ♦ L'unité ne fonctionne pas normalement bien que les instructions d'utilisation soient respectées.
- ♦ N'utilisez que les commandes qui sont abordées dans le mode d'emploi. Le réglage incorrect d'autres commandes peut être à l'origine de dommages qui nécessiteront beaucoup de travail pour qu'un technicien qualifié puisse réparer l'unité.
- ♦ Tenez le câble de catégorie 5e/6 le plus éloigné possible des sources potentielles d'interférences électromagnétiques, telles que les câbles électriques, transformateurs et appareils d'éclairage. Ne nouez pas les câbles à des conduits électriques et ne les faites pas passer sur des installations électriques.

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.

Specifications

KG0016 / KG0032

Function		KG0016	KG0032
Console Connections	Local	N/A	N/A
	Remote	16	32
Computer Connections	Direct	16	32
Port Selection		GUI	
Connectors	USB Port	2 x USB Type A Female (Reserved for future expansion)	
	KVM Port	16 x RJ-45 Female	32 x RJ-45 Female
	SFP+ Uplink Ports	2 x SFP+ Slots	
	Serial	2 x RJ-45 Female (Reserved for future expansion)	
	Power	2 x IEC 60320/C14	
	Input	2 x 2-pin DI (Reserved for future expansion)	
	Relay	2 x 3-pin Relay (Reserved for future expansion)	
Switches	Reset	1 x Semi-recessed Pushbutton	
	Power	2 x Rocker Switches	
LEDs	KVM Ports	16 (Green)	32 (Green)
	Power	2 (Green)	
Panel Spec	Size	1.6"	
	Resolution	128 x 64	
Pushbuttons	Select	3 x Pushbuttons (Up, Down, Enter)	
Emulation	Keyboard / Mouse	USB	
Video	Remote	1920 x 1200 @ 60 Hz	
Maximum Input Power Rating		100 – 240 V~, 2.5A max, 50 – 60 Hz	
Power Consumption		AC110V:34.1W:117BTU AC220V:34.6W:118BTU	AC110V:46.8W:160BTU AC220V:46.9W:160BTU
Environment	Operating Temp.	0 – 40 °C	
	Storage Temp.	–20 – 60 °C	
	Humidity	0–80% RH, Non-condensing	

Function		KG0016	KG0032
Physical Properties	Housing	Metal	
	Weight	6.43 kg (14.16 lb)	6.53 kg (14.38 lb)
	Dimensions L x W x H	43.36 x 37.90 x 4.40 cm (17.07 x 14.92 x 1.73 in)	

Troubleshooting

General Operation

Problem	Resolution
I am confused about which equipment the terms <i>Local</i> and <i>Remote</i> refer to.	See <i>Terminology</i> , page xvi for details
Erratic Operation	Press and release the <i>Reset</i> switch (see <i>reset button</i> , page 10).
I have been given an account but I am unable to log in.	<ol style="list-style-type: none"> 1. Make sure that you have correctly specified your Username and Password. 2. Make sure that the administrator has given you the necessary permission to access the KVM over IP OmniBus Gateway.
I can't access the device, even though I have specified the IP address and port number correctly.	If the device 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 195, for details.
When logging in from a browser, the following message appears: <i>404 Object Not Found</i> .	If a login string has been set, make sure to include the forward slash and correct login string when you specify the KVM over IP OmniBus Gateway IP address. (See <i>Login String</i> , page 141.)
Sudden loss of network connection.	Close your connection to the KVM over IP OmniBus Gateway. Wait approximately 30 seconds, and log in again.
No remote server video display on the client computer.	<p>Check that your KVM DigiProcessors's firmware version is the same as the version stored in the device's Main firmware.</p> <p>Set the remote server resolution to 1280 x 1024 or less.</p>
The display on the client computer is distorted.	<p>Switch ports to a port with a different resolution, then switch back.</p> <p>If the above didn't resolve the problem, change the resolution and refresh rate for the system running on the port. Afterward, you can either run at the new resolution, or switch back to the original resolution.</p>
The Lock Key LEDs on the Control Panel don't accurately reflect the actual locked status of my keyboard input.	When you first connect, the LED display may not accurately reflect the LEDs on your keyboard. To resolve the problem, click the LEDs on the Control Panel until they match your keyboard. Afterward, when you change them from the keyboard they will change on the Control Panel.

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.	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 201, for details.
In multiuser operation I had exclusive (or occupy) rights on the port I was viewing. After I recalled the Port Access page and then came back to the port I was occupying, it had been taken over by another user. Why did this happen?	If you try to return to the port by selecting again in the tree, the KVM over IP OmniBus Gateway acts as if you are accessing the port for the first time. If another user was waiting on the port, he takes precedence and gets the port. The correct way to return to the port is to click the <i>Close</i> icon at the top right of the Port Access page
My ATEN over IP unit is not listed in the Device List of IP Installer.	<ul style="list-style-type: none">◆ Make sure the Broadcast function is enabled from your KVM over IP OmniBus Gateway or router in order for the auto-discover to work properly.◆ Make sure to turn off your firewall and/or antivirus software temporarily in order for the auto-discover to work properly.◆ Make sure the ATEN over IP unit and the PC are under the same network segment.

Mouse Problems

Problem	Resolution
Mouse and/or Keyboard not responding.	<p>Check that your KVM DigiProcessors Cable's firmware version is the same as the version stored in the KVM over IP OmniBus Gateway's Main firmware.</p> <p>Unplug the cable(s) from the console port(s), then plug it/ them back in.</p>
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 51) so that less video data is transmitted.
There are two mouse pointers after the remote server is accessed.	You can select another pointer type. See <i>Mouse Pointer Type</i> , page 57 for details
When the mouse pointer is in Single Pointer mode, I can't access the Control Panel.	Recall the Control Panel and immediately change the pointer to Dual mode.
Why is there a Dual Pointer mode?	When you are not in Mouse DynaSync Mode, you need the two pointers so that you know the remote server pointer is actually at the location you think it is at. Otherwise, you might perform a mouse operation and because of net lag the remote server pointer may not be at the location that your client computer pointer is at.
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 <i>Toggle Mouse Display</i> , page 61, and <i>Mouse Pointer Type</i> , page 57.
When I log in with my Windows system, the local and remote mouse pointers do not sync.	<ol style="list-style-type: none"> 1. Check the status of the <i>Mouse Sync Mode</i> setting (see <i>Mouse DynaSync Mode</i>, page 55). If it is set to <i>Automatic</i>, change the setting to <i>Manual</i> and refer to the information for <i>Manual Mouse Synchronization</i> on page 82. 2. If you are in Manual mode, use the <i>AutoSync</i> feature (see <i>Video Settings</i>, page 51), to sync the local and remote monitors. 3. If that doesn't resolve the problem, use the <i>Adjust Mouse</i> feature (see <i>Adjust Mouse</i>, page 61) 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 198, for further steps to take.

Problem	Resolution
When I log in with my Mac system, the local and remote mouse pointers do not sync.	There are two automatic Mouse DynaSync settings: the default, and Mac2. If mouse synchronization is not satisfactory with the default, try the Mac 2 setting. See the Note on page 82 for details.
When I log in with my Sun system, the local and remote mouse pointers do not sync	Automatic Mouse DynaSync sync only supports USB mice on Windows and Mac (G4 or higher) systems. You must sync the pointers manually. See <i>Mouse DynaSync Mode</i> , page 55, and <i>Manual Mouse Synchronization</i> , page 82, for further details. After doing the above, refer to <i>Sun / Linux</i> , page 199, under <i>Additional Mouse Synchronization Procedures</i> for further steps to take.
When I log in with my Linux system, the local and remote mouse pointers do not sync.	Automatic Mouse DynaSync sync only supports USB mice on Windows and Mac (G4 or higher) systems. You must sync the pointers manually. See <i>Mouse DynaSync Mode</i> , page 55, <i>Manual Mouse Synchronization</i> , page 82, and <i>Mac and Linux Considerations</i> , page 82, for further details. After doing the above, refer to <i>Sun / Linux</i> , page 199, (under <i>Additional Mouse Synchronization Procedures</i>), for further steps to take.

Virtual Media

Problem	Resolution
Virtual Media doesn't work.	The remote server's mainboard does not support USB. If there is a newer firmware and BIOS version for the remote server's mainboard – one that supports USB – get it from the manufacturer and upgrade the server's mainboard firmware and BIOS.
There is no Virtual Media icon on my Control Panel.	You must have Administrator privileges on your client computer. This is a Windows limitation.
I can't boot my remote server from my Virtual Media drive.	Your remote server's BIOS doesn't support booting from a USB drive. Get the latest firmware and BIOS version for your mainboard from the manufacturer and upgrade your mainboard BIOS.
If I connect a USB floppy drive to a remote server, it can boot the remote server. But, if I map it to the remote server as a Virtual Media drive, it cannot boot the remote server.	USB floppy drives have two types of format: UFI and CBI. Both can be used for OS level virtual media functions, but currently only UFI is supported for BIOS level (such as boot) functions.
I cannot mount a Folder as a Virtual Media device.	If the actual Folder is formatted with the FAT16 file system, it cannot be mounted if its size exceeds 2GB.

Web Browser

Problem	Resolution
After upgrading the firmware, after logging in with my web browser, the KVM over IP OmniBus Gateway appears to still be using the old firmware version.	<p>The device is using the new firmware version but the browser is displaying a page that is stored in its cache. Simply log out and clear your browser's cache.</p> <ul style="list-style-type: none"> ◆ IE: Tools → Internet Options → Temporary Internet Files → Delete Files ◆ Firefox: Tools → Clear Private Data

The WinClient AP

Problem	Resolution
My KVM over IP OmniBus Gateway units don't show up in the <i>Server List</i> window when I start the WinClient AP program.	Only units whose Access Port settings for <i>Program</i> (see page 126) match the number specified for <i>Port</i> in the Server area of this dialog box appear in the Server List window. Make sure that your entry for Port matches the entry you have specified for Program on the Device Management <i>Network</i> page.
The WinClient AP won't connect to the KVM over IP OmniBus Gateway.	DirectX 8.0 or higher must be installed on your client computer.
A "Login Failed" error appears and Windows Client Viewer cannot be run.	<ol style="list-style-type: none"> 1. Make sure your KVM over IP OmniBus Gateway is updated to the latest firmware version. 2. Make sure the required service ports, such as 80, 443, and 9000, are allowed by your Firewall. See <i>Service Ports</i>, page 126 for details. 3. Close the viewer and try again.
After upgrading the firmware, the WinClient AP do not run.	The old version of your .ocx file was not deleted. You must delete the old file. There are two methods to delete the file. For the WinClient AP: Open Explorer and search for WinClient.ocx. Delete all occurrences.

Sun Systems

Problem	Resolution
Video display problems with HDB15 interface systems (e.g. Sun Blade 1000 servers).*	<p>The display resolution should be set to 1024 x 768 @ 60Hz:</p> <p>Under Text Mode:</p> <p>Go to OK mode and issue the following commands:</p> <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> 2. Log out 3. Log in

Problem	Resolution
Video display problems with 13W3 interface systems (e.g. Sun Ultra servers).*	<p>The display resolution should be set to 1024 x 768 @ 60Hz:</p> <p>Under Text Mode:</p> <p>Go to OK mode and issue the following commands:</p> <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>fbconfig -res 1024x768x60</pre> 2. Log out 3. Log in

* 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
When I log in to the KVM over IP OmniBus Gateway with my Safari browser, it hangs when I use the Snapshot feature.	<p>Force close Safari, then reopen it. Don't use the Snapshot feature in the future.</p> <p>To use the Snapshot feature with Safari, upgrade to Mac OS 10.4.11 and Safari 3.0.4.</p>

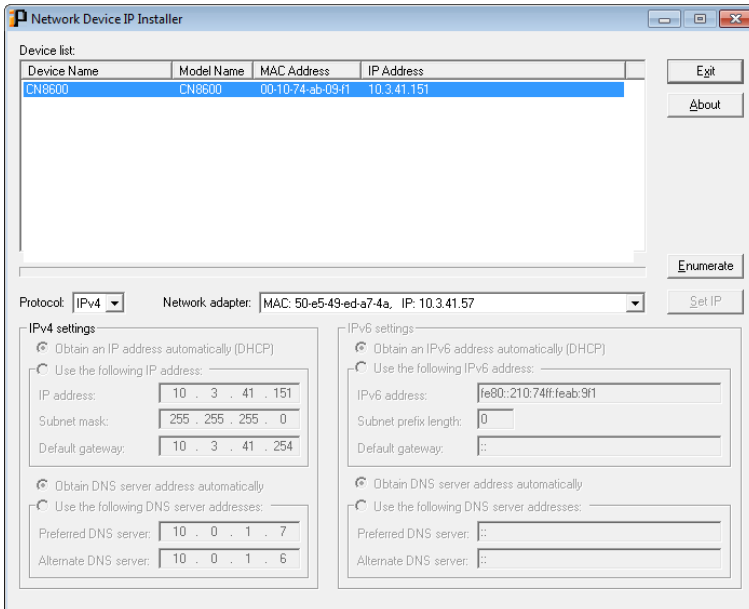
IP Address Determination

If you are an administrator logging in for the first time, you need to access the KVM over IP OmniBus Gateway in order to give it an IP address that users can connect to. There are three methods to choose from. In each case, your client computer must be on the same network segment as the KVM over IP OmniBus Gateway. After you have connected and logged in you can give the KVM over IP OmniBus Gateway its fixed network address. (See *Network*, page 126.)

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 *Download* area of our website. Look under *Driver/SW*, and the model of your KVM over IP OmniBus Gateway. 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:



3. Select the KVM over IP OmniBus Gateway in the *Device List*.

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

2. If there is more than one device in the list, use the MAC address to pick the one you want. The KVM over IP OmniBus Gateway MAC address is located on its bottom panel.
-

4. Use the drop-down menu to select the **Protocol** (IPv4 or IPv6) and then configure the IP settings below.
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. Select either *Obtain DNS server address automatically*, or *Use the following DNS server addresses*. If you chose the latter, fill the Preferred DNS Server and Alternate DNS server with the IP addresses appropriate to your network.
7. Click **Set IP**.
8. After the IP address shows up in the Device List, click **Exit**. See *IP Installer*, page 192 for more information.

Browser

1. Set your client computer's IP address to 192.168.0.XXX
Where XXX represents any number or numbers except 60. (192.168.0.60 is the default address of the KVM over IP OmniBus Gateway.)
2. Specify the KVM over IP OmniBus Gateway'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 KVM over IP OmniBus Gateway that is suitable for the network segment that it resides on.
4. After you log out, reset your client computer's IP address to its original value.

IPv6

At present, the KVM over IP OmniBus Gateway supports three IPv6 address protocols: *Link Local IPv6 Address*, *IPv6 Stateless Autoconfiguration*, and *Stateful Autoconfiguration (DHCPv6)*.

IPv6 Stateless Autoconfiguration

If the KVM over IP OmniBus Gateway network environment contains a device (such as a router) that supports the IPv6 Stateless Autoconfiguration function, the KVM over IP OmniBus Gateway 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 in the *General* list box of the *Device Management* → *Device Information* page (see page 122).

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win 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 *Windows Client AP Login*, page 29).

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 that comes in over a particular port to.









For example, if the KVM over IP OmniBus Gateway 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

Mac Keyboard







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

PC Keyboard	Mac Keyboard
[Shift]	Shift
[Ctrl]	Ctrl
	
[Ctrl] [1]	
[Ctrl] [2]	
[Ctrl] [3]	
[Ctrl] [4]	
[Alt]	Alt
[Print Screen]	F13
[Scroll Lock]	F14
	=
[Enter]	Return
[Backspace]	Delete
[Insert]	Help
[Ctrl] 	F15

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

Sun Keyboard

The PC compatible (101/104 key) keyboard can emulate the functions of the Sun keyboard when the Control key [Ctrl] is used in conjunction with other keys. The corresponding functions are shown in the table below.

PC Keyboard	Sun Keyboard
[Ctrl] [T]	Stop
[Ctrl] [F2]	Again
[Ctrl] [F3]	Props
[Ctrl] [F4]	Undo
[Ctrl] [F5]	Front
[Ctrl] [F6]	Copy
[Ctrl] [F7]	Open
[Ctrl] [F8]	Paste
[Ctrl] [F9]	Find
[Ctrl] [F10]	Cut
[Ctrl] [1]	
[Ctrl] [2]	
[Ctrl] [3]	
[Ctrl] [4]	
[Ctrl] [H]	Help
	Compose
	Meta

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

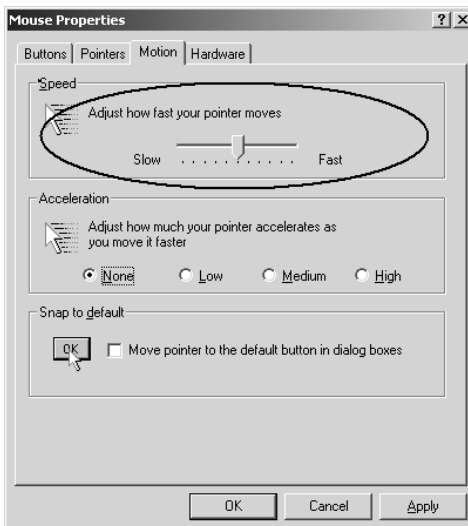
Additional Mouse Synchronization Procedures

If you use Manual Mouse Synchronization, you should perform the following operations on the servers that connect to the device.

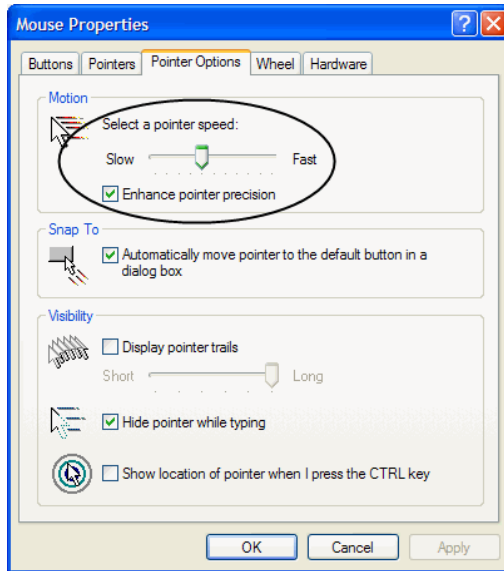
- Note:** 1. These procedures are to be performed on the servers attached to the KVM over IP OmniBus Gateway's ports - not on the client computer you are using to access the KVM over IP OmniBus Gateway.
2. In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the Windows operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

Windows:

1. Windows 2000:
 - a) Open the Mouse Properties dialog box (Control Panel → Mouse → Mouse Properties)
 - b) Click the *Motion* tab
 - c) Set the mouse speed to the middle position (6 units in from the left)
 - d) Set the mouse acceleration to *None*



2. Windows XP / Windows Server 2003:
 - a) Open the Mouse Properties dialog box (Control Panel → Mouse)
 - b) Click the *Pointer Options* tab
 - c) Set the mouse speed to the middle position (6 units in from the left)
 - d) Disable *Enhance Pointer Precision*



3. Windows ME:

Set the mouse speed to the middle position; disable mouse acceleration (click **Advanced** to get the dialog box for this).
4. Windows NT / Windows 98 / Windows 95:

Set the mouse speed to the slowest position.

Sun / Linux

Open a terminal session and issue the following command:

```
Sun: xset m 1
```

```
Linux: xset m 0
```

or

```
xset m 1
```

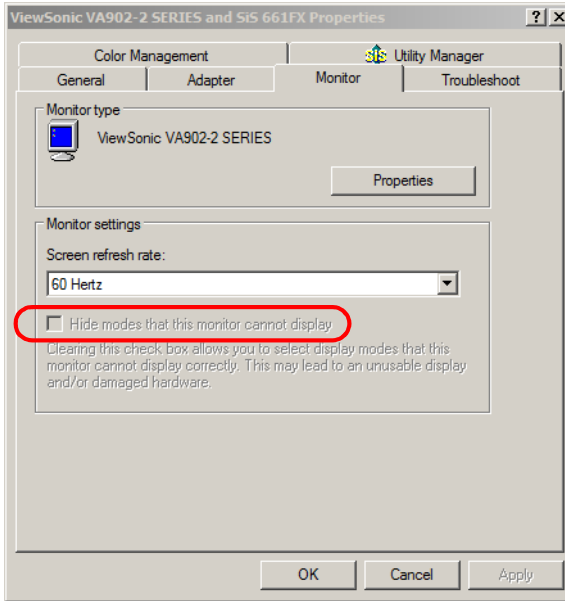
(If one doesn't help, try the other.)

```
Linux using the Redhat AS3.0 mouse mode: xset m 1
```

Additional Video Resolution Procedures

If you are running Windows, and wish to use new refresh rates, do the following:

1. Open Control Panel → Display → Settings → Advanced → Monitor.
2. In the dialog box that comes up, make sure that the *Hide modes that this monitor cannot display* checkbox is unchecked.



3. Click the arrow at the right of the *Screen refresh rate* listbox, and select the refresh rate you want from the list that appears.

Note: Make sure that your monitor supports the refresh rate you choose – if not, you may seriously damage your monitor.

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.



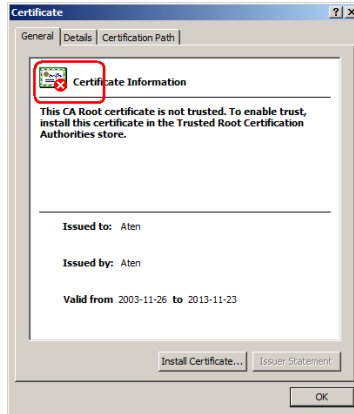
The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

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

Installing the Certificate

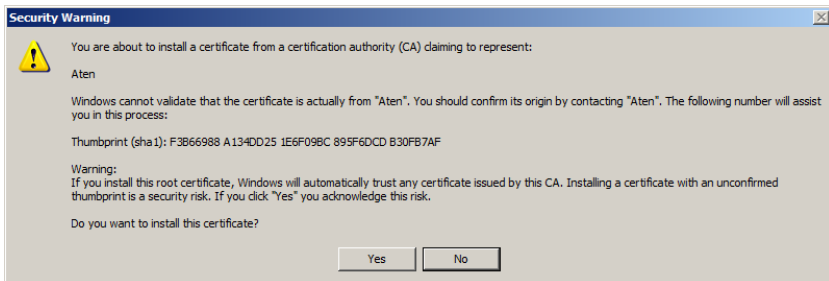
To install the certificate, do the following:

1. 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.

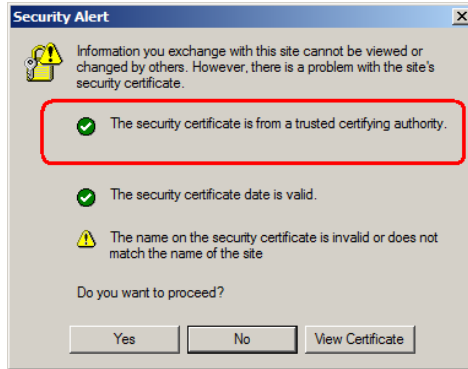
2. Click **Install Certificate**.
3. Follow the Installation Wizard to complete the installation. Unless you have a specific reason to choose otherwise, accept the default options.
4. When the Wizard presents a caution screen, click **Yes**.



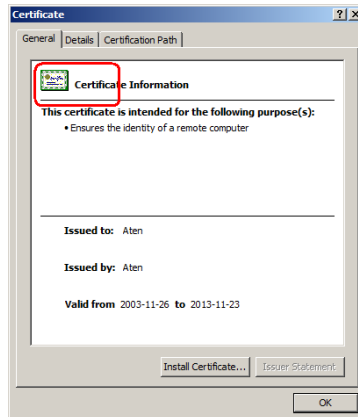
5. Click **Finish** to complete the installation; then click **OK** to close the dialog box.

Certificate Trusted

The certificate is now trusted:

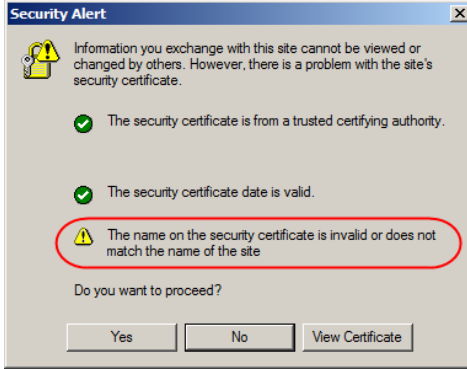


When you click *View Certificate*, you can see that the red and white X logo is no longer present – further indication that the certificate is trusted:



Mismatch Considerations

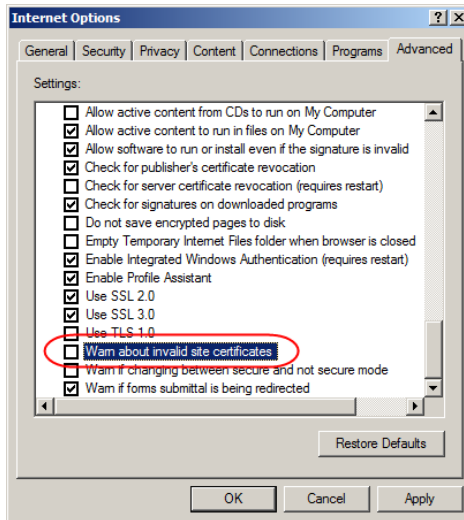
If the site name or IP address used for generating the certificate no longer matches the current address of the KVM over IP OmniBus Gateway a mismatch warning occurs:



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 *Security*, page 138, and *Private Certificate*, page 144).

Factory Default Settings

The default settings are as follows:

Setting	Default
Language	English
GUI Hotkey	[Scroll Lock] [Scroll Lock]
Port ID Display	Port Number + Name
Port ID Display Duration	3 Seconds
Screen Blanker	0 Minutes (disabled)
Beeper	On
Microphone/Speaker	On
Viewer	Auto Detect
Welcome Message	Hide
Accessible Ports	<ul style="list-style-type: none">◆ Super Administrators – Full for all ports◆ All other users – None for all ports.

Virtual Media Support

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
- ◆ Smart Card Readers – Read/Write

* These drives can be mounted either as a Drive or as a Removable Disk (see *Virtual Media*, page 80). Removable disks allow the user to boot 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

ATEN Standard Warranty Policy

Limited Hardware 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](#). For UPS products, the device warranty is two [2] years but battery is one [1] year. 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/>

© Copyright 2023 ATEN® International Co., Ltd.
Released: 2023-12-26

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