Prima® IP

LKV-9208/16IP

8/16-PORT
IP KVM SWITCH

CASCADABLE RACKMOUNT
USB AND PS/2 TYPE
OSD, FRONT-PANEL BUTTONS, KEYBOARD HOTKEYS

User Guide

Revision 1.6

About this manual

This *User Guide* is the complete reference to the Prima IP KVM Switch, its functional features and usage. The User Guide can be found on the Prima IP Support CD-ROM disc.

Prima IP documentation List

Installation Guide	Printout / Prima IP support CD-ROM disc
User Guide	Prima IP Support CD-ROM disc
How to generate your own set of Certificates	Prima IP Support CD-ROM disc

FCC Statement

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

CE Statement

This is a Class B product in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FC CE

TABLE OF CONTENTS

1 INTRODUCTION

The Prima IP 8 / Prima IP 16 is a 8/16-port IP-based KVM Switch with single-port KVM Link Extender over IP. In addition to the traditional local console, it provides a remote access over the LAN/Internet IP network. It is functionally versatile, robust and ultra-secure. It supports full 1024-bit PKI authentication, 256-bit SSL data encryption, LDAP, RADIUS as well Active Directory authentication and RADIUS accounting.

Prima IP KVM Switches

Today, the IP-based KVM Switch with multi-port capacity has been regarded as a reliable solution to address the critical issue of server rack management with admin's ready access anytime anywhere. Prima IP 8 / Prima IP 16 is designed with a view to offer a cost-effective yet full-featured functionality under these scenarios.

Total server control from BIOS level up anytime anywhere

The Prima IP 8 / Prima IP 16 gives users total control over its total 8 / 16 server ports, from *preboot stage* such as the BIOS-level CMOS setting up to the *GUI applications* and *daily maintenance routines* such as power cycling (power control unit required). And all these could be nicely done either on local console or using a thin-client software viewer on any computer. All you need for accessing your computer remotely is to login, download the viewer, and get yourself connected to a whole bunch of servers in seconds.

Upgrade and Configuration Backup is just a breeze

The Prima IP 8 / Prima IP 16 is fully Web-enabled to allow software upgrade and configuration upload/backup over the Web Management Interface. All you need to do is upload the files from its web management interface, and restart it to work with latest functionalities within minutes and can be performed across oceans-by an SUPERADMIN remotely!

Total Control Anytime Anywhere

With Prima IP 8 / Prima IP 16, the server administrator can access enterprise server room or data center on his own seat without toils and troubles of going anywhere from across the street to oversea. Organizations can enjoy a centralized and cost-effective control over its dispersed servers in different branch offices around the world, saving money for outsourcing costs.

Rackmount Cascadable with OSD Menu Control

In addition to keyboard hotkeys and front-panel buttons, Prima IP 8 / Prima IP 16 also provides OSD Menu for intuitive KVM switching operations. Its cascadable feature can upscale the server number up to 256 by cascading with other PRIMA-4, PRIMA-8 or PRIMA-16 KVM Switch.

Both USB and PS/2 interface support on PC side offers maximum convenience in a computing environment that accommodates both newer USB-enabled computers and older computers with only PS/2 interfaces.

Versatile backup connection featuring a PPP Server or PPP Client

To provide a redundancy of a backup connection system while network might no longer function in critical situation, Prima IP also allows an easy and convenient PPP connection over the dial-in modem phone line. It could serve as a PPP server to accept a peer computer to make PPP connection request over a dial-in modem phone line. On the other hand, Prima IP could also serve as a PPP client to dial-in to your ISP or enterprise PPP serve r to connect to internet. Thus, the PPP server/client feature allows users a second backup system, which offers a direct cable/modem dial-in access to your connected servers via PSTN while your network is down.

Critical Advantage over other remote server management solution

The advantages of using Prima IP KVM Switch, as compared to the conventional software remote control solution is that: The hardware-based remote control solution such as Prima IP is capable of accessing the connected servers regardless of the server states while software remote control solution cannot be functional while the server is still in the POST or preboot stage or in a “blue screen of death”. The Prima IP offers a server management capacity of up to 256 connected servers by cascading with Prima KVM switches. There is no need to install any software utility on the server side. Prima IP also offers power on/off alternatives if used with a remote power control unit.

KVM Switch Management

Prima IP 8 / Prima IP 16 not only provides remote user access, but also plays the role of KVM management. It manages the software version of all KVM switches connected in the daisy-chain, and upgrades automatically any KVM switches whose software is not the latest. It displays the KVM error and information messages into its server log. It permits to setup remotely the name of computers that are displayed in the OSD, the local user name and password.

Stability and ultra-security with flexibility and convenience

The Prima IP distinguishes itself among its peer products not only in its stability and durable performance, but also in its industry-standard security features such as full 1024-bit PKI Authentication and 256-bit SSL data encryption. Together with 3 levels of viewer connection security levels in combination with 3 types of password policies plus three categories of user privileges, all these make Prima IP a ultra-powerful IP KVM Switch with ultra-flexibility for a customized balance between data safety and user convenience. On the other hand, the robustness and the ease of maintenance of the embedded systems involve zero costs for the unit management and maintenance.

Global Time Zone and Time Servers Support

To make Prima IP really comfortable with all the global time zones it will be deployed in, it is vital to provide a convenient Global Time Zone support for a correct time stamp to all logging events, alert e-mail notifications. This will not leave server administrators in troubles with calculating time differences. Additionally, the Prima IP also supports NTP time server and keep its time always sync with the timer server you specify. The Prima IP is even sophisticated enough to take care of the daylight saving time in each and every Time Zone/Region, thus saving troubles for updating time frame with daylight saving specifics every six months.

Upgrade and Configuration Backup is just a breeze

Prima IP is fully Web-enabled to allow software upgrade and configuration upload/backup over the Web Management Interface. All you need to do is to upload the files to Prima IP over Web interface and it is freshly restarted and begins working with those latest update functionalities and features. Web update can be easily performed across internet-by a remote SUPERADMIN!

Advantages Galore

With Prima IP, the server administrator can access enterprise server room or data center on his own seat without toils and troubles of going anywhere from across the street to oversea. And organizations can enjoy a uniquely centralized and cost-effective control over its dispersed servers in different branch offices around the world, saving money for outsourcing costs.

1.1 Primary Features

General features

- 8/16-port IP-based Cascadable 19" Rackmount USB PS/2 KVM Switch w/ OSD
- Provides 1 Ethernet port for remote control over IP
- Port capacity scalable up to a maximum of 256 computers with cascaded configuration of other Prima KVM Switches (Prima 4/Prima 8/Prima 16)
- PS/2 local [analog] console for local rack server management
- USB and PS/2 Dual Interface Support on PC side
- Operation and channel selection by front-panel buttons, keyboard hotkeys, OSD menu and Viewer interface
- Dual numerical LED displays and LED port indicators for easy bank/port status monitoring
- Autoscan mode for quick browsing of all connected computers
- Serial port for external modem/remote power control device
- Multiple users can login in a same remote server desktop
- Total control over the remote server from BIOS level up to GUI applications
- Remote Power On/Off support
- Ultra-security using full 1024-bit PKI Authentication / 256-bit SSL encryption
- Work with LDAP / RADIUS / Active Directory Servers
- Ethernet 10/100 and serial PPP server and client connections

TCP/IP remote connection

- 256-bit SSL-encrypted Web Management Interface for all settings and upgrade / backup features

Thin-client Viewer Program

- Win-32 viewer and Java viewer for cross-platform compatibility
- Connection options configurable for optimized performance
- Shared, Non-Shared and View Only sessions
- Easy download and installation
- Multiple viewer instances can be run on a same client computer
- Options for Automatic video centering and optimization

Hi-Speed PPP Connection

- PPP Connection support over serial interface [RJ12] up to 1 Mbps
- PPP server enabling for PPP connection across a pair of modems for secure or backup direct access
- PPP client enabling for PPP connection to the internet with a modem

Video server

- Support up to 1600 x 1200 @ 60 Hz resolution
- 8/16-bit color
- 3 Video Quality settings
- 4 Video Compression schemes
- 8-bit color reduction
- Configurable database to set up new or unknown VGA modes
- Virtually compatible to any KVM Switch through automatic video quality optimization

Power ON-OFF Control Support

- Remote power ON-OFF control over serial interface
- Serial commands configurable to fit serial power control devices
- Power ON-OFF privilege only for the SUPERADMIN users

Security

- 1024-bit Public key Authentication using certificates generated by an external CA
- 256-bit SSL Encryption for keyboard, mouse and video signal transmissions
- Remote authentication support for LDAP or RADIUS servers
- RADIUS accounting support
- 3 SSL security levels :
    - No authentication – No encryption
    - Server Authentication – SSL encryption
    - Server & Client authentication – SSL encryption
- 3 password policies :
    - No Password
    - One global password for all users
    - One different password for each user

Alarms and Notifications

- Alert e-mail notification and SNMP trap messages for critical server events such as No Video, Blue Screen and NumLock Test Failure

User Management

- User login either by querying the local user database or by connection to remote LDAP or RADIUS server
- 3 user privileges :
    - SUPERADMIN – to access complete set of management features and user features, including Power ON-OFF remote servers
    - ADMIN – partial set of management and all user features
    - USER – only user features

User Group management

- Create specific user groups, each of which is assigned with privilege to access only those computers that are within that group

Global Time Zone Support

- Time support for all continents and major cities
- Time synchronization by connection to any NTP time servers
- Automatic Daylight Saving management

Maintenance and KVM management

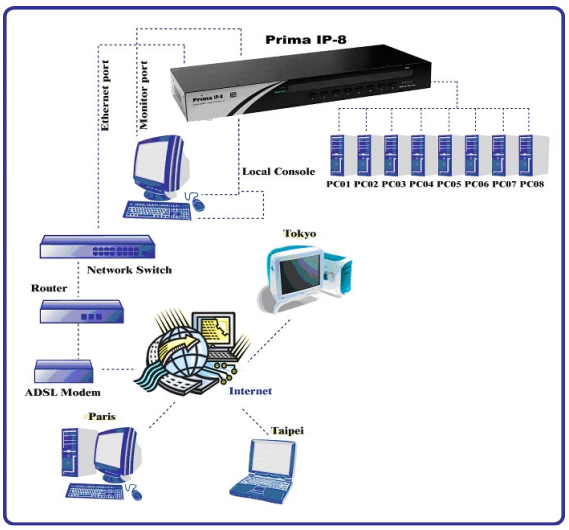
- Manages the software version of all KVM switches connected in the daisy-chain
- Upgrades automatically any KVM switch whose software is not the latest
- Record the error and information messages of all KVM switches in the daisy-chain within its server log
- Setup remotely the name of computers that are displayed in the OSD, the local user name and password

1.2 System Architecture

The Prima IP is based on an embedded Linux platform for computing power and rugged stability. The Prima IP employs a High speed Processor to ensure excellent video quality and fast keyboard / mouse response across the Internet, even when bandwidth availability is limited.

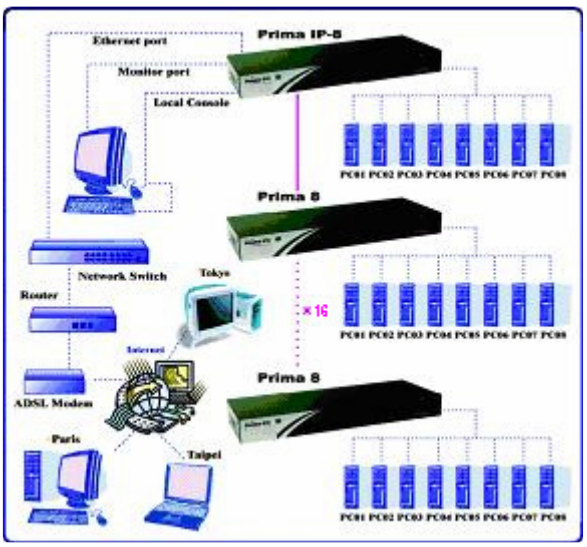
LAN/WAN Configurations

The Prima IP KVM switch enables local and remote access of the connected computers / servers behind anytime anywhere.



Prima IP KVM Switch - Basic Configuration

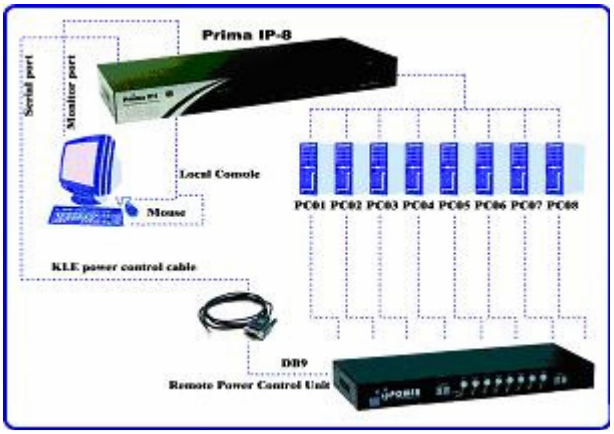
The Prima IP KVM switch can be daisy-chained with multiple Prima KVM switches (up to 16 units) to upscale port capacity up to hundred computers/servers.



Prima IP KVM switch daisy-chained with other Prima KVM Switches.

Power Control Configuration

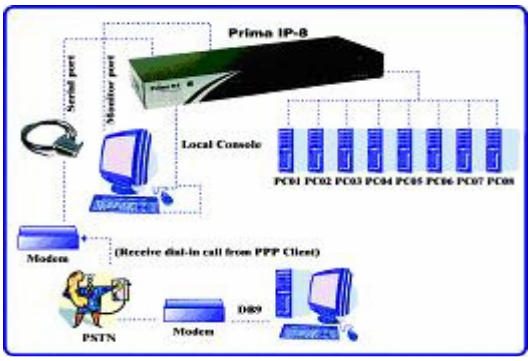
The Prima IP KVM switch supports Serial Power Control device to facilitate the remote Power ON/OFF and power cycling of the connected computers/servers.



Prima IP connected to a Remote Power Control Device

PPP connections

The Prima IP KVM switch can serve either as a PPP client or a PPP server to support PPP connection. The Prima IP offers a second backup connection over modem phone line in case the network is down.

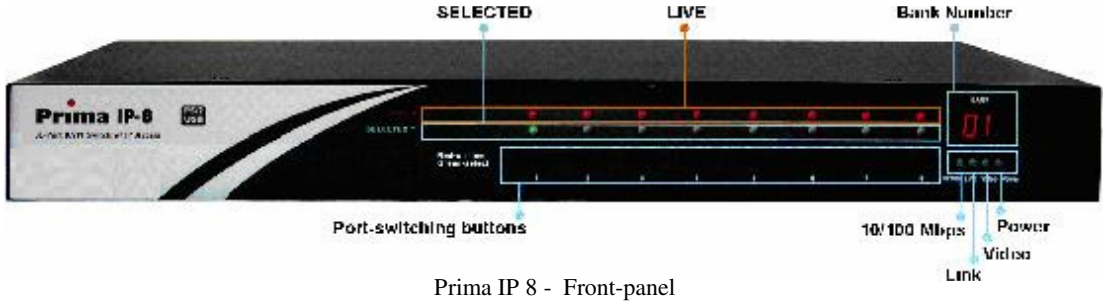


Prima IP as PPP server to accept dial-in request from a remote PPP client via modem line

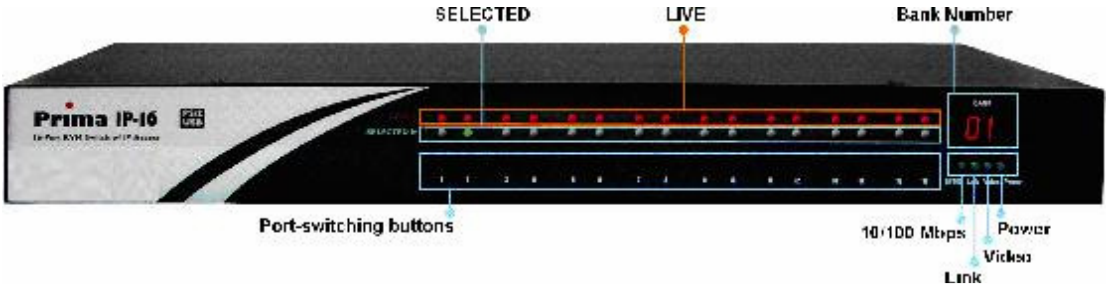
Prima IP as PPP client to dial-out to ISP for remote clients to access via internet

1.3 Prima IP External Views

Prima IP Front View



Prima IP 8 - Front-panel

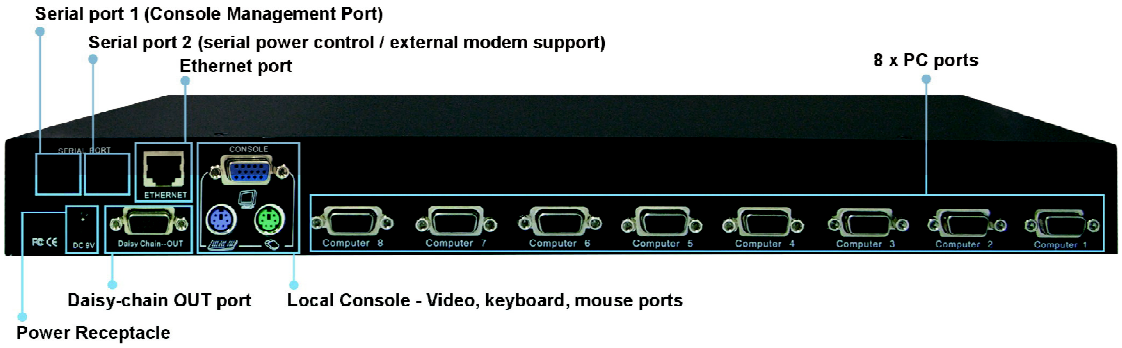


Prima IP 16 - Front-panel

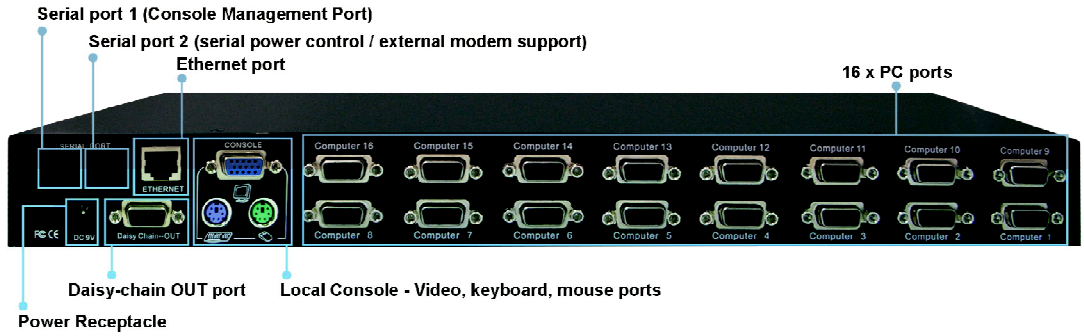
Status LEDs

The Dual Numerical LED shows bank number of the Prima IP KVM Switch within a Daisy-chain.
The *10/100Mbps* LED is lit as solid orange when the current digital link is running on 100Mbps speed.
The *Link/Act* LED gives off solid green light when a network link is established and flashes whenever network transmission are perceived on the digital port.
The *Power* LED indicates the Power On status when it is lit as solid red.
The *Video* LED indicates the normal functioning of video server when it is blinking orange.

Prima IP Rear View



Prima IP 8 - Rear-panel



Prima IP 16 - Rear-panel

8/16 x PC ports

The *PC port* is where you connect to your computer. The PC port is a HDB 15 connector integrated with USB and PS/2 keyboard, mouse and video. To connect PC port to one of your computer, you may either use USB-VGA KVM Combo Cable, or 3-in-1 USB PS/2 KVM Combo Cable, depending on your package option.

Local Console - PS/2 Keyboard port

This is where you connect the PS/2 keyboard for local console.

Local Console - PS/2 Mouse port

This is where you connect the PS/2 mouse for local console.

Local Console - Monitor Port (HDB-15)

This is where you should plug in the Monitor for your local console on Prima IP.

Ethernet Port (RJ-45)

The *Ethernet port* offers anytime anywhere access of Prima IP and subsequently the conventional KVM Switch(es) and servers/computers connected behind it to the remote login clients from LAN/Internet.

The Daisychain OUT Port (HDB-15)

The *Daisychain OUT port* is of a HDB 15 female connector, where you can daisy- chain downstream to a Prima KVM switch.

Serial Port 1 (RJ-12)

This is the so-called *Console Management port*, and it is where you connect the serial console cable for advanced console management of Prima IP unit via a serial terminal emulation utility such as Windows HyperTerminal or Minicom on Linux/Unix.

Serial Port 2 (RJ-12)

The *serial control port* allows you to connect to either an external modem or a power control unit or to a cascaded chain of power control units. When added with an external modem to its serial control port, Prima IP could serve either as a PPP server to allow direct cable connection or dial-in connection from its peer computers, or as a PPP client to dial-in to the ISP or an enterprise PPP server. Furthermore, through serial commands sent over its serial control port, Prima IP can perform remote power on/off and power cycling task via the (cascaded) power control module(s).

Prima IP Power Receptacle

You should use the DC9V 4A Adapter provided within the package. The center pin is of a positive polarity. Use of any other adapter will nullify the warranty.

Restore-to-Default Button

The *Restore-to-Default button* is a tiny recessed button located to the left of the Power Receptacle, and can only be accessed by prying down with a pointed needle tip. To depress the recessed button for over 5 seconds, and upon release, it will restore restore Prima IP to factory default – the default IP settings and user account settings that come with factory default.

2 PRIMA IP INTALLATION

Before installing the KVM switch, you should run through the following peripheral checklist to ensure a proper setup of your KVM Switch….

2.1 Checklist Before Installation

- Suitable KVM cables to connect the Prima IP KVM Switch to the keyboard, video and mouse ports of each of your PC. For each USB style (or PS/2 style) computer connected, you should have the USB-VGA KVM Combo Cable (all male), or the 3-in-1 USB PS/2 KVM Combo Cable. The 3-in-1 USB PS/2 KVM Combo Cable is highly recommended for your convenience.
- A monitor with a standard D-sub 15-pin video connector (HDB-15) that you have verified to be working when connected directly to each of your PCs.
- A standard PS/2 or USB style Microsoft or Logitech keyboard.
- A standard PS/2 or USB style Microsoft or Logitech compatible 5-key mouse.
- Daisy-chain cable(s), necessary only if you need to connect to other Prima KVM Switch (Prima 4/Prima 8/Prima 16).
- Terminator, necessary only if you need to daisy-chain multiple Prima KVM Switches.

Figure 2-1 The USB-VGA KVM Combo Cable

Figure 2-2 The 3-in-1 USB PS/2 KVM Combo Cable

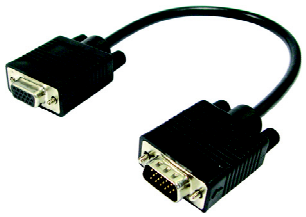


Figure 2-3 The Daisy-chain Cable [M-HDB15-to-HDB15-F]

Figure 2-4 The [Daisy-chain] Terminator

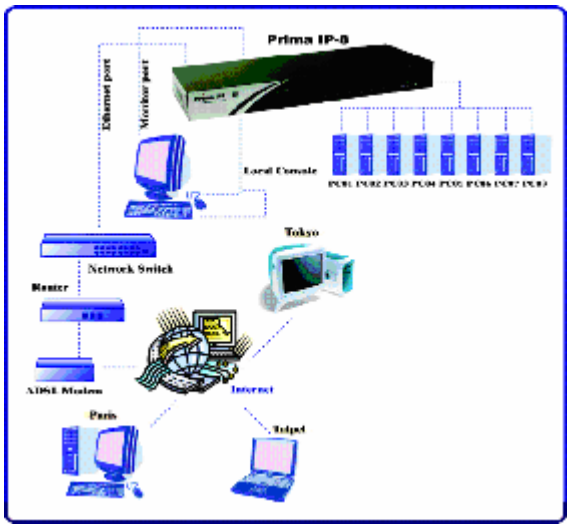
2.2 Set Up The Physical Connections

Step 1. Power on the Prima IP: Connect the Prima IP Power adapter to power on the Prima IP KVM Switch.

Step 2. Set up a local console on Prima IP: If a local console (that is a physical keyboard, mouse and monitor connected to the Prima IP) is required, connect a keyboard and mouse to the Prima IP local console ports (that is keyboard, mouse and monitor port specifically).

Step 3. Connect to computers: If you have no intention to daisy-chain your Prima IP KVM switch with either of the Prima KVM switches (Prima 4/Prima 8/Prima 16).You just connect each PC port to a computer, using the USB-VGA KVM Combo Cable , or the 3-in-1 USB PS/2 KVM Combo Cable.

If you are using any PS/2 computer: Please make sure all of your PS/2 computers are powered off before connecting to the KVM Switch. Otherwise, the non-PnP PS/2 interfaces might not recognize the PS/2 keyboard and mouse later. However, USB computers do not have this limitation.



Prima IP configuration – Single server mode

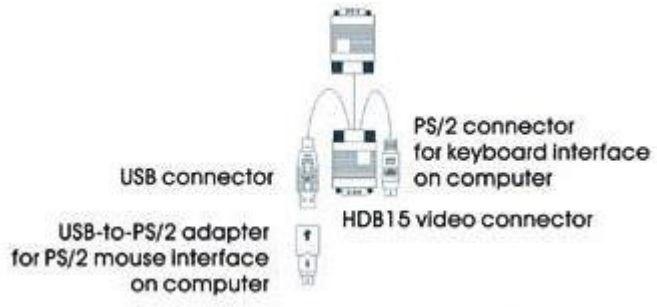
3.1 Make sure (at least the PS/2) computers that are to be connected to the KVM switch are powered off. If not, power them off before you proceed with the following steps.

If you use only one single Prima IP KVM switch in non-cascaded application, you should ignore step 3.2, 3.3, and 3.4 then jump directly to step 4.

If you want to daisy-chain multiple Prima KVM Switches to the [master] Prima IP KVM switch, go to step 3.2. You can daisy-chain up to 16 levels of KVM Switches.

3.2 Use the daisy-chain cable (M-HDB15-HDB15-F) to connect the DaisyChain Out Port (HDB 15 female) of the [master] Prima IP KVM Switch to the DaisyChain IN Port (HDB 15 male) of the second Prima KVM switch. Then connect the power adapter cord to the second Prima KVM switch to power it on.

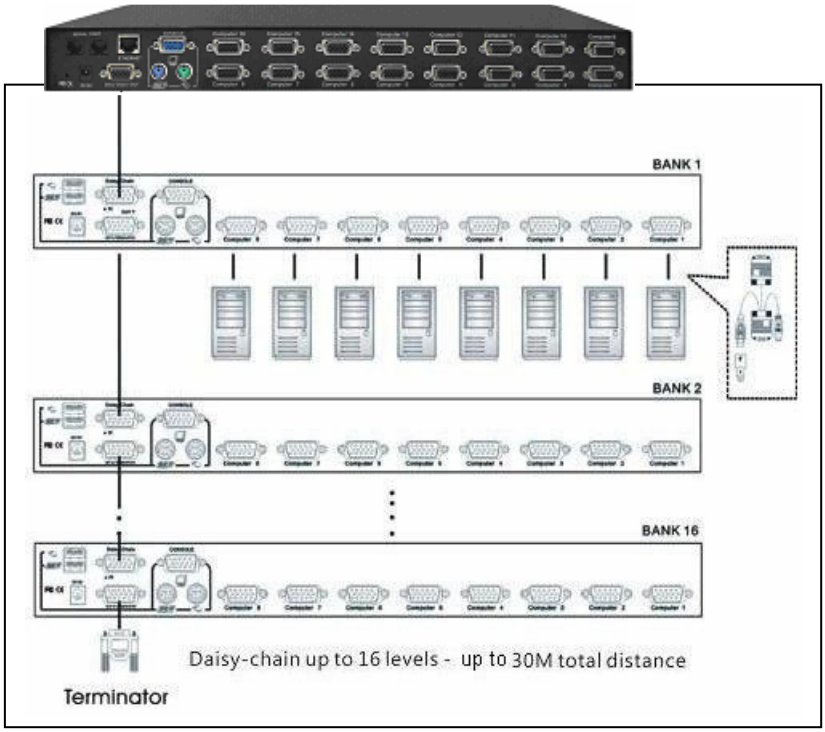
3.3 If you have yet another switch to be daisy-chained, just repeat step 3.2 to connect them. You can daisy-chain up to 16 units. Remember to plug a Terminator onto the Daisy-chain Out Port of the last Prima KVM switch unit.



The 3-in-1 USB PS/2 KVM Combo Cable

3.4 (Now your Prima IP KVM switch, and those Prima KVM Switches daisy-chained below should have been powered-up and initialized….) Connect each computer to a PC port on the backpanel of the KVM switch(es). You should use the special USB-VGA KVM Combo Cable (3-in-1 USB PS/2 KVM Combo Cable with the USB-to-PS/2 adapter) for connection to a USB computer (PS/2 computer). (Other types of cables may be used accordingly.)

The special 3-in-1 USB PS/2 KVM Combo Cable provides a PS/2 keyboard connector, a USB connector and a HDB video connector for the computer connection. When connecting with a USB computer, just plug the USB connector to it and leave the PS/2 connector free. When connecting with a PS/2 computer, just add a USB-to-PS/2 adapter to the USB connector and you'll have a PS/2 connector for mouse. **DO NOT try to connect both USB connector and PS/2 keyboard connector to a computer at the same time.**



Step 4. Boot up connected computers (if they are not powered-on yet): After the computers has booted. Then, you can go forth to verify the connections with each of the connected computers. On the Prima local console you should switch to every computer and verify that the keyboard, mouse and monitor are all working on each of the connected server(s).

Now that you have set up your local console on Prima IP, you can now configure your connected servers just by using the ready access provided by Prima IP's local console.

2.3 Configure Your Servers For Connections To Prima IP

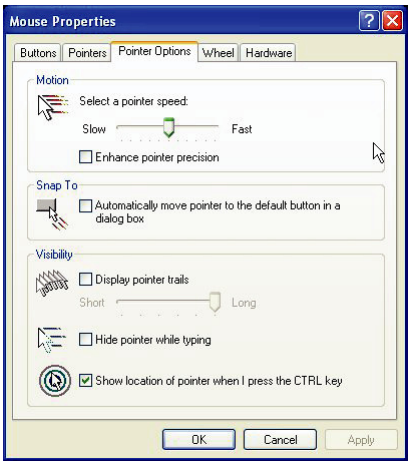
Mouse acceleration is not supported in Prima IP. Therefore, you must turn off mous acceleration on all your connected servers.

Turn off mouse acceleration and "Snap to" option

Windows XP Platform

Access *Control Panel/Mouse*. On the *Mouse Properties* tab, select the *Pointer Options* page :

1. Adjust the pointer speed slide bar to the exact middle.
2. Uncheck the *Enhance pointer precision* option.
3. Uncheck the *Automatically move pointer to the default button in dialog box.*

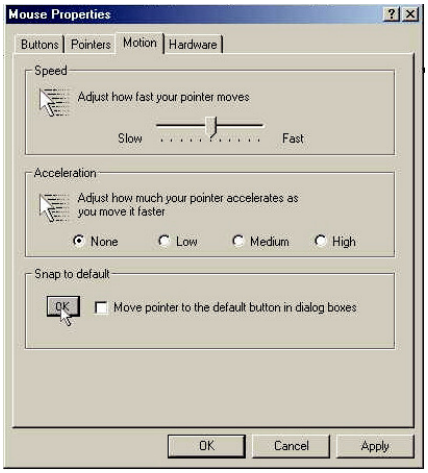


Click *OK.*

Windows 2000 Platform

Access *Control Panel/Mouse*. On the *Mouse Properties* tab, select the *Pointer Options* page :

1. Adjust the pointer speed slide bar to the exact middle.
2. Select the Acceleration as *None.*
3. Uncheck the *Move pointer to the default button in dialog box.*

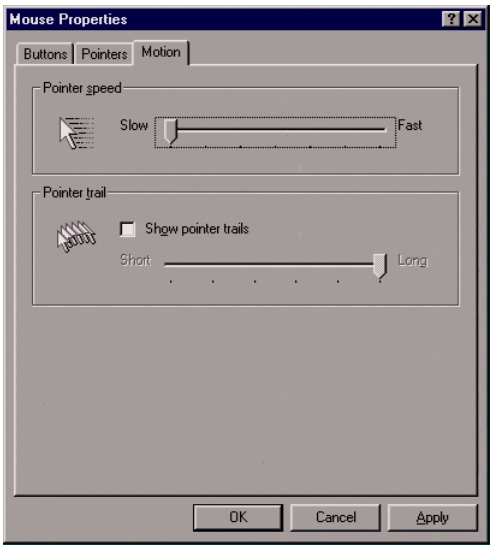


Click *OK.*

Windows 98

Access *Control Panel/Mouse*. On the *Mouse Properties* tab, select the *Motion* page. Under the *Pointer Speed* category:

1. Adjust the pointer speed slide bar to the slowest (leftmost) position.



Click *OK*.

The mouse setting page on different Windows platforms might be quite different, some gives mouse acceleration option and some don't. If you see any mouse acceleration option, please uncheck it. If there is no mouse acceleration available on the setting page, you can adjust the mouse speed slide bar to either x1 or the slowest position (such as on Linux platforms). But sometimes, it requires a middle position on the speed slide bar to make mouse synchronization on the viewer side, for example, Windows XP requires a middle position on mouse speed. Anyway, the worst case is that you have to make some trial and error to make your mouse acceleration off and the speed as x 1 (could be at the slowest position or the middle position).

2.4 More Tips For Server Desktop Configuration

There are several aspects that have to be taken into consideration and maybe configured on your computers or servers for best performance:

(1) Resolution modes should refrain from too much peculiarity and better adopt ones that are within Prima IP's standard support.

(2) Turn off the Menu special transition effects on your operating system (especially on Windows XP, if you are using any) such as *fade* for best video refreshing effect, especially when you are using Medium or Low Video Quality as your video filter setting on Prima IP.

(3) Adjust the server desktop backgrounds as containing preferably plain, solid colors with simple designs (only for improving video refreshing speed when bandwidth is critically limited. No need to do so when bandwidth is ample).

Configure display resolution on your server

Prima IP supports most display modes up to 1600 x 1200. However, you might encounter some display problems when your display card is outputting an unusual display mode. These possible problems are either no video or abnormal display on viewer screen.

To simplify the display factor before connection to Prima IP, we suggest you use more standard display modes such as: 800 x 600 @ 60Hz/75Hz, 1024 x 768 @ 60Hz/70Hz, etc. For the suggested display modes, please refer to the following table.

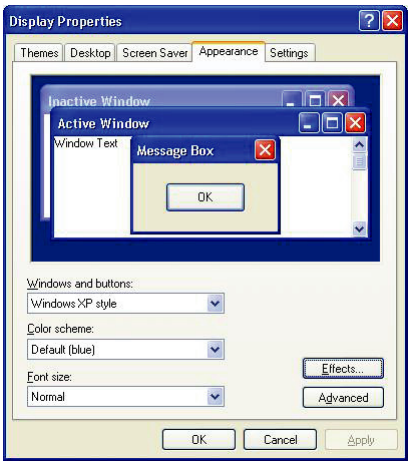
	640 x 400	640 x 480	800 x 600	1024 x 768	1152 x 864	1280 x 1024	1600 x 1200
56Hz							
60Hz		✓	✓	✓	✓	✓	✓
61Hz							
64Hz							
70Hz	✓			✓	✓	✓	✓
72Hz		✓	✓				
74Hz							
75Hz		✓	✓	✓			
76Hz				✓			
78Hz					✓		
84Hz							
85Hz	✓	✓	✓	✓			
100Hz		✓	✓	✓		✓	

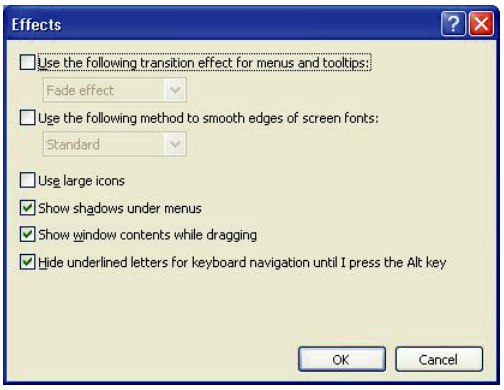
Note: These are suggested display modes for server desktop-connected Prima IP. However, the actual display modes for as specific server desktop will be dependent on its display card. Some display modes listed here might not be feasible with some display card. Try to do some trials to determine the best display mode for your desktop on Prima IP viewer.

Disable special transition effects on the screen outputs of your connected servers

Go to *Control Panel / Display / Appearance / Effects*. And then uncheck the option to disable transition effects such as *Fade* for the menus and tool tips. You should perform the same check on each of your connected servers.

On Windows platforms such as Windows 98, 2000, XP and 2003 Server, some transition effects might yield undesirable video refreshing artifacts, especially when you are using Medium or Low Video Quality as your video filter settings. To avoid undesirable artifacts from appearing on your screen, please turn off the special transition effects.





Choose plain and solid server desktop backgrounds for your connected servers

To optimize the bandwidth efficiency and speed up video performance across bandwidth-limited environment, one should preferably adopt a server desktop which should be as plain as a color background with a solid and light-colored graphics. Complex patterns or color gradients should be avoided, if bandwidth is critical in your application, since they will create more bandwidth demands for their transmission across internet.

2.5 Configure IP Address And Port Base

Step 1. Connect your Prima IP to the Ethernet LAN.

The factory default network settings for Prima IP are as follows:

IP address : 192.168.1.200
Net mask : 255.255.255.0
Gateway : 192.168.1.254
DNS : 192.168.1.254

Step 2. Access Prima IP Web Browser Management interface by typing the following in the address box of your browser window on a remote client:

https://192.168.1.200:5908

Step 3. A login screen will ask you for the account name and password. Use the default account and password:

```
User Name   : superuser
Password    : superu
```

After log in, you will see the Prima IP Web Browser Management Interface.

Step 4. Go to the Main / LAN TCPIP page on the Prima IP Browser Management Interface and modify the IP address and port base for your Prima IP KVM switch. For example, if you choose your IP setting for the Prima to be 192.168.1.210 with a port base of 5900. Refer to *Section 4.5, Main / TCP/IP Settings – Port and IP Settings.*

Step 5. Apply the new setting by clicking *Apply Settings*.

Step 6. Verify Prima IP's network connection.
Connect to Prima IP by Web Management Interface using the new IP address.
Note that the IP address should be followed immediately by a colon and the port base +8 for port number.

https://<IP_address>:<PortBase+8>.

For example, if the IP address is 192.168.1.210 and the port base number is 5970, then you should enter

https://192.168.1.210:5978

Remember that it's a secure SSL encrypted connection, so you should type "https" instead of the usual "http". Otherwise, the connection will not be established.
If you are satisfied with the default port base setting as 5900, you can leave the port base unmodified.

The default port base for Prima IP connection is set at 5900. This means it will use port 5900 (port base) for viewer connection and port 5908 (port base + 8) for https web browser connection.

<Port base> – used for viewer connection
<Port base + 8> – used for secure browser connection

However, if you intend to use your own port base setting, just access the Web Management interface and configure the port base.
For example, if you choose 5970 as your port base, then you have:

5970 – used for viewer connection
5978 – used for secure browser connection

Click *Submit* button and *Apply Settings* button to validate your new setting.

Now you have installed Prima IP within your Local Area Network environment, and can try to establish a remote viewer connection…

2.6 Configure Your Firewall/Router For Accessing Prima IP Across Internet

To allow access to the Prima IP behind corporate firewall/router, please configure the following settings on your firewall/router (not on your Prima IP):

Step 1. Configure a virtual server on your router: you should configure (or ask your network administrator to configure for you) a virtual server as mapped to the Prima IP local IP address.

Step 2. Open a port range (<port_base> ~ <port_base+9>) both inbound and outbound for the virtual server: you should open a port range according to what you have configured as port base for Prima IP previously.
Taking previous example, if you configure Prima IP as having a port base of 5970, then you should open port range 5970~5979 (that is, <port_base> ~ <port_base +9>) both for inbound and outbound, in which,

<port_base> = 5970 is the Prima IP viewer connection port
. . . . . .
<port_base + 8> = 5978 is the browser SSL connection port
<port_base + 9> = 5979 is for viewer internal communication, etc.

For example:
Router internet IP ⇦⇨ virtual server (port range open) ⇦⇨ Prima IP local IP
61.232.134.120 ⇦⇨ virtual server (port 5970~5979 open) ⇦⇨ 192.168.1.7

Once you haved configure a virtual server with appropriate port range open (**<port_base> ~ <port_base_+_9>**), you can then try to access your Prima IP across internet by using the public IP address and designated port number. For example, in this case,

Browser access: https:// 61.232.134.120:5978
Viewer access: 61.232.134.120:5970

If you have domain name mapping to the public IP address, you can also use the domain name, for example:

Browser access: https:// www.mycompany.com:5978
Viewer access: www.mycompany.com:5970


Once you have changed the port base of your Prima IP, you should also modify the open port range on your router accordingly, if you want internet access to come across.

2.7 Install Certificates On Prima IP

You could use the default set of certificates (could be found on CD-ROM) to practice making some PKI - authenticated connections as long as your network safety is not jeopardized. We advise that it is better to do the practices within your Local Area Network, which is supposed to be well secured with adequate firewall and other due precautions against network intrusions. Or if you have already obtained a set of certificates with the file names and formats required by Prima IP, you can then use them for Prima IP viewer authentication. However, if you simply use the default set of certificates that comes with Prima IP, anybody who has a copy of the default certificates may establish a connection to your servers. . So we strongly recommend that you obtain your own certificates for Prima IP or go forth to generate them using software like XCA ….. For certificate generation using XCA, please refer to How to Generate Prima IP Certificates using XCA (could be found on the Prima IP support CD-ROM).

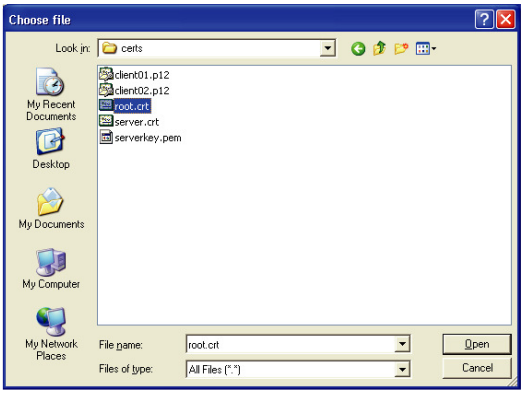
First you have to have these certificates ready on your client computers for uploading to Prima IP via a Web browser. If you haven't obtained your own Prima IP certificates, you can use the default set of certificates (could be found on the Prima IP support CD-ROM).

Certificates for the PKI Authentication to be installed on Prima IP:
(1) the root certificate (root.crt)
(2) the server certificate (server.crt), and
(3) the server private key (serverkey.pem)

Certificates for the LDAP Authentication to be installed on Prima IP:
(1) the LDAP certificate (ldapcert.crt)
(2) the LDAP private key (ldapkey.pem)

Step 1: Access Prima IP Web Management Interface and go to the Security page.

Step 2: Click the *Browse* Button and use the *Choose File* dialog box to browse to your certificate files ….



Step 3. Click UPLOAD button to upload the root certificate to Prima IP. After the uploading is completed, you can then see the prompt page for reboot.

Click *Reboot* and wait till Prima IP is booted up, then likewise try to import the *server.crt* and the *serverkey.pem*.

The certificate and key for LDAP authentication could be uploaded likewise.

You don't have to reboot each time when you finish uploading one certificate. You could do one complete reboot at the end when you finish uploading all of them. To return to the previous Security page for uploading another certificate without going to immediate reboot, you just click the *Security* page hyperlink on the left frame of the browser window.

2.8 Select A Security Level For Viewer Connection

Step 1. Go to the *Security* page on the Prima IP Web management interface and select a viewer connection security level.
There are three security levels for choice:

- Level 1: No encryption (No SSL)
- Level 2: 256-bit encryption, no user certificate required for user authentication
- Level 3: 256-bit encryption, user certificate required for authentication (PKI)

Security level 1 offers a non-secured connection, and hence should be used with caution when Prima IP is intended to be accessed through external network. For level 1, there's virtually no encryption.
Security Level 2 offers a secured SSL connection that provides encryption for mouse, keyboard and video but uses no PKI-authentication.
Security Level 3 offers a secured SSL connection that provides encryption for mouse, keyboard and video, and uses 1024-bit PKI-authentication.

The choice of a security level to be implemented for the Prima IP viewer connection is of most importance, especially when your remote server connections requires a high security that can keep your servers safe from unauthorized entries and/or network sniffers.

Step 1-a. If you choose to implement PKI authentication feature on Prima IP viewer, you have to select Level 3 viewer security connection on the Security page of your Prima IP browser interface.

Here you should enter the password that has encrypted the *server private key* in the server private key file, *serverkey.pem*. You should enter the correct server password here in order to make successful viewer connection with Prima IP in level 3 security setting. If you use the standard set of certificates provided on the Support CD ROM disc, the password that encrypts the server private key is **serverpwd**

However, if you use your own set of certificates, you should get the correct server password from the Certificate Authority that issues those certificates.

Step 2. Go to the *Apply Setting* page and hit the *Apply Setting* button to validate your selection.

2.9 Select A User Password Policy

Step 1. Select a User Password Policy.
Prima IP offers three types of password policies On the drop-down combo box, you can select your password policy for viewer connections:

- **No Password**
- **Global Password**
- **User Password**

No Password – the viewer will prompt you for no password. Anyone who is with the viewer and passes the security level check of the viewer could well establish the connection.

Global Password – the viewer will prompt you for a global password, which is used by all who want to make viewer connections to Prima IP.

User Password – the viewer will prompt you with user-specific password. With this setting, each login user will be checked against his or her corresponding password before allowing viewer connection.

Global user password : If you adopt the Global Password Policy. Here you should enter the password that is used when the global user password setting is enabled as your active password policy.

Step 2. Go to the *Apply Setting* page and hit the *Apply Setting* button to validate your selection.

 There are altogether nine (3 x 3) possible combinations of Viewer Security Levels + Password Policies that are available for a flexibility to adapt to your security needs. The administrator can choose an optimized combination of user password policy and the SSL / PKI Authentication according to his security/convenience concern.

	User Password Policy			
SSL / PKI Authentication		No password	Global Password	User-specific Password
	No SSL-No PKI	N – N – N	G – N – N	U – N - N
	SSL – No PKI	N – S – N	G – S – N	U – S - N
	SSL - PKI	N – S – P	G – S – P	U – S - P

G – Global Password
S – 256-bit SSL Encryption
P – 1024-bit PKI Authentication
N – Not available
U – User-specific Password

 Please note: Either Password Policy or Security Level (SSL/PKI authentication) settings should be used with due precaution: If you adopts No Password Policy and No SSL encryption/No SSL authentication, anyone with a viewer and knowledge of the access IP and port number of Prima IP can establish a remote connection.

Now your Prima IP is ready for a PKI-authenticated plus SSL-encrypted viewer connection! All you have to do is to distribute the followings to you remote connection client:

1. Certifidcates: as you have obtained from your CA (Certification Authority). They are required only if you select level 3 viewer security.

   root.crt
   client_name.p12.
   (client_name is freely chosen)

2. Certificate password: as you have obtained from your CA. It is required only if you select level 3 viewer security.

   clientpwd
   (if you use the default set of certificate provided on Prima IP CD-ROM)

3. User account and password: as you have specified in the User Management page. It is required only if you choose User Password policy.

   Superuser / superu
   Admin / 123456
   User / 123456
   (if you use the default user accounts/passwords)

4. Global Password: as you have specified in the Security Page. It is required only if you use the Global Password Policy.
   (you will be prompted when choosing it as your password policy on the Security Page)

3 MAKING A VIEWER CONNECTION

The Prima IP provides a win32 viewer for Windows clients and a Java viewer for cross-platform on any major operating systems.

3.1 Install Win32 Viewer On The Client Computer

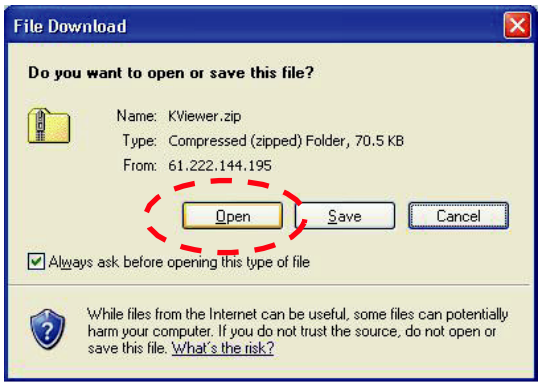
Go to the *Download* page to download the Win32 viewer, *Kripview_install.exe.* Install the viewer program on the client computer that will connect to Prima IP. After installation, a desktop icon will be created on your client desktop.

3.2 Install Java Viewer On The Client Computer

Before you can use the java viewer, *KViewer.jar*, on any OS platform, you should first install the Java Runtime Environment, JRE 1.5.0 or higher, which is downloadable from http://www.java.com.

To download Java Viewer, just go to the Download page of the Web Managemen interface.

After all, to run the small java program, you don't have to actually save the Kviewer.jar to your local hard disk, since it is small (only 70 KB), you can choose to open it directly while download is completed.



On some client platforms such as Linux, after you have installed the JRE on your client platform, you have to set the path information in order for the client system to know where the Java compiler program is.

3.3 Import Certificates To Prima IP Viewer On The Client Computer

If you will be using only the non-PKI authenticated viewer connections to Prima IP (such as Level 1 – No encryption and No Authentication, and Level 2 – 256-bit SSL encryption and only server authentication by client), you are not obliged to use or import any certificates. If so you can skip this section and proceed to the next.

To make full PKI authenticated viewer connection with Prima IP, you need to import client certificates to the Win32 viewer and Java Viewer on the client computer.

The **Prima IP** is already preinstalled with a default set of certificates. You can use the default client certificates provided on CD ROM. However, it also allows you to use your own set of certificates.

Note that if you intend to use your own set of certificates instead of the default set of certificates, you should not only import the client certificates to the win32 viewer/java viewer on remote client computer, but you should also import the root certificate, server certificate and the server private key to the Prima IP. To import certificates to the Prima IP, please go to the Security page of the Prima IP Web Management to upload your own set of certificates. For details, please refer to Section 4.4, Main/Security – Certificate Installation, Viewer Encryption and Password Policies.

Generally, the naming requirements of these certificates are as follows:

[Certificates and private key for Prima IP to authenticate viewer user logins]

root.crt - Prima IP root certificate, mandatory file name
server.crt - Prima IP server certificate, mandatory file name
serverkey.pem - Prima IP server private key, mandatory file name

[Certificates for remote login users with viewer connections]

client_name1.p12 - client certificate, client name could vary
client_name2.p12 - client certificate, client name could vary

Specifically, we should import client certificate(s) in *.p12* format, to the win32 viewer and Java Viewer on your client computer, using each of their own certificate import utilities.

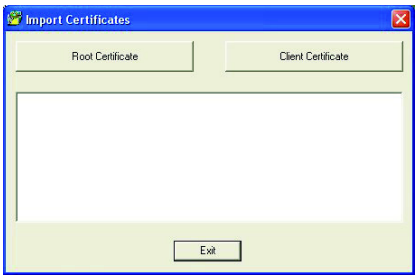
First, you have to have your certificates ready, either on a removable media or you can copy them to your local disk on the client computer.

Note that if you copy certificates to your local hard disk, you might need to delete them from your local hard disk after finishing importation, so that others won't have access to your certificate files. Although the personal client certificate (that is, the client_name1.p12) is password-protected, more caution is never to blame!

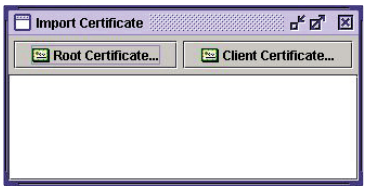
Note that the win32 viewer and the java viewer require separate certificate importation utility to get the job done.

Import Client Certificate To Win32 Viewer

Run the importation utility by accessing *Start / Programs / PROSUM / Prima IP Viewer / Import Certificates*. Click *Root Certificate* to import root certificate and then click *Client Certificate* to import client certificate.



Import The Certificates For The Java-based Prima IP Viewer



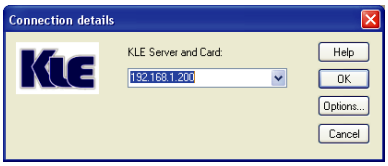
Now you have imported certificates to the viewers on the client computer and are now ready for making a viewer connection of any security level setting ….

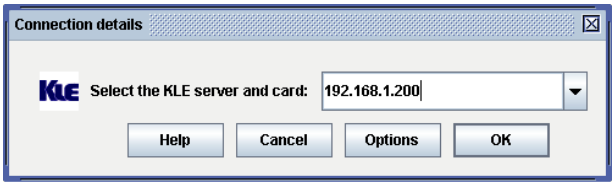
3.4 Specify The Viewer Connection Option Before Making A Connection

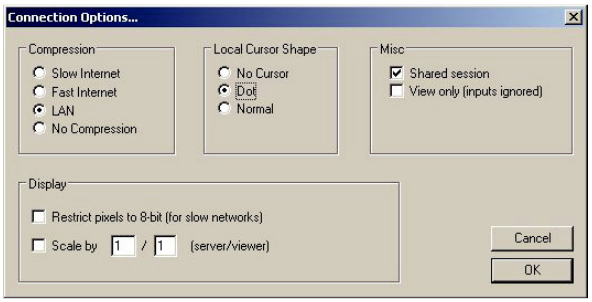
The viewer connection option interface provides you with several alternative options to use in combination for optimization of your viewer connection.

Connection details box

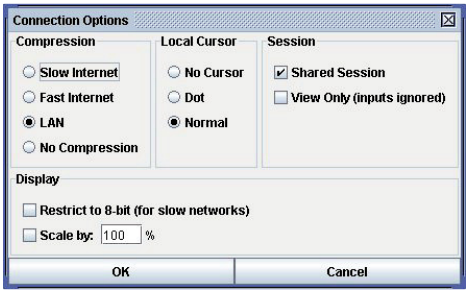
Click the *Options* button on the *Connection Details* dialog box.







Win32 Viewer



Java Viewer

Setting connection options

Encoding

Slow Internet: Video quality is optimized for viewer connection with slower internet bandwidth.
Fast Internet: Video quality is optimized for viewer connection with better internet bandwidth.
LAN: High Video Quality for viewer connection over LAN.
No Compression: Best Video Quality with no compression.

Local Cursor Shape

No cursor: local cursor invisible on Prima IP Viewer.
Dot: dot shape for local cursor on Prima IP Viewer.
Normal: arrow shape for local cursor on Prima IP Viewer.

Misc

Shared Session: multiple users access same server desktop.
View Only (inputs ignored): Keyboard and mouse inputs are ignored (not restricting keyboard and mouse access on other users).

Display

Restrict pixels to 8-bit (for slow networks): color reduction to 256 colors for slow connection.

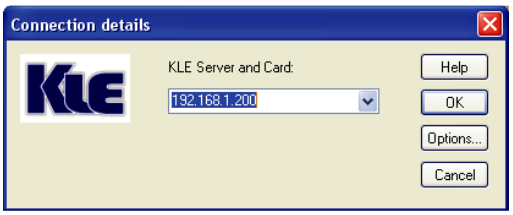
Scale x/y (server/viewer): Scale the display output on viewer (not affecting the actual transmission bandwidth).

3.5 Establish The Viewer Connection

Using Win32 Prima IP Viewer for Connection

First, run the viewer program, enter the access IP and port number for Prima IP.

Default IP address: 192.168.1.200



Login dialog box (Win32 Viewer)

At the password or private path phrase prompt, just enter the user name and password as required:

Default user & specific password:
User : superuser
Password : superu

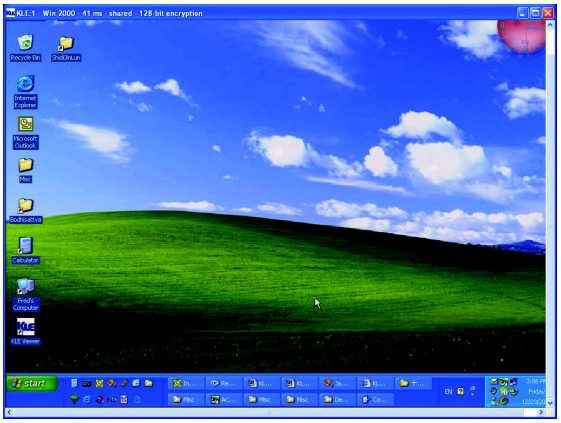
Or, if you are using the Global Password policy setting …

Default global password: 123456

Or, if you are using the Level 3 security setting that requires installation of certificates for PKI authentication (For details, please refer to Section 3.3, Import certificates to Prima IP Viewer on the client Computer, and Section 4.4, Main/Security –Certificates Installation, Viewer Encryption and Password Policies.)

Default private path phrase: clientpwd

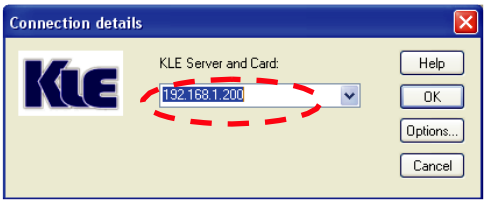
After you have entered either the global password, user name and password, or private path phrase as its security and password policy require, a viewer connection will be established successfully.



Some Tips About Viewer Connection

If you want to specify the type of your viewer connection rather than using the default one, you can click the Options button and optimize your connection parameters. Please refer to previous section for details.

Note that you can simply type in the access IP of Prima IP server without specifying its port number only when the port number is default to 5900




```
IP_address [only if port number is default to 5900]
192.168.1.200
```

Of course, you can always type

```
IP_address:port_number
192.168.1.200:5900
```

However, if the port setting on Prima IP is already changed to other port number, you have to specify its specific port number following the IP address. For example, if you want to connect to port 5910 on the Prima IP server, type, for example:

```
192.168.1.8:5910
```

To configure the port base number, please refer to Section,4.5., Main/LAN TCP/IP – Port and IP Settings.

Connection Performance Tuning

However, if you are using a dial-up modem line and experiencing slow keyboard mouse movement and response, you might check whether you are using the default LAN encoding scheme or even the No Compression scheme, which requires much more packet quantity in transmitting a video frame; or there is a network bottleneck somewhere in between Prima IP and your client desktop. For more details, please refer to *Section 3.13 , Common Video Display Problem Troubleshooting*.

3.6 Mouse Cursors Synchronization

Normally, you will see both the local cursor and the remote cursor on the view area. You can specify the shape of the local cursor as seen within the Viewer Window either as a dot, an arrow or none (not showing any local cursor within the viewer area). Also if these two cursors become out of sync, all you need to do is to hit default the mouse synchronization hotkey *(right) Ctrl – (right) Ctrl – Home* to synchronize the two cursors.

Mouse cursors out of sync

Mouse cursors in Sync

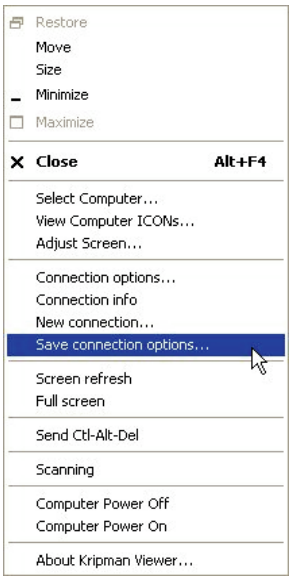
Local / remote mouse cursor resynchronization hotkey - RCtrl-RCtrl-Home

Note that, while operating your mouse, it is not necessary to wait till the remote cursor has actually caught up with the local one before you can click on the target in the view area. Actually, you can click the target just using the local cursor well before your remote cursor catches up the target!

3.7 Save The Connection Options

After you have optimized you connection options, you might want to save the connection options. Next time when you log in with the Prima IP viewer to Prima IP server, the viewer on that specific client computer will use the stored connection parameters as well as the password (but not the private path phrase, which is not saved since it is used by secured/PKI-authenticated connection) for connection with Prima IP.

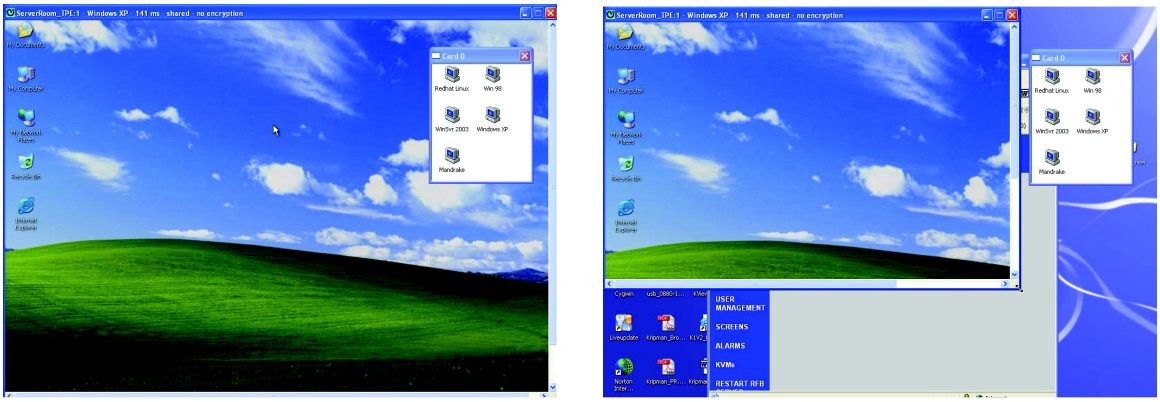
To save connection options, click the Prima IP icon on the Viewer title bar to call forth the Viewer Quick Menu and select *Save the connection options*.



Prima IP Viewer Quick Menu (Win32 viewer)

3.8 Win32 Viewer Characteristics

Adjust The Window Size



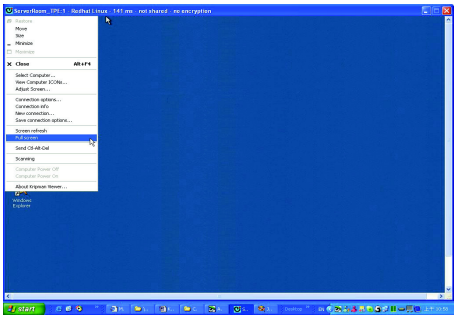
Viewer Window with scroll bars (Win32 viewer)

The size of the Prima IP viewer window can be adjusted by dragging the border of the viewer windows.

Change The Viewer Size To Full Screen Mode

Note that only the win32 viewer supports full screen mode. The java viewer does not support full screen mode.

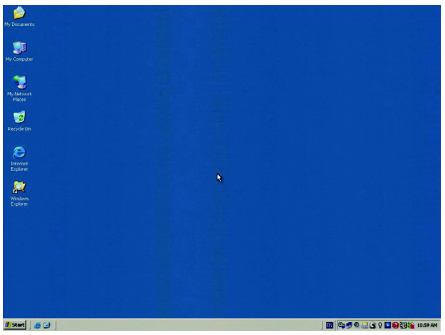
Click the Prima IP viewer icon on the title bar of the viewer window to evoke the *Quick Menu*. Select the *Full Screen* option on the *Quick Menu.*



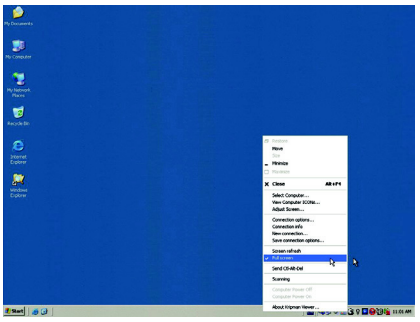
A message box will appear to remind you how to exit the full screen mode:

Full screen prompt – Ctrl – Esc to return to normal mode

Click *OK*, and the viewer goes to full screen mode.

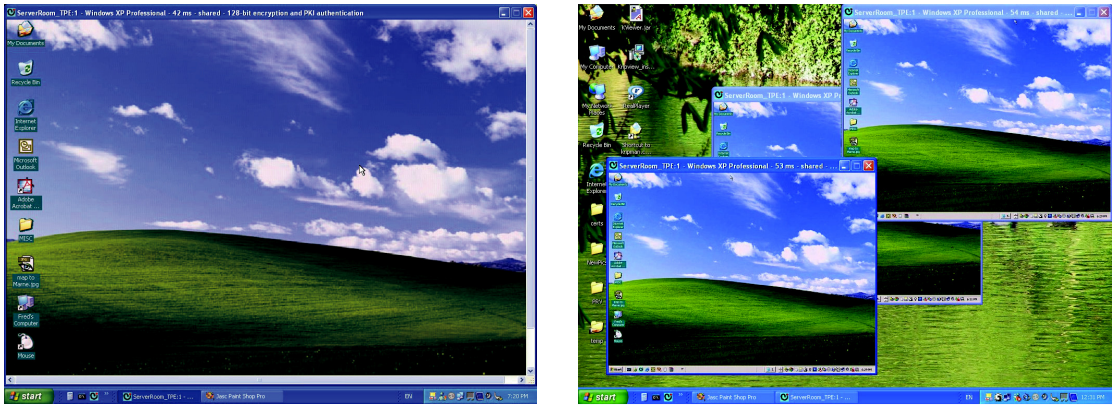


To exit the full-screen mode, just hit Ctrl-Esc to bring up the local task bar. Right-click the viewer taskbar icon to bring up Quick Menu, then click to deselect the full screen mode to restore it to window mode.



Scale The Window Size Of Your Viewer

Click the Prima IP viewer icon on the title bar of the viewer window to evoke the Quick Menu. Select *Connection options* on the Quick Menu.

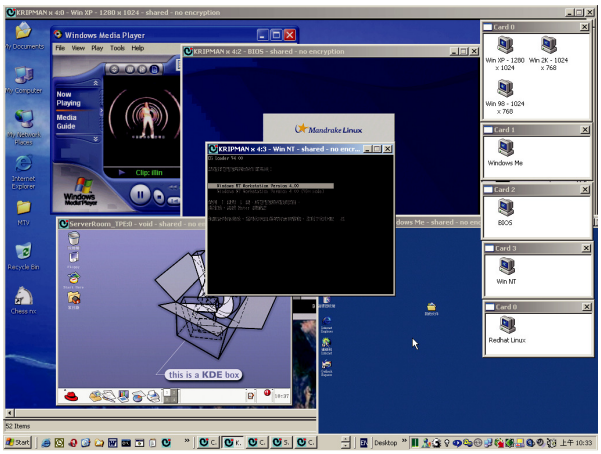


Scale the viewer window to ½ size

On the *Connection Options* dialog box, specify the preferred proportions of the viewer window, for example: ½, and then check the option. Click *OK* to scale the window to half size.

Centralize your remote servers control

If you have multiple Prima IP units installed in a distributed manner among your global branch offices, you can then simultaneously monitor different remote servers distributed over this IP KVM Link Extender infrastructure on a single client desktop.

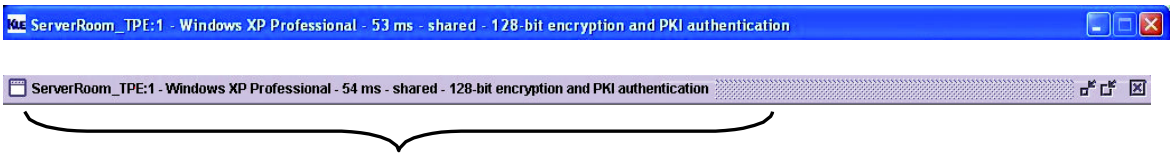


Five Win32 viewers on a Windows client desktop
(each showing one different remote server desktop)

Four Java Viewers on a Linux client desktop
(each showing one different remote server desktop)

3.9 Title Bar Information

ServerRoom_TPE: This is the name you specified for your Video Server.
Window XP Professional: This is the name you specified for this connected computer.
53 ms: This is the capture time that is used for capturing the video image.
Shared: This is a shared session that allows other authorized user logins.
OPTIMISING: This indicates that the Prima IP video server is optimizing the video capture from the server desktop.
Not shared: This indicates a non-shared session that blocks others from subsequent logins.
No Encryption: This indicates no encryption for signal transmission (Level 1).
256-bit encryption: The current viewer session is using 256-bit SSL connection (Level 2 and 3).
PKI Authentication: The current viewer session is PKI-authenticated (Level 3).



Connection Information shown on the Title

3.10 The Select Computer Box

Win32 Viewer

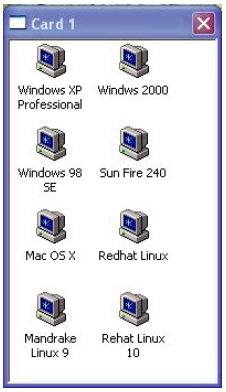
The Select Computer box allows the user to perform intuitive *Click-and-Switch* operation without memorizing the varying port-switching hotkey commands of all kinds of KVM Switches possibly installed behind Prima IP. However, to use the *click-and-switch* feature provided by it, you must first configure the KVM switching hotkey commands for that KVM Switch model via the Web Management Interface.

The *Select Computer* box shows always on top of your screen once the Prima IP Viewer connection is successfully made. On the box, you can see the computer icons together with the computer names you have already specified for each of them using the web management interface.

Click-and-Switch

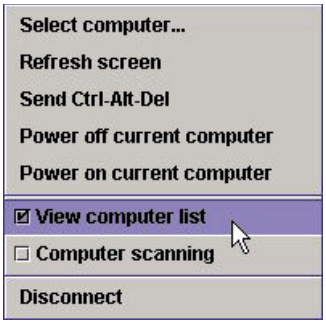
To switch to a computer, just click a computer icon on the box.

Note that, those computer icons represents only the computer names you have already registered using Prima IP Web management interface, not indicating any status of its connection such as whether it is in powered-on or powered-off state.



Java Viewer

To bring up the *Select Computer Box*, click the Viewer Computer List option on the *Quick Menu*. For the java viewer, the Select Computer Box will not appear by default.



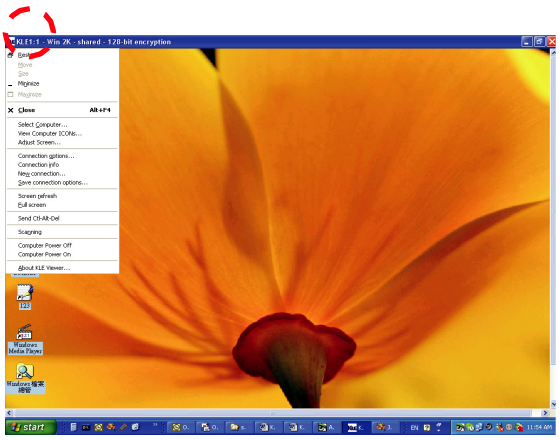
Quick Menu (Java Viewer)

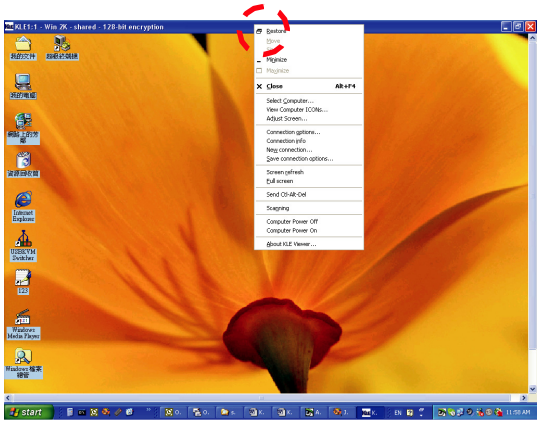
To switch to specific computer, just click any item on the listing …

Select Computer Box (Java Viewer)

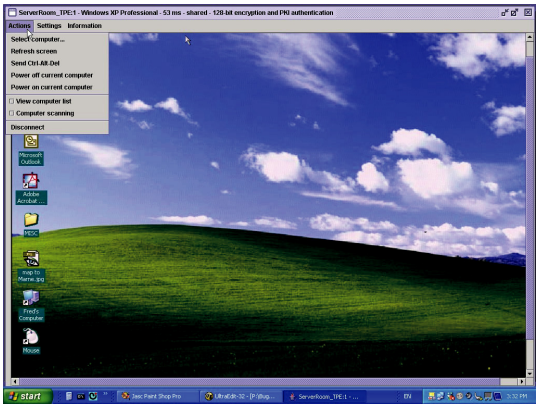
3.11 Viewer Quick Menu

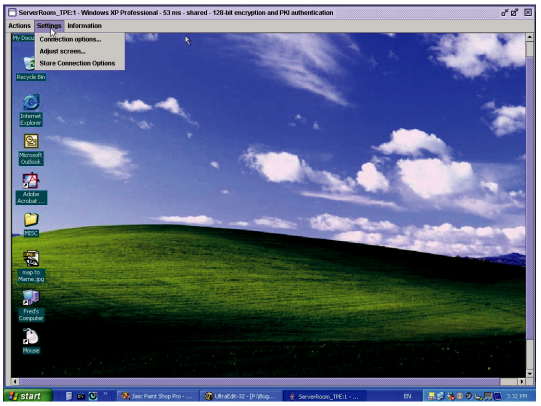
The ***Quick Menu*** of Prima IP's Win32 Viewer can be evoked by clicking the program icon on the leftmost of the title bar, or right-clicking anywhere on the title bar.

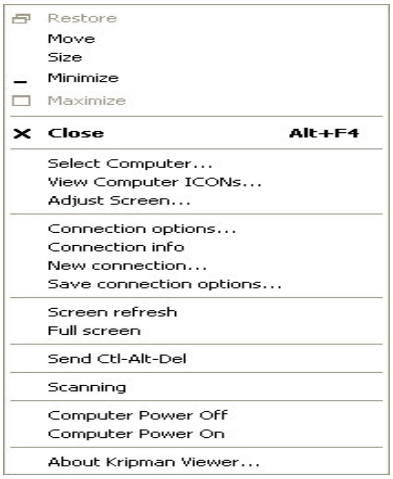




For the Java Viewer, Just click the Menu options under the Title Bar to evoke the Quick Menu.







Select computer

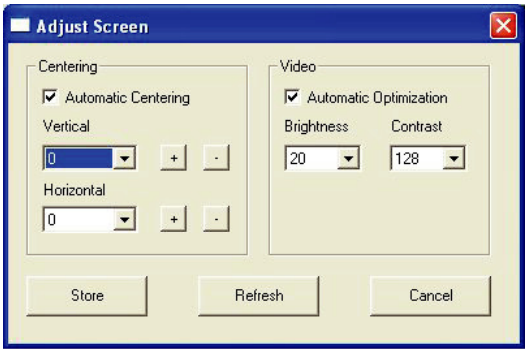
Select the remote computer by a drop-down combo box.

View Computer ICONs

Open the *Select Computer* box for computer selection by clicking icons.

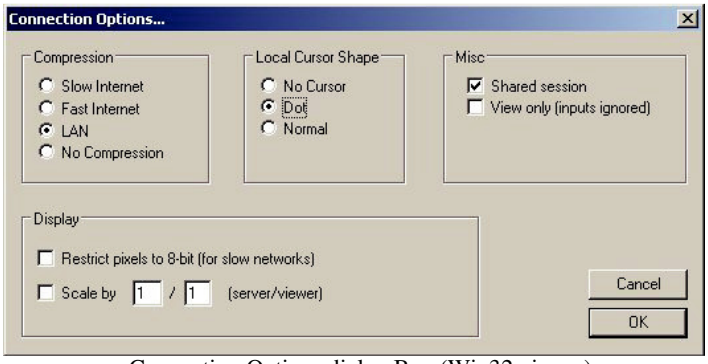
Select Computer Box (Win32 viewer)

Adjust Screen
Fine-tune the screen area by pixel shifts.



Adjust Screen Box (Win32 viewer)

Connection options
Open the *Connection Options* dialog box



Connection Options dialog Box (Win32 viewer)

Connection info
Show the Connection information of the viewer session.

Connection Info (Win32 viewer)

New connection
Make another new connection by the viewer.

Save connection options
Save the connection options settings such as those connection parameters specified within the *Connection Options* Box and also the password within the registry of the client computer.
By selecting this option, you can save your session password as well as other connection parameters in the registry of your client computer, so that next time when you log in the viewer for a new session, you will not be prompted for session password again. However the client path phrase required in the connection of Level 3 security (*256-bit SSL encryption* and *PKI Authentication*) will not be saved and will be asked for every time when you login under Level 3 security setting.

Screen Refresh
Force updating of the viewer screen output

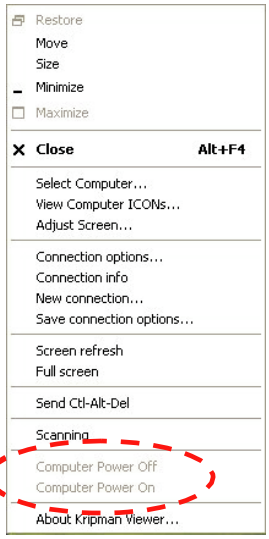
Full Screen
Change the viewer screen to Full Screen mode (Only the Win32 Viewer supports this Full Screen option).

Send Ctrl-Alt-Del
Send a *Log On (Log Off)* key sequence to the remote end.

Scanning
Start scanning through computers by issuing a programmable port switching commands with a delay time to a conventional KVM Switch behind Prima IP.

Computer Power Off
Send a Power Off serial port command to the remote power control unit (Only SUPERADMIN or ADMIN is allowed).

Computer Power On
Send a *Power On* serial port command to the remote power unit (Only SUPERADMIN or ADMIN is allowed)



Power-on / off options grayed-out (unavailable for User privilege)

Now you have got yourself well familiar with Prima IP viewer interface, so go ahead to use and enjoy the remote viewer connection!

3.12 Java Viewer Characteristics

You can perform likewise operations (except full screen) on java viewer. Although the java viewer has slightly different menu arrangement, you should find it as easy to operate on as the win32 viewer interface.

3.13 Common Video Display Problem Troubleshooting

Prima IP video server supports most major display modes up to 1600 x 1200. However, some display problems will occurs, when either there is abnormal or unusual display output from your server or the display resolution is over the biggest support of 1600 x 1200, or the display vertical frequency is beyond the support range in that pixel dimension.

To yield best video results on the viewer screen display on remote login client, you should also refer to *Section 2.3, Prepare your Computers for Connections to Prima IP,* and *Section 2.4, More Tips for Server Desktop Configuration* for more details about how to prepare your servers/computers before getting them connected to your Prima IP.

The followings are some common video display problems and their troubleshooting….

Q. There seems to be many artifacts or residuals not getting refreshed on the viewer screen. Is there any way to improve the video display quality on viewer screen?

A: The causes of these artifacts or residuals could be:

(1) The video filter currently active on Prima IP is either set at Medium Quality or Low Quality Level. These two video filter levels are for faster response than the High Quality Level as to increase the response speed over limited bandwidth condition. If your bandwidth

allows or you need higher video quality instead of higher speed, just change the video filter from Low to Medium or even to High to increase the video display quality on viewer screen on the remote login client. To raise the Video Filter Level, please go to the *Video Server* Page in Prima IP Web Management Interface, and select the filter as either Medium or High Quality according to your requirements. Note that, High Quality video filter gives high quality always on the expense of video response speed on the viewer screen.

(2) The transitional effect of Windows XP is enabled. The transition effects of menu will cause refreshing problems in Low/Medium Video Filter settings. Thus, if you are using a Low/Medium Quality Level of video filter, either try to raise the video filter level to High Quality (at the expense of response speed) or just turn off the transitional effects of Windows XP. To turn off the transitional effects of menu on Windows XP, please refer to *Section 2.3, Prepare your Computers for Connections to Prima IP.* Also note that Prima IP local console is not affected at all by the Video Filter settings or by the transitional effects on Windows XP.

Q. The Prima IP booting time has become unduly longer over several minutes. What's wrong?

A: Please make sure that the external authentication, PPP server/client, time server as well as power control settings are correct. If you don't use all these features or the authentication/time servers are not available, just try to disable them to save booting time since if you don't have all these servers present, the Prima IP will try to look for them till timeout. That will waste Prima IP booting time considerably.

Q: Video response seems slower in limited bandwidth condition, are there ways to increase the response speed?

A : There are several ways to increase the response speed on the viewer screen:

(1) Under bandwidth limited condition, you should select a more economical encoding scheme such as Slow Internet or Fast Internet Encoding scheme instead of the LAN or No Compression Encoding scheme from the viewer connection option menu. However, if the connection is made only within LAN with plenty connection bandwidth, LAN or No Compression Encoding scheme should be (paradoxically) quicker than Internet scheme – since your client computer won't dissipate extra computing power for decoding the more-compressed internet scheme.

(2) Use 8-bit color reduction (with only 256 colors instead of the 65K colors in 16-bit settings).

(3) You can enable Automatic Filter Adjustment (Web Management/Video Server page) for automatic video optimization according to different bandwidth condition.

(4) On the other hand, if you don't want to use Automatic Filter Adjustment, you could always select either Medium Quality/Low Quality level for more speed as your Video Filter setting (Web Management/ Video Server Page). You could also do something to increase the response speed: use a server desktop of small resolution (such as 800 x 600) and use a solid plain color background for server desktop.

(5) Finally, you should check also the networking environment to find if there is some bottleneck that can be improved or eliminated for more bandwidth throughput.

Q. When connection is first made, the display on the viewer screen seems not centered correctly and there is black margin on the edge of the viewer screen. How could I eliminate the black strip?

A. The black strip is the offset that will be seen when the display on viewer screen is not centered corrected. Probably you have not enabled automatic centering option on Prima IP, so please check the followings:

When the viewer connection is made, select the *Adjust Screen* option on Viewer's Quick Menu, and the Adjust Screen dialog box appears. On it, check whether you have *Automatic Centering* enabled. If it is not yet enabled, please check this option to enable it. If it is already checked, please uncheck it and then wait for at least 15 seconds and then check the option again to force the video server to align (center) the display in the viewer screen.

Q: I can log in and make successful browser connection with Prima IP. However, I cannot make a valid viewer connection or the Prima IP does not respond to my viewer connection request. What can I do about it?

A: The Prima IP video server might not function properly. First, make sure your account have the SUPERADMIN privilege. If not, you should request one that has the SUPERADMIN privilege to do the troubleshooting job for you. Next, go to the Apply Settings Page on the Web Management Interface and then hit the Apply Settings button to restart Prima IP. Then wait for at least 10 more seconds for it to start completely. Try to make the viewer connection again to see if it is back to normal. Second, If the Apply settings button could not bring back the Prima IP video server to normal working condition, try to hit the Emergency Reboot button (could be found on the Maintenance Page of the Web Management Interface) for a complete start from ground level. An Emergency Reboot is a clean reboot, and it takes longer time for Prima IP system and video server to load, thus you have to wait at least a minute for the system to be up and running. Then try to make the viewer connection again to see if it is brought back to normal function again. A cold boot of Prima IP is always a last resort to bring the Prima IP back – just try to disconnect the power adapter form Prima IP and wait for sometime (30 seconds) before plugging in again for a cold start over.

4 PRIMA IP UNIT MANAGEMENT OVER A SECURE HTTPS BROWSER CONNECTION

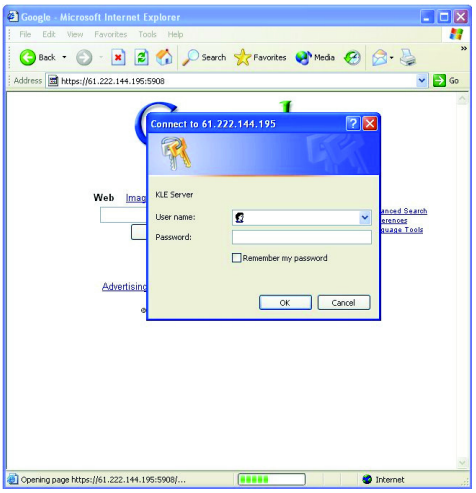
Prima IP's Web Management interface uses only password authentication to authenticate login user's identity. After user identity is authenticated (that is, if you have typed in the right user name with a right password in the login prompt…), an SSL-secured browser connection using 256-bit cipher strength is established.

4.1 Web-based Management Interface

Type in the correct Prima IP's IP address and port number,

https://<IP_address>:<port_number>

` For example: https://61.222.144.195:5908



Remember that it's a secure SSL encrypted connection, so you should type "https" instead of the usual "http". Otherwise, the connection will not be established. The port number might vary according to its setting on the PRIMA IP server. By default, the browser connection uses port 5908. Both the user name and password are case-sensitive.

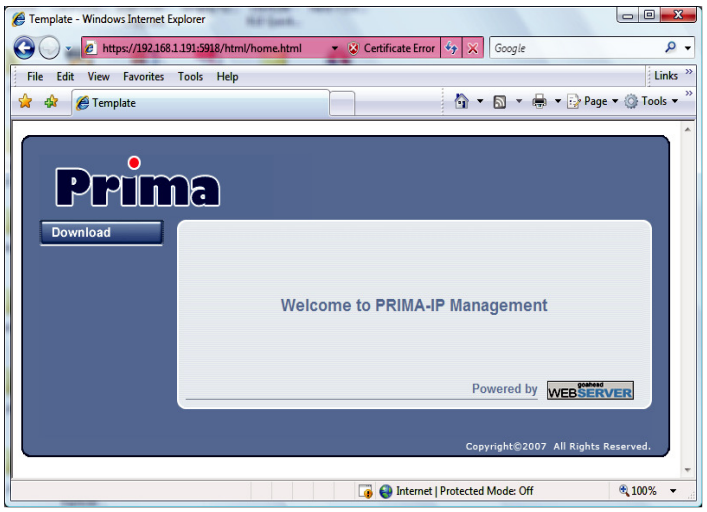
Three User Privileges – SUPERADMIN, ADMIN, USER

PRIMA IP offers three categories of user privileges for Web Management: SUPERADMIN, ADMIN and USER.

SUPERADMIN – Full access to Web Management features [and Power ON-OFF feature on viewer]
ADMIN - Partial access to Web Management features [and Power ON-OFF feature on viewer]
USER – Only minimal access to Web Management features (only the Download and the Logout pages)

Full access – SUPERADMIN

Partial access – ADMIN



Minimal Access (User privilege)

PRIMA IP Browser Management Access Privilege			
Feature Page	SUPERADMIN	ADMIN	USER
Download	√	√	√
Main	√	√	x
KVM Servers	√	√	x
Users	√	x	x
Alarms	√	√	x
Maintenance	√	x	x
Apply Settings	√	√	x

4.2 Download/Viewers – Download Programs For Viewers

The *Download* page allows you to download both the Windows and the Java (TM) Viewers.

PRIMA IP Viewer Download Page

Windows

The viewer for Windows can run on all of Windows platforms: 2000 / 2000 Server / XP / 2003 Server / Vista / Windows 7. Click *Download* and follow the installation instructions.

Note: If you wish to use the secure full SSL connection (security level 3), get a set of certificates from your administrator. Install the certificates on your computer by running the ImportCertificate utility provided with this viewer. Refer to the Security page.

Java ™

The viewer for Java is truly cross-platform for all major Operating Systems including Windows, Linux, Mac OS, etc. However, before you can run the Java viewer on any computer, you must first install the Java Runtime Environment (JRE), which is freely available from Sun at http://www.java.com/. It is recommended to get JRE 5.0 or higher.

On Windows machines, a simple double mouse click should permit to start the viewer for Java. If the viewer does not start automatically, check the .JAR file association on your computer. It must be javaw.exe (and NOT javaws.exe). On other machines, download the KViewer.jar file into a folder and type:

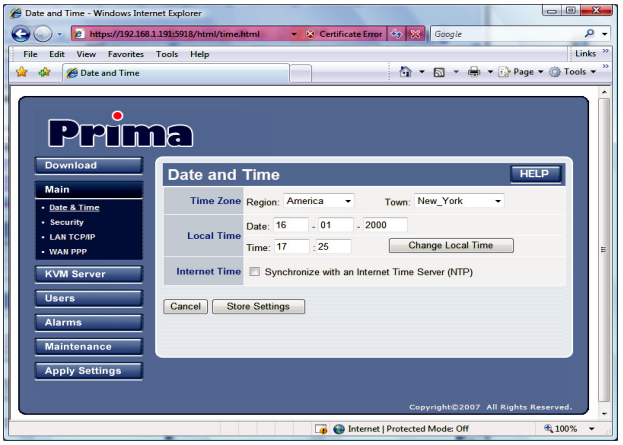
```
java -jar KViewer.jar
```

Note: Some Browser will automatically change the file extension from .jar to .zip while you are downloading the file. If this is the case, please change the file extension back to .jar, so that you can run it properly.

Note: If you wish to use the secure full SSL connection (security level 3) with the Java Viewer, get a set of certificates from your administrator, download the Import Certificate Utility Impcert.jar file into a folder and type: java -jar Impcert.jar. Refer to the Security page.

4.3 Main/Date & Time – Date, Time, Global Time Zone Support And NTP Server Synchronization

The *Date and Time* page allows you to configure time-related settings of your PRIMA IP, including Time Zone settings, Local Time and Internet Time.
After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!



Time Zone

Select the *Time Zone / Region* and *City / Town* from the available list as seen in the drop down combo boxes. For example: If the PRIMA IP is located in Los Angeles, you can choose America as your Time Zone, and Los Angeles as your Region. The advantage of setting up the correct Time Zone is that you don't have to change your local time setting every time when you relocate the PRIMA IP to a different time zone. Instead, you just change the Time Zone settings and the PRIMA IP will readjust the local time for you.

Local Time

Enter the correct date (dd-mm-yyyy) and time (hh:mm) here and click *Change Local Time* button to set current system time on PRIMA IP. Note that if you check the option to automatically synchronize with an Internet Time Server (NTP), the time setting will be periodically synchronized to the time of NTP server specified on each restart of the PRIMA IP and every hour.

Internet Time

This option, Synchronize with an Internet Time Server (NTP), is for the automatic time synchronization of PRIMA IP with an available time server on the internet. You can check the option and then specify the time servers you prefer. The PRIMA IP will try to synchronize with the timer servers every time it starts or restarts and will continue to synchronize every hour thereafter.
The NTP Server1 is the server, with which the PRIMA IP will first try to synchronize, and the NTP Server2 is the backup time server, with which the PRIMA IP will synchronize when the first time server is not available.

Just enter the domain name of the time server and click Store Settings to save, then click *Apply Settings / Restart Servers* to validate all the modifications you have made for time settings.

Note: if you choose this option the original Current Date and Time settings you manually entered will be refreshed with the time provided by the internet time server.

Note: There are many internet time servers available. You can search in the Internet for ones that are nearer to the location where you install the PRIMA IP. You should choose your internet time servers based on the principle that a time server nearer to you will reduce time latency in synchronization.

4.4 MAIN/Security – Certificates Installation, Viewer Encryption And Password Policies

The Security page enables you to configure and implement security-related settings of your PRIMA IP, such as uploading your certificates for the PRIMA IP server side, selecting the security level of the viewer connections, and also the password policy for the viewer and browser connections.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

Certificates and Keys

Certificates are only needed if you intend to implement full PKI authentication for the viewer connections.
If an SSL-encrypted session is already enough for your security requirements, you can just ignore this aspect of PKI authentication.

Where can you get the certificates? There are a default set of certificates in your support CD ROM. You can use them to practice the certificates uploads. In real world scenario, you can either generate the certificates by yourself, since there are some freeware or shareware such as XCA for this purpose. Or you can buy certificates from companies that provide authentication service.

The valid file names and formats of the certificates and Keys to be uploaded to the PRIMA IP should be exactly as below:

- root.crt
- server.crt.
- serverkey.pem
- ldapcert.crt
- ldapkey.pem

Security Level of Viewer Connections

The browser connections to the web management are always using SSL connections. The viewer connections can use different levels of security.

Security Level (SSL): The PRIMA IP offers three levels of security for viewer connections. On the drop-down combo box, you can just choose either one of the three viewer security levels as appropriate to you real demands on viewer connection security:

- Level 1 - No SSL encryption, no SSL authentication
- Level 2 - 256-bit encryption, server authentication by client
- Level 3 - 256-bit encryption, full authentication (requires the installation of certificates)

Level 1 uses No SSL data encryption and No authentication. This is the most straightforward setting that opens most convenience if there are no security concerns at all. Anyone who have a viewer and an Internet connection can easily connect to PRIMA IP as long as the user passes the password policy requests.

Level 2 uses SSL encryption for viewer connection, but only requires server authentication by viewer client. Remote users are not require to install any certificates on their client computers. However, the viewer connection is encrypted with 256-bit SSL technology to ensure that all data contents transmitted via the viewer connection are protected, including keyboard, mouse and video signals.

Level 3 uses 256-bit encryption and a bi-directional PKI authentication between PRIMA IP server and viewer client. With this level of security, all remote users who want to make viewer connections must install a proper client certificate on their computer. This client certificate must come from the same CA that issued the root.crt certificate of PRIMA IP.

There are altogether nine possible combinations of Viewer Security Levels + Password Policies that are available for a flexibility to adapt to your security needs.

KVM Server Password: This item will only appear if you choose to implement Level 3 security. Here you should enter the password that has been used to protect the server private key serverkey.pem. If you use the standard set of certificates provided by default on the Support CD ROM disc, the server password is serverpwd. However, if you use your own set of certificates (as you should do for a real secure installation), you must set the correct server certificate password you got from the Certificate Authority that issued those certificates.

First, you should get a set of certificates from your administrator. If your certificates files have different names, change them to the valid names before uploading.

To upload the certificates, click the *Browse* button to go to the location where your certificates reside. Select a certificate file and then click *Upload* to upload your certificates, one at a time, to the PRIMA IP. After the uploading is completed, you should see the prompt page for reboot. However you don't have to reboot before you have uploaded all the necessary certificates. Just reboot once after you have uploaded all the necessary certificates:

- root.crt
- server.crt
- serverkey.pem

You must upload two extra certificates if you need to SSL-encrypt the LDAP connection for user remote authentication:

- ldapcert.crt
- ldapkey.pem

User Password

User-Password Policy: The PRIMA IP offers three types of password policies for selection, you can select here your password policy for viewer connections:

- **No Password**: the viewer will not prompt you for any user password - the door is open unless you are using security level 3.
- **Global Password**: the viewer will prompt you for a global user password, which is used by all users - a sort of building door code.
- **User Password**: the viewer will prompt you for your user-specific password - a sort of apartment door code.

Note: The viewer can also prompt you for the client certificate password if you are using the security level 3.

Global User-Password: This item only appears if you select Global Password as password policy. Enter the common password used by all users here.

Note: Either Password or Security (SSL/PKI authentication) settings should be used with due precaution. If the PRIMA IP security settings are set to No Password and no SSL or no PKI authentication (Viewer connection security - Level 1), anyone with a viewer and knowledge of the IP address and port number of PRIMA IP can establish a remote connection. With these settings, there is no password protection and no data encryption. Unless you have taken other proper security measures or simply have no security concern, these “unsafe settings” cannot permit to survive longer than 15mn on the Internet.

4.5 MAIN/TCP/IP Settings – Port And IP Settings

The *LAN TCP/IP* page is where you can set up the TCP/IP settings of your PRIMA IP. Here you can specify the IP address, net mask, gateway address, DNS address and access port base for viewer and for browser (port base +8), or whether you want to use DHCP. However, before you go on with the various settings on this page, you might need to check first with your network administrator for proper settings. If you do not configure those TCP/IP settings properly, you will not be able to make valid connections to the PRIMA IP.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

TCP/IP Settings

TCP Port Base: You can freely specify the port base for viewer connection with the PRIMA IP server. You can choose any available port base, starting form the lowest alternative of port 5900 with an increment of 10 right up to port 6090. The port base you choose is exactly the port number that PRIMA IP uses for viewer connection. And "port base + 8" is the exact port number you will use for secure http connection for the browser. After you have made the port base modification, remember to hit the *Store Settings* button, and then hit the *Apply Setting / Restart Servers* to validate your changes.
Host Name: The host name is the name that the PRIMA IP will assume on your Local Area Network.
Domain Name: Specify here the domain name for your PRIMA IP as it appears on your LAN. (Leave it empty if you don't know).
Use DHCP: This option allows the PRIMA IP to get all TCP/IP settings automatically from a DHCP server.
IP Address: Enter a fixed IP address (in dotted decimal format such as 192.168.1.200) that will be used by the PRIMA IP in your LAN.
Network Mask: Enter a net mask value (in dotted decimal format such as 255.255.

255.0) that will be used by PRIMA IP in your LAN.
Gateway: Enter the fixed IP address (in dotted decimal format such as 192.168.1.254) of the gateway (i.e. router) to access the Internet.
DNS: Enter the IP address (in dotted decimal format such as 80.10.246.30) of the DNS server that will be used by PRIMA IP for domain name resolution. Ask your network administrator if you don't know.

Note: You must enter a valid DNS server IP address to allow the email alert of the PRIMA IP to be effective.

4.6 Main/WAN PPP – Logging Server Events

The WAN PP page is where you can set up the PPP server / client mode of your PRIMA IP. Here you can enable either the PPP server mode, or the PPP client mode, or you can disable the PPP modes altogether. The PRIMA IP can either serves as a PPP server for the remote computers to dial-in for connection, or as a PPP client to dial in a PPP server to connect to a network or the Internet. The PPP connection can serve as a backup connection mode when direct network connection is not available or just broken down. The PRIM IP's high speed serial interface can offer excellent bandwidth to PPP connections either when the PRIMA IP is connected as PPP server or PPP client.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

PPP Modes

There are three PPP options for selection:

- PPP Disabled: by default.
- PPP Server mode: for connection request from a peer computer.
- PPP Client mode: for dial-in connection to a PPP server (your ISP or an Enterprise PPP Server).

The PPP Server mode allows users to connect to your servers without the Internet understructure. It can be used as a backup access in case of Internet failure or an ultra-secure access by the use of private lines and modems.

The PPP Client mode can be used when there is no LAN or router available for a direct Internet access by using a modem.

Note: The PPP connection can work simultaneously with the LAN connection.

Note: The PPP connection uses the same serial interface as the Power management. These two features are mutually exclusive. By enabling the PPP you automatically disable the power management and vice versa.

If you have a LAN connection, normally you don't have to choose the PPP connection as your connection mode. However, if no LAN connection is available or if you want to use , you could choose to enable either the PPP server mode or the PPP client mode according to the real connection scenarios.

PPP Server Settings

Current Local IP Address: This is where you can check up the IP address of the PRIMA IP when a PPP connection is established. However, if the PPP connection is not yet established, the IP address will be shown as Unknown. This address is normally which one is set into Local IP Address.

Note: This IP address must be distinct from the one that is used by the PRIMA IP on the LAN.

Local IP Address: Enter here the IP address (default = 192.168.2.200) to be used by the PRIMA IP in the PPP connection. This IP address will be used only in PPP connection by PRIMA IP alone, and should be distinct from the IP address (default = 192.168.1.200) that is specified in the *LAN TCP/IP* page and used for connection via direct local area network.

Peer IP Address: Enter the IP address (default= 192.168.2.201) that will be assigned by PRIMA IP to the peer client at connection time.

Maximum Speed: Specify the modem connection speed. The PRIMA IP supports a high-speed serial connection up to 1 Mbps (Megabits per second).

Note: The modem connection speed is NOT the PPP connection speed, which depends on the modem technology. For example, even if the modem connection speed is 115 200 bps, a 56K modem will provide only a 56 000 bps PPP connection.

User Name: Specify the user name that must be used for the PPP connection login by the peer computer on the other side of the phone line/serial connection.

Password: Specify the password that must be used by the peer computer, then type in the same password in the next entry field to confirm the password.

Note: PRIMA IP can support only one User Name / Password and one PPP connection at a time.

Modem Initialization (chat script): The modem initialization script is a chat script that will initialize the modem to be ready for connection. The standard script provided by default permits to connect a Windows client to PRIMA IP in server mode over a direct serial cable (Null Modem).

```
TIMEOUT 3600
CLIENT CLIENTSERVER
```

In other words: wait for "CLIENT" one hour before timeout, and respond CLIENTSERVER without carriage return.

Note: Refer to Power Management page for more details about the chat program. Refer also to your modem documentation. We also strongly recommend you refer to the standard man pages of pppd and chat programs on Linux. In server mode, the modem should be set to await and automatically connect when receiving remote calls.

PPP Client Settings

Current Local IP Address: This is where you can check up the dynamic IP address that has been assigned to the PRIMA IP by the PPP server at connection time, for example: 62.147.111.39. However, if the PPP connection is not yet established, the IP address will be shown as *Unknown*.

Note: This IP address is used by the PRIMA IP either as a PPP client, and thus is distinct from the one that is used by the PRIMA IP on the LAN.

Maximum Speed: Specify the modem connection speed. The PRIMA IP supports a high-speed serial connection up to 1 Mbps (Megabits per second).

Note: The modem connection speed is NOT the PPP connection speed, which depends on the modem technology. For example, even if the modem connection speed is 115 200 bps, a 56K modem will provide only a 56 000 bps PPP connection.

User Name: Specify the user name that will be used by the PRIMA IP to connect to the PPP server.
Password: Specify the password that will be used by the PRIMA IP to connect to the PPP server.

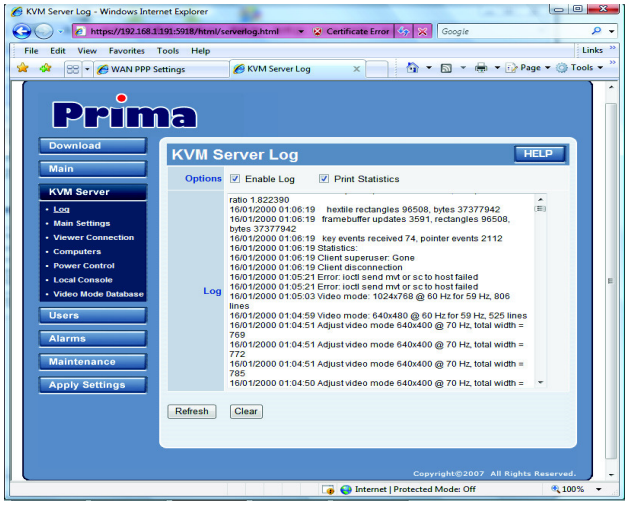
Note: The user Name and Password are normally provided by the ISP at subscription time.

Modem Initialization (chat script): The modem initialization script is a chat script that will initialize the modem to be ready for connection. The standard script provided here by default cannot work for a client connection. Replace it with your own initialization script depending on your modem.

Note: Refer to Power Management page for more details about the chat program. Refer also to your modem documentation. We also strongly recommend you refer to the standard man pages of pppd and chat programs on Linux. In client mode, the modem should be set to dial automatically at start time.

4.7 KVM Sever/Log – Logging Server Events

This Server Log Page keeps a detailed record of events, beginning from each restart, of each user's login, port switching actions, and video modes therewith. It also records each login attempt and the IP address from which the login attempt has originated, even the attempt is not successful. Also it will show certain technical details such as the compression ratio, encoding scheme and bytes transmitted in each successful viewer session. This is the place where you should go check first if you want to know the usage/health conditions of your PRIMA IP.



Enable Log: Check this option to enable the logging of PRIMA IP server events. If you choose not to enable this option, no logging will be done.

Print Statistics: If you need to know more about the PRIMA IP server statistics such as the compression ratio, bytes transmitted, rectangles drawn, frame buffer updates, and key events received, etc., you can check this option so that you can have quantified data for the profile of each session. To record the statistics of the video server and port switching activity by PRIMA IP remote users, you should check this option to print statistics to the server log file.

Each log entry is preceded by date code, time stamp and then the description of the specific log event. You can check here for the IP address that is assumed by the login user when they made the login attempt, and you can also check the statistics of each session as a useful reference for the quantified data of each viewer connection. Note that the log file is of a definite size, older log entries will be erased when the log file has reached it's maximum size while newer logging events keep coming in.

Click the *Refresh* button to refresh the screen output of the log file. Since newer server log events may have happened and being logged to the database after your previous access of this server log page, you need to click the *Refresh* button to reload the log messages.

Click the *Clear* button to erase the log file contents in the database.

Note: The server log is erased each time you perform a complete reboot remotely by hitting the *Reboot* button in the *Maintenance / Reboot* page or when PRIMA IP suffers a power loss.

4.8 KVM Server/Main Setting – KVM Server Main Settings

This page allows you to set up the KVM server operation: video quality and optimization, KVM switch model, auto scanning function.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Server*s!

Video Quality

Filter Level: Specify here the Video Filter Level for the PRIMA IP video server. Based on the bandwidth availability, you can select one of the three modes of video filter levels:

- High Quality, Low Video
- Medium Quality, Medium Speed
- Low Quality, High Speed

Each of the three video filter levels is adapted to different combination of video quality and bandwidth requirements. Users can select their preference according to their actual video quality preference and network bandwidth availability. However, there's always a trade off between video quality and response speed when under limited network bandwidth availability.

High Quality, Low Speed (Light Filter): This level is recommended for high bandwidth networks such as LAN or broadband internet. It requires more bandwidth than the other two filter levels and video refresh speed is slower (however, only noticeable when bandwidth is very limited). This filter provides the best image quality.

Medium Quality, Medium Speed (Medium Filter): This level is recommended for internet connection.

It requires more bandwidth than the Low Quality High Speed, option. This is most often the best speed / bandwidth compromise.

Low Quality, High Speed (Strong Filter): This level is recommended for very limited bandwidth conditions, such as a dial-up modem line to the Internet. With this setting, the viewer screen is updated only on big video changes. Most of time there will be no transmission at all.

Automatic Filter Adjustment: When this option is checked, PRIMA IP can tune the video filter automatically for optimized performance according to the current bandwidth availability.

Automatic Screen Alignment: When this option is checked, PRIMA IP tries to center the view screen automatically to eliminate the offsets sometimes seen in the viewer screen as black gaps.

Automatic Image Optimization for Speed: When this option is checked, PRIMA IP tries to optimize the video settings (phase, light and contrast) to produce images of better quality with higher compression.

Attached KVM

Model: If you ever use a KVM Switch behind the PRIMA IP for connection with multiple computers, you should then select the model of the KVM Switch. If the KVM switch model does not appear in the list, you can always add it or even add more KVM switch models to augment the list, so that your computer icons (as you see on the Select Computer box) can support the port switching hotkeys of that specific KVM Switch upon clicking. For more information on how to add a KVM switch model to the KVM switch database, please refer to the *KVM Switch Database* page. For more information on how to name a computer as it appears on the computer icon of the *Select Computer* box, please refer to the *Computers* page.

Number of Computers: Specify a maximum allowable number for total connected PCs for the KVM Switch attached behind PRIMA IP. You can specify a maximum of 256 computers, as you might have a configuration of several cascadable KVM Switch units behind PRIMA IP.

Scanning

Scanning Period: The scanning period is the default scanning duration for each connected PC, if no KVM (Keyboard - Video - Mouse) event happens to interrupt the scanning. If there is a KVM event such as keyboard/mouse movement or video resolution change, the scanning will be temporarily held until it reaches the timeout of the scanning delay, and then go scanning to the next. Here you can specify the scanning period in seconds.

Scanning Delay: The scanning delay is the time that the PRIMA IP will wait after it last perceives a KVM (Keyboard - Video - Mouse) event before it switches to the next connected PC.

Performing the NumLock Test while scanning: The NumLock test is a way to detect whether a computer is still responding to keyboard action. If you check this option, , the PRIMA IP will send a NumLock signal to the PC while scanning. If the PC returns a response, then he NumLock LED will be lit. The NumLock test can serve as

a test to see if the connected PC is still responsive to keyboard event. And also the NumLock signal will serve as a "wake up" signal if the PC is in sleep mode. If the NumLock test has failed, it most likely indicates that your computer is in trouble. Check this option if you want to use auto scanning to monitor whether each of your computers has stayed alive or not.

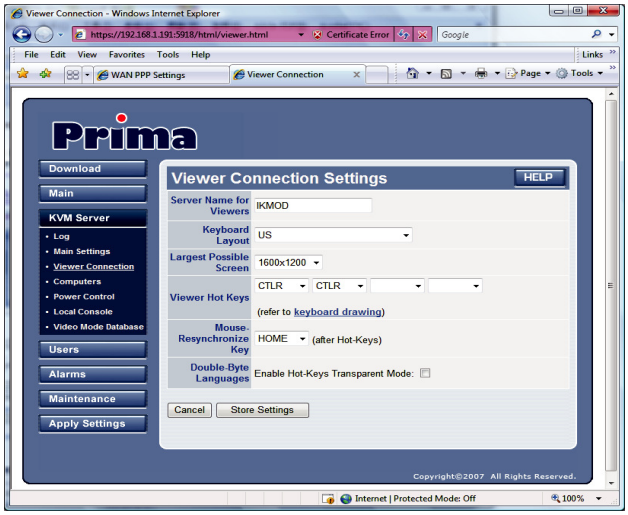
You can also specify which computer will be included and which computer will not be included within the auto scanning process. For more information on how to add or remove computers from the auto scanning list, please refer to the Computers page.

Also, if combined with the Alarm options, auto scanning can detect critical server problems such as No Video, Blue Screen, NumLock Test failure on first timing basis, and send either an alert email or SNMP message, or power cycling commands to a Serial Power Control device to power cycle the server in problem. For more information on how to configure the alarm features of the PRIMA IP, please refer to the *Alarms* pages.

4.9 KVM Server/Viewer Connection – Video Server Name And Keyboard Type Settings

This Viewer Connection Settings page allows you to configure settings proper to the viewer itself, including the name as it appears on the title bar of the viewer window, the keyboard layout that PRIMA IP will assume as to be consistent with the one you use on the client side, the biggest resolution support, the mouse re-sync hotkey sequence, and also the very convenient and useful feature for anyone who uses double-byte language such as Chinese, Japanese or Korean (the CJK languages) and some other languages.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!



Server name for Viewers: Enter here the server name you chose for the Video Server on the PRIMA IP, and it will appear on the title bar of your PRIMA IP Viewer window.

Keyboard Layout: Choose the keyboard layout for the PRIMA IP according to the real keyboard you are using on the remote login client. Choosing the correct keyboard layout for your keyboard is very important since some key codes are represented by different key locations in different keyboard layout. And a correct keyboard layout setting ensures that you will have a matching keycode output on the server side as what you have input on the physical keyboard from the client computer side. The default keyboard layout is the *US* keyboard (*US*). The PRIMA IP supports more than 60 types of keyboards all over the world.

Largest Possible Screen: The PRIMA IP supports a maximum resolution up to 1600 x 1200 pixel dimension. Normally, if you select the biggest resolution support of 1600 x 1200, it will be most accommodating to all display resolution requirements. However, you can still select a smaller workable resolution for your display device.

If you choose a smaller resolution, you have to be aware that any screen larger than what you specify here will not be shown on the viewer. The PRIMA IP supports resolutions as follows:

- 640 x 400
- 640 x 480
- 800 x 600
- 1024 x 768
- 1152 x 864
- 1280 x 1024
- 1600 x 1200

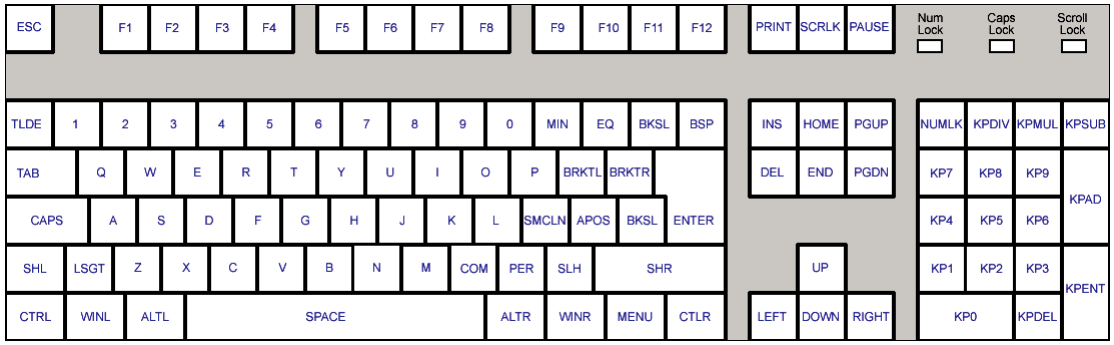
Refer to the *Video Mode Database* page for more detailed information about the refresh rate support.

Hot Keys

PRIMA IP can detect a special sequence of keystrokes when you type on your remote keyboard. This special sequence is used to ask PRIMA IP to resynchronize the local and the remote mouse cursors in a fast and convenient way. For example, it is faster to type CTLR–CTLR–Home on the keyboard than to use the mouse and select a command into a menu. For compatibility with higher devices, this command is divided in two parts called *Viewer Hot Keys* and *Mouse Resynchronization Key*.

Please be aware that the *Viewer Hot Keys* are transmitted to the KVM or server attached to the PRIMA IP. On the contrary, the *Mouse Resynchronization Key* is eaten by the PRIMA IP. Thus, because the *Viewer Hot Keys* are transmitted, they must be as harmless as possible. *Viewer Hot Keys* such as NumLock- NumLock, Scrlk-Scrlk or Ctrl-Ctrl can work because they produce generally no effect. On the contrary, the *Mouse Resynchronization Key* can be anything since it is not transmitted by PRIMA IP.

The *Hot Keys* can be configured to fit your needs. To find out the key positions on a standard keyboard, please refer to the Keyboard Drawing.



Note 1: The *Viewer Hot Keys* are transmitted to the KVM attached. Thus they must be chosen so that they don't interfere with the KVM hot keys.

Note 2: If you are running the Java viewer on Mac OS, you might find that the default mouse resynchronization sequence – CTLR-CTLR-Home - does not work. That is because the Right Control key on Mac keyboard sends out a different key code as the PC keyboard. If that is the case, you might consider to configure your *Hot Keys* as for example, CTLL-CTLL and S.

Viewer Hot Keys: Enter here your preferred keystroke sequence that will serve as Viewer Hot Keys. By default this is CTLR–CTLR, in other words, two consecutive keystrokes of the Right Ctrl key (CTLR).
Please note that this is NOT the Left Control key (CTLL).

Mouse Resynchronize Key: This is the only command supported by PRIMA IP. It permits to synchronize the local and the remote mouse cursors. By default this is the HOME key . Thus by default you have to hit *CTLR–CTLR–HOME* to synchronize the remote and the local mouse cursors.

Double-Byte Languages: This feature makes PRIMA IP compatible with double-byte languages such as Chinese, Japanese or Korean. When using the viewer, if the remote computer and/ or your local computer is running a double- byte system, just type Alt and then Shift or Ctrl and then Shift sequentially instead of simultaneously to produce the same effects as usually.

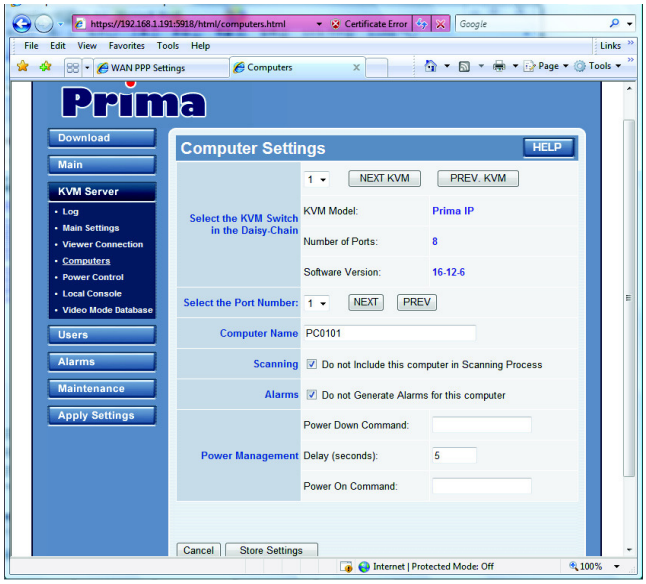
Enable Hot-Keys Transparent Mode: Check this option if you are using double-byte language inputs on the local and/or the remote computer to facilitate switching between single-byte and double-byte inputs. Leave this option disabled if you don't use any double-byte language.

4.10 KVM Server/Computers – Port And IP Settings

This page permits to provide PRIMA IP with information about all KVM-attached computers. This information is used by PRIMA IP to do some actions automatically in order to simplify your job:

- Select a specific KVM Switch in the Daisy-chain and show the information of each, concerning model name, port number and software version.
- Work with computer names instead of KVM port numbers.
- Generate automatically the KVM switch hot keys to select computers. This allows you to select a computer with a simple mouse click or by using the computer name.
- Generate automatically (or on request) the power down and power on cycling if a power control unit is connected.
- Exclude some computers from the auto scanning process.
- Not generate alarms for some computers.

Note: You can also work without supplying any computer information. In this case just keep the values by default. You will have to remember on which KVM port your computers are attached and generate the specific KVM hot keys by hand. Note that this is the way most of low-end IP KVM extenders work.
After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!



Select the KVM switch in the Daisy-chain:

The various settings on this page are KVM-switch-specific as well as KVM-port-specific because a computer is first identified by the KVM Switch and the KVM port it is attached to. Before configure any port specific settings, you have to choose the KVM switch on which you will configure the port-specific settings.

Select the Port Number:

Select the KVM port on which your subsequent settings on this page are directed. You can use the drop- down combo box as well as use the *Previous* and the *Next* button to navigate to a specific port.

Computer Name

Enter a character string of 32 characters maximum to identify the computer attached to the selected port.

Note: The computer names you specify here for each port will appear in the Windows and Java viewers.

Scanning:

If you do not want this computer be included in the auto-scanning, check *Do not include in scanning process*. Thus, you can put a specific computer out of your radar screen if it is of no monitoring value.

Alarms:

If you do not want the scanning process to generate alarm or SNMP messages for this specific computer, check *Do not generate alarm* to exclude it.

If you require power control for your connected computers, you can connect a serial power control (SPC) device to the serial port on the back side of the PRIMA IP, and then enable the power control feature on the PRIMA IP. Hence, remote users can then perform power on/off and power cycling either via the viewer interface, or by pre-defined alarm-triggered action. The PRIMA IP can support most of standard serial power control device via its serial port (RJ12) on back panel (Don't mix it up with the serial console port on the front panel). To enable the PRIMA IP power control feature, please refer to the *Power Control* page.

Important Note: when using a power control device, please note that some newer computers will require some BIOS option adjustment to restart when power is coming back. Otherwise they will not restart without a push of the computer power button. Usually, you should enable the *Power Loss Restart* option on your computer BIOS (or similar option depending on the BIOS vendor), so that your computer can boot up when the power control device is feeding power again.

Power Management:

Power Down Command: Specify here the command that must be sent to the power control unit to power down the computer. Refer to your power control unit documentation.

Note: To remotely power-down this computer from the Windows or the Java Viewers, switch to this computer and then click Power off in the Viewer menu. The command specified here will be sent automatically by PRIMA IP to the power control unit.

Delay: Here you should specify the delay time between the sending of power-down and power-on commands to complete a power cycling. A power cycling is processed only if you have selected *Restart Computer* into the *Alarm* page. By default this delay is 5 seconds.

Power On Command: Specify here the command that must be sent to the power control unit to power on the computer. Refer your the power control unit documentation.

Note: To remotely power-on this computer from the Windows or the Java Viewers, switch to this computer and then click *Power off* in the *Viewer* menu. The command specified here will be sent automatically by PRIMA IP to the power control unit.

4.11 KVM Server/Power Control – Enable The Power Control

The Power Control page allows you to enable or disable the power control feature via the serial port on the back panel of your PRIMA IP. You can also specify the login script of your power control device, if it requires a login script.
After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

Enable Power Control through the Serial Interface

Check the *Enabled* option to activate the remote power control support feature of the back panel serial port of the PRIMA IP. Once this option is checked, a subsequent *Power Device Login* option will appear for you to decide whether to enter the login script.

Simple Users Can Control Power

Check this box if you want that simple users be able to power on and power off the computers.

Power Device Login

Depending on the Serial Power control device you used behind PRIMA IP, sometimes you will need a login script to login or initialize your power control device. If that is the case, just check the *Power Device Needs a Login* option, and a Login Dialog field will appear for you to enter your login script.

Login Dialog (chat style)

This editable field is where you should enter the login script for your power control device, if it is required by your power control device. You should refer to the user guide of your power control device for correct information. A script consists of one or more "expect-send" pairs of strings, separated by spaces as in the following example:

```
login: myid
password: mypass
```

This script indicates that the PRIMA IP should expect the string "login:". Once it received "login:" prompt the PRIMA IP will send the string "myid" and then expect the prompt "password:". When it receives the prompt for the password, it will send the password "mypass". A carriage return is normally sent following the reply string. It is not expected in the expect string unless it is specifically requested by using the \r character sequence. If the script must start by sending something instead of waiting for an expect string, use the null sequence '' (two quotes with no space in between) as expect string:

```
'' restart
login: myid
password: mypass
```

In other words send "restart", expect "login:", send "myid", expect "password", send "mypass". The expect sequence should contain only what is needed to identify the string. For example, to help correct for characters which may be corrupted during the initial sequence, look for the string "ogin:" rather than "login:". It is possible that the leading "l" character may be received in error and you may never find the string even though it was sent by the power device. For this reason, the script should look for "ogin:" rather than "login:" and "ssword:" rather than "password:" like this:

```
ogin: myid
ssword: mypass
```

In other words, expect "ogin:", send "myid", expect "ssword:", send "mypass". A comment is a line which starts with the # (hash) character in column 1. Such comment lines are just ignored. If a '#' character is to be expected as the first character of the expect sequence, you should quote the expect string. If you want to wait for a prompt that starts with a # (hash) character, you would have to write something like this:

```
# Now wait for the prompt and send "logout"
'# ' logout
```

ESCAPE SEQUENCES:

The expect and reply strings may contain escape sequences. All of the sequences are

legal in the reply string. Many are legal in the expect. Those which are not valid in the expect sequence are so indicated.
Expects or sends a null string. If you send a null string then it will still send the return character. This sequence may either be a pair of apostrophe or quote characters.

\b Represents a backspace character.

\c Suppresses the newline at the end of the reply string. This is the only method to send a string without a trailing return character. It must be at the end of the send string. For example, the sequence hello\c will simply send the characters h, e, l, l, o. (not valid in expect.)

\d Delay for one second. (not valid in expect.)

\n Send a newline or linefeed character.

\N Send a null character. The same sequence may be represented by \0. (not valid in expect.)

\p Pause for a fraction of a second. The delay is 1/10th of a second. (not valid in expect.)

\r Send or expect a carriage return.

\s Represents a space character in the string. This may be used when it is not desirable to quote the strings which contains spaces. The sequence 'HI TIM' and HI\sTIM are the same.

\t Send or expect a tab character.

\\ Send or expect a backslash character.

To get more detailed information refer to the Linux chat program man page (man 8 chat).

4.12 KVM Server/Local Console – Configure Local Console Authentication And Mouse Acceleration

The Local Console page allows you to enable or disable the user password authentication feature on the Prima IP Local Console, and to adjust the mouse acceleration on the local console.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

Local User Needs Authentication

Here you can enable/disable the password authentication on the Local Console. To enable the password authentication on the Prima IP local console, you have to check this option. And to disable it, just uncheck. When you have done with the modification, always remember to hit the *Apply Setting / Restart Servers* button.

Acceleration Rate

This option will allows you to select the mouse acceleration factor for the local console. Mouse acceleration factor range is from 1 x to 20 x for your selection.

Acceleration threshold

This option will allow you to select the mouse acceleration threshold in pixels. The mouse acceleration threshold is a value (in pixels), only when the cursor moves beyond which, will the local console mouse acceleration factor be effected.

Note: In order for the mouse resynchronization to work fine on the viewer, the mouse acceleration on each of the connected servers or computers has to be turned off. A zero acceleration mouse on a remote server will not reflect on the viewer since the mouse cursor on the remote server should

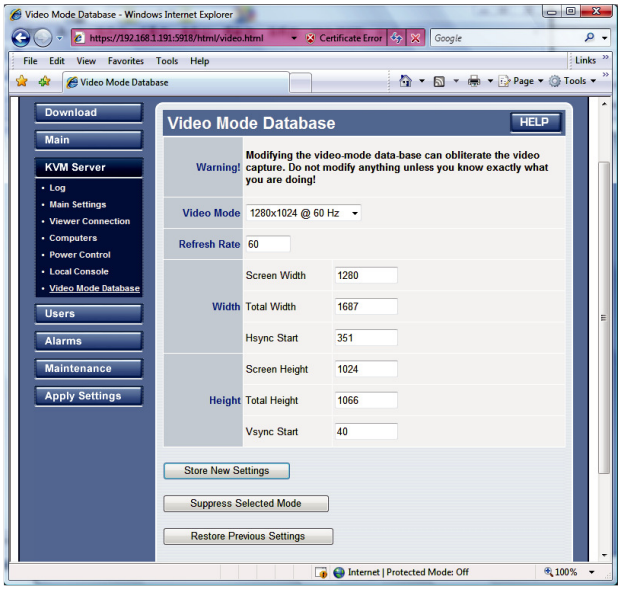
catch up with the mouse on the viewer side, which could use any acceleration factor. However, on the local console of Prima IP KVM Switch, you will experience zero mouse acceleration and the low efficiency when trying to move your mouse. Thus, you can try to enable the mouse acceleration on the local console, for more efficient mouse maneuvering. To enable local console mouse acceleration will not affect the mouse acceleration on the connected server since it is only imposed atop its original zero acceleration on the local console.

4.13 KVM Server/Video Mode Database – Keeping, Modifying And Augmenting Your Video Display Mode Database

The *Video Mode Database* page allows you to modify, create and suppress the VGA modes supported by the device.

Important Note: Carelessly modifying a video mode on this video database might obliterate the video capture, thus DO NOT MODIFY anything unless you know exactly what you are doing.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

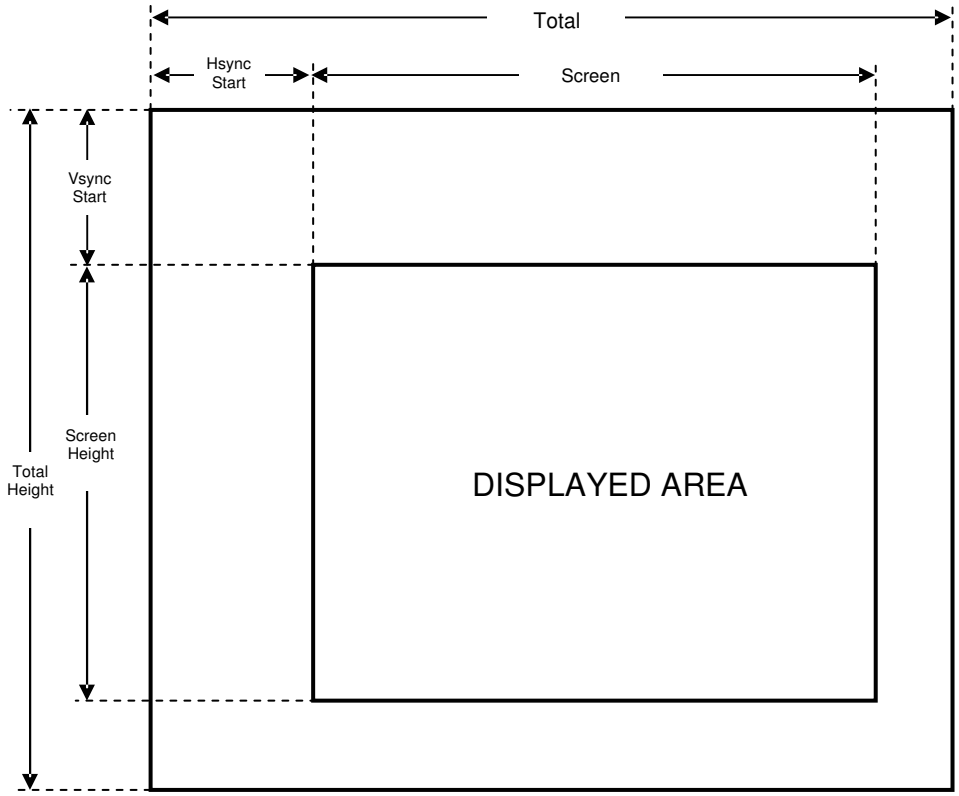


Use the drop down box to select a video mode from the video mode database. Each video mode is indicated by the pixel dimension (length by width) at a certain refresh frequency:

Width_in_pixels x Height_in_pixels @ Refresh_Rate_in_Hz

For example, 1024 x 768@60Hz is a video mode and 1024 X 768@72 Hz is another video mode. Together with the refresh rate and the pixel dimensions, a video mode can be adjusted with those parameters such as screen width, total width, Hsync start, as well as screen height, total height, and Vsync start.

The following diagram explains the geometric relations between the VGA parameters.



Refresh Rate: Here you can modify the refresh rate of the target VGA mode.

Width: Here you can modify the various width parameters of the target VGA mode:

- **Screen Width:** specify the width of the visible part of the screen.
- **Total Width:** specify the total width of the screen (active + hidden).
- **Hsync Start:** specify where the VGA horizontal synchronization should start with reference to the beginning of the line.

Height: Here you can modify the various height parameters of the target VGA mode:

- **Screen Height:** specify the height of the visible part of the screen.
- **Total Height:** specify the total height of the screen (active + hidden).
- **Vsync Start:** specify where the vertical synchronization should start with reference to the top of the page.

Store New Settings: Click this button to save your modification/addition to the video mode database.

Suppress Selected Mode: Click this button to remove the selected video mode from the video mode database. Normally, one does not have to suppress a video mode from the existing database for no particular purpose.

Restore Previous Settings: Click to undo the previous addition or elimination of a video mode.
Note that you can only undo one move.

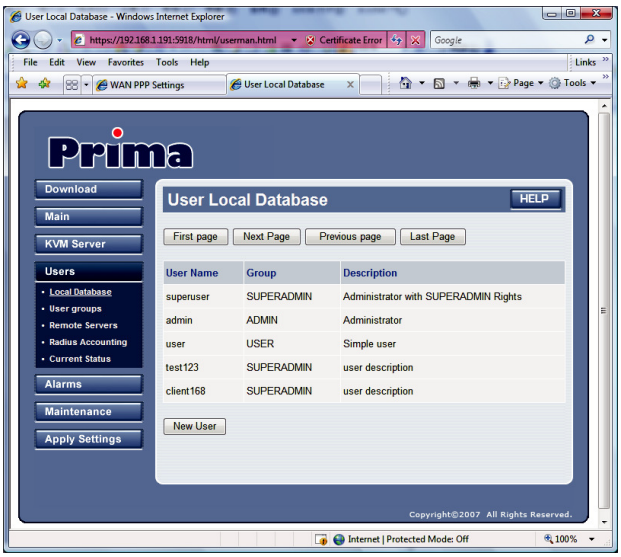
4.14 Users/Local Database - Managing The User Accounts

The *User Local Database* page is for the purpose of user account management for the PRIMA IP. You can see the listing of the existing user entries, together with the user group the specific user belongs to and the description for the user.

You can use the buttons on the top row – *First Page / Next Page / Previous Page / Last Page* to navigate through the first/next/previous/last page of the user database listing.

To modify, add or delete an entry, click the target user name on the listing and a User Edit screen will appear for you to make further modifications or to create a new user entry.

After you have made necessary modifications, remember to hit the *Store User* button to save it into the user account database.



The PRIMA IP offers three categories of user groups for selection: **SUPERADMIN, ADMIN and USER**. Each of these user group are with different rights into the Web Management Interface and into the viewers:

User Group	*Management*	*Viewer*
SUPERADMIN	Full access	All functions
ADMIN	Partial access (see table below)	All functions
USER	No access except the Download page	No power on/off feature

Note: Only SUPERADMIN users can manage user accounts.

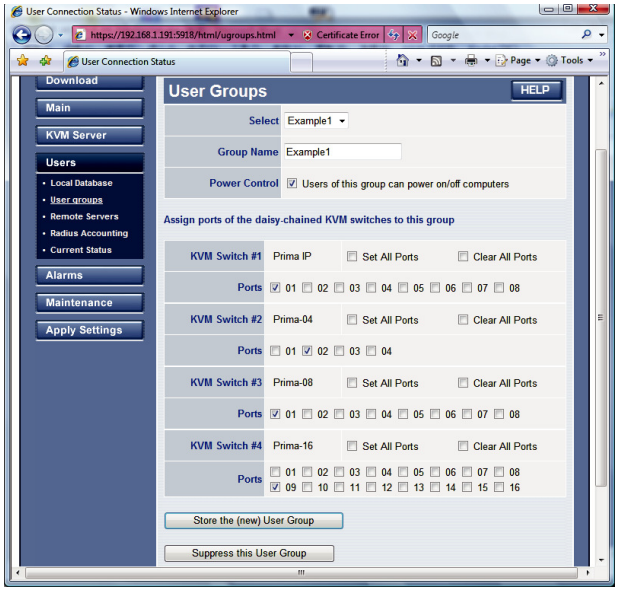
Refer to the table below for detailed list of Web Management rights:

Management Page	*SUPERADMIN*	*ADMIN*	*USER*
Download/Viewer	x	x	x
Main/Date & Time	x	x	-
Main/Security	x	-	-
Main/LAN TCP-IP	x	-	-
Main/WAN PPP	x	-	-
KVM Server/Log	x	x	-
KVM Server/Main Settings	x	x	-
KVM Server/Viewer Connection	x	x	-
KVM Server/Computers	x	x	-
KVM Server/Power Control	x	x	-
KVM Server/Local Console	x	x	-
KVM Server/Video Mode database	x	x	-
Users/local database	x	-	-
Users/User Groups			
Users/Remote [Authent] Servers	x	-	-
Users/Radius Accounting	x	-	-
Users/Current Status	x	-	-
Alarms/Emails	x	x	-
Alarms/SNMP	x	x	-
Alarms/Selection	x	x	-
Maintenance/Software Version	x	-	-
Maintenance/Software Upgrade	x	-	-
Maintenance/Firmware Upgrade			
Maintenance/Config. Save/Restore	x	-	-
Maintenance/Reboot	x	-	-
Apply Settings/Restart Servers	x	x	-

4.15 Users/User Groups – Tuning In With The Remote Authentication Servers

This page allows you to modify, to create or to suppress user groups.

After you have made all modifications, click *Store the (new) User Group* to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart* Servers!



In the *Select* drop down combo box, you can take a brief look of all the currently user groups stored into the PRIMA-IP database.

User Groups

It is possible to define several groups of users (up to 64). When modifying or creating a new user, you must select which *User Group* he will belong to (see User Edit page). When using the user-password policy (see Security page) , users are identified at connection time, their group is retrieved and the group properties are applied.

Each *User Group* has a name and a set of properties specifying which computers can be accessed and whether the users of this group can power on and power off the computers they can access.

There are two preset *User Groups*: ADMIN and SUPERADMIN that cannot be changed. Users belonging to one these groups can access ALL computers with no restrictions.

Note: The local console user is slightly different. When the authentication applies (see Local Console page), the local user cannot select the forbidden ports, but he can still access a computer that would be selected by a remote authorized user.

Important Note: User groups have NO effect if the password policy is not set to User Password. If you are using other password policies such as No Password or Global Password, users willl not have any access restriction, since when adopting these policies you imply that the distinction of user identities is not necessary. For more information on password policies, please refer to the Security page.

Settings

Select: Select a user group from the local database.

Group Name: Modify this field if you want to create a new user group. Don't touch this field if you want only to change the port list of the current user group.

Power Control: Check this box to allow users belonging to this group to "manually" power on and power off the computers they can access through the Viewers. Note that you must use a power control device for that. (See the Power Control page).

For each KVM switch into the daisy-chain, select which ports will be authorized for this user group. Check Set all Ports to select all KVM ports, check Clear all Ports to remove all KVM ports, or select each KVM port individually.

4.16 Users/Remote Servers – Tuning In With The Remote Authentication Servers

The *User Remote Authentication* allows you to authenticate the users that try to connect to the PRIMA IP from centralized servers running a Radius service or hosting a directory that can be accessed through the LDAP protocol (Active Directory for example). This feature permits to integrates the PRIMA IP into your global enterprise user management.

By default, the Remote Authentication is configured as None, i.e., all remote authentications are disabled. In this case, the authentication is all done locally by using the database on PRIMA IP only.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

Authentication Server Type

Here you can select whether you want to disable or enable either the remote server authentication by LDAP or RADIUS server. Before you go forth with subsequent settings on this page, you should check with your network administrator for the availability of either a LDAP server or a RADIUS server.

- To disable the remote authentication support: Select *None* for the Authentication Server Type.
- To enable LDAP authentication support: Select *LDAP* for the Authentication Server Type.
- To enable RADIUS authentication support: Select *RADIUS* for the Authentication Server Type.

Directory Server Using LDAP

SSL Access: Check this option if you want to enable SSL access of the LDAP authentication.

However, to use this option, you should make sure your LDAP server support SSL, and also you have to install a distinct set of certificates – ldapcert.crt and ldapkey.pem – onto the PRIMA IP by uploading them through the *Security page*. Normally these certificates are generated by the directory server itself.

Port: Enter here the port number used in LDAP authentication. By default, it is set to port 389.

LDAP Server: Enter here the IP address of the directory server.

Second Server (if any): If there is a second LDAP server available for authentication, enter its IP address here.

User Base Search DN: Here you should enter the User Base Search DN, which is typical to the LDAP server you use for authentication. By default, the User Base Search DN is:

cn=users, dc=abc, dc=kle, dc=com

However, you should enter your own appropriate one. If you don't know, you should contact your LDAP server administrator.

RADIUS Server

Port: Enter here the port number used in RADIUS authentication. By default, it is set to port 1812.

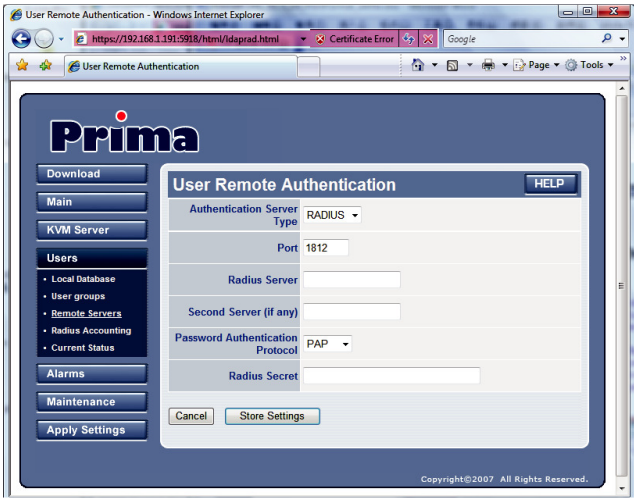
RADIUS Server: Enter here the IP address of the RADIUS server.

RADIUS server authentication: If there is a second RADIUS server for authentication, enter its IP address here.

Password Authentication Protocol: Select the password authentication protocol to be

either CHAP or PAP.

RADIUS secret: Specify here the RADIUS secret (or Shared Secret), between the PRIMA IP and the RADIUS server. Note that the RADIUS secret is a text string that is used as a password between the RADIUS client and the RADIUS server. Ask the RADIUS secret to your server administrator.



4.17 Users/Radius Accounting – Configure The Setting For The Radius Accounting Server

Normally, RADIUS accounting is disabled by default. However, if you have RADIUS accounting enabled on a RADIUS server or LDAP server, you can check the option of RADIUS Accounting and subsequently configure its relevant settings to take advantage of this feature.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

Enable RADIUS Accounting : Check this option, if you want to enable RADIUS accounting support on Prima IP.

Accounting Server : Here you should enter the IP address of the server that offers RADIUS accounting service.

Port : Here you should specify the port that is used for Radius accounting. By default, it is set to 1813.

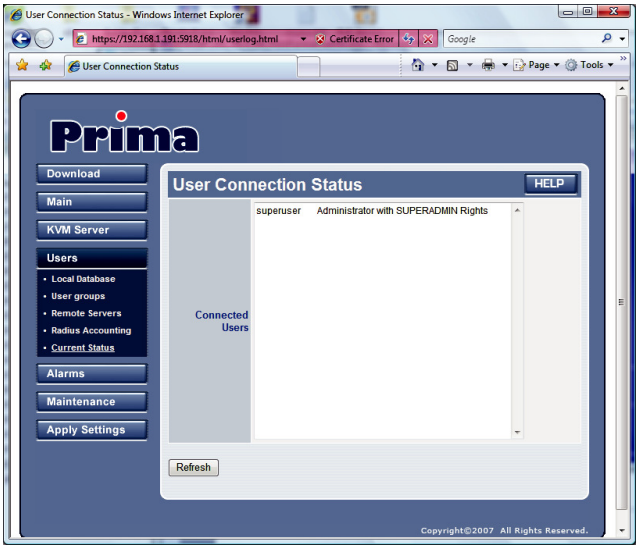
Secondary Accounting Server (if any) : Here you should enter the IP address of the secondary server, if you've got any backup RADIUS accounting server that offers RADIUS accounting service.

RADIUS secret : Here you should specify the RADIUS secret, or Shared Secret, between the RADIUS client (i.e. Prima IP) and the RADIUS server. Note that the RADIUS secret, or the Shared Secret, is a shared text string that is used as a password between the RADIUS client and RADIUS server.

4.18 Users/Current Status – Showing The Currently Connected Users

This page will show forth the remote users that are connected at the time you access this status page. However, this status page will not refresh itself. In order to know whether there's any change to the connection status, you should refresh this page by clicking the Refresh button for current information on connected users.

Important Note: Only when you have selected your password policy to be User Password policy, will the currently connected users be registered and shown on this page. If you are using other password policies such as No Password or Global Password, you will not have any connected users shown on this page, since when adopting these policies you imply that the distinction of user identities is not necessary. For more information on password policies, please refer to the *Security* page.



4.19 Alarms/Emails – Sending Email Notifications For Critical Server Events

This *Email Alarms* Page allows you to set up the email notification for alarm events.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart Servers*!

Email from: Sender email address used by the PRIMA IP for alarm emails.

For example: myemail@myaddress.any

It must be accepted by the SMTP server. This email address can help identify which PRIMA IP is the sender.

Email to: E-mail address of PRIMA IP alarm email addressee.

Note: You can use commas for multiple recipients: support@myaddress.net, emma@international.com, joe@netview.co.jp

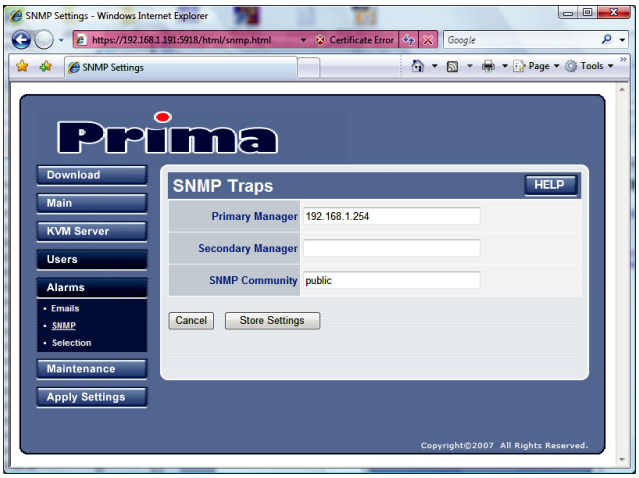
Copy to: E-mail address of addressees who should get a "carbon copy" of alarm emails.

SMTP Server: Enter the name or IP address of the SMTP server (outgoing mail server) that will route the PRIMA IP email alarms to recipients.

4.20 Alarms/SNMP – Sending SNMP Messages For Critical Server Events

Here you can set up the SNMP traps sent by the PRIMA IP, provided you selected the SNMP traps somewhere into the *Alarm* page.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart* Servers!



Settings

Primary Manager: Specify here the IP address of the Primary SNMP manager device on your network.

Secondary Manager: Specify here the IP address of the Secondary SNMP manager device on your network (if any).

SNMP Community: Specify here the name of the SNMP Community to which your SNMP Management host and SNMP agent should belong.

Note: The SNMP manager and agents must belong to an SNMP community identified by its name, which is a collection of hosts grouped together for administrative purposes.

4.21 Alarms/Selections – Select The Alarm Triggering Events

The PRIMA IP is capable of sending immediate alerts, either as emails, SNMP traps, or performing automatically a power cycling when there is blue screen, no video, or NumLock test failure from a remote computer. This feature should be used in conjunction with the autoscanning function, so that the PRIMA IP will help carry on a constant surveillance on the health conditions of your connected servers.

Note: This Alarm Selection page is where you can select which action PRIMA IP must do when it detects an event. This page is NOT the place where you can specify how the action is to be implemented. To do so, refer to SNMP Traps, Email Alarms and Computers.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings / Restart Servers* to validate these new settings. Every change you have made on this page will NOT apply until you hit *Apply Settings / Restart* Servers!

There are three types of alarm-triggering events the PRIMA IP can respond to:

- No Video
- Blue Screen
- NumLock test failure

Each one of these events can be configured to trigger any one of these three types of actions:

- Send an email
- Send an SNMP trap message
- Restart the computer (Power cycling)

No Video Alarm (Blank Screen)

No Video could be a result from power failure or an unsupported video mode, i.e., an out-of-range video mode or most often a video mode not yet set up into the video database.

If you want the PRIMA IP to respond immediately to this sort of events, just check the Enable Alarm option, then specify what type(s) of action you would like to do: either Restart Computer, Send an Email, or Send an SNMP trap.

Blue Screen Alarm (Text mode)

Blue screen is a result of Windows Operating System fatal error. A blue screen can be detected by its low resolution video mode.

If you want the PRIMA IP to respond immediately to this event, just check the Enable Alarm option. Nex specify what type(s) of screen resolution you will regard as Blue Screen: 600 x 400 or 600 x 480, and subsequently select either Restart Computer, Send an Email, or Send an SNMP trap as action to do.

NumLock Test Alarm (Frozen Keyboard)

The NumLock test is to send a NumLock signal to the computer, and the computer normally should return a response immediately so that the NumLock LED indicator on the keyboard will be lit to indicate the success of the test. The failure of a NumLock test indicates at least a keyboard failure to respond to this NumLoc signal, or it might be due to bigger problem such as system failure, or simply a powered-off state.

If you want the PRIMA IP to respond to this alarm-triggering event, just check the Enable Alarm option. Next specify what type(s) of action you would like to do: Restart Computer, Send an Email, or Send an SNMP trap.

4.22 Maintenance/Software Version – Flash Image And KVM Firmware Version Information

The *Software Version* page shows you the current resident software and firmware version information. For example, here you can check the linux kernel version, and also the time it is built, together with the software application and KVM firmware build and their time stamp.

Linux Kernel	2.6.17	built on 04/21/07-15:12:55
Applications		Built on 05/16/07-09:04:37
KVM Firmware		17-11-06

4.23 Maintenance/Software Upgrade – Upgrading The Software Via Web

The *Software Upgrade* page is where you can browse to the path location of software upgrade file, and upload it to the PRIMA IP across LAN or internet.

Note: The PRIMA IP upgrade file must have a name starting with "ikmod" followed by the date, such as ikmod-yy-mm-dd (for example ikmod-07-03-29).

Note: The upgrade file is of an accumulative nature, which means that normally you only have to apply the single latest upgrade patch to keep your PRIMA IP most up-to-date.

When you receive the upgrade file, you must first copy it to a local computer. Then use the PRIMA IP's Web management interface to perform the update across your LAN or across the Internet.

Performing a software upgrade

Just hit the *Browse* button to browse to the location of the update file and then click *Upload* . A running progress indicator bar will be running to indicate the on-going upload process. Depending on the upgrade file size and also the bandwidth availability across the network, file upload time could vary from 1 minute to 20 minutes. When the upload process is complete, the PRIMA IP will reboot by itself. After the reboot is completed, it should be working right away.

4.24 Maintenance / Firmware Upgrade – Upgrading The Firmware Via Web

The *Firmware Upgrade* page is where you can browse to the path location of firmware upgrade file, and upload it to the PRIMA IP across LAN or internet.

KVM Firmware Upgrade

Generally, the Prima IP upgrade file comes with a file name such as kvmfirm-*xx-xx-xx*, for example kvmfirm-*06-07-29*. It is also of an accumulative nature. You can upgrade the KVM part of the Prima IP just like you upgrade the firmware of the its IP module.

To perform software/firmware upgrade for Prima IP …..

File Path : Just browse to the location of the update file and then click the *UPLOAD* button.

A running progress indicator bar will be running then to indicate the on-going upload process. Depending on the upgrade file size and also the bandwidth availability across the network, file upload time could vary from 1 minute to 20 minutes. When the upload process is complete, Prima IP will reboot by itself.

4.25 Maintenance/Configuration Save And Restore – Configuration Backup And Upload

This page allows you to save your current PRIMA IP settings to a single .tgz file for more portability and usability. It is wise to backup your configuration after any change. It can be used also to set up several PRIMA IP with same or similar configuration.

To backup the configuration file

Click the *Backup* button, choose the location for saving your configuration file (*.tgz), and then click *Save*.
The configuration file name format is: kconfig-yyyymmdd.tgz, with a timestamp in it.

To upload the configuration file

Hit the *Browse* button to browse to the location of the update file (kconfig-yyyymmdd.tgz) and then click *Upload* . You will be prompted for a reboot when the upload process is complete. Reboot to validate the new configuration.

4.26 Maintenance/Reboot – Configuration Backup And Upload

In case your PRIMA IP has crashed and beyond restoration simply by hitting the *Apply Settings / Restart* Servers button, you can always have the last resort to completely reboot the PRIMA IP from ground level up by hitting the *Reboot Device* button.

In most of the cases, you don't need to use this *Reboot* button to restart your PRIMA IP from ground level up. Normally, you should use the *Apply Settings* button on the *Apply Settings* page for almost all the cases of restarting/rebooting PRIMA IP with new settings. However, if you find the *Apply Setting / Restart Servers* button could not bring the PRIMA IP to a restart that works properly with the viewer, you can then try to use the *Reboot* button here. But as a rule of thumb, you should try the *Apply Settings / Restart Servers* button first, before you try the *Reboot* button here on this page.

4.27 Apply Settings/Restart Servers – Validate New Settings & Restart Video Servers

All the new settings you have made could only be committed to the PRIMA IP's database by clicking the *Store Settings / Store / Store User* button on each setting page. However, just clicking any of these buttons won't have these new settings immediately validated. You should hit the *Restart Servers* button so that new settings can be put into use at once.

Note: The *Restart Servers* button will disconnect all current viewer connections.

Note: In addition to the *Restart Servers* button, the PRIMA IP also provides an *Reboot* button (on Maintenance / Reboot page). This *Reboot* button is used only when the *Restart Servers* button could works no longer to bring the PRIMA IP to normal restart for a proper viewer connection. If you find the *Restart Servers* button no longer works to bring the PRIMA IP to an effective restart, you can click the *Reboot* button on the Maintenance / Reboot Page. Only bear in mind that the reboot brought about by hitting the *Reboot* button is a total reboot and takes longer time to boot up completely, while *Restart Servers* is much quicker (just few seconds) since it restarts only the server programs on the PRIMA IP.

5 LOCAL CONSOLE OPERATION

This chapter provides general guidelines for the Prima IP KVM Switch Local Console operations. Before you begin operation of the Local console, it is strongly recommended that you read this chapter in advance. The Quick Reference Sheet in the Quick Installation Guide can also serve as an equal reference.

5.1 Control Interfaces

There are three ways to operate your **Prima IP 4 / Prima IP 8 / Prima IP 16** KVM Switch—either by **Front-panel buttons**, **keyboard hotkeys** and **OSD Menu options**. The operation details of these three control methods are detailed as follows:

Front-panel Buttons

The front panel push buttons are used to directly select the active computer channel that can be controlled by the shared keyboard, mouse and monitor. Pressing the key during normal operation will cause the corresponding channel to be selected.

Keyboard Hotkeys

Some computer professionals prefer hotkey control as it is the most convenient and quickest way to operate the KVM switch on the local console. Most of the hotkey control commands are preceded by two consecutive Scroll Lock keystrokes (done within 2 seconds), and then followed by specific command key or key sequence:

Hotkey control command = ScrLk + ScrLk + Command key (sequence)

Within 2 seconds

In most cases, it will take at least three keystrokes to complete a command. In certain case, it will need 6 strokes (such as in selecting specific bank and port number for active channel) to complete one.
All the available hotkey commands and OSD Menu options are summarized in the following table for your convenience.

Command	Hotkeys / OSD Menu option
Select PC	ScrLk + ScrLk + (a) + (b) + (y) + (z) 1 *ab = 2-digit bank number* *yz= 2-digit channel number*
Next lower channel	ScrLk + ScrLk + ↑ (arrow up)
Next higher channel	ScrLk + ScrLk + ↓ (arrow down)
Next lower bank	ScrLk + ScrLk + PgUp
Next higher bank	ScrLk + ScrLk + PgDn
Beep Sound On/Off	ScrLk + ScrLk + B
Show OSD Menu	ScrLk + ScrLk + (Space Bar)
OSD Title Bar ON/OFF	ScrLk + ScrLk + T
OSD Title Bar Position	*[OSD Main Menu/Setup/Title Bar]*
Auto Logout Timeout	*[OSD Main Menu/Setup/Auto Logout]*

Notes:
1 Note that a, b, y and z each denotes a number key. (ab) = 01 ~ 16 ; (yz) = 01 ~ 04 or 01 ~ 08 or 01 ~ 16.

Table 5-1 Summary for Hotkey Sequences

On Screen Display

Note that while OSD is activated, all the front-panel buttons and mouse activity will be made inactive.

To activate the OSD Menu, use the hotkey sequence

Show OSD Menu = 

OSD (On Screen Display) is a menu that is superimposed on your screen display. On the OSD Menu, you will see a listing of the available banks and channels for selection and the currently online status of each channel. You can use the OSD to control the KVM switch with more convenient and intuitive menu-driven operation. The OSD menu also allows you to rename your computer (up to 8 characters), and to find a specific computer by its name. It also allows you to password-protect your KVM switch system.

OSD Main Menu

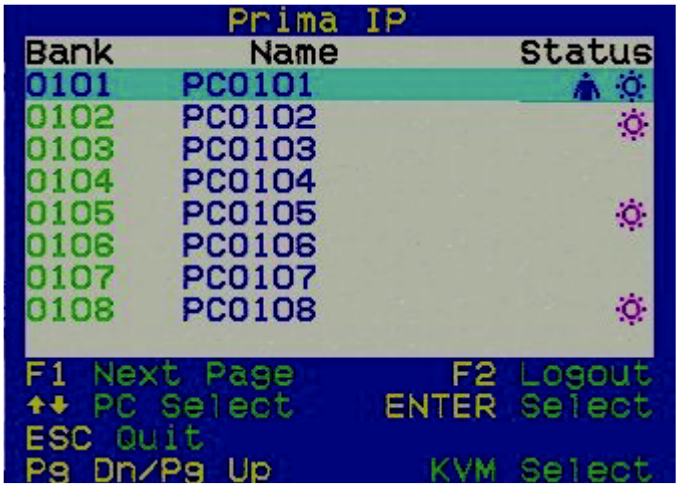


Figure 3-1 OSD Main Menu

The computer name that is followed by a human symbol,  , means that computer is currently the active channel you can monitor on your local console now.

The computer name that is followed by a little solar symbol,  , indicates that it is currently connected to the KVM Switch via PS/2 interface and feeding power to the KVM Switch.

On the other hand, the computer name that is followed by a USB symbol,  , indicates that it is connected to the KVM switch via the USB interface and feeding power to the KVM switch. Others that are not seen with either of both symbols after them are currently either not connected, or the PS/2 or USB interface does not feed power to the KVM switch.

The computer name that is inversely illuminated by a background color indicates that it is currently in focus, and you can perform operation on it by your keyboard.

F1 : Go to the Setup Page
F2 : Logout
Enter : Select
Esc : Quit
Pg Dn/Pg Up: KVM Select

 User the left, right, up, down cursor keys to navigate. Hit Enter key to select and Inset key to edit. On the bottom part of the OSD menu, there are OSD operation tips for your reference.

OSD Setup Menu

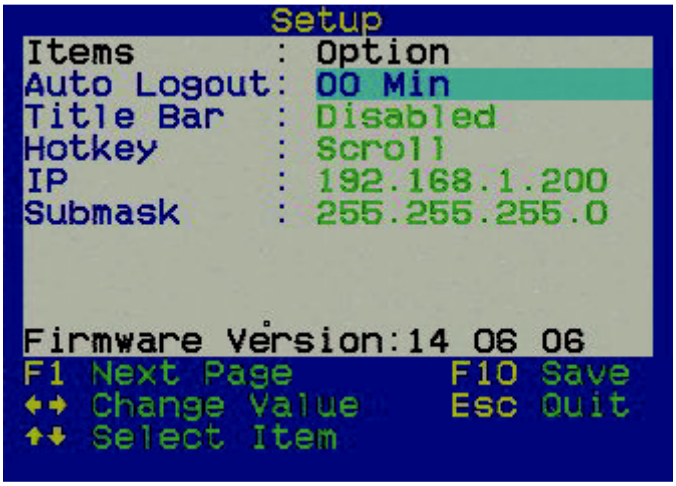


Figure 3- 2 OSD Main Menu

Auto Logout : Specify time for autologout (00~99 min).
Title Bar : Specify the position of the OSD title bar.
Hotkey : Specify the hotkey preceding sequence.
IP : Specify the local IP address for the Prima IP KVM Switch.
Submask : Specify the submask for the Prima IP KVM Switch.
Firmware Version : Show for the firmware version of the KVM switch.

5.2 Local Console Hotkey Operations

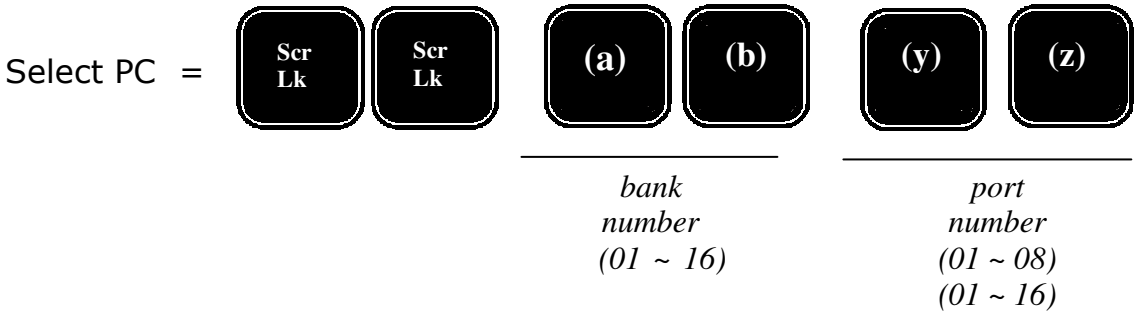
The followings describe each local console hotkey command operation of the Prima IP KVM Switch and available ways to execute the command, either by a front-panel button, a keyboard hotkey sequence or an OSD Menu option.

<Select PC>

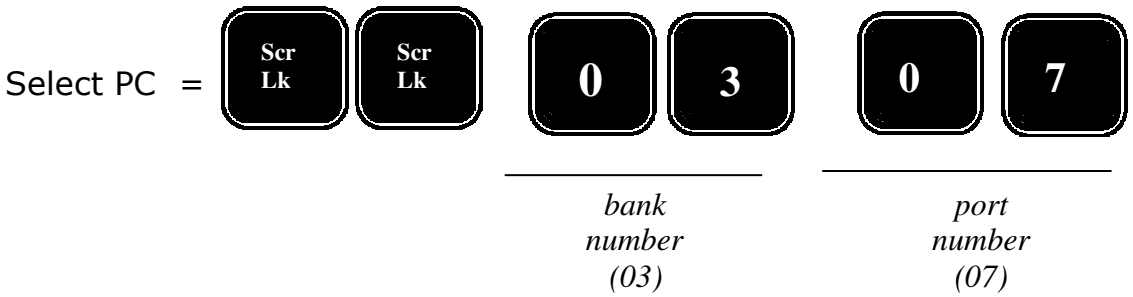
Front-Panel Button

Press the corresponding button on the specific switch, to which the channel you want to select is connected.

Hotkey



For example, when with a configuration of multiple daisy-chained Prima KVM Switches, if you want to select bank 3 port 7, you should press the following keystrokes:



However, when using single KVM Switch configuration, if you want to select port 7, you should first press its default bank number 01 and then the port number 07:

Select PC = Scr Lk, Scr Lk, 0, 1, 0, 7

bank number (01) *port number (07)*

Since the single KVM Switch bank number is default to 01 (i.e. itself a master KVM Switc on its own), therefore you should always specified its bank number by "01".

OSD

To switch to a specific PC using the OSD Menu, you have to activate the OSD Menu first, Hit *ScrLk* + *ScrLk* + *Space Bar* to activate the OSD Menu. Then use the cursor keys to navigate to the channel you want and then hit *Enter* key to select the PC channel.

In a daisy-chained configuration, you may want to select specific channel on a specific bank (when you have daisy-chained multiple KVM switch units), just use the *Page up/Page Down* key for bank selection and navigate the OSD Menu by cursors key to the channel you want and hit Enter to make it your active channel.

<Next lower channel>

Front Panel Button

Press the corresponding button.

Hotkeys

Next lower channe = Scr Lk, Scr Lk, ↑

<Next Higher Channel>

Hotkeys

Next higher channel = 

OSD

Select the corresponding OSD Menu option.

<Next Lower Bank> (when daisy-chained)

Front Panel Button

Press the corresponding button.

Hotkeys

Previous bank= 

OSD

While the OSD is activated on the console screen, press the Page Up key to rotate through the bank selections upwards.

<Next Higher Bank> (when daisy-chained)

Front Panel Button

Press the corresponding button.

Hotkeys

Next bank = 

OSD

While the OSD is activated on the console screen, press the Page Down key to rotate through the bank selection backwards.

<Beep Sound On/Off>

While autoscanning, port-switching or issuing a hotkey command, a beep sound will be heard. If you want to turn on/off this beeping, try the following hotkey sequence.

Hotkey

Beep sound on/off = Scr Lk, Scr Lk, B

<Show OSD Menu>

Hotkey

Show OSD Menu = Scr Lk, Scr Lk, *(space bar)*

<OSD Title Bar ON/OFF>

Hotkey

The OSD Title Bar will show the computer name on the screen. You can toggle the OSD Title bar ON/Off just by the hotkey:

OSD Title Bar on/off = Scr Lk, Scr Lk, T

<OSD Title Bar Position>

OSD

You can select the OSD Title Bar Position to be either on the left or right side of the screen Use cursor keys to navigate to the OSD Title Bar option on the OSD Setup Menu, and then hit *Enter* to select and cursor key to toggle the Left/Right option. The OSD Menu Timeout is default to 60 seconds. The OSD Title Bar Position is default to right side of the screen.

<Auto Logout>

OSD

Use cursor keys to navigate to the Auto logout option on the OSD Setup Menu, and then hit *Enter* to select and edit the Auto logout timeout value. The OSD Menu Timeout is disabled by default. You can specify a timeout value between 0 and 99 min. [00 means disabled]