



*Digi Passport
I-KVM*

User's Guide

©Digi International Inc. 2009. All Rights Reserved.

The Digi logo and Passport are registered trademarks of Digi International, Inc.

All other trademarks mentioned in this document are the property of their respective owners.

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International.

Digi provides this document “as is,” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

This product could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes may be incorporated in new editions of the publication.

Notice to Users

Proper back-up systems and necessary safety devices should be utilized to protect against injury, death or property damage due to system failure. Such protection is the responsibility of the user.

This device is not approved for use as a life-support or medical system.

Any changes or modifications made to this device without the explicit approval or consent of Sena Technologies will void Sena Technologies of any liability or responsibility of injury or loss caused by any malfunction.

This equipment is for indoor use and all the communication wirings are limited to inside of the building.

Table of Contents

Notice to Users.....	2
Table of Contents	3
Digi contact information	5
Product Overview	7
Product Specifications	8
Getting started.....	11
Panel layout.....	11
Connecting the hardware	12
Accessing the system console.....	16
Accessing the Web Browser Management Interface	20
Discovering and Configuring the I-KVM unit	22
Locator LEDs.....	23
Network configuration	25
IP Configuration	25
Simple Network Management Protocol (SNMP) Configuration	29
Dynamic DNS configuration	32
SMTP configuration	34
IP filtering	36
SYSLOG server configuration.....	39
Network File System (NFS) server configuration	39
Serial port configuration	41
Serial Port Configuration.....	41
Overview.....	41
About basic and advanced serial port settings	41
Basic port configuration settings	41
Port management	42
Host mode configuration	43
Serial port parameters	44
Port logging.....	46
User access control	48
Alert configuration.....	50
KVM Configuration	53
Connections	57

Serial port connection	59
KVM viewer client	63
Login	63
Viewer screen	70
KVM toolbar icons	73
System status and log	81
System log configuration	82
System administration	83
User administration	83
Authentication	86
Change password	89
Device name configuration	89
Date and time settings	90
Configuration management	90
Security Profile	93
Firmware upgrade	96
System statistics	101
Network interfaces statistics	101
Serial ports statistics	102
IP statistics	102
ICMP Statistics	105
TCP statistics	108
UDP Statistics	111
Guide to the Boot loader program	112
Firmware upgrade menu	112
CLI guide	115
Utilities	116
Important File Locations	116
Config Files	116
Appendix A: Connections	117
Ethernet Pin outs	117
Console and serial port pin-outs	118
Appendix B: Well-known port numbers	119
Appendix C: Hotkey sequence codes	121
Permissible key presses	121
Creating macro sequences	122

Digi contact information

For more information about Digi products, or for customer service and technical support, contact Digi International.

To Contact Digi International by:	Use:
Mail	Digi International 11001 Bren Road East Minnetonka, MN 55343 U.S.A.
World Wide Web:	http://www.digi.com/support/
email	http://www.digi.com/support/
Telephone (U.S.)	(952) 912-3444 or (877) 912-3444
Telephone (other locations)	+1 (952) 912-3444 or (877) 912-3444

Product Overview

C H A P T E R 1

The Passport I-KVM is a secure single-port KVM (keyboard, video and mouse) over IP and 1-port serial console access server for remote host computer access via IP network. The compact form factor and strong security features of Passport I-KVM makes it an ideal remote server management solution for distributed computing environment with small installation space such as Kiosk, ATM, remote branch offices. Also its non-blocked access capability makes it a perfect solution for data center applications that require 24/7 non-blocked access from internal or external network.

The list of the main features I-KVM supports is as below:

- Hybrid server management solution with single-port KVM-over-IP and 1-port serial console access server
- Full BIOS-level access of the remote host via KVM-over-IP
- Non-blocked server access via KVM-over-IP using web browser or widely available VNC viewers on wide range of platforms
- High video performance up to 1600 x 1200 @ 60Hz resolution
- Hardware based AES 128-bit encryption of keyboard, mouse and video data
- Telnet/SSH to the serial port with various management features including user access group, port logging and SNMP/SMTP based event alert feature
- Remote user authentication support: LDAP, Radius, TACACS+, Kerberos
- "Zero U" form factor with locking-type power connector
- Supports server-powered through USB port of the server
- Highly scalable using daisy-chain type Ethernet and power cascading
- Virtual Media support for file transfer to remote servers
- Adaptive video compression algorithm for highly efficient network bandwidth use
- IPv4/IPv6 dual stack

Product Specifications

Hardware interfaces

- Network: 2 x 10/100Base-T Ethernet Ports for uplink and cascading
- Keyboard/Mouse: USB or PS/2
- Video: HDD15 VGA up to 1600x1200@60Hz
- Serial Console:RS-232 up to 115.2 Kbps for Serial Port Redirection and/or Unit Configuration
- Virtual media: USB

Remote server requirements

- PC, MAC, Sun, IBM System P (RS/6000) and DEC Alpha
- HDD15 VGA output up to 1600x1200@60Hz
- PS2 or USB keyboard and mouse interface

Client OS requirements

- Industry standard web browsers with Sun Java 2 Runtime environment
- Platform-independent VNC viewers available for wide range of platforms including Windows 98/2000/2003/XP/Vista, Unix, Linux, Mac OS X, Palm OS*, Windows CE*, iPhone* (* by 3rd party software only).

KVM-over-IP features

- Non-blocked server access up to 4 simultaneous users
- Adaptive video compression algorithm for highly efficient network bandwidth use
- Virtual Media support for file transfer to remote servers
- Private/shared mode switching
- User access privilege support
- International keyboards support: United States, United Kingdom, Japan, Spain, France, Germany, Italy, Netherlands, Belgium, Norway, Sweden, Denmark, and Switzerland.

Serial console features

- Serial port redirection using Telnet/SSH or Raw TCP
- Keyword based event alert using SNMP and/or SMTP
- Local and Remote Port logging using Syslog and/or NFS

Security

- Hardware based AES 128-bit encryption of keyboard, mouse and video data
- Rule based IP address filtering
- Strong security support based on PAM, SSH, HTTPS, RSA, AES encryption
- User/Group management with access control
- Remote user authentication support: LDAP, Radius, TACACS+, Kerberos

Power requirements

- Input: 5 ~ 12VDC
- Power consumption: 5.78 Watt
- Locking type power connector
- Server powered design through USB port of the server
- Optional DC power supply

Regulatory approvals

- FCC
- CE
- UL

Environmental requirements

- Operating Temperature: 0~50 C

Storage Temperature: -20~60 C

- Relative humidity: 0~90% (non-condensing)
- Serial port surge protection (ESD): ±15kV

Physical dimensions

- Width: 2.83 in (7.2 cm)
- Height: 1.26 in (3.2 cm)
- Weight:
 - Passport I-KVM PS2: 9.24 oz (262 g)
 - Passport I-KVM USB: 7.87 oz (223 g)

Getting started

CHAPTER 2

This chapter describes how to set up and configure the I-KVM using the following figures.

- Panel Layout explains the layout of the panel and LED indicators.
- Connecting the Hardware describes how to connect the power, the network, and the equipment to the I-KVM.
- Accessing System Console describes how to access the console port using a serial console or a Telnet or Web menu from remote location.

The following items are required to get started.

- One power cable (included in the package)
- One console/Ethernet cables
- One Video/Mouse (PS/2 or USB) cable (included in the package)

Panel layout

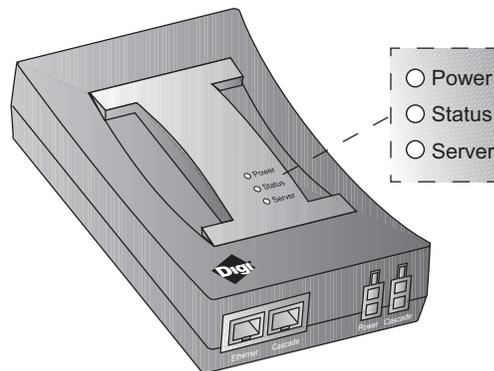


Figure 2-1: Panel layout of the I-KVM

The I-KVM has three LED indicator lamps to display the status, as shown in Figure 2-1 (i.e. Power, Status, Server). The first lamp indicates power, the second lamp indicates server status, and the third lamp indicates server connection.

The front panel shows Ethernet port and power sockets and the rear panel shows the serial ports with RJ45 connector, and the console switch.

Table 2-1: LED indicator lamps of the I-KVM

Lamps	Function
Power	Turned on if power is supplied
Status	Turned on if system is ready to run
Server	Turned on if Host computer video is connected.

Connecting the hardware

This section describes how to connect the I-KVM to the equipment for initial testing.

- Connect a power source to the I-KVM
- Connect the I-KVM to an Ethernet hub or switch
- Connect the host computer

Connecting the power

The I-KVM can be powered from the USB port of the host computer or from a separate DC power supply. To power the I-KVM from the USB port of the host computer, the USB port should be able to supply more than 5.78 Watt (1.2A@5VDC). If the power is properly supplied, the [Power] lamp will light up green. When external DC power supply is used to power the I-KVM unit(s), make sure to use proper Digi parts for safety. To power a single unit, use the external power supply included: part number 76000765 (US), or 76000764 (EU), HON KWANG ELECTRIC CO LTD, HK-R107-A12). To power multiple units up

to 8, use Digi part number 76000766 (US), or 76000767 (EU), (CHANNEL WELL TECHNOLOGY CO LTD, PAA060F). See figure 2-2.

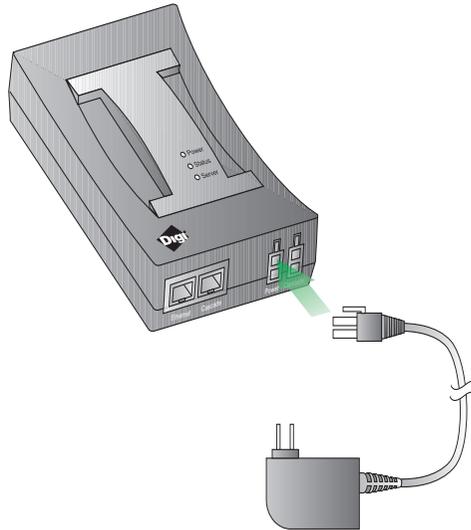


Figure 2-2: Connecting the power to the I-KVM

Connecting to the network

Plug one end of the Ethernet cable to the I-KVM Ethernet port. The other end of the Ethernet cable should be connected to a network port. If the cable is properly connected, the I-KVM will have a valid connection to the Ethernet network. This will be indicated by: the [Link] lamp will light up green. See figure 2-3.

The [Act] lamp will blink to indicate incoming/outgoing Ethernet packets.

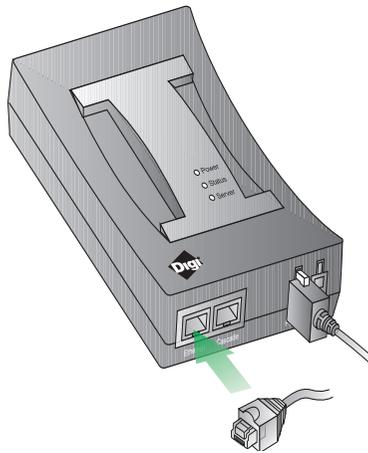


Figure 2-3: Connecting a network cable to the I-KVM

Connecting to the host computer

Connect the Video/Mouse cable to host computer. To connect to the host computer the user needs to consider the type of video and mouse type provided by the device itself. For

more information, see figure 2-4 below and refer the cabling diagram in Appendix A of this document.

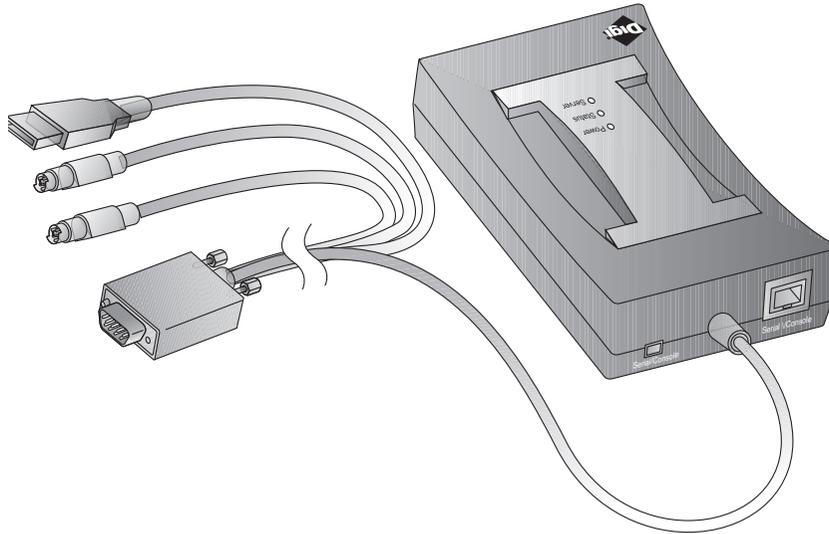


Figure 2-4: Connecting a Video/Mouse cable to host computer

Cascading multiple I-KVM units

The I-KVM supports cascading up to 8 units for power and for the Ethernet so multiple I-KVM units can run from only one power source and one Ethernet port switch. For power cascading, a separate larger capacity power supply should be purchased instead of a regular power supply unit. The power output connector of the power supply should be connected to the power connector of the first I-KVM unit, then one end of the power cascade cable should be connected to the "Cascade" port of the first I-KVM and the other end should be connected to the "Power" connector of the second I-KVM. Connect the same way for the rest of the units. Power cascade cables (76000768) need to be purchased separately.

The Ethernet cable from the external hub/switch should be connected to the "Ethernet" port of the first I-KVM unit. Run additional Ethernet cable from the "Cascade" port of the

first I-KVM unit to the "Ethernet" port of the second I-KVM units. Repeat the same connection until the last unit is connected. See figure 2-5 below.

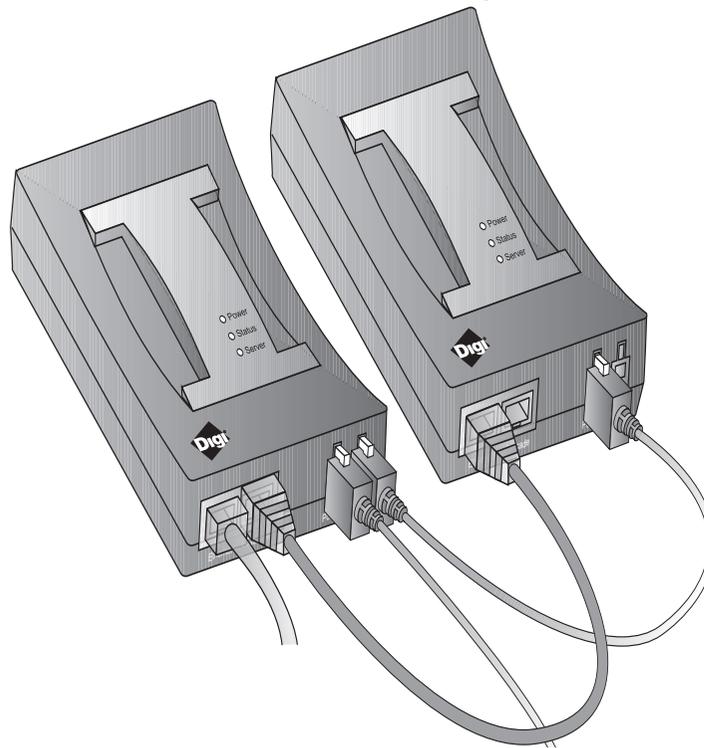


Figure 2-5: Cascading multiple I-KVM units

Accessing the system console

There are several ways to access the I-KVM. These methods are dependent on whether the user is located at a local site or a remote site, or whether s/he requires a menu-driven interface, graphic menu system or CLI (Command Line Interface).

- **System console:** Local users can connect directly to the system console port of the I-KVM using the console/Ethernet cable with the corresponding adapter.
- **Remote console:** Remote users who require a menu-driven interface can utilize Telnet (port 23) or SSH (port 22) connections to the I-KVM using a terminal emulator.

- **Web:** Remote users who want to use a web browser to configure the I-KVM can connect to the I-KVM using conventional web browsers, such as Internet Explorer or Mozilla Firefox.

Note: These methods require the user to be authenticated by the I-KVM system.

Using the system console

- 1 Connect one end of the console/Ethernet cable to the console port on the I-KVM.

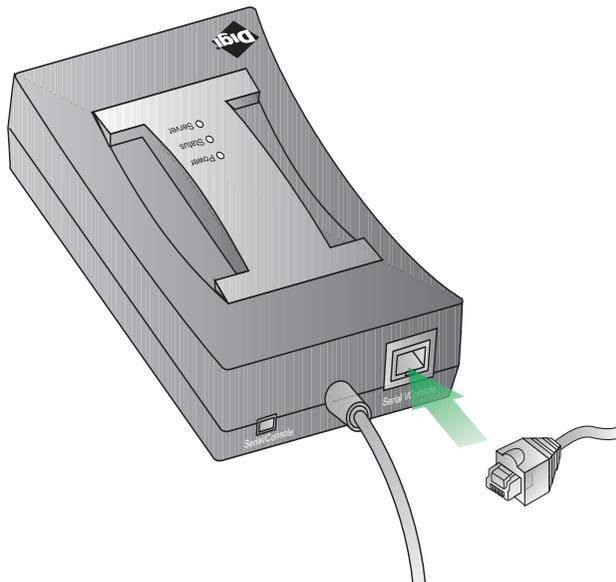


Figure 2-6: *Connecting a system console cable to the I-KVM*

- 2 Connect to the user's computer with the RJ45-DB9 female adapter.
- 3 Connect the other end of the cable to the serial port of the user's computer.
- 4 Run a terminal emulator program (i.e. HyperTerminal). Set up the serial configuration parameters of the terminal emulation program as follows:
 - 9600 Baud rate
 - Data bits 8
 - Parity None
 - Stop bits 1
 - No flow control

- 5 Press the [ENTER] key.
- 6 Enter user name and password to log into the I-KVM. The factory default user settings are as follows.

Login: root	Password: dbps
Login: admin	Password: admin

```
I-KVM login: root
Password:****
root@I-KVM:~#
```

```
192.168.161.5 login: admin
Password:

Welcome to ...
```

- 7 Upon authentication, the corresponding user interface is displayed. Either the text-menu driven interface or the CLI are initially provided for configuration. For more information, refer to the section, “User Administration” within this document.
- 8 If the default interface is set up as text menu, the menu screen below will appear.

```
-----
Welcome to Digi Passport I-KVM configuration menu

Hostname:      I-KVM
Current time:  Fri, 09 Jan 2009 11:33:26 -0600
F/W Rev.:     v1.0.0rc2          Bios Rev.: v0.8.3
MAC addr.:    00:01:95:77:77:02  IP addr.:  10.9.101.30
-----

Select menu:
 1. Network configuration
 2. KVM & Serial port
 3. System status & logs
 4. System administration

[h]elp, [s]ave, [a]pply, e[x]it, [q]uit
COMMAND> █
```

Figure 2-7: Main menu screen

From the main menu screen, the user may select the menu item for the configuration of the I-KVM parameters by typing the menu number and pressing the [ENTER] key. In the submenu screen, users can configure the required parameters guided by online comments.

All the parameters are stored into the non-volatile memory space of the I-KVM, and it will not be stored until users type "s"([s]ave). All the configuration change will be effective after typing "a"([a]pply).

Using remote console

The IP address of the I-KVM must be known before users can access the I-KVM using the remote console. For more information, refer to the Network Configuration section of this document. The default I-KVM IP address is 192.168.161.5.

The remote console access function can be disabled in the remote host access option. For more information, refer to the IP filtering in section of this document. The I-KVM supports both Telnet and SSH protocol for remote consoles.

The following instructions will assist in setting up the Remote Console functionality:

- 1 Run either a Telnet (or SSH) program or a program that supports Telnet (or SSH) functions (i.e. TeraTerm-Pro or HyperTerminal). The target IP address and the port number must match the I-KVM. If required, specify the port number as 23 (or 22). Type the following command in the command line interface of user's computer

```
telnet 192.168.161.5 (or ssh admin@192.168.161.5 )
```

or run a Telnet program with the parameters shown below::

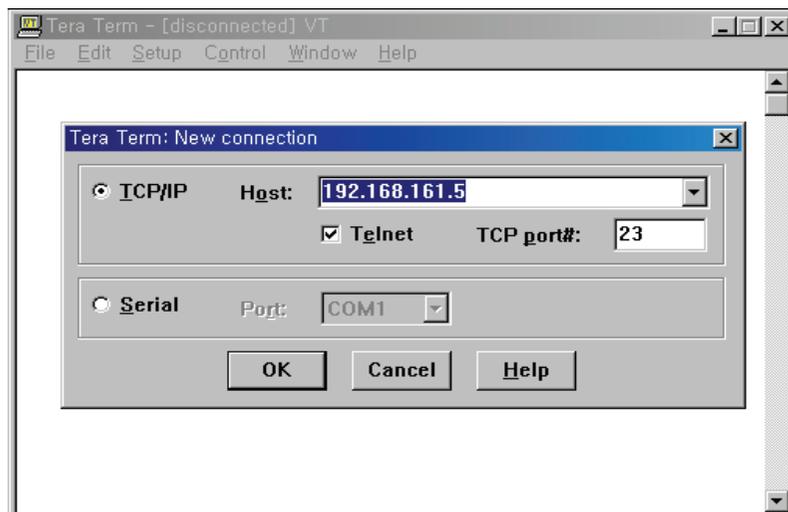


Figure 2-8: Telnet program set up example

- 2 The user must log into the I-KVM. Type the user name and password. A factory default setting of the user name is **root** and password is **dbps** for the system root and **admin** for the system administrator. For more information, refer to the section, “User Administration” within this document.
- 3 Upon authentication by the I-KVM, one of the CLI prompts or text menu screens are shown to the user according to the default shell configuration of the user's account. The menu-driven interface allows the user to select a menu item by typing the menu number and then pressing **[ENTER]**. The corresponding screen allows user configuration of the required parameters. For more information, refer to the section, “CLI guide” within this document.

Accessing the Web Browser Management Interface

The I-KVM supports both HTTP and HTTPS (HTTP over SSL) protocols. The I-KVM also provides its own Web management pages. To access the I-KVM Web management page, enter the I-KVM IP address or resolvable hostname into the web browser's URL/ Location field. This will direct the user to the I-KVM login screen. The user must authenticate themselves by logging into they system with a correct user name and password. The factory default settings are:

Login: root	Password: dbps
Login: admin	Password: admin

Note: Before accessing the I-KVM Web management page, the user must check the I-KVM IP address (or resolvable Hostname) and Subnet mask settings.

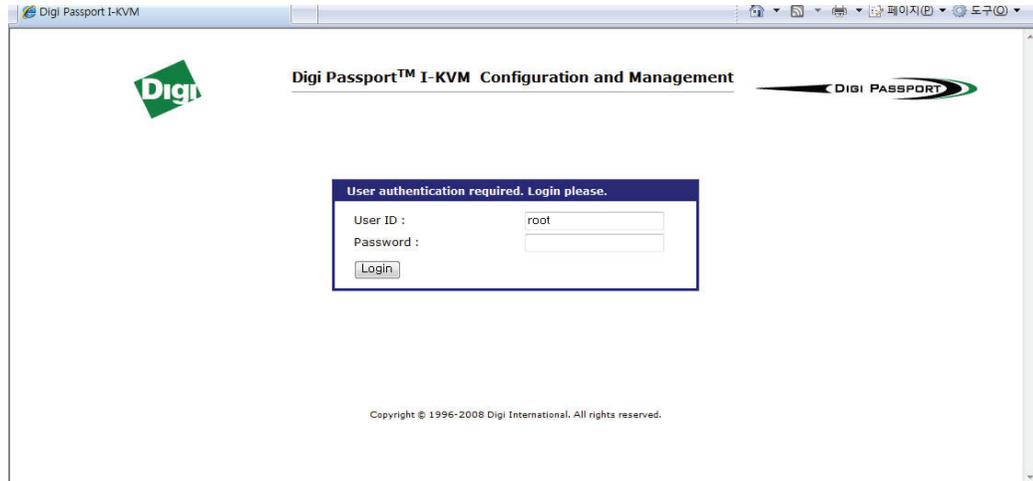


Figure 2-9: Login screen of the I-KVM Web Management

The figure below shows the user homepage of the I-KVM Web management interface. A menu bar is provided on the left side of the screen. The menu bar includes the uppermost configuration menu groups. Selecting an item on the menu bar opens a tree view of all the submenus available under each grouping. Selecting a submenu item will allow the user to modify parameter settings for that item.

Every page will allow the user to **[Save to flash]**, **[Save & apply]** or **[Cancel]** their actions. After changing the configuration parameter values, the users must select **[Save to flash]** to save the changed parameter values to the non-volatile memory.

To apply all changes made, the user must select **[Apply Changes]**. This option is available on the bottom of the menu bar. Only when the user selects **[Apply changes]** will the new parameter values be applied to the I-KVM configuration.

The user also can select **[Save & apply]** to save parameters and apply changes in one step. If the user does not want to save the new parameter values, the user must opt to **[Cancel]**. All changes made will be lost and the previous values restored.

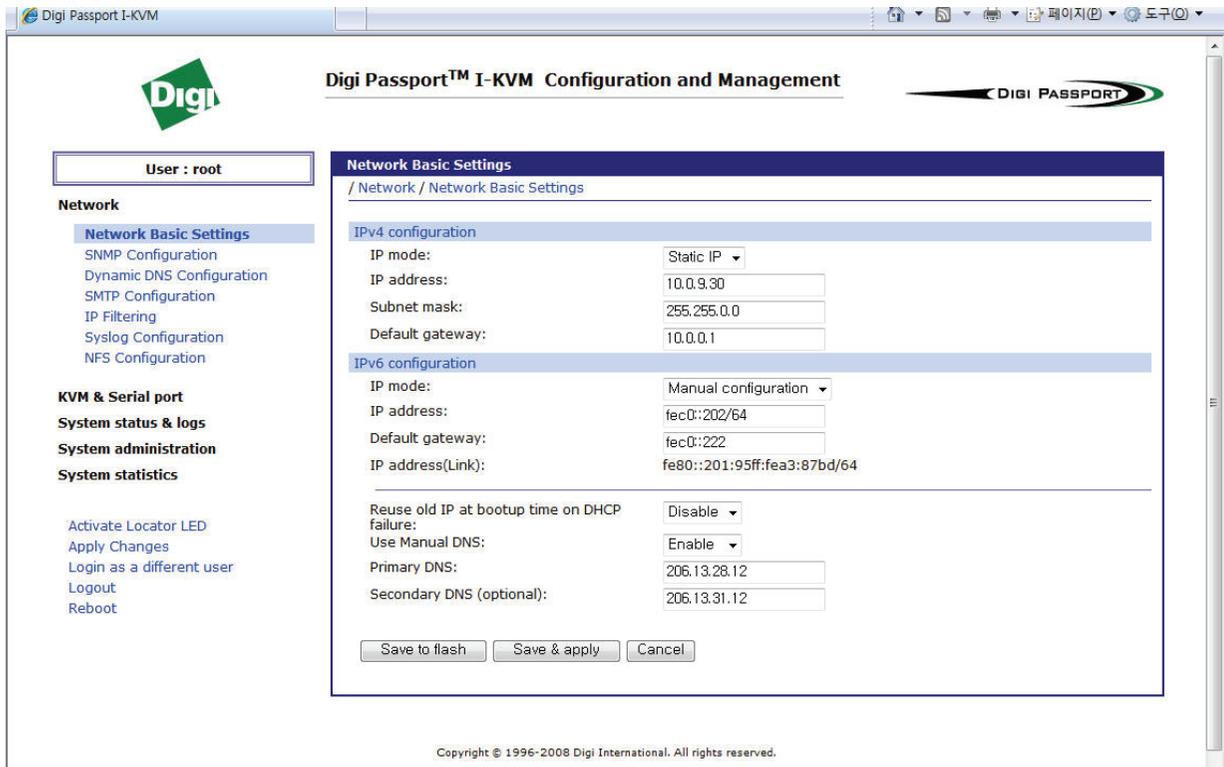


Figure 2-10: The I-KVM web management screen

Discovering and Configuring the I-KVM unit

To discover the I-KVM unit on the network, insert the Software and Documentation CD in your computer's CD drive, and select the Digi Device Discovery program. This program uses the Digi-proprietary Advanced Digi Discovery Protocol (ADDP) to discover all devices on a network. Once discovered, devices can be viewed and configured. Start the program and click the correct device to configure.

The Digi Device Discovery program knows the default password for the I-KVM unit. If the password has been changed from the default, dbps, a prompt for entering the password is displayed. Configure the IP address. Once the Digi Passport is configured with a valid IP address, log in to the Web user interface with username admin, password admin.

Locator LEDs

The I-KVM unit can be physically located easily by using the Locator LED feature. If this feature is enabled, the I-KVM will blink two LEDs labeled Status and Server together so user can recognize which I-KVM unit he or she is accessing currently:

- 1 Enable Locator LEDs
 - Log into the Web interface as admin or root.
 - In the Web interface menu, click Activate Locator LED and the locator LED will blink.
- 2 Turn Off locator LEDs
 - In the Web interface, click Deactivate Locator LED.

Network configuration

CHAPTER 3

IP Configuration

The I-KVM requires a valid IP address (v4/v6) to operate within the user network environment. If the IP address is not readily available, contact the system administrator to obtain a valid IP address for the I-KVM.

Note: The I-KVM requires a unique IP address to connect to the user's network.

The users may choose one of two Internet protocols in setting up the I-KVM IP address:

- Static IP
- DHCP (Dynamic Host Configuration Protocol)

The I-KVM is initially defaulted to Static IP mode, with a static IP address of 192.168.161.5. The table below shows the configuration parameters for all three IP configurations, and the web-based GUI to change the user's IP configuration.

Table 3-1: Configuration parameters

Static IP (v4)	IP address
	Subnet mask
	Default gateway
	Use manual DNS (Enable only) / Primary DNS / Secondary DNS (Optional)
Static IP (v6)	IP address
	Default gateway
	IP address (Link)
	Use manual DNS (Enable only) / Primary DNS / Secondary DNS (Optional)
DHCP	Use manual DNS / Primary DNS / Secondary DNS (Optional)
	Reuse old IP at bootup time on DHCP failure

The users can disconnect the I-KVM from the network by setting **IP mode** as **Disable**. For information on how to enable and configure a secondary address, refer to “Using a static IP address” below.

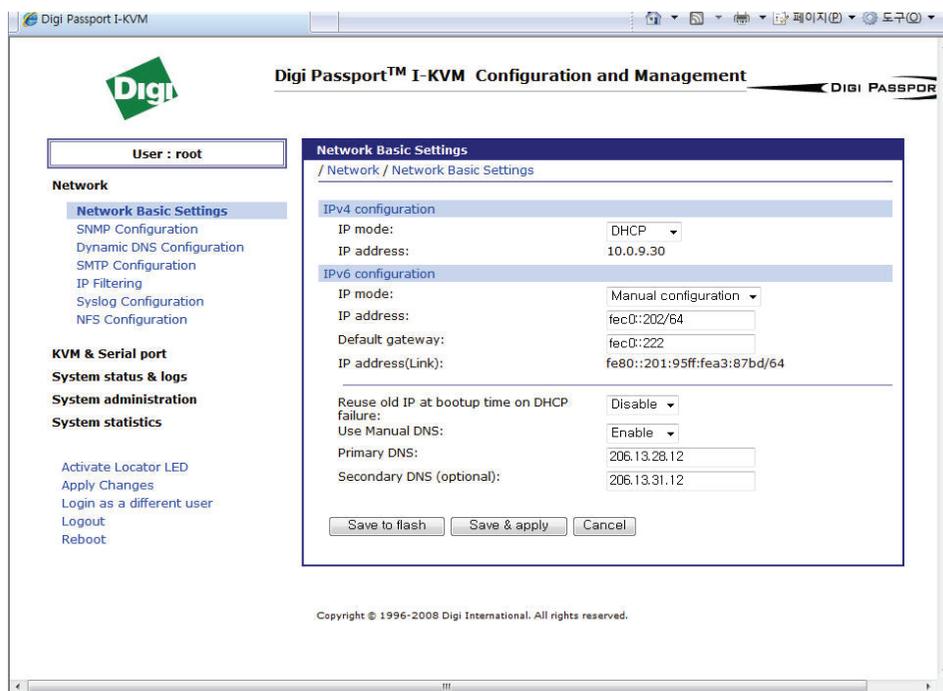


Figure 3-1: IP configuration

Using a static IP address

When using a static IP address, the user must manually specify all the configuration parameters associated with the I-KVM IP address. These include the IP address, the network subnet mask, the gateway computer and the domain name server computers. This section will look at each of these in more detail.

Note: The I-KVM will attempt to locate all this information every time it is turned on.

IP address

A Static IP address acts as a "static" or permanent identification number. This number is assigned to a computer to act as its location address on the network. Computers use these IP addresses to identify and talk to each other on a network. Therefore, it is imperative that the selected IP address be both unique and valid in a network environment.

Note: The static IP address **192.168.1.x** will never be assigned by and ISP (Internet Service Provider). IP addresses using this form are considered private. Actual application of the I-KVM Series may require access to public network, such as the Internet. If so, a valid public IP address must be assigned to the user's computer. A public IP address is usually purchased or leased from a local ISP.

Subnet mask

A subnet represents all the network hosts in one geographic location, such as a building or local area network (LAN). The I-KVM will use the subnet mask setting to verify the origin of all packets. If the desired TCP/IP host specified in the packet is in the same geographic location (on the local network segment) as defined by the subnet mask, the I-KVM will establish a direct connection. If the desired TCP/IP host specified in the packet is not identified as belonging on the local network segment, a connection is established through the given default gateway.

Default gateway

A gateway is a network point that acts as a portal to another network. This point is usually the computer or computers that control traffic within a network or a local ISP (Internet service provider). The I-KVM uses the IP address of the default gateway computer to communicate with hosts outside the local network environment. Refer to the network administrator for a valid gateway IP address.

Primary and Secondary DNS

The DNS (Domain Name System) server is used to locate and translate the correct IP address for a requested web site address. A domain name is the web address (i.e. www.yahoo.com) and is usually easier to remember. The DNS server is the host that can translate such text-based domain names into the numeric IP addresses for a TCP/IP connection.

The IP address of the DNS server must be able to access the host site with the provided domain name. The I-KVM provides the ability to configure the required IP addresses of

both the Primary and Secondary DNS servers addresses. (The secondary DNS server is specified for use when the primary DNS server is unavailable.)

Using Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of IP addresses centrally in an organization's network. DHCP allows the network administrator the ability to supervise and distribute IP addresses from a central point and automatically send a new IP address when a computer is plugged into a different network location.

When in static IP mode, the IP address must be entered manually at each computer. If a computer is moved to another network location, a new IP address must be assigned. DHCP allows all the parameters, including the IP address, subnet mask, gateway and DNS servers to be automatically configured when the IP address is assigned. DHCP uses a "lease" concept in assigning IP addresses to a computer.

DHCP limits the amount of time a given IP address will be valid for a computer. All the parameters required to assign an IP address are automatically configured on the DHCP server side, and each DHCP client computer receives this information when the IP address is provided at its boot-up.

Each time a I-KVM is reset, the I-KVM broadcasts a DHCP request over the network. The reply generated by the DHCP server contains the IP address, as well as the subnet mask, gateway address, DNS servers and the "lease" time. The I-KVM immediately places this information in its memory. Once the "lease" expires, the I-KVM will request a renewal of the "lease" time from the DHCP server. If the DHCP server approves the request for renewal, the I-KVM can continue to work with the current IP address. If the DHCP server denies the request for renewal, the I-KVM will start the procedure to request a new IP address from the DHCP server.

Note: While in DHCP mode, all network-related parameters for the I-KVM are to be configured automatically, including the DNS servers. If the DNS server is not automatically configured, the user may manually configure the settings by entering the primary and secondary DNS IP addresses. To force an automatic configuration of the DNS address, set the primary and secondary DNS IP addresses to 0.0.0.0 (recommended).

A DHCP sever assigns IP addresses dynamically from an IP address pool, which is managed by the network administrator. This means that the DHCP client, i.e. the I-KVM, receives a different IP address each time it boots up. The IP address should be reserved on

the DHCP server side to assure that the user always knows the newly assigned I-KVM address. In order to reserve the IP address in the DHCP network, the administrator needs the MAC address of the I-KVM found on the label sticker at the bottom of the I-KVM.

Setting **Reuse old IP at bootup time on DHCP failure** as **Enable**, if the I-KVM fails to receive an IP address from the DHCP server on booting up, the users can set the IP configurations of the I-KVM with the previous IP configurations and connect it to the network. When the "lease" expires, the I-KVM requests a renewal.

Simple Network Management Protocol (SNMP) Configuration

The I-KVM has the SNMP (Simple Network Management Protocol) agent supporting SNMP v1 and v2 protocols. Network managers like NMS or SNMP Browser can exchange information with I-KVM, as well as access required functionality.

SNMP protocols include GET, SET, GET-Next, and TRAPs. With these functions, a manager can be notified of significant events (TRAPs), query a device for more information (GET), and make changes to the device state (SET). SNMPv2 adds a GET-Bulk function for retrieving tables of information and security functions.

With the SNMP configuration panel, the user can configure MIB-II System objects, access control settings and TRAP receiver settings. The manager configured in this menu

can perform both information exchange and action control. The figure below shows a SNMP configuration screen via a web interface.

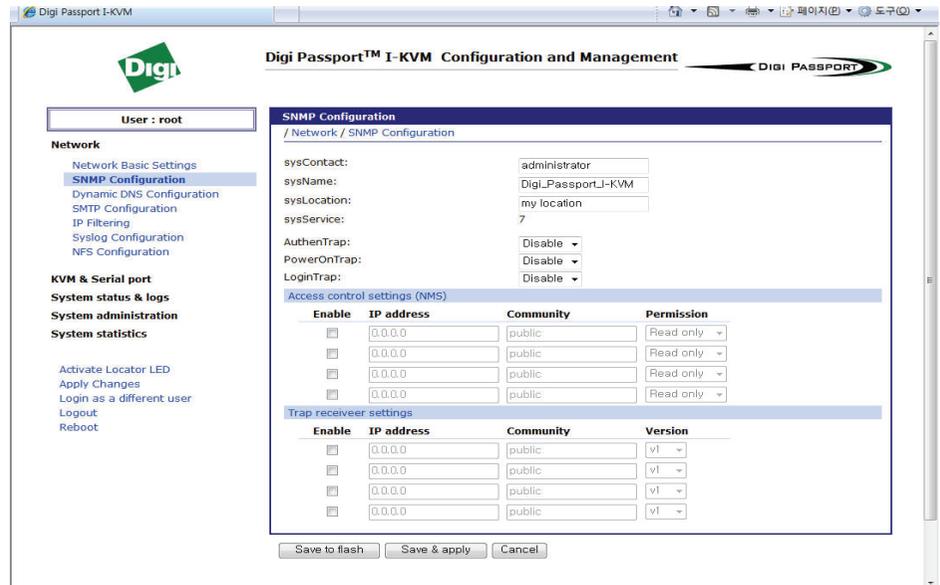


Figure 3-2: SNMP configuration

MIB-II System objects configuration

MIB-II System objects configuration sets the System Contact, Name, Location, and Authentication-failure traps used by the SNMP agent of the I-KVM. These settings provide the values used for the MIB-II sysName, sysContact, sysLocation, snmpEnableAuthenTraps, snmpEnablePowerOnTrap and snmpEnableLoginTrap Object Identifications (OIDs).

Brief descriptions of each OIDs are as follows,

- sysContact: Identification of the contact person for the managed system (I-KVM), and a description of how to contact the person.
- sysName: Name used to identify the system. By convention, this is the fully qualified domain name of the node.
- sysLocation: The physical location of the system (e.g., Room 384, Operations Lab, etc.).

- **sysService (Read Only):** A series of values, separated by commas, that indicate the set of services that the system provides. By default, I-KVM only supports an Application(7) service level.
- **EnableAuthenTrap:** Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authentication-failure traps may be disabled.
- **EnablePowerOnTrap:** Indicates whether the SNMP agent process is permitted to generate power-on traps.
- **EnableLoginTrap:** Indicates whether the SNMP agent process is permitted to generate system login traps.

If support is needed for adding or modifying MIBs, contact Digi technical support.

For more information about the MIBs and SNMP, see the RFCs 1066, 1067, 1098, 1317, 1318 and 1213.

Access control settings

Access Control defines accessibility of managers to the I-KVM SNMP agent. Only the manager set in this menu can access I-KVM SNMP agent to exchange information and control actions. If there is no specified IP address (all IP address are defaulted to 0.0.0.0), a manager from any host can access the I-KVM SNMP agent.

Trap receiver settings

The Trap receiver defines managers, which can be notified of significant events (TRAP) from the I-KVM SNMP agent.

Management using SNMP

The I-KVM can be managed through the SNMP protocol using NMS (Network Management System) or SNMP Browser. Before using the NMS or SNMP Browser, the user must set the access control configuration properly so that the I-KVM permits host

access where the NMS or SNMP Browser is executed. The figure below shows a screen shot of a typical SNMP browser with MIB-II OIDs of the I-KVM SNMP agent.

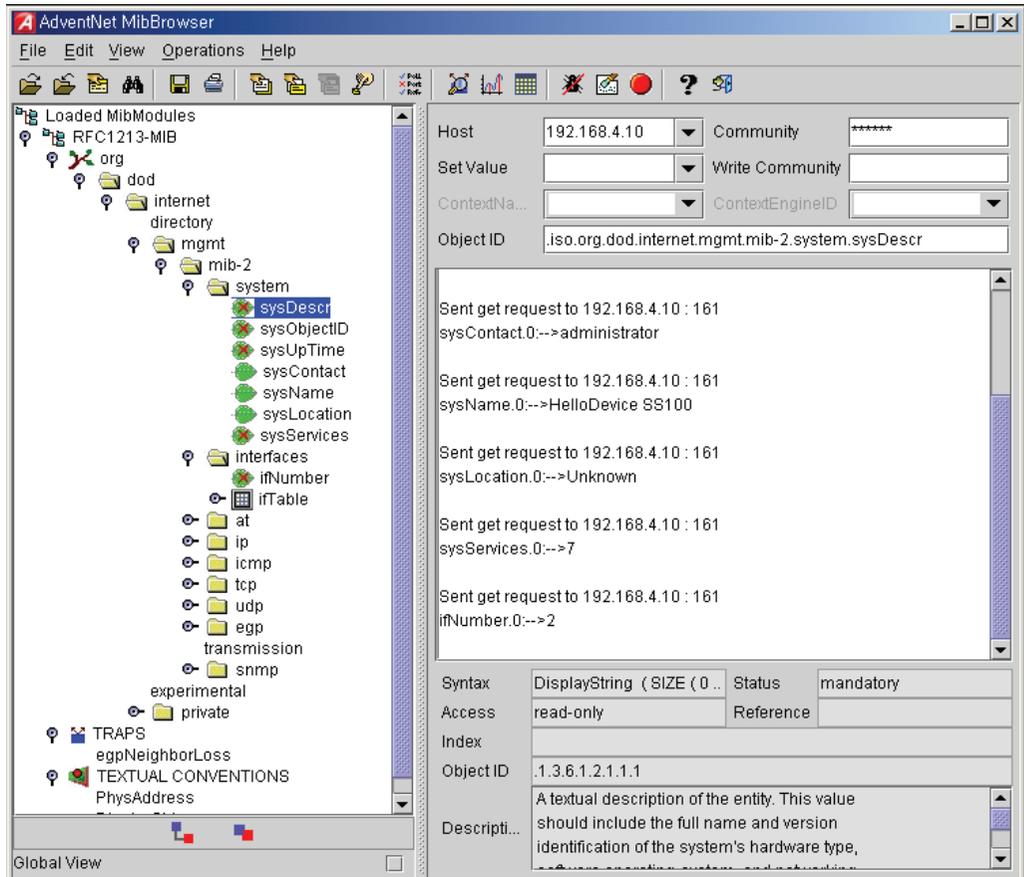


Figure 3-3: Browsing MIB-II OIDs of I-KVM SNMP agent using SNMP Browser (AdventNet MibBrowser)

Dynamic DNS configuration

When users connect the I-KVM to a DSL line or use a DHCP configuration, the IP address might be changed whenever it reconnects to the network. It can therefore be very difficult to post all related contacts for each new IP address. In addition, if the administrator only has access through the remote console, there is no way to know if an IP address has changed, or what the new IP address is.

A Dynamic DNS service is provided by various ISPs or organizations to deal with the above issue. By using the Dynamic DNS service, users can access the I-KVM through the hostname registered in the Dynamic DNS Server regardless of any IP address change.

By default, the I-KVM only supports Dynamic DNS service offered at Dynamic DNS Network Services, LLC (www.dyndns.org). Contact Sena technical support for issues regarding other Dynamic DNS service providers.

To use the Dynamic DNS service provided by Dynamic DNS Network Services, the user must set up an account in their Members' NIC (Network Information Center):

<http://members.dyndns.org>

The user may then add a new Dynamic DNS Host link after logging in to their Dynamic DNS Network Services Members NIC.

After enabling the Dynamic DNS service in the Dynamic DNS Configuration menu, the user must enter the registered Domain Name, User Name, and Password. After applying the configuration change, users can access the I-KVM using only the Domain Name.

The figure below shows the Dynamic DNS configuration web interface.

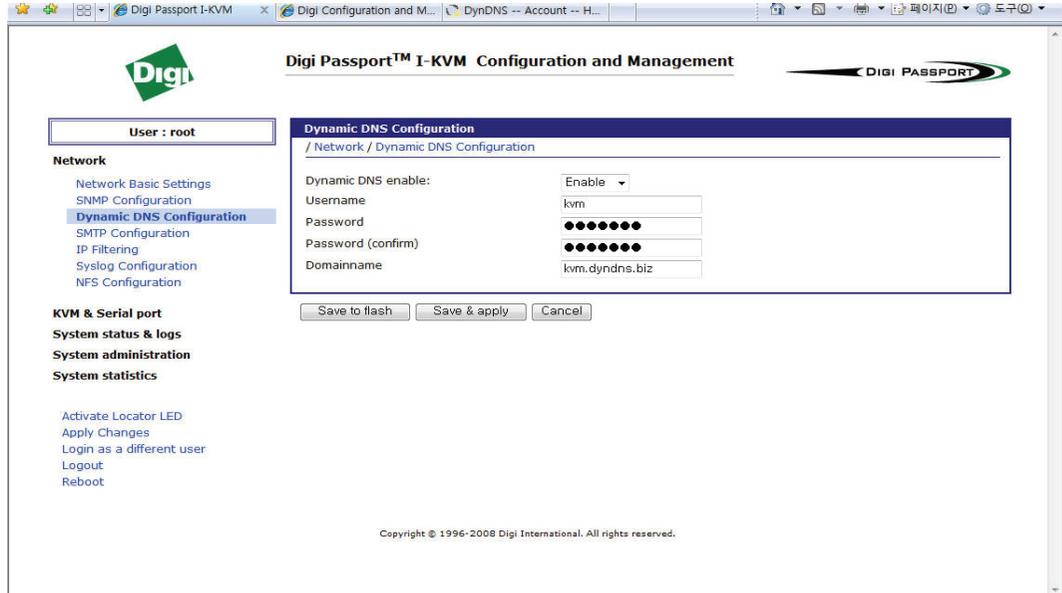


Figure 3-4: Dynamic DNS configuration

SMTP configuration

The I-KVM can send an email notification when the number of system log messages reaches a certain value and/or when an alarm message is created due to an issue with serial port data. The user must configure a valid SMTP server to send these automatically generated emails. The I-KVM supports three SMTP server types:

- SMTP without authentication
- SMTP with authentication
- POP-before-SMTP

The figures below shows examples.

Required parameters for each SMTP configuration include:

- SMTP server name
- SMTP mode
- SMTP user name

- SMTP user password
- Device mail address

SMTP configuration

/ Network / SMTP configuration

SMTP enable:	Enable ▾
SMTP server	smtp.server.address
SMTP mode:	SMTP with authentication ▾
Username	user@smtp.server
Password	••••
Password (confirm)	••••
Device mail address	user@smtp.server

Save to flash Save & apply Cancel

Figure 3-5: SMTP configuration

SMTP configuration

/ Network / SMTP configuration

SMTP enable:	Enable ▾
SMTP server	smtp.server.address
SMTP mode:	SMTP with authentication ▾
Username	POP before SMTP
Password	SMTP without authentication
Password (confirm)	SMTP with authentication
Device mail address	user@smtp.server

Save to flash Save & apply Cancel

Figure 3-6: SMTP mode selection in SMTP configuration

The device mail address specifies the sender's email address for all log and alarm delivery emails. SMTP servers often check only the sender's host domain name of the email address for validity. Consequently, the email address set for the device can use an

arbitrary username with a registered hostname (i.e. arbitrary_user@yahoo.com or anybody@digi.com).

The SMTP user name and SMTP user password are required when either SMTP with authentication or POP-before-SMTP mode is selected.

IP filtering

The I-KVM keeps unauthorized hosts from accessing to the I-KVM by specifying IP filtering rules. An IP filtering rule consists of **Option**, **IP address/Mask**, **Protocol**, **Port** and **Chain rule**.

Option

The Option determines that this rule will be applied to the hosts included or excluded in hosts range specified by the **IP address/Mask**. It can be one of these two values:

- Normal: applied to the hosts included
- Invert: applied to the hosts excluded

IP address/Mask

The **IP address/Mask** specifies the host range by entering base host IP address followed by "/" and subnet mask. The host range can be one of the following scenarios by changing the value:

- Only one host of a specific IP address
- Hosts on a specific subnet
- Any host

Table 3-2: Input examples of IP address/mask

<IP v4>_{mask}

Specified host range	Input format	
	Base Host IP address	Subnet mask
Any host	0.0.0.0	0.0.0.0
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 ~ 192.168.1.254	192.168.1.0	255.255.255.0

192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 ~ 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 ~ 192.168.1.254	192.168.1.128	255.255.255.128

<IP v6>

Specified host range	Input format	
	Base Host IP address	Subnet mask
Any host	::0	0
fec0::111	fec0::111	128
fec0::1 ~ fec0::ffff	fec0::0	112
fec0::1 ~ fec0::ffff.ffff	fec0::0	96
fec0::1 ~ fec0::f	fec0::0	124
fec0::8000 ~ fec0::8fff	fec0::8000	113

Protocol

The Protocol determines which protocol the host uses to communicate with the I-KVM. It can be one of two values such as TCP and UDP.

Port

The Port is a port or port range of the I-KVM which hosts try to access to. The port range can be specified by entering port1:port2 where the port range starts with port1 and ends with port2.

Chain rule

The Chain rule determines whether the access of the hosts is allowed or not. It can be one of the these two values:

- ACCEPT: access allowed
- DROP: access not allowed

The figure below shows IP filtering configuration.

The screenshot displays the IP Filtering configuration interface. It is divided into two main sections: IPv4 filtering and IPv6 filtering. Each section contains a table of rules with columns for No., Option, IP address/mask, Protocol, Port, and Chain rule. There are also 'Remove' and 'Add' buttons for each rule.

No.	Option	IP address/mask	Protocol	Port	Chain rule	
1	Invert	192.168.0.0/255.255.0.0	TCP	22	DROP	Remove
2	Invert	192.168.0.0/255.255.0.0	TCP	23	DROP	Remove
3	Normal	192.168.1.0/255.255.255.0	TCP	80	ACCEPT	Remove
4	Normal	192.168.2.0/255.255.255.0	TCP	80	ACCEPT	Remove
5	Normal	0.0.0.0/0.0.0.0	TCP	80	DROP	Remove
6	Normal	192.168.1.0/255.255.255.0	TCP	443	ACCEPT	Remove
7	Invert	192.168.2.0/255.255.255.0	TCP	443	DROP	Remove
New	Normal		TCP		ACCEPT	Add

No.	Option	IP address/mask	Protocol	Port	Chain rule	
No rules						
New	Normal		TCP		ACCEPT	Add

Figure 3-7: IP filtering configuration

The #1 IP filtering rule at Figure 3-7 means the hosts which is not included (Option: invert) in the host range from 192.168.0.1 to 192.168.255.254 (IP address/Mask: 192.168.0.0/255.255.0.0) are not allowed (Chain rule: DROP) to connect to SSH (port: 22). The #1 rule allows only the hosts whose subnet is 192.168.x.x to access to the I-KVM through SSH. The #2 IP filtering rule allows those which belongs to the subnet 192.168.x.x to connect to the I-KVM through telnet.

No host is allowed to connect to the I-KVM through http (port 80) by the #5 rule but the hosts whose subnet is 192.168.1.x is allowed by the #3 rule and 192.168.2.x by the rule #4. So, only the hosts which belong to the subnet 192.168.1.x or 192.168.2.x can access to the I-KVM through http by the #3, #4 and #5 rules.

No host except the hosts whose subnet is 192.168.1.x is allowed to connect to the I-KVM through https (port 443) by the #7 rule. But, hosts included in the subnet 192.168.1.x are allowed by the #6 rule. So, only the hosts which belong to the subnet 192.168.1.x or 192.168.2.x can access to the I-KVM through https by the #6 and #7 rules.

Users can add a new IP filtering rule by setting the properties at adding line and then clicking the **Add** button. User can remove a rule by clicking the **Remove** button. Users

can also edit the rules if they set the rule properties and click the **Save to flash** or the **Save & apply** button. The I-KVM will not filter the access of the hosts according to the IP filtering rules before users apply the changes by clicking the **Save & apply** button or selecting **Apply changes** at menu.

SYSLOG server configuration

The I-KVM supports a remote message logging service, SYSLOG service for the system and port data logging. To use the remote SYSLOG service, the user must specify the SYSLOG server's IP address or domain name and the facility to be used. The figure below shows the SYSLOG server configuration page of the supplied Web interface.

Syslog Configuration	
/ Network / Syslog Configuration	
Syslog enable:	Enable ▾
Syslog server	192.168.200.100

Figure 3-8: SYSLOG server configuration

To receive log messages from the I-KVM, the SYSLOG server specified in the I-KVM configuration must be configured as "remote reception allowed." If there is a firewall between the I-KVM and the SYSLOG server, the user must add a rule that will allow all outgoing and incoming UDP packets the ability to travel across.

If the SYSLOG service is enabled and the SYSLOG server configuration is properly set up, the user can specify the storage location for the I-KVM system log or port data log as SYSLOG server. For more information, refer to the sections, "Port logging" and system log configuration" within this document.

Network File System (NFS) server configuration

The I-KVM supports Network File System (NFS) service for system or port data logging functions. The user must specify the NFS server's IP address and the mounting path on the NFS server to use it. The figure below shows the web based NFS server configuration page.

To store the I-KVM log data to the NFS server, the NFS server specified in the I-KVM configuration must be configured as "read and write allowed." If there is a firewall between the I-KVM and NFS server, the user must add a rule that will allow all outgoing and incoming packets to travel across.

If the NFS service is enabled and the NFS server configuration is properly set up, the user can specify the storage location for the I-KVM system log or port data log as the NFS server. For more information, refer to the sections, "Port logging" and system log configuration" within this document.

NFS Configuration	
/ Network / NFS Configuration	
NFS enable:	Enable ▾
NFS server	0.0.0.0
Timeout (in seconds, 5-3600)	5
Retry interval (in seconds, 5-3600)	10
Mount path	/

Save to flash Save & apply Cancel

Figure 3-9: NFS server configuration

Required parameters for each NFS server configuration include:

- NFS server IP address
- Timeout
- Retry interval
- Mount path

Timeout specifies time out value for I-KVM to check how long it will wait for the response from the NFS server if NFS server is not responding for some time. If there is no response from the NFS server during the **Timeout** interval, I-KVM releases (unmount) a local directory which is mounted to the directory of NFS server (mounting path on NFS server) and changes data logging location to memory automatically if it is needed.

Retry interval specifies time intervals for I-KVM to check whether connecting to NFS server is possible. The I-KVM checks whether connecting to NFS server is possible for every **Retry** interval. And if connection to the NFS server is possible, I-KVM remounts mounting path on NFS server on its local directory again and changes data logging location to NFS server automatically if it is needed.

Serial port configuration

C H A P T E R 4

Serial Port Configuration

Overview

This chapter shows how to configure the serial ports. It reviews basic and advanced serial port settings, which can be modified from the factory default settings as needed.

Key serial port configuration settings include whether the port is enabled or disabled, the protocol, authentication, user access restrictions, and serial communication attributes.

Next, the chapter reviews basic and advanced serial port settings, which can be modified or restored to the factory default settings, and resetting port connections. The serial port configuration capability allows the user to configure serial communication parameters, port logging parameters and other related parameters.

About basic and advanced serial port settings

Serial port settings can be modified from their factory defaults. The I-KVM has two levels of serial port configuration settings:

- Basic configuration: Basic serial port settings needed for all ports.
- Advanced configuration: The complete set of serial port settings including Port management, Port title, Host mode configuration, Serial port parameter, Port logging, User access control, Alert configuration.

Basic port configuration settings

The Basic configuration page sets the essential parameters required to access the device attached to the corresponding serial port, including:

- Enabling or disabling the serial port
- Port title

- Host mode fixed to "Console server"
- The listening TCP port, or network port

The listening TCP port is the TCP network port specified when connecting directly to the port using Telnet or SSH.

- Protocol

The Protocol setting configures the communication protocol used over the serial port. There are three protocol options: RawTCP, SSH, and Telnet.

- Serial port parameters

The user can configure basic serial port parameter.

Port management

The Port management page displays managing port menu. Enable/Disable port, Resetting port, Setting the port to factory default.

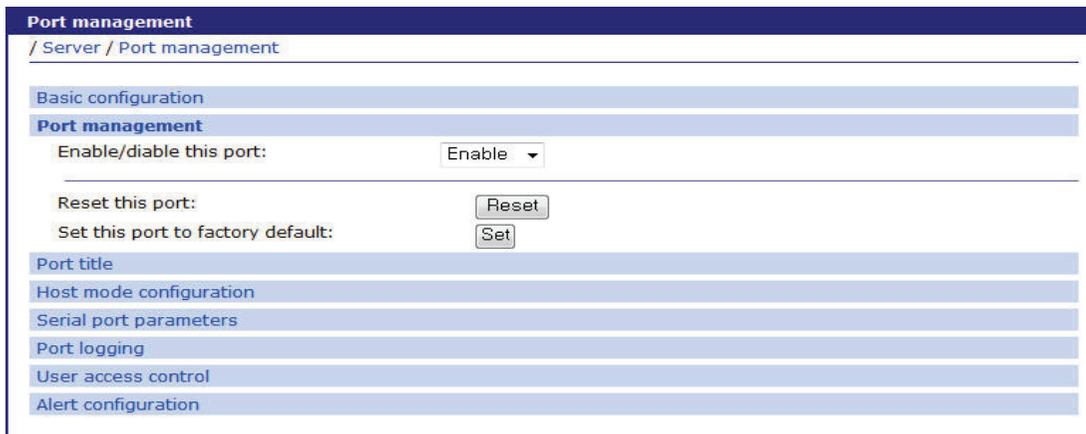


Figure 4-1: Port management

Host mode configuration

I-KVM supports only console server host mode. This mode utilizes a TCP server socket, which listens for a Telnet or SSH client connection. Once a Telnet or SSH client session is opened, the data stream can be sent back and forth to the device connected to the serial port.

The screenshot shows a web-based configuration interface for 'Host mode configuration'. The breadcrumb path is '/ Server / Host mode configuration'. The interface has several sections: 'Basic configuration', 'Port management', 'Port title', and 'Host mode configuration'. The 'Host mode configuration' section is expanded and shows the following settings:

Host mode:	Console server
TCP port (1024-65536):	7001
Protocol:	SSH
Inactivity timeout (1~3600, 0 for unlimited):	0
Port escape sequence:	Ctrl+Z
Port break sequence:	~break

Below the 'Host mode configuration' section are other expandable sections: 'Serial port parameters', 'Port logging', 'User access control', and 'Alert configuration'.

Figure 4-2: Host mode configuration

Console server mode configuration

Listening TCP port number

The user can also access a serial port through the IP address of the I-KVM and the listening TCP port number of the serial port. The user must use the TCP port number as well as the I-KVM IP address to the Telnet/SSH client.

If the IP address of the I-KVM and the serial port are assigned as 192.168.1.100 and 192.168.1.101, the user can connect to the port as follows:

```
telnet 192.168.1.100 6001
```

Protocol

Select Telnet, SSH or Raw TCP as the protocol. If the users are using a Telnet client program, select Telnet. If the users are using an SSH client program, select SSH. When Raw TCP is selected, direct TCP socket communication is available between the I-KVM and the remote host.

Inactivity timeout

The purpose of the inactivity timeout parameter settings is to maintain the TCP connection state as either Closed or Listen. If there is no activity between the I-KVM and the Telnet/SSH client during the specified inactivity timeout interval, the existing session will automatically be closed. If the user wants to maintain the connection indefinitely, configure the inactivity timeout period to 0. Although the inactivity timeout is disabled, the I-KVM will continue to check the connection status between the Telnet/SSH client and the I-KVM by sending "keep alive" packets periodically. If the Telnet/SSH client does not answer the packets, system will assume that the connection is down unintentionally. The I-KVM will close the existing Telnet/SSH connection, regardless of the inactivity setting.

Port escape sequence

When users connect to a port, they will get the port escape menu by entering the port escape sequence.

In order to send port escape sequence, enter the port escape sequence character twice or enter the **port escape sequence** character at the port escape menu.

Port break sequence

The user can send a break signal to the serial port by entering the break sequence that is configured as the port break sequence in the configuration menu

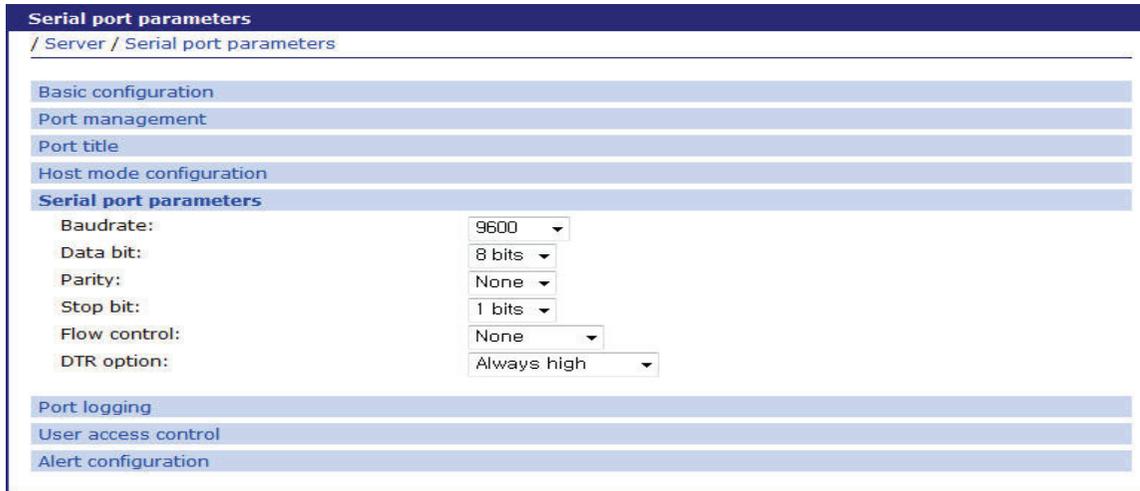
Serial port parameters

To connect the serial device to the I-KVM serial port, the serial port parameters of the I-KVM should match exactly to that of the serial device attached. The serial port parameters are required to match this serial communication.

The parameters required for the serial communication are:

- Baud rate

- Data bits
- Parity
- Stop bits
- Flow control
- DTR behavior



Serial port parameters

/ Server / Serial port parameters

Basic configuration

Port management

Port title

Host mode configuration

Serial port parameters

Baudrate: 9600

Data bit: 8 bits

Parity: None

Stop bit: 1 bits

Flow control: None

DTR option: Always high

Port logging

User access control

Alert configuration

Figure 4-3: Serial port parameters configuration

Baud rate

The valid baud rates for the I-KVM are as follows:

75, 150, 200, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, and 230400

The factory default setting is 9600.

Data bits

Data bits can be 7 bits or 8 bits. The factory default setting is 8 bits.

Parity

Parity can be none, even or odd. The factory default setting is none.

Stop bits

Stop bits can be 1 bit or 2 bits. The factory default setting is 1 bit.

Flow control

Flow control can be **none**, **software(Xon/Xoff)** or **hardware(RTS/CTS)**. The factory default setting is none.

DTR behavior

The DTR output behavior of a serial port can be configured as: **always high**, **always low** or **High when open**. If the DTR behavior is set to **High when open**, the state of the DTR pin will be maintained high as long as the TCP connection is established.

Port logging

With the port-logging feature while in console server mode, the data sent through the serial port is stored to MEMORY or a mounting point on an NFS server. It can also be stored to a SYSLOG server at the same time..

The configuration parameters for port logging are as follows:

- Port logging
- Direction to log
- Time stamp to port log
- Port log to remote syslog server
- SYSLOG facility for port logging
- Port log to NFS

- Filename to log on NFS

Port logging

/ Server / Port logging

Basic configuration

Port management

Port title

Host mode configuration

Serial port parameters

Port logging

Port logging: Enable ▾

Direction to log: Server output ▾

Time stamp to port log: Disable ▾

Port log to remote syslog server: Disable ▾

SYSLOG facility for port logging: LOCAL0 ▾

Port log to NFS: Disable ▾

Filename to log on NFS:

Port log

User access control

Alert configuration

Figure 4-4: Port logging configuration

Port logging

This parameter defines whether to enable or disable the port-logging feature. The factory default setting is [disable].

Direction to log

This parameter defines whether the incoming and the outgoing data are logged with direction arrows or not. The factory default setting is [Server output].

Time stamp to port log.

If Time stamp to port log is enabled, every line of log data includes time stamp. Factory default setting of this parameter is disable

Port log to remote syslog server

Enable to store port logs to a SYSLOG server.

SYSLOG facility for port logging

The user can select facility(LOC0~LOC7) for log level to be displayed in log files.

Port log to NFS

Enable to store port logs to NFS.

Filename to log on NFS

Filename to be stored in NFS

User access control

The user access control configuration can be used for restricting or permitting users who try to connect to a serial port of the I-KVM.

The access controls of <<Everyone>> specifies the access control of all the users except the users who are added in the user list or access list of user access control. Users whose access controls are different from those of <<Everyone>> should be added in the user list or access list of user access control.

Users should be not only identified by I-KVM or authentication server according to authentication configuration but also permitted by I-KVM according with user access control in order that they may connect to a serial port. For more information, refer the section, “Authentication” within this document.

User access control

/ Server / User access control

Basic configuration

Port management

Port title

Host mode configuration

Serial port parameters

Port logging

User access control

User	Access Type					Action
	Read	Write	Control	Log	Break	
<<Everyone>>	<input checked="" type="checkbox"/>					
user1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Remove user
<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	Add user				

Enable/disable multiple session Enable ▾

Session display mode Server output ▾

Display data direction arrows Disable ▾

Alert configuration

Figure 4-5: User access control configuration for serial ports

User access control

Access type consists of Read/Write/Control/Log/Break control.

The access controls of <<Everyone>> are applied to all the users who are not added to user list or access list of user access control. The users should be added to user list or access list if their access controls do not match <<Everyone>> access controls.

If the administrator wants to specify users who must be restricted from accessing a specific serial port, the administrator may check <<Everyone>> access control and add them to user list with option unchecked. If the administrator wants to specify the users who are allowed to access a specific serial port, he may uncheck <<Everyone>> access control and add them to user list with option checked.

Enable/Disable multiple session

The user can enable/disable multiple connections to the serial port.

Session display mode

server output: View all data to a serial port from a remote connection

user input: View all data from a serial port to a remote connection

both: See all data transmitted or received through a serial port

Display data direction arrows

Enable/Disable: Displays arrows to indicate the direction of data to or from the server.

When the second user accesses the port, the global "Port escape menu" is displayed.

Alert configuration

Email agent process sends email depending on email alert configurations and SNMP agent process transfers a SNMP trap to an administrator depending on SNMP trap configurations when the events related to the serial port such as port login.

The configuration parameters for alert configuration are as follows:

- Enable/Disable email alert for port login
- Title of email
- Recipient's email address
- Enable/Disable SNMP port login trap
- Trap receiver settings

Alert configuration
/ Server / Alert configuration

Basic configuration
Port management
Port title
Host mode configuration
Serial port parameters
Port logging
User access control

Alert configuration

Email alert configuration
Email alert for port login: Disable ▾
Title of email: Console Port: Notification for Login
Recipient's email address:

SNMP trap configuration
SNMP trap for port login: enable ▾

Trap receiver settings

Enable	IP address	Community	Version
<input type="checkbox"/>	0.0.0.0	public	v1 ▾
<input type="checkbox"/>	0.0.0.0	public	v1 ▾

Figure 4-6: Alert configuration

Enable/Disable email alert for port login

This parameter defines whether the email is sent when a user logs in and out the serial port.

Title of email

This parameter defines the title of email.

Recipient's email address

This parameter defines to whom the email is sent

Enable/Disable port login trap

This parameter defines whether the SNMP trap is transferred when a user logs in and out the serial port.

Trap receiver settings

For more information, refer to the section “SNMP Configuration” within this document.

KVM Configuration

CHAPTER 5

When controlling a host computer using the locally connected keyboard, video monitor and mouse, it is possible to use the VNC viewer or JRE browser (if the host computer is networked).

This section describes how to configure viewer parameters and user access control properties.

KVM configuration

/ KVM & Serial port / KVM configuration

Basic configuration

Host keyboard layout :	<input type="text" value="US"/>
Mouse/Keyboard type :	<input type="text" value="USB"/>
Menu bar toggle hot key :	<input type="text" value="F5"/>
Encryption :	<input type="text" value="Always On"/>
Idle timeout(seconds) :	<input type="text" value="0"/>
Protocol timeout(seconds) :	<input type="text" value="30"/>
Mouse rate(milliseconds) :	<input type="text" value="20"/>
Background refresh rate :	<input type="text" value="Medium"/>
Single mouse mode mouse switch :	<input type="text" value="Middle+Right Button"/>
Behaviour for admin connections when limit reached :	<input type="text" value="Replace oldest connection"/>
Single user mode :	<input type="text" value="Disable"/>
Single user mode username :	<input type="text"/>
Single user mode password :	<input type="text"/>

User access control

User	Access Type		Action
	Admin	User	
<<Everyone>>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Add user"/>

Figure 5-1: KVM configuration

The configuration parameters for KVM configuration are as follows:

Host keyboard layout

Configure keyboard layout expected by the host system. The I-KVM supports international keyboard layout of US, UK, Japan, Spain, France, Germany, Italy, Netherlands, Belgium, Norway, Sweden, Denmark and Swiss.

Mouse type

Configure Mouse type depends on the I-KVM model type.

USB model - USB mouse

PS/2 model - USB or PS/2 mouse

Menu bar toggle key

Configure function key (F5~F7, F9~F12) to toggle menu-bar of viewer.

Encryption

Three options are available: Always on, prefer off, prefer on. The one to choose depends on the specific details of the installation. The use of encryption imposes a slight performance overhead of roughly 10% but is highly secure against third party intrusion. For more information, refer to the section, “KVM viewer client” within this document.

Idle timeout

Determines the period of inactivity on a remote connection before the user is logged out. The idle timeout period can be set to any time span, expressed in seconds.

Protocol timeout

Sets the time period by which responses should have been received to outgoing data packets. If the stated period is exceeded, then a connection is considered lost and terminated

Mouse rate

Defines the rate at which mouse movement data are transmitted to the system. The default option is 20ms, which equates to 50 mouse events per second. This default rate can prove too fast when passed through certain connected KVM switches from alternative manufacturers. In such cases, data is discarded causing the local and remote mouse

pointers to drift apart. If this effect is encountered, increase the mouse rate to around 30ms (data is then sent at a slower rate of 33 times per second).

Background refresh rate

Select refresh rate for screen images via remote links. This allows the user to tailor the screen refresh to suit the network or modem connection speeds. The options are: Slow, Medium, Fast or Disabled. When the disabled option is selected, the remote users will need to manually refresh the screen.

Single mouse mode mouse switch

This allows the user to select the mouse button combination that can be used to exit from single mouse mode (when active). Options are: Disabled, Middle+Right Button, Middle+Left Button

Behaviour for admin connections when limit reached

Defines behavior of admin connections when limit reached. The I-KVM supports up to 4 simultaneous admin users log-in to the same KVM session. Options are: Replace oldest connection, Replace newest connection, Reject new connection .

Single user mode

Some VNC clients such as VNC clients for PDA don't require username for authentication. In order to connect with these VNC clients, this option should be enabled.

However, the Real VNC client still needs a username for authentication even if this option is enabled. In this mode, the User access control menu is disabled, and the single-user has the Admin authority.

Single user mode username

Username for authentication.

Single user mode password

Password for authentication.

User access control

Access type consists of Admin/User control. The user who has admin authority can set the viewer private mode even though other users are using the viewer private mode. For more information, refer to the section, “KVM viewer client” within this document.

The access controls of <<Everyone>> are applied to all the users who are not added to user list or access list of user access control. The users should be added to user list or access list if their access controls do not match <<Everyone>> access controls.

If the administrator wants to specify users who must be restricted from accessing I-KVM by viewer, the administrator may check <<Everyone>> access control and add them to user list with option unchecked. If the administrator wants to specify the users who are allowed to access a specific serial port, he may uncheck <<Everyone>> access control and add them to user list with option checked.

Connections

C H A P T E R 6

The I-KVM provides a web-based connection of serial port and KVM viewer which enables the user to access without remote port client and KVM viewer client.

Java Runtime Environment (JRE) must be installed on the client device. The user can install from SUN homepage(www.sun.com) linked on connection page.

The user can also download VNC viewer client program from VNC homepage by clicking hyperlink "VNC Viewer Client download (www.realvnc.com)." For more information, refer to the section, "KVM viewer client" within this document.



Figure 6-1: Connection

KVM connection

The user can connect to the web-based viewer by selecting "VNC Viewer JAVA Applet" link on connection page. Connection windows appears as below and the login window appears when the OK button is clicked.

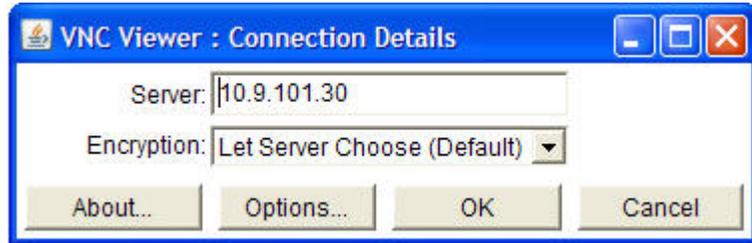


Figure 6-2: Viewer connection

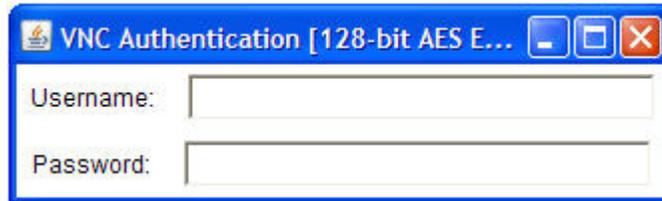


Figure 6-3: Viewer login

When **Enter** is pressed, the user can see viewer applet window. For more information, refer to the section, "KVM viewer client" within this document.

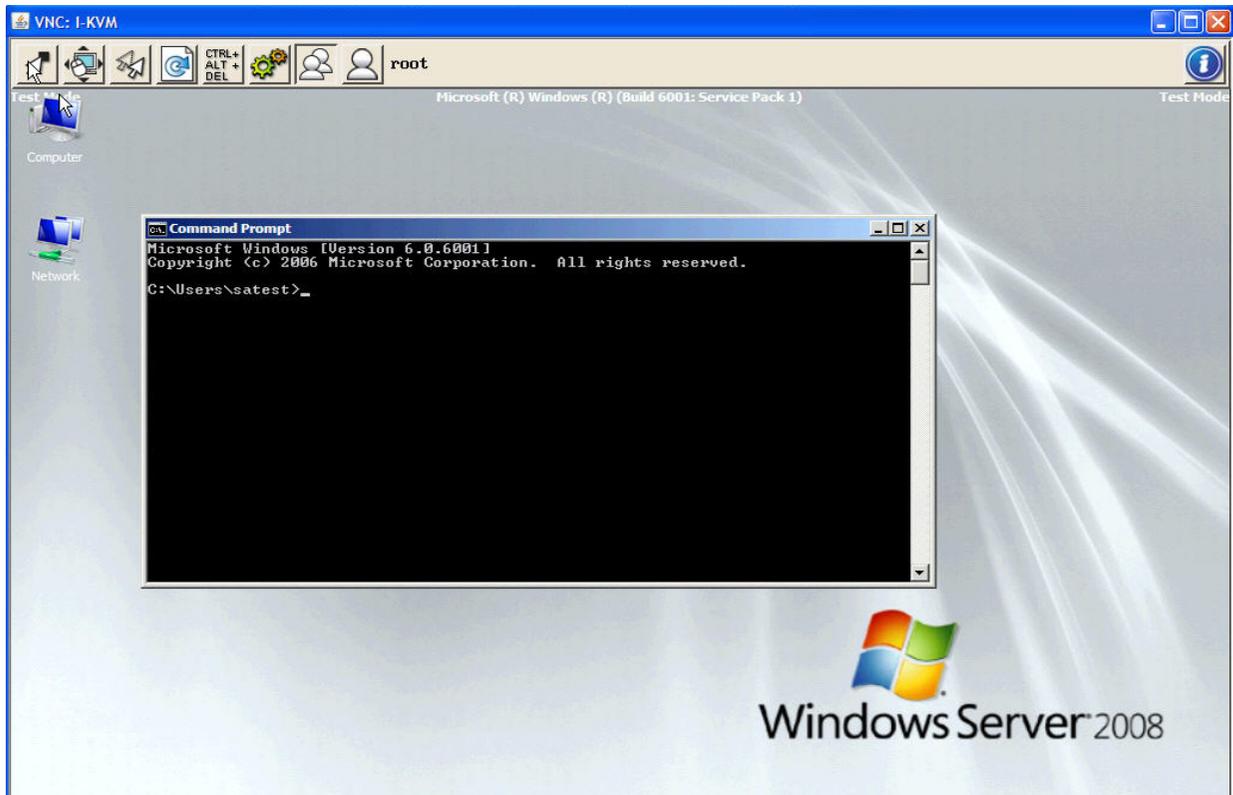


Figure 6-4: Viewer applet

Serial port connection

The user can access the serial port without using the telnet or SSH client program. The user may access the serial port by clicking the hyperlink "Serial connection (Telnet or SSH depends on Serial port configuration)". The terminal emulation pop-up window will be opened to grant user access to the port.

A Java applet is used to provide the text-based user interface to access the serial port. This Java applet supports only Telnet or SSH connection. The user cannot access the port via the web when the host mode of the port is set to Raw TCP connection. The user is asked to enter his/her user ID and password to access the port. Once authenticated, the user now has access to the port. The title bar of the pop-up window and the Java applet shows the information regarding the connection, i.e. Telnet or SSH, connection status, the port

number and the port title. On the bottom of the screen, there are hot key buttons accessible to connect, disconnect or send break.

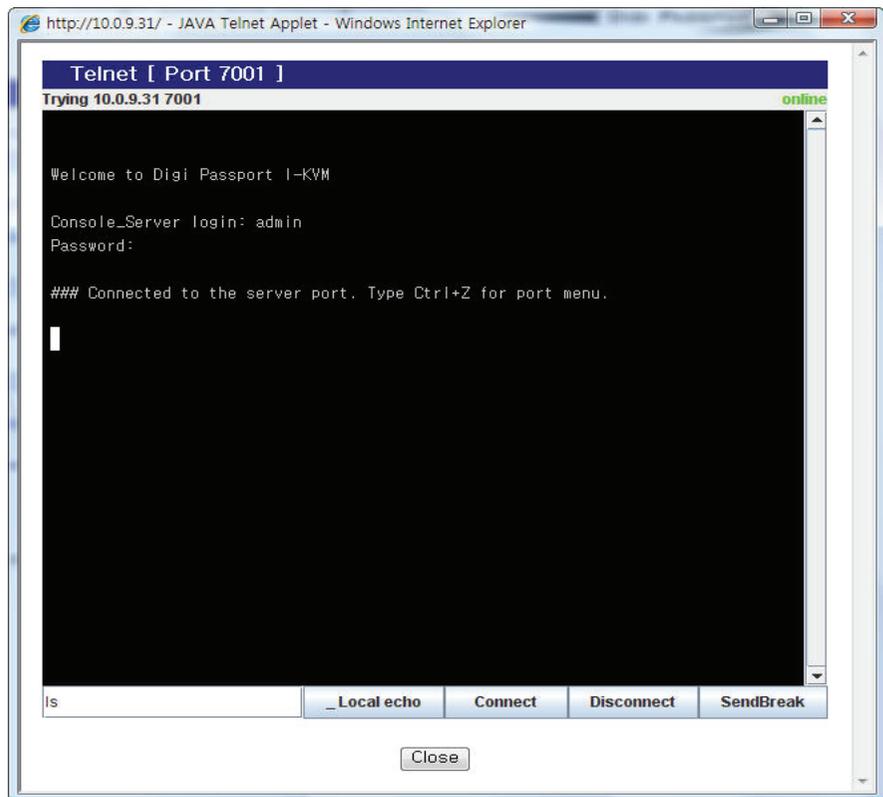


Figure 6-5: JTA window for Telnet

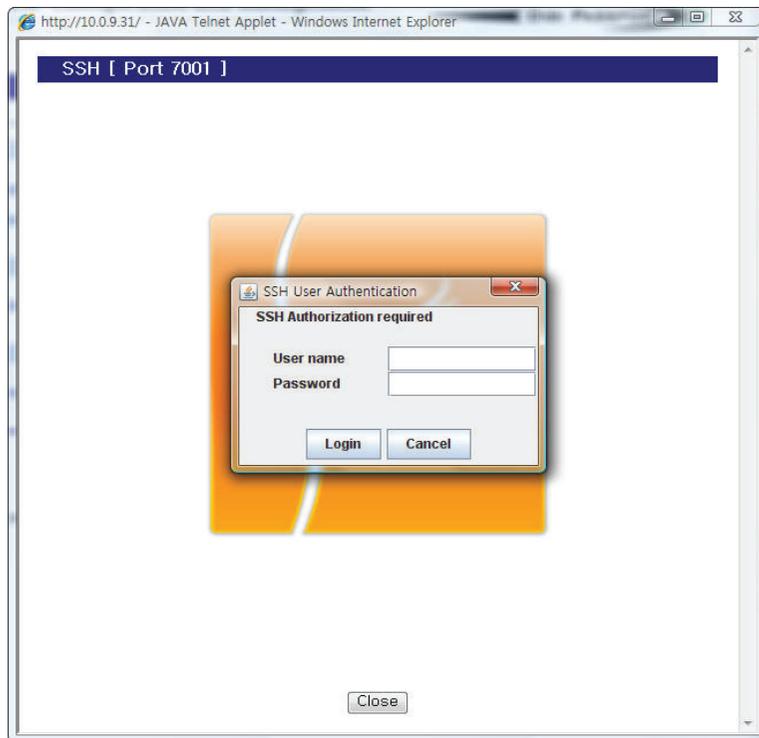


Figure 6-6: JTA window for SSH

Note: The users registered with their SSH public key cannot access the port through the web because the Java applet does not provide an SSH public key authentication.

KVM viewer client

C H A P T E R 7

The KVM viewer client (VNC viewer) is a compact application that runs on a remote system and allows the user to view and use the I-KVM and its host computer(s). KVM viewer client is readily available from a number of different sources:

- from the I-KVM product installation CD,
- from the RealVNC website (www.realvnc.com)

Note: The I-KVM supports equivalent feature set of RealVNC Enterprise version. Users can download and use RealVNC Enterprise version client software to make best use of all the I-KVM features such as encryption feature.

Login

Launch the KVM viewer client by clicking its desktop icon or by selecting it from the Start menu. A connection details dialog will be displayed.



Figure 7-1: Viewer client login

Server

I-KVM server IP address(IPv4 or IPv6).

Note: When using an IPv6 address, the address must be entered enclosed in

[] such as

[3ffe:5341:1:1:201:95ff:fe77:7702]

Encryption

- Let server choose - This setting will follow the configuration of the I-KVM. If the I-KVM has a preference to encrypt the link, then it will be so, otherwise the link will not be encrypted.
- Always on - This setting will ensure that the link is encrypted, regardless of the I-KVM encryption setting.
- Prefer off - This setting will configure an un-encrypted link if the I-KVM will allow it, otherwise it will be encrypted.
- Prefer on - If the I-KVM allows it, this setting will configure an encrypted link, otherwise it will be un-encrypted.

Options

When clicking the Options button the option window appears as below.

The Display tab on the VNC Viewer Properties dialog allows configuration of how the remote server should be displayed in the viewer:

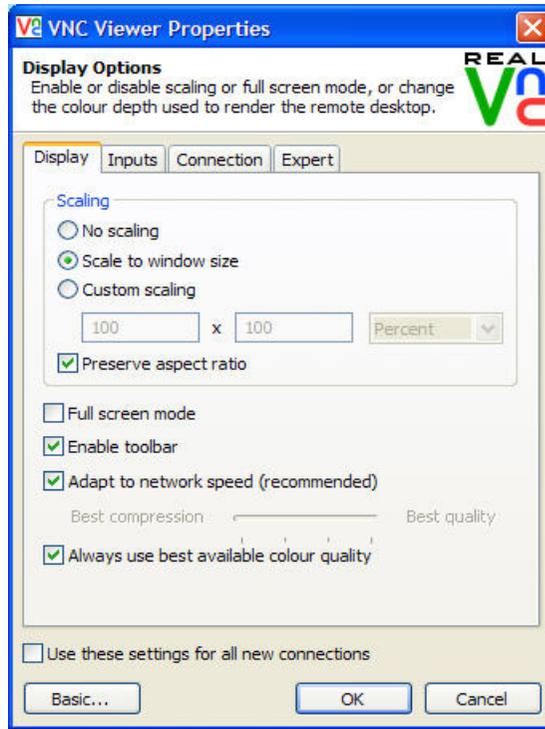


Figure 7-2: Viewer option - display

- No scaling - Remote screen is displayed on the viewer at without any stretching or squeezing
- Scale to Window Size - Adjust the server screen image to suit the size of the viewer window.
- Custom scaling - Remote screen is scaled to fit a pre-chosen scaling size or to fit a given size.
- Preserve Aspect Ratio - The aspect ratio of the remote screen is maintained regardless of the viewer window size.
- Full screen mode - The remote server screen is maximized to fit the viewer screen, and may be displayed with scroll bars.
- Enable toolbar - The quick access toolbar is displayed at the top of the viewer window. Refer to the figure, “Viewer screen,” below.)

- Adapt to network speed(recommended) - Viewer automatically select a balance between the number of colours displayed and viewer responsiveness, based on the connection speed
- Best compression/Best Quality - Allows the user to manually select a balance between the number of colours displayed and viewer responsiveness.
- Always use best available colour quality - Forces viewer to use the maximum number of colours even on a slow connection. Form example, to view photographs.
- The Inputs tab on the VNC Viewer Properties dialog allows the user to configure which events (keyboard, mouse etc) are transmitted to the server:

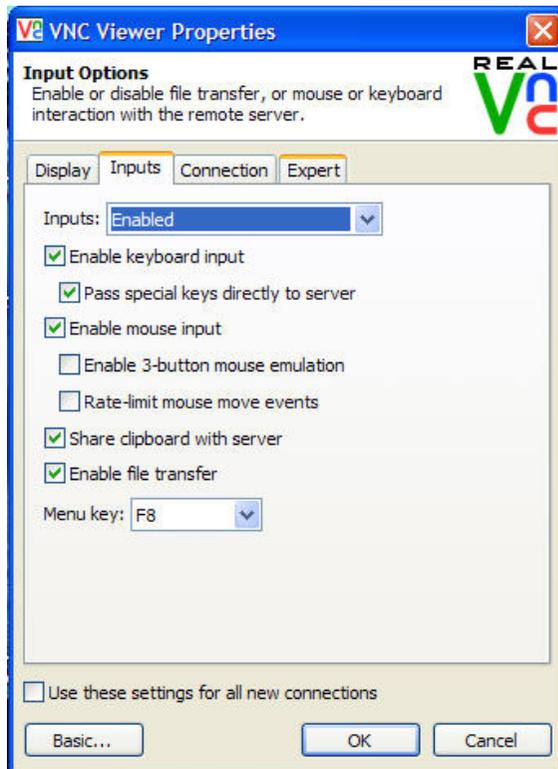


Figure 7-3: Viewer option - Inputs

- Inputs - Select "Enabled" on the Inputs drop-down list to allow all inputs. Select "Disabled" to viewer runs in "View Only" mode. Select Custom to select options required.

- Enable keyboard input - Keyboard events are passed to the server.
- Pass special keys directly to server - Windows key, Print Screen, Alt+Tab, Alt-Escape, Ctrl+Escape.
- Enable mouse input - Mouse movements and clicks are passed to the server.
- Enable 3 button mouse emulation - Allows enabling of a 3 button mouse to the remote server system using a 2 button mouse. To replicate the middle mouse button, press the left and right button simultaneously.
- Rate-limit mouse events - When enabled, the mouse position will be sent less frequently to the remote server. This can be useful for slow modem connections because bandwidth is reduced. However, it can result in a noticeable "jerkiness" to mouse pointer movement.
- Share clipboard with server - Any text that is cut or copied to the Windows clipboard or the server and vice versa. This allows cut, and paste to and from the server and vice versa.
- Enable file transfer - Allows the user to send files from the viewer to the server
- Menu Key - Allows the user to alter the function key, (usually F8) that displays the option menu within the VNC Viewer window. Choose None to disable this feature.

The Connections tab allows configuration the connection to the remote server:

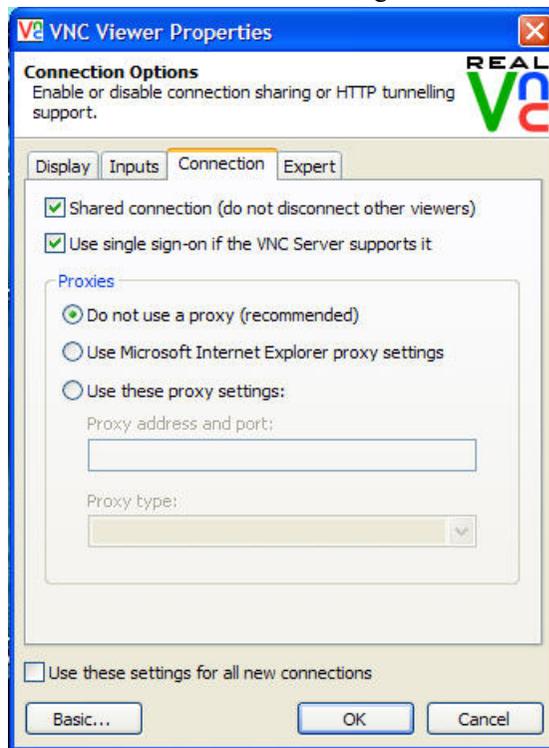


Figure 7-4: Viewer option - connection

- Shared connection (do not disconnect other viewers) - When enabled, the VNC Viewer will NOT request that any other existing connections to the remote server are terminated.
- Use single sign-on if the VNC Server supports it - When enabled, if the server supports single sign-on, the Viewer's user logon credentials will be presented to the server automatically. If these credentials are refused, then the user will be prompted to supply a username and password.
- Do not use a proxy (recommended) - VNC Viewer will make a direct connection to any VNC Server. In most cases, a proxy server will not be necessary to use VNC, and so this option is the recommended default.
- Use Microsoft Internet Explorer proxy settings - VNC Viewer will use the same proxy servers as Microsoft Internet Explorer uses (if any). In environments where a proxy server is needed to access computers on other

networks and the Internet, Microsoft Internet Explorer may already be set up with the necessary proxy server settings to allow the user to make these connections. This option will attempt to use those settings if they exist.

- Use these proxy settings - VNC Viewer will use the proxy server details supplied in the boxes below. Please contact a network administrator to determine the correct settings for these boxes.

Viewer screen

By clicking "Connect" button on the login window. Viewer screen will be displayed:

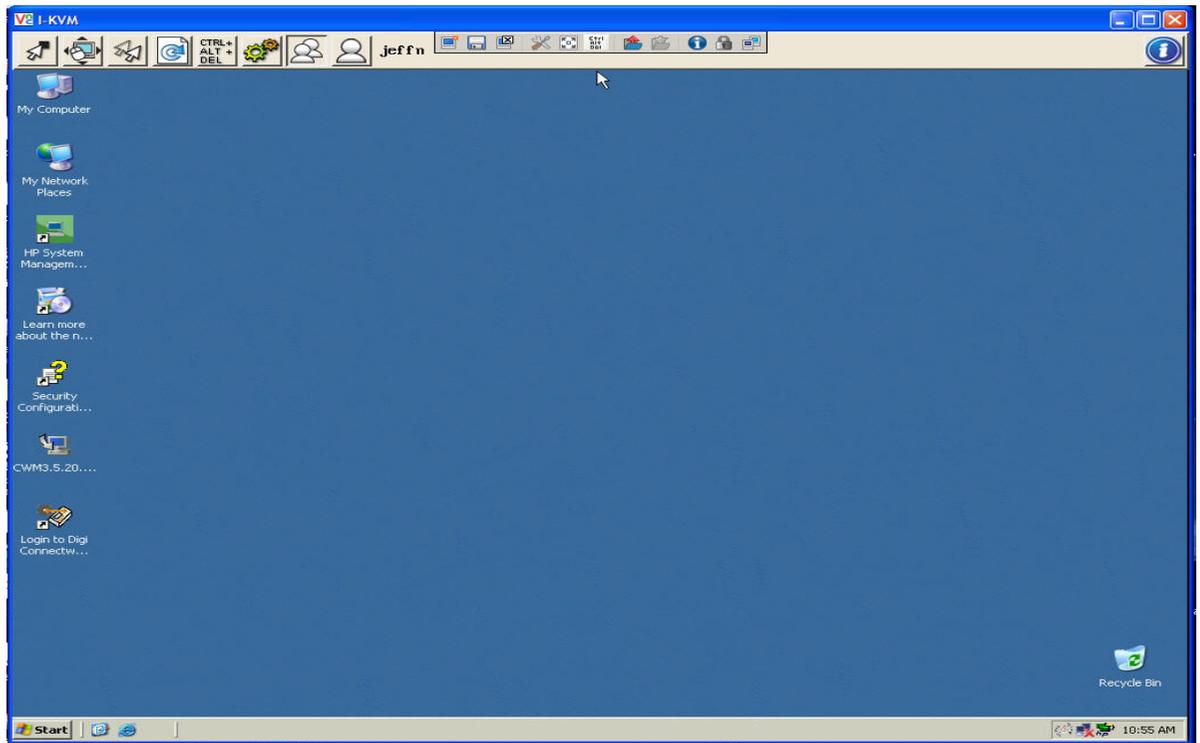


Figure 7-5: Viewer screen

VNC Toolbar (only appears when VNC client software is used)

Hover the mouse at the top of the VNC Viewer window to see the VNC Viewer Toolbar:



: New Connection – Creates a new VNC Viewer connection to a remote server in another window



: Save Connection – Saves the configuration settings for the current connection into the VNC

Address book



: Close Connection – Closes the current VNC Viewer connection



: Options - Displays the VNC Viewer Properties dialog



: Full Screen Mode – Uses the entire screen to display the remote sever desktop. Click again to exit Full Screen Mode.



: Send Ctrl +Alt +Delete – Sends a Ctrl+Alt+Delete command to the remote server. You can also press Shift+Ctrl+Alt+Delete.



: Send Files to Server – Sends a file from the local machine to the remote server. You can also copy files to the clipboard.



: Fetch Files from Server - Fetches a file from the remote server to the local machine. Files offered by the server are also placed on the clipboard and can be pasted. This icon is green when files are available.



: Connection Information – Displays the settings for the current VNC connection, including line speed etc.



: Connection Encrypted – Displays whether or not the VNC connection is encrypted



: Connection Speed – Displays the connection speed of the current VNC connection and indicates when there is network activity

VNC viewer window options

Click the VNC icon in the top left corner of the viewer window (or press F8) to display the window options. All menus are similar to VNC toolbar except Virtual Media.

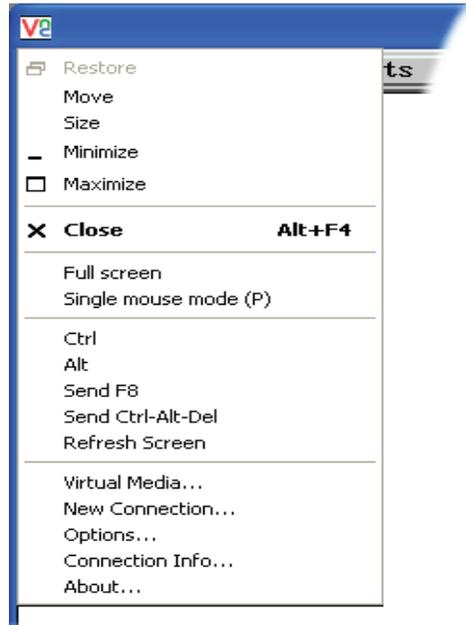


Figure 7-6: Viewer window menu

When Virtual Media menu is clicked, dialog appears as below. The user can send disk image or folder or file to host. The virtual media would be send to server by USB connection. The user can see USB connecting dialog on the window screen when connected.

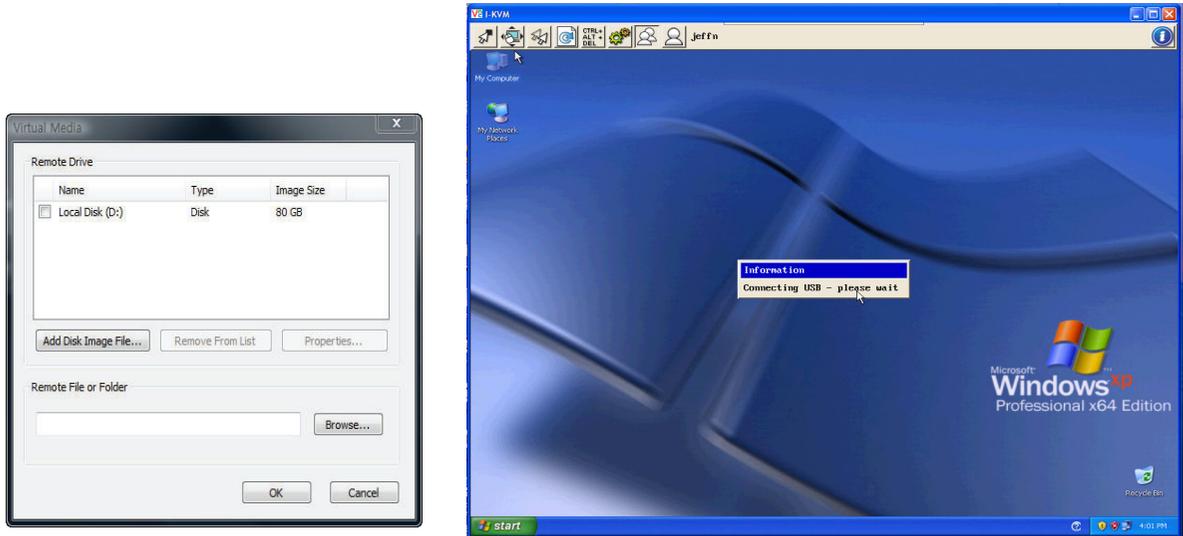


Figure 7-7: Window option menu - virtual media dialog

Note : USB cable must be connected from I-KVM to host to use virtual media function

KVM toolbar icons

At the top of the VNC Viewer window will be the KVM Toolbar icons:



Resync mouse: Ensures that the mouse pointer which is moved and the mouse pointer on the host system are correctly synchronized.



Auto calibrate - Determines the optimum video and/or mouse settings for the host computer. The user should click this button when first connecting or changing host window resolution. When clicked, Calibrate dialog appears.

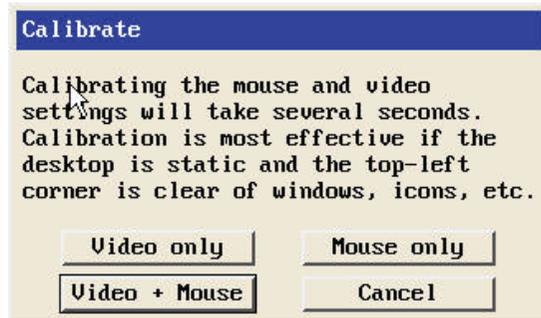


Figure 7-8: KVM calibration dialog



Single mouse mode - Change to single mouse mode. To escape to double mouse mode press function key (usually F8 + P or Middle + Right mouse button). For more information refer to the section of the manual, KVM Configuration.



Refresh screen



Sends a Ctrl + Alt + Delete command to the remote server



Controls - Displays a menu of options concerning keyboard, video and mouse operation.

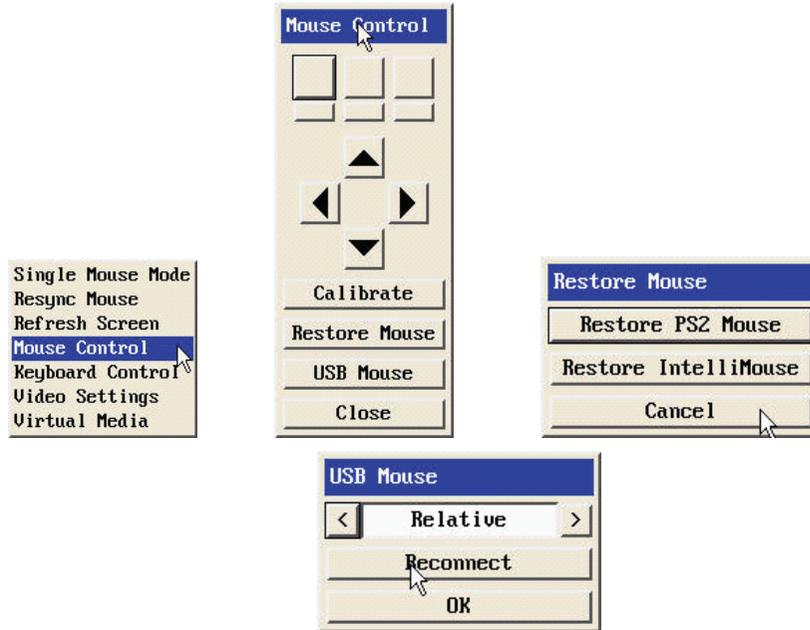


Figure 7-9: Mouse control dialog

Mouse control -When the remote cursor is not correctly responding to mouse movements, even after using the Re-sync mouse option, this option is useful.

Restore Mouse : Reinstates a mouse that has failed to operate correctly.

USB Mouse : For a USB mouse, the user can choose between relative and absolute positioning modes.



Figure 7-10: Keyboard control dialogs

Keyboard control - This dialog is useful when sending keyboard combinations (to the host) that are needed regularly or that are trapped by the I-KVM. . When entering codes:

"+" means press down the key that follows

"-" means release the key that follows

"+-" means press down and release the key that follows

"*" means wait 250ms (note: if a number immediately follows the asterisk, then the delay will equal the number, in milliseconds)

It is automatically assumed that all keys specified will be released at the end, so there is need to specify -Ctrl or -Alt if these keys are to be released together.

See Appendix-C for a list of key sequence codes that can be used.

Examples:

'Ctrl + Alt 12' would be expressed as: +Ctrl+ Alt+1-1+2

+N means press the 'N' key

+Scroll means press the Scroll lock key

+Space means press the space key

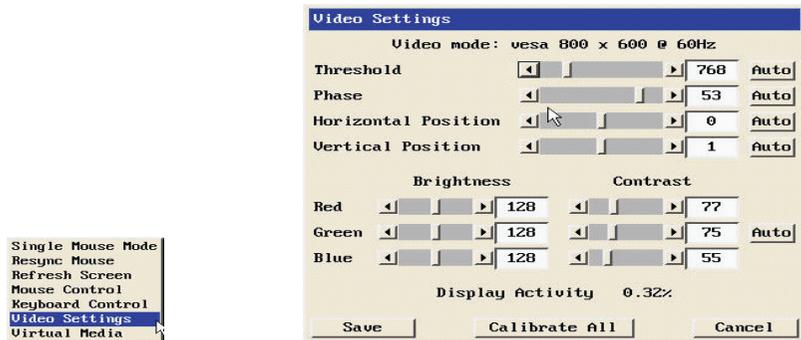


Figure 7-11: Video settings dialog

Video settings - This dialog provides access to all of the key video settings that determine image quality and link performance.

Threshold - The threshold is effectively a noise filter that differentiates between valid video signals and background noise or interference. This has the effect of reducing unnecessary video signals between the I-KVM and the remote system, thus improving performance.

Phase - The phase setting adjusts the alignment of the host video output and the remote system video display to achieve the sharpest image.

Horizontal position - Determines the horizontal position of the host screen image within the viewer window.

Vertical position - Determines the vertical position of the host screen image within the viewer window.

Colour brightness & contrast - Provides manual sliders and also an automatic setting button to optimize these important video constituents for the current host and connection speed.

Calibrate all - Click to determine the optimum settings for all aspects of video the video connection from the host system.

Display Activity - Indicates the level of video activity currently in progress.

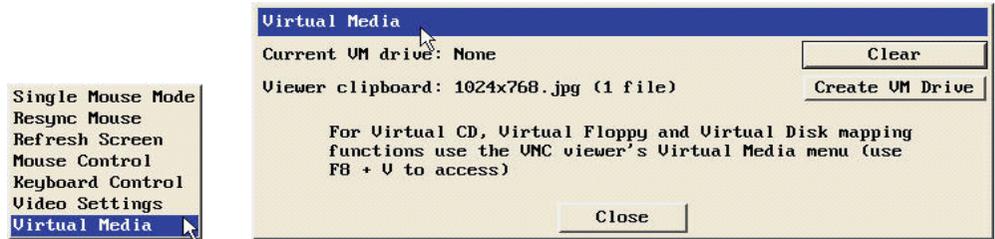


Figure 7-12: Virtual media dialog

Virtual media - The I-KVM Virtual Media feature is similar to virtual media option on "VNC viewer window options" section above.

The difference is that the user can simply locate and copy the required file, folder or drive to the clipboard and within the VNC viewer window, click the Controls button. The user can see copied file, folder or drive within the dialog.

Click **Create VM Drive** to announce file availability to the host computer, whereupon a pop up will confirm that the new virtual media disk is built.

Note: USB cable must be connected from I-KVM to host to use virtual media function.



Shared access mode



Private access mode



Information - KVM device information dialog appears as below



Figure 7-13: Information dialog

System status and log

CHAPTER 8

The I-KVM displays the system status and the log data via a Status Display Screen. This screen is to be used for management purposes. System status data includes the device name, serial number, hardware version, firmware version, bootloader version and the network configuration of the I-KVM. The user may configure the location where the log file is to be stored.

System status	
/ System status & logs / System status	
System information	
Device name	I-KVM
Serial number	won0.1
Hardware version	won0.1h
Firmware version	v0.0.1-won
Bootloader version	won1.0b
MAC address	00:01:95:A3:87:BD
Uptime	14:59:57 up 5:59, load average: 0.41, 0.35, 0.35
IPv4 information	
IP mode	Static IP
IP address	10.0.9.31
Subnetmask	255.255.0.0
Gateway	10.0.0.1
IPv6 information	
IP mode	Static IP
IP address(Global)	
IP address(Site)	fec0::202/64
IP address(Link)	fe80::201:95ff:fea3:87bd/64
Gateway	fec0::222
DNS information	
Primary DNS	206.13.28.12
Secondary DNS	206.13.31.12

Figure 8-1: System status display

System log configuration

The I-KVM provides both the system logging feature and the system log status display.

System log to SYSLOG server

The system log data can be stored to the SYSLOG server.

System log to NFS server

The system log data can be stored to the NFS server in addition to the SYSLOG server at the same time.

System log filename

System log filename defines a log file to be logged to the NFS server. The factory default filename is logs.

The figure below shows the configuration and system log view screen.



Figure 8-2: System log configuration and view

System administration

C H A P T E R 9

The I-KVM utilizes two user profile types to manage accessibility to different functions. These two levels of user types include: system admin and user.

The system admin group has full read/write access of the I-KVM configuration. The system admin can view or edit all I-KVM configurations, as well as use the I-KVM without any limitations.

The user group has no right to modify any of the I-KVM configurations. The user may access the serial port and KVM connection screen on the web interface to connect to the serial ports and KVM viewer.

In addition to the local authentication method, the I-KVM also supports an authentication server based method for user authentication. If a remote authentication method (i.e. RADIUS, TACAS+, and Kerberos LDAP) is enabled, the I-KVM will confirm the username and password with the remote authentication server and check the response from the server. The users can also use the cascaded authentication method such as remote authentication first and then local authentication if the remote authentication fails, or vice versa.

The users can configure the I-KVM's device name, date and time settings, the current user's password, and import / export configurations in this menu group. The users can also upgrade the firmware of the I-KVM using the web interface, remote consoles or serial console.

User administration

The I-KVM manages three user-level groups. Access of the configuration interfaces and of the serial ports is based on the user's group level.

User: general user group

Users who belong to this group can access serial port and KVM.

Group	Super user	System administrator	Users
Interface Program	Text menu	Text menu	Text menu
SSH public key upload	Yes	Yes	Yes
CLI access	Yes	Yes	Yes
Configuration text menu access	Yes	Yes	Yes
Web UI Access	Yes	Yes	*
System parameter	Yes	Yes	No
Change user Edit/Removal	Yes	Yes	No

* The user may access only the connection work space for the serial port / KVM.

Note: The figure below shows the initial user administration web interface.

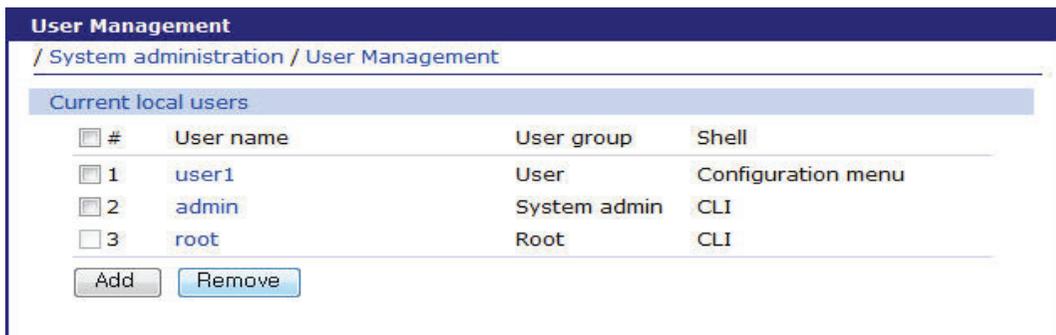


Figure 9:1: User administration

To add a user, Open add user screen by clicking the [Add] button, type the username, group and password at the add user screen, and then click the [Add] button. The figure below shows the **Add User** screen.

The following parameters should be properly set to create a user's account:

- **User name**
- **User group:** One of User, System admin
- **User password**
- **Shell program:** One of CLI, Configuration menu

- **SSH public key authentication:** One of **Enabled** or **Disabled**
- **SSH public key file**

If the SSH public key is uploaded into the I-KVM, the users who connect to the I-KVM using the SSH client program will be automatically authenticated using this key file. Otherwise, a password-based authentication will be done.

Note: User ID and password should be at least three characters or more for user add and change. There will be an error message if they are shorter than or equal to 2 characters.

The screenshot shows a web browser window with the title 'User Management'. The breadcrumb navigation is '/ System administration / User Management / add'. The form contains the following fields and controls:

- User name :** A text input field.
- Select group :** A dropdown menu with 'User' selected.
- Password :** A text input field.
- Confirm password :** A text input field.
- Shell program :** A dropdown menu with 'Configuration menu' selected.
- SSH public key authentication :** A dropdown menu with 'Disable' selected.
- SSH public key file:** A text input field with a '찾아보기...' (Browse...) button next to it.

Figure 9:2: Adding a user

To remove a user,

- Check the users at the **User administration** screen
- Click the [Remove] button

To change the parameters of the user account, open the edit user screen by selecting the user name at the **User administration** screen and then edit the parameters of user account like adding user.

Authentication

Users can select an Authentication method for Web login, KVM Viewer login and CLI login via serial console and telnet/SSH remote console. The I-KVM currently provides authentication methods of Local, RADIUS server, RADIUS server - Local, Local - RADIUS server, RADIUS down - Local, TACACS+ server, TACACS+ server - Local, Local - TACACS+, TACACS+ down - Local, LDAP server, LDAP server - Local, Local - LDAP server, LDAP down - Local, Kerberos server, Kerberos server - Local, Local -

Kerberos server, Kerberos down - Local using Linux-PAM (Pluggable Authentication Modules for Linux).

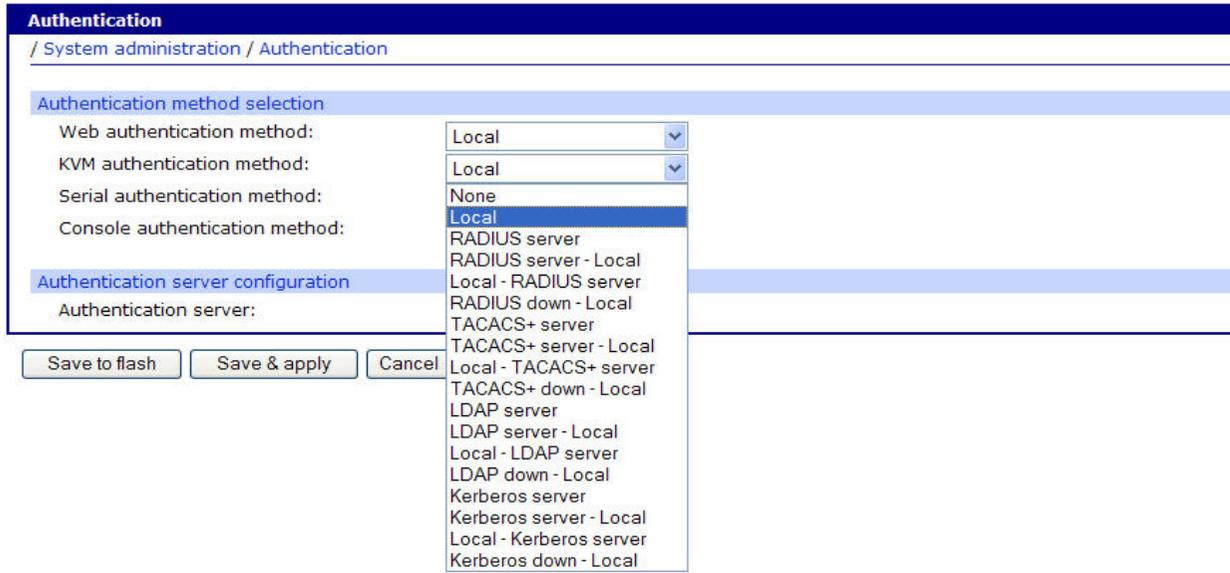


Figure 9:3: Authentication configuration - select method

\

Authentication

/ System administration / Authentication

Authentication method selection

Web authentication method:

KVM authentication method:

Serial authentication method:

Console authentication method:

Authentication server configuration

Authentication server:

First authentication server:

Second authentication server:

Shared secret:

Timeout (0-300 seconds): second(s)

Retries (1-50 times): times(s)

Figure 9:4: Authentication configuration - specify server

Change password

The figure below shows the change password screen. To change the current user's password, type the current password and a new password and then confirm the new password.

Change Password
 / System administration / Change Password

Current user name : root

Enter current password :

Enter new password :

Confirm new password :

Figure 9:5: Change password

Device name configuration

The I-KVM has its own name for administrative purposes. Figure 9-6 shows the device name configuration screen. When a user changes the Device name, the hostname and the CLI prompt of the I-KVM will also change corresponding to the new Device name.

Device Name
 / System administration / Device Name

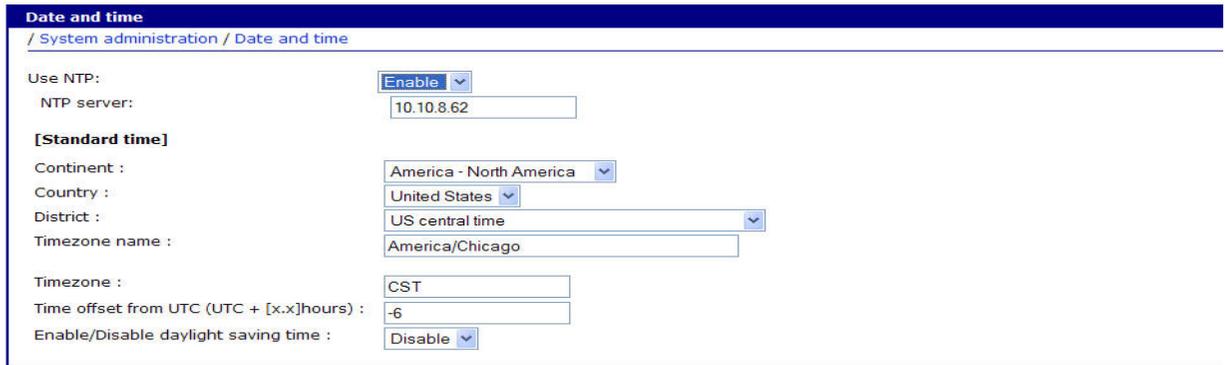
Device name I-KVM

Figure 9:6: Device name configuration and prompt on CLI

Note: A user cannot use a space character as part of the device name and the device name cannot be left blank or an error message will be generated.

Date and time settings

The I-KVM maintains current date and time information. The user can change the current date and time, as shown in the figure below.



The screenshot shows a web-based configuration page titled "Date and time" with a breadcrumb trail "/ System administration / Date and time". The page contains several configuration options:

- Use NTP:** A dropdown menu set to "Enable".
- NTP server:** A text input field containing "10.10.8.62".
- [Standard time]** A section header.
- Continent :** A dropdown menu set to "America - North America".
- Country :** A dropdown menu set to "United States".
- District :** A dropdown menu set to "US central time".
- Timezone name :** A text input field containing "America/Chicago".
- Timezone :** A text input field containing "CST".
- Time offset from UTC (UTC + [x.x]hours) :** A text input field containing "-6".
- Enable/Disable daylight saving time :** A dropdown menu set to "Disable".

Figure 9:7: Date and time configuration

There are two date and time settings. The first is to use the NTP server to maintain the date and time settings. If the NTP feature is enabled, the I-KVM will obtain the date and time information from the NTP server at each reboot. In this case, the I-KVM should be connected from the network to the Internet. The second method is to set date and time manually without using the NTP server. This will allow the date and time information to be kept until reboot.

Configuration management

The user may export the current configurations to a file at such locations as NFS server, user space or local machine and import the exported configurations as current configurations from NFS server, user space or local machine.

The user may restore the factory default settings at any time by selecting "Factory default" at location property at the import part or by pushing the factory default reset switch on the side panel of the I-KVM.

The figure below shows the configuration management screen.

Configuration Management
/ System administration / Configuration Management

Configuration Export

Location : User space(/ark) Local machine Primary NFS server

Encrypt : Yes ▾

File name : .syscm

Configuration import

Location : User space(/ark) Local machine Primary NFS Server Factory default

Configuration selection : Configuration ▾

Select all

Network configuration (Including IP configuration)

KVM configuration

Serial port configuration

System user configuration

System configuration

Encrypt : Yes ▾

File selection : ----- Select file ----- ▾ Local :

Figure 9:8: Configuration management

Configuration export

Location : Location to export to.

Encrypt : One of **Yes** or **No**

File name

Configuration import

Location : Location to import from. By selecting Factory default, the user may restore the factory settings.

Configuration selection : Determines what kinds of configurations are imported.

Encrypt : One of **Yes** or **No**. If location is Factory default, it does not apply.

File selection : List all the exported files satisfying the encrypting option at the selected location which is one of NFS server and user space.

Local : Helps to browse the exported file at local machine if location is local machine.

To export the current configurations:

- 1 Select the location to export to.
- 2 Select the encrypting option.
- 3 Type the file name.
- 4 Click the [Export] button.

To import the exported configurations:

- 1 Select the location to import from.
- 2 Select the configurations to import.
- 3 Select the encrypting option.
- 4 Select the file to import from the file selection list box if location is not local machine nor factory default.
- 5 Select the file to import by clicking browse button if location is local machine.
- 6 Click the [Import] button.

Security Profile

The security policy for the I-KVM management is configured in this section. It contains configuration options the system level of security, individual services and network security. The figure below shows the default Security Profile.

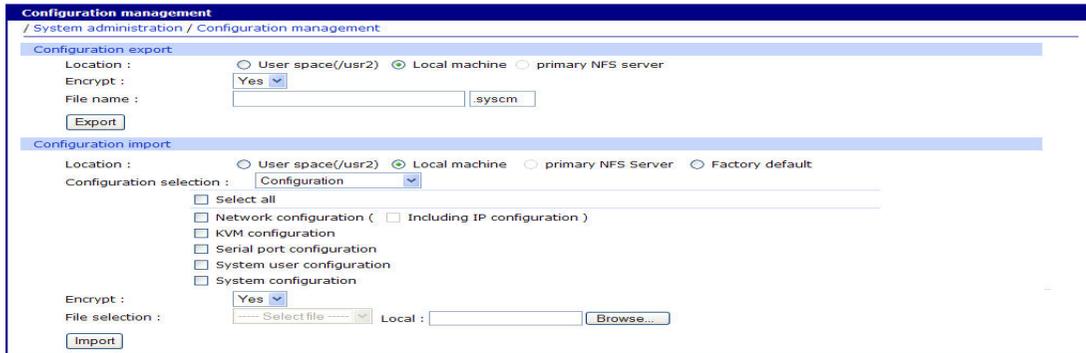


Figure 9:9: Security profile

The configuration parameters for services are as follows:

Level of security

SNMP (get/set)

Telnet

SSH

HTTP

HTTPS

Stealth mode

Level of security

This parameter determines the level of security policy. It can be one of custom, standard or secure. User can configure any security item in the case of custom. Otherwise, each security item is configured corresponding to the security level as follows:

Security Item	Custom	Standard	Secure
SNMP (get/set)	Configurable	Disable	Disable

Telnet	Configurable	Disable	Disable
SSH	Configurable	Enable	Enable
HTTP	Configurable	Redirect to HTTPS	Disable
HTTPS	Configurable	Enable	Enable
Stealth mode	Configurable	Disable	Enable

SNMP (get/set)

This parameter determines whether the service to get or set the status of the I-KVM is enabled or not.

Telnet

This parameter determines whether the telnet console service is enabled or not. It is implemented by adding or changing the IP filtering rule as follows:

Status	Interface	Option	IP address/ mask	Port	Chain rule
Disable	all	Normal	0.0.0.0/0.0.0.0	23	DROP
Enable	all	Normal	0.0.0.0/0.0.0.0	23	ACCEPT

For more information refer to the section, “IP filtering” within this document.

SSH

This parameter determines whether the SSH console service is enabled or not. It is implemented by adding or changing the IP filtering rule as follows:

Status	Interface	Option	IP address/ mask	Port	Chain rule
Disable	all	Normal	0.0.0.0/0.0.0.0	22	DROP
Enable	all	Normal	0.0.0.0/0.0.0.0	22	ACCEPT

For more information refer to the section, “IP filtering” within this document.

HTTP

This parameter determines whether Web service through HTTP is enabled or not. It is implemented by adding or changing the IP filtering rule as follows:

Status	Interface	Option	IP address/ mask	Port	Chain rule
Disable	all	Normal	0.0.0.0/0.0.0.0	22	DROP
Enable	all	Normal	0.0.0.0/0.0.0.0	22	ACCEPT

If it is set as the **Redirect to HTTPS**, the request of web interface through HTTP is lead to the request through HTTPS. For more information, refer to the section, “IP filtering” within this document.

HTTPS

This parameter determines whether Web service through HTTPS is enabled or not. It is implemented by adding or modifying the IP filtering rule as follows:

Status	Interface	Option	IP address/ mask	Port	Chain rule
Disable	all	Normal	0.0.0.0/0.0.0.0	HTTPS port	DROP
Enable	all	Normal	0.0.0.0/0.0.0.0	HTTPS port	ACCEPT

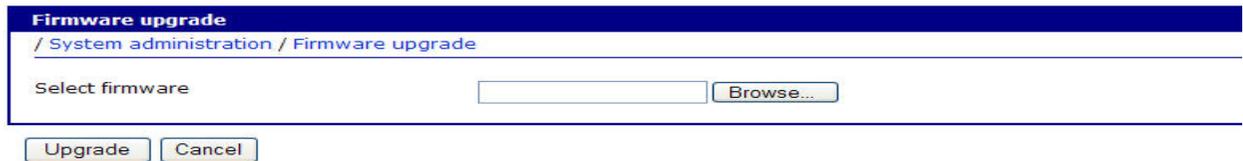
Stealth mode

If this parameter is set as Enable, the I-KVM does not reply to the request instead of refusing when a client tries to connect to the port which it does not listen to.

Firmware upgrade

Firmware upgrades are available via serial, remote console or web interface. The latest upgrades are available on the Digi web site at <http://www.digi.com>.

The figure below shows the firmware upgrade web interface.



The screenshot shows a web interface for firmware upgrade. At the top, there is a blue header with the text 'Firmware upgrade'. Below the header, there is a breadcrumb trail: '/ System administration / Firmware upgrade'. The main content area contains a text input field labeled 'Select firmware' and a 'Browse...' button. Below the input field, there are two buttons: 'Upgrade' and 'Cancel'.

Figure 9:10: Firmware upgrade

To upgrade firmware via the web:

1. Select the latest firmware binary by clicking browse button.
2. Once the upgrade has been completed, the system will reboot to apply the changes..

To use either a remote or serial console to upgrade firmware, the TELNET/SSH or terminal emulation program must support Zmodem transfer protocol. After the firmware upgrade, the previous settings will be reset to the factory default settings, except the IP configuration settings.

To upgrade firmware via a remote console:

- 1 Obtain the latest firmware.
- 2 Connect either TELNET/SSH or a serial console port using the terminal emulation program.

(TELNET or SSH is recommended since the process of firmware upgrade by serial console requires extremely long time.)

- 3 Select from the firmware upgrade menu as shown in Figure 9-12.
- 4 Proceed following steps as guided by online messages to transfer the firmware binary file using the Zmodem protocol.

- 5 Once the upgrade has been completed, the system will reboot to apply the changes. If the firmware is upgraded successfully, the I-KVM will reboot automatically.
- 6 If the firmware upgrade has failed, the I-KVM will display error messages as shown in the figure below and it will maintain the current firmware version.

```
-----
Welcome to Digi Passport I-KVM configuration menu

Hostname: I-KVM
Current time: Thu, 01 Jan 1970 12:18:23 +0900
F/W Rev.: v1.0.0          Bios Rev.: v1.0.0
MAC addr.: 00:95:12:34:AB:CD  IP addr.: 192.168.60.30
-----

Select menu:
 1. Network configuration
 2. KVM & Serial port
 3. System status & logs
 4. System administration

[h]elp, [s]ave, [a]pply, e[x]it, [q]uit
COMMAND> 4
-----

System administration

Select menu:
 1. User management
 2. Authentication
 3. Change password: *****
 4. Device name: I-KVM
 5. Date & Time
 6. Configuration management
 7. Security profile
 8. Firmware upgrade

[h]elp, [s]ave, [a]pply, e[x]it, [q]uit
COMMAND> 8
-----

Firmware upgrade

Select menu:
 1. Firmware version: v1.0.0 (Read-only)
 2. Start firmware upgrade

[h]elp, [s]ave, [a]pply, e[x]it, [q]uit
COMMAND> 2
Would you like to upgrade firmware of this unit? (y/n):y
Transfer the firmware image file by using Z-MODEM protocol.
Press Ctrl+X several times to cancel.
?*B0100000023be50eive.**B0100000023be50
```

Figure 9:11: Firmware upgrade using remote/serial console

```
COMMAND> 2
Would you like to upgrade firmware of this unit? (y/n):y
Transfer the firmware image file by using Z-MODEM protocol.
Press Ctrl+X several times to cancel.
?wupdate -b dialup.ttl**B0100000023be50
Failed to upgrade firmware
```

Figure 9:12: Firmware upgrade failure message

System statistics

CHAPTER 10

The I-KVM Web interface provides system statistics menus. The user can use these menus to access statistical data and tables stored in the I-KVM memory. Network interfaces statistics and serial ports statistics display statistical usage of the link layer, **lo**, **eth** and serial ports. IP, ICMP, TCP and UDP statistics display usages of four primary components in the TCP/IP protocol suite.

Network interfaces statistics

Network interfaces statistics display basic network interfaces usage of the I-KVM, **lo** and **eth0**. **lo** is a local loop back interface and **eth0** is a default network interface of I-KVM.

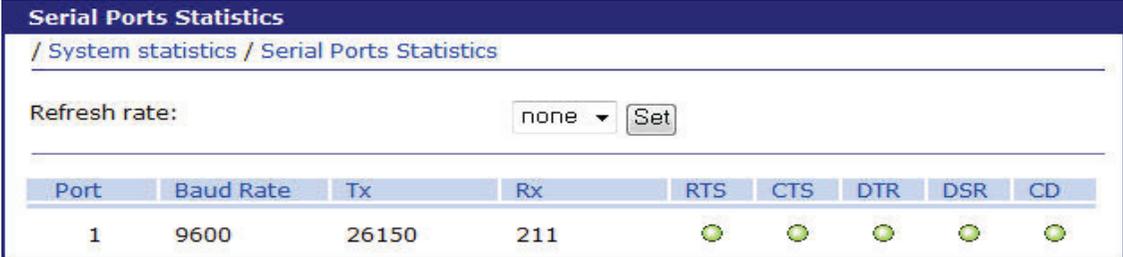
Network Interface Statistics			
/ System statistics / Network Interface Statistics			
Refresh rate:		none ▾	Set
Interface		lo	eth0
Receive	bytes	942814514	842347057
	packets	808728376	24665
	errs	0	0
	drop	0	0
	fifo	0	0
	frame	0	0
	compressed	0	0
	multicast	0	10202
Transmit	bytes	25288	2330261
	packets	872	10628
	errs	0	0
	drop	0	0
	fifo	0	0
	colls	0	0
	carrier	0	0
	compressed	0	0

Figure 10-1: Network interfaces statistics

Serial ports statistics

Serial ports statistics display the usage history of serial port, baud rate configurations and port's pin status.

( : On  : Off)



Port	Baud Rate	Tx	Rx	RTS	CTS	DTR	DSR	CD
1	9600	26150	211					

Figure 10-2: Serial ports status

IP statistics

The IP Statistics screen provides statistical information about packets/connections using an IP protocol. Definitions and descriptions of each parameter are described below:

Forwarding:

Specifies whether IP forwarding is enabled or disabled.

DefaultTTL:

Specifies the default initial time to live (TTL) for datagrams originating on a particular computer.

InReceives:

Shows the number of datagrams received.

InHdrErrors:

Shows the number of datagrams received that have header errors. InHdrErrors is the number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

InAddrErrors:

Specifies the number of datagrams received that have address errors. These datagrams are discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E).

ForwDatagrams:

Specifies the number of datagrams forwarded.

InUnknownProtos:

Specifies the number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

InDiscard:

Specifies the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.

InDelivers:

Specifies the number of received datagrams delivered.

OutRequests:

Specifies the number of outgoing datagrams that an IP is requested to transmit. This number does not include forwarded datagrams.

OutDiscards:

Specifies the number of transmitted datagrams discarded. These are datagrams for which no problems were encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space.) This counter would include datagrams counted in Datagrams Forwarded if any such packets met this (discretionary) discard criterion.

OutNoRoutes:

Specifies the number of datagrams for which no route could be found to transmit them to the destination IP address. These datagrams were discarded. This counter includes any packets counted in Datagrams Forwarded that meet this "no route" criterion.

ReasmTimeout:

Specifies the amount of time allowed for all pieces of a fragmented datagram to arrive. If all pieces do not arrive within this time, the datagram is discarded.

ReasmReqds:

Specifies the number of datagrams that require reassembly.

ReasmOKs:

Specifies the number of datagrams that were successfully reassembled.

ReasmFails:

Specifies the number of datagrams that cannot be reassembled.

FragOKs:

Specifies the number of datagrams that were fragmented successfully.

FragFails:

Specifies the number of datagrams that need to be fragmented but couldn't be because the IP header specifies no fragmentation. For example, if the datagrams "Don't Fragment" flag was set, the datagram would not be fragmented. These datagrams are discarded.

FragCreates:

Specifies the number of fragments created.

IP Statistics	
/ System statistics / IP Statistics	
Refresh rate:	none <input type="button" value="Set"/>
Forwarding	2
DefaultTTL	64
InReceives	20931
InHdrErrors	0
InAddrErrors	0
ForwDatagrams	0
InUnknownProtos	46
InDiscard	0
InDelivers	11407
OutRequests	11688
OutDiscards	0
OutNoRoutes	0
ReasmTimeout	0
ReasmReqds	6659
ReasmOKs	2230
ReasmFails	0
FragOKs	0
FragFails	0
FragCreates	0

Figure 10-3: IP statistics

ICMP Statistics

The ICMP Statistics screen provides statistical information about packets/connections using an ICMP protocol. Definitions and descriptions of each parameter are described below:

InMsgs, OutMsgs:

Specifies the number of messages received or sent.

InErrors, OutErrors:

Specifies the number of errors received or sent.

InDestUnreachs, OutDestUnreachs:

Specifies the number of destination-unreachable messages received or sent. A destination-unreachable message is sent to the originating computer when a datagram fails to reach its intended destination.

InTimeExcds, OutTimeExcds:

Specifies the number of time-to-live (TTL) exceeded messages received or sent. A time-to-live exceeded message is sent to the originating computer when a datagram is discarded because the number of routers it has passed through exceeds its time-to-live value.

InParmProbs, OutParmProbs:

Specifies the number of parameter-problem messages received or sent. A parameter-problem message is sent to the originating computer when a router or host detects an error in a datagram's IP header.

InSrcQuenchs, OutSrcQuenchs:

Specifies the number of source quench messages received or sent. A source quench request is sent to a computer to request that it reduces its rate of packet transmission.

InRedirects, OutRedirects:

Specifies the number of redirect messages received or sent. A redirect message is sent to the originating computer when a better route is discovered for a datagram sent by that computer.

InEchos, OutEchos:

Specifies the number of echo requests received or sent. An echo request causes the receiving computer to send an echo reply message back to the originating computer.

InEchoReps, OutEchoReps:

Specifies the number of echo replies received or sent. A computer sends an echo reply in response to receiving an echo request message.

InTimestamps, OutTimestamps:

Specifies the number of time-stamp requests received or sent. A time-stamp request causes the receiving computer to send a time-stamp reply back to the originating computer.

InTimestampReps, OutTimestampReps:

Specifies the number of time-stamp replies received or sent. A computer sends a time-stamp reply in response to receiving a time-stamp request. Routers can use time-stamp requests and replies to measure the transmission speed of datagrams on a network.

InAddrMasks, OutAddrMasks:

Specifies the number of address mask requests received or sent. A computer sends an address mask request to determine the number of bits in the subnet mask for its local subnet.

InAddrMaskReps, OutAddrMaskReps:

Specifies the number of address mask responses received or sent. A computer sends an address mask response in response to an address mask request.

ICMP Statistics	
/ System statistics / ICMP Statistics	
Refresh rate:	none <input type="button" value="Set"/>
InMsgs	4
InErrors	4
InDestUnreachs	4
InTimeExcds	0
InParmProbs	0
InSrcQuenchs	0
InRedirects	0
InEchos	0
InEchoReps	0
InTimestamps	0
InTimestampReps	0
InAddrMasks	0
InAddrMaskReps	0
OutMsgs	32
OutErrors	0
OutDestUnreachs	32
OutTimeExcds	0
OutParmProbs	0
OutSrcQuenchs	0
OutRedirects	0
OutEchos	0
OutEchoReps	0
OutTimestamps	0
OutTimestampReps	0
OutAddrMasks	0
OutAddrMaskReps	0

Figure 10-4: ICMP statistics

TCP statistics

The TCP Statistics screen provides statistical information about packets/connections using a TCP protocol. Definitions and descriptions of each parameter are described below:

RtoAlgorithm:

Specifies the retransmission time-out (RTO) algorithm in use. The Retransmission Algorithm can have one of the following values.

0 : CONSTANT - Constant Time-out

1 : RSRE - MIL-STD-1778

2 : VANJ - Van Jacobson's Algorithm

3 : OTHER - Other

RtoMin:

Specifies the minimum retransmission time-out value in milliseconds.

RtoMax:

Specifies the maximum retransmission time-out value in milliseconds.

MaxConn:

Specifies the maximum number of connections. If the maximum number is set to -1, the maximum number of connections are dynamic.

ActiveOpens:

Specifies the number of active opens. In an active open, the client is initiating a connection with the server.

PassiveOpens:

Specifies the number of passive opens. In a passive open, the server is listening for a connection request from a client.

AttemptFails:

Specifies the number of failed connection attempts.

EstabResets:

Specifies the number of established connections that have been reset.

CurrEstab:

Specifies the number of currently established connections.

InSegs:

Specifies the number of segments received.

OutSegs:

Specifies the number of segments transmitted. This number does not include retransmitted segments.

RetransSegs:

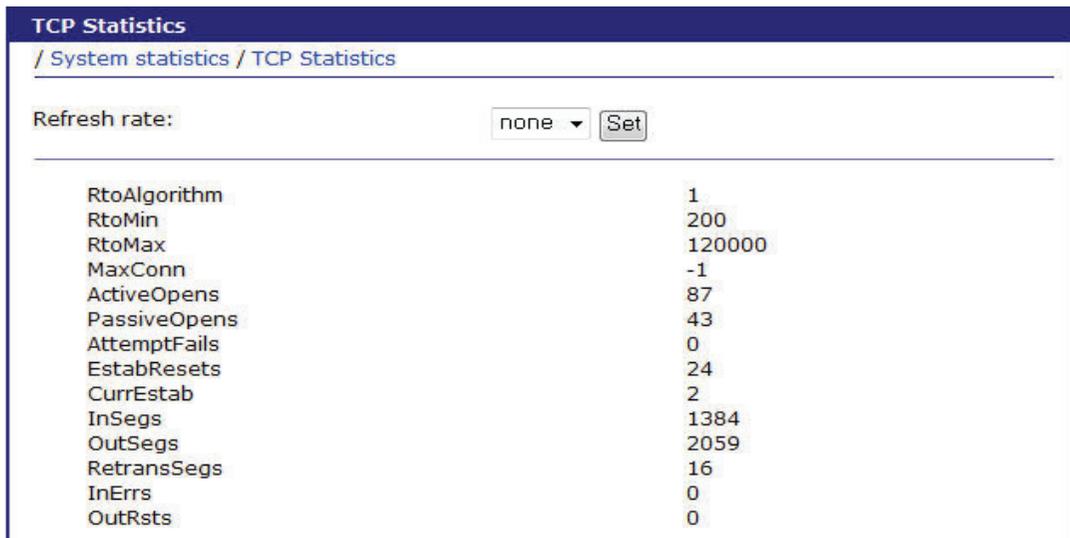
Specifies the number of segments retransmitted.

RetransSegs:

Specifies the number of errors received.

OutRsts:

Specifies the number of segments transmitted with the reset flag set.



The screenshot shows a window titled "TCP Statistics" with a breadcrumb path "/ System statistics / TCP Statistics". Below the path is a "Refresh rate:" label, a dropdown menu set to "none", and a "Set" button. A table of statistics follows, listing various metrics and their corresponding values.

Metric	Value
RtoAlgorithm	1
RtoMin	200
RtoMax	120000
MaxConn	-1
ActiveOpens	87
PassiveOpens	43
AttemptFails	0
EstabResets	24
CurrEstab	2
InSegs	1384
OutSegs	2059
RetransSegs	16
InErrs	0
OutRsts	0

Figure 10-5: TCP statistics

UDP Statistics

The UDP Statistics screen provides statistical information about packets/connections using a UDP protocol. Definitions and descriptions of each parameter are described below:

InDatagrams:

Specifies the number of datagrams received.

NoPorts:

Specifies the number of received datagrams that were discarded because the specified port was invalid.

InErrors:

Specifies the number of erroneous datagrams that were received. Datagrams Received Errors is the number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

OutDatagrams:

Specifies the number of datagrams transmitted.



UDP Statistics	
/ System statistics / UDP Statistics	
Refresh rate:	none <input type="button" value="Set"/>
InDatagrams	10134
NoPorts	37
InErrors	0
OutDatagrams	10182

Figure 10-6: UDP statistics

Guide to the Boot loader program

The purpose of the boot loader menu is to provide a way to recover the I-KVM unit using TFTP as a disaster recovery option. If the user presses the <ESC> key within 3 seconds after the I-KVM unit is powered up, he or she can enter the bootloader menu. Within this bootloader menu, the user can perform firmware upgrade.

```
Digi Passport I-KVM Bootloader Version v0.7.3 (Oct 16 2008-19:32:06)
DRAM Configuration:
Bank #0: at address 0x0 (0 KB)
Check for Intel flash(16bit x1)          DDI1=0x89, DDI2=0x8818 (yes)
Flash: (16 MB)
*** Using default environment
Hit <ESC> to stop autoboot:  3
-----
Welcome to Digi Passport I-KVM bootloader configuration menu
-----
Select:
1. Firmware upgrade
2. Exit and boot from flash memory
3. Exit and reboot
-->
```

Figure 10-7: Main Menu Page of Bootloader Menu

Firmware upgrade menu

By using the 'Firmware upgrade' menu, the user can upgrade the firmware of the unit. Before firmware upgrade, the user can verify the current firmware version. The firmware upgrade is done using TFTP for remote firmware download. User must set the IP address for the unit properly. The default IP address for the unit is 192.168.161.5.

To perform the firmware upgrade properly, a firmware file configured as [Firmware file name] on the server configured as [Server's IP address] must exist.

```
-----  
Firmware upgrade  
-----  
  
Current firmware version: v0.8.4  
  
Select:  
1. Tftp server's IP address: 192.168.11.100  
2. IP address assigned to Ethernet interface: 192.168.11.3  
3. Firmware file name: "I-KVM-v0.8.4.img"  
4. Start firmware upgrade  
-->
```

Figure 10-8: Firmware upgrade menu within Bootloader Menu

If the user selects [Start firmware upgrade], the firmware upgrade process will start. This process cannot be cancelled until it is finished.

After finishing the firmware upgrade process, the program will display the menu again along with a success message.

CLI guide

I-KVM runs an embedded Linux operating system. The command line interface for configuration purposes is accessible only by the root and/or administrator user. By default the root and administrator user is connected to the command line interface (CLI) when accessing the I-KVM unit through Telnet or SSH. To gain access to the command prompt, the root user uses the username root and the root password. The default root password is dbps. This chapter includes the Linux commands available on the embedded Linux operating system and the location of files useful to the root user for administrative purposes.

Back Up All Configuration Files Before Using Commands

The root user should be aware that deleting or corrupting files may prevent the I-KVM unit from booting properly. Before editing any files, be sure to back up configuration files.

Linux Commands

This section lists various Linux commands available on the I-KVM unit. This is simply a listing of commands and does not detail what the commands do or give their particular parameters. For more detailed command information, see the man pages on a Linux system.

Commands for Applying Changes

I-KVM has a command that are very important for applying changes.

applyconf: Immediately applies the configuration changes.

The configuration files are located in directory /usr2/conf.

Commands for configuring I-KVM unit and serial ports

Several commands are used for accessing and configuring the I-KVM unit and the serial ports.

configmenu: A menu for system administrators to configure the I-KVM unit. It has essentially the same functionality as the web interface for configuring a unit.

connect: Connects to local port

Utilities

- **Shell and Shell utilities :**

ash bash echo env false grep egrep fgrep more pwd sed sh clear

- **File and Disk utilities :**

cat chmod chown cp dd df du find gunzip gzip ln ls lsx lrz mkdir mknod mount mv rm
rmdir scp head tail tar touch vi umount zcat

- **System utilities :**

date free hostname id init insmod kill killall lsmmod modprobe poweroff ps reboot reset
rmmod sleep stty telnet uname who whoami

- **Network utilities :**

tftp ip ifconfig iptables ip6tables netstat ping ping6 route ssh

Important File Locations

I-KVM unit has several files that are important for administrative use. This section lists and briefly describes some of the files that the root user or system administrator may wish to view, monitor, and edit.

Config Files

Config files are located directory `/usr2/conf`. There are 6 directories for different type of configurations.

- **`/usr2/conf/kvm` – config files for configure I-KVM viewer.**
- **`/usr2/conf/network` – config files for network setting for I-KVM unit.**
- **`/usr2/conf/serial` – config files for serial port settings.**
- **`/usr2/conf/statistics` – config files for system statistics setting.**
- **`/usr2/conf/sysadmin` – config files for system administrator settings.**
- **`/usr2/conf/syslogs` – config files for system logs settings.**

Appendix A: Connections

Ethernet Pin outs

The I-KVM uses the standard Ethernet connector that is shielded connector compliant with AT&T258 specifications.

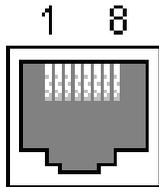


Figure A-1: Pin layout of the RJ45 connector

The table below shows the pin assignment and wire color.

Table A-1: Pin assignmnet of the RJ45 connector for Ethernet

Pin	Description	Color
1	Tx+	White with orange
2	Tx-	Orange
3	Rx+	White with green
4	NC	Blue
5	NC	White with blue
6	Rx-	Green
7		White with brown
8		Brown

Console and serial port pin-outs

The I-KVM uses an RJ45 connector for console and serial ports. The pin assignment of the RJ45 connector for console and serial ports is summarized in Table A-2. Each pin has a function according to the serial communication type configuration.

Table A-2: Pin assignment of RJ45 connector for console and serial ports

Pin	Description
1	CTS
2	DSR
3	RxD
4	GND
5	DCD
6	TxD
7	DTR
8	RTS

Appendix B: Well-known port numbers

Port numbers are divided into three ranges:

- Well Known Ports,
- Registered Ports, and
- Dynamic and/or Private Ports.

Well Known Ports are those from 0 through 1023. Registered Ports are those from 1024 through 49151. Dynamic and/or Private Ports are those from 49152 through 65535.

Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. Table C-1 shows some of the well-known port numbers. For more details, go to the IANA website:

<http://www.iana.org/assignments/port-numbers>

Table B-1: Well-known port numbers

Port number	Protocol	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure SHell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UDP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	BOOTP server	UDP
68	BOOTP client	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

Appendix C: Hotkey sequence codes

These codes are used when defining hotkey switching sequences (macros) for host computers and allow you to include almost any of the special keys on the keyboard.

Permissible key presses

Main control keys (see 'Using abbreviations')

Backspace | Tab | Return | Enter | Ctrl | Alt | Win | Shift | LShift | RShift
 LCtrl | RCtrl | LAlt | AltGr | RAlt | LWin | RWin | Menu | Escape | Space
 CapsLock | NumLock | PrintScreen | Scrolllock

Math operand keys (see 'Using abbreviations')

Add (Plus) | Subtract (Minus) | Multiply

Central control keys (see 'Using abbreviations')

Insert | Delete | Home | End | PageUp | PageDown
 Up | Down | Left | Right | Print | Pause

Keypad keys (see 'Using abbreviations')

KP_Insert | KP_Delete | KP_Home | KP_End | KP_PageUp
 KP_PageDown | KP_Up | KP_Down | KP_Left | KP_Right | KP_Enter
 KP_Add | KP_Subtract | KP_Divide | KP_Multiply
 KP_0 to KP_9

Function keys

F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12

ASCII characters

All characters can be entered using their ASCII codes, from 32 to 126 (i.e. A,B,C, ... 1,2,3 etc.) with the exception of the special characters '+', '-', '+-' and '*' which have special meanings, as explained below.

Codes with special meanings

+ means press down the key that follows

- means release the key that follows

+ - means press down and release the key that follows

* means wait 250ms (note: if a number immediately follows the asterisk, then the delay will equal the number, in milliseconds)

Note: Hotkey sequences are not case sensitive.

Creating macro sequences

Hot key macro sequences can be up to 256 characters long. All keys are assumed to be released at the end of a line, however, you can also determine that a key is pressed and released within a sequence. Any of the following three examples will send a command that emulates a press and release of the Scroll Lock key:

+SCROLL-SCROLL

+ - SCROLL

+SCROLL-

Example:

+ - SCROLL + - SCROLL + 1 + ENTER

Press and release scroll twice, press 1 then enter then release all keys (equivalent definition is +SCROLL-SCROLL+SCROLL-SCROLL+1+ENTER-1-ENTER)

Using abbreviations

To reduce the length of the key definitions, any unique abbreviation for a key can be used. For example: "scroll", "scr" and even "sc" all provide an identifiable match for

"ScrollLock" whereas "en" could not be used because it might mean "Enter" or "End" ("ent" would be suitable for "Enter").

Note: Hotkey sequences and abbreviations are not case sensitive.



PN (1P): 90001000 A