# DIGITAL KVM OVER IP SWITCH USER MANUAL

MODELS 503723 & 503730




*Shown: 16-Port , Model 503730*

INTELLINET NETWORK SOLUTIONS

INT-503723/503730-UM-0808-01

# INTRODUCTION

Thank you for purchasing the INTELLINET NETWORK SOLUTIONS™ Digital KVM over IP Switch, Model 503723 (8-Port) or Model 503730 (16-Port).

This switch is the perfect solution for any organization that demands secure and flexible local and remote administration of its critical systems, offering revolutionized remote server management by combining industry-leading remote control technology with a proven Enterprise-class digital KVM switch.

The Digital KVM over IP Switch attaches to your local KVM switch and can be used to support multiple servers and computers from a single console. The maximum number of devices you can manage depends on the type of local KVM switch you use, and when cascaded can result in up to 128 computers remotely managed via a LAN or WAN.

Server management is further simplified by an advanced on-screen display menu. In addition, the Digital KVM over IP Switch provides BIOS-level control and full interaction with the system's boot process; its SSL encryption guarantees the safety you expect for your company's network. The switch can alert you in case the remote server stops responding by sending out alert e-mails or by issuing SNMP traps, adding an important layer of security to your installation.

The easy-to-follow instructions in this user manual help make setup and operation quick and simple, so you'll also soon be enjoying the benefits of these additional features:

- Connects to any PS/2- or USB-based PC, server or KVM switch
- Local console connection (through PS/2 and VGA ports)
- PC port connection via PS/2 and USB
- Simultaneous access from multiple users; no user limitation
- Supports video resolutions up to 1600 x 1200 @ 60 Hz
- Security using full 1024-bit PKI authentication / 256-bit SSL encryption
- Supports LDAP, RADIUS and Active Directory servers
- Win32 viewer and Java viewer for cross-platform compatibility
- Time synchronization by connection to any NTP time server
- Lifetime Warranty

**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 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 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.

***NOTE:*** Some product images have been compressed and some screen images have been modified to fit the format of this user manual.

# TABLE OF CONTENTS

section page


**SYSTEM ARCHITECTURE ..... 5**
LAN/WAN Configurations ..... 5
Power Control Configuration ..... 6
PPP Configuration ..... 7
**HARDWARE ..... 8**
Front Panel ..... 8
Rear Panel ..... 8
**INSTALLATION ..... 9**
Digital KVM over IP Switch Setup ..... 9
Server Configuration ..... 9
Network Settings ..... 12
Port Base Settings ..... 13
Configuration of the Firewall/Router for Access across the Internet ..... 14
Installation of Certificates ..... 14
Selection of a Security Level for Viewer Connection ..... 16
Selection of a User Password Policy ..... 17
**VIEWER CONNECTION ..... 18**
Installation of a Win32 Viewer ..... 18
Installation of a Java Viewer ..... 18
Importing Certificates to a Viewer on a Client Computer ..... 19
Viewer Connection Options ..... 20
Establishing the Viewer Connection ..... 21
Cursor Settings/Synchronization ..... 21
Saving Connection Settings ..... 21
Win32 Viewer Settings ..... 22
Title Bar Information ..... 24
Select Computer Box ..... 24
Viewer Quick Menu ..... 24
Video Display Troubleshooting ..... 26
**MANAGEMENT OVER A SECURE HTTPS BROWSER ..... 27**
Web-Based Management Interface ..... 27
Download ..... 29
Main: Date & Time ..... 30
Main: Security ..... 31
Main: LAN TCP/IP ..... 33
Main: WAN PPP ..... 34
KVM Server: Log ..... 37
KVM Server: Main Settings ..... 38
KVM Server: Viewer Connection (Settings) ..... 40
KVM Server: Computers ..... 42
KVM Server: Power Control ..... 44
KVM Server: Local Console ..... 46
KVM Server: Video Mode Database ..... 47
Users: Local Database ..... 48
Users: User Groups ..... 50
Users: Remote Servers (User Remote Authentication) ..... 51
Users: RADIUS Accounting ..... 53
Users: Current Status ..... 54

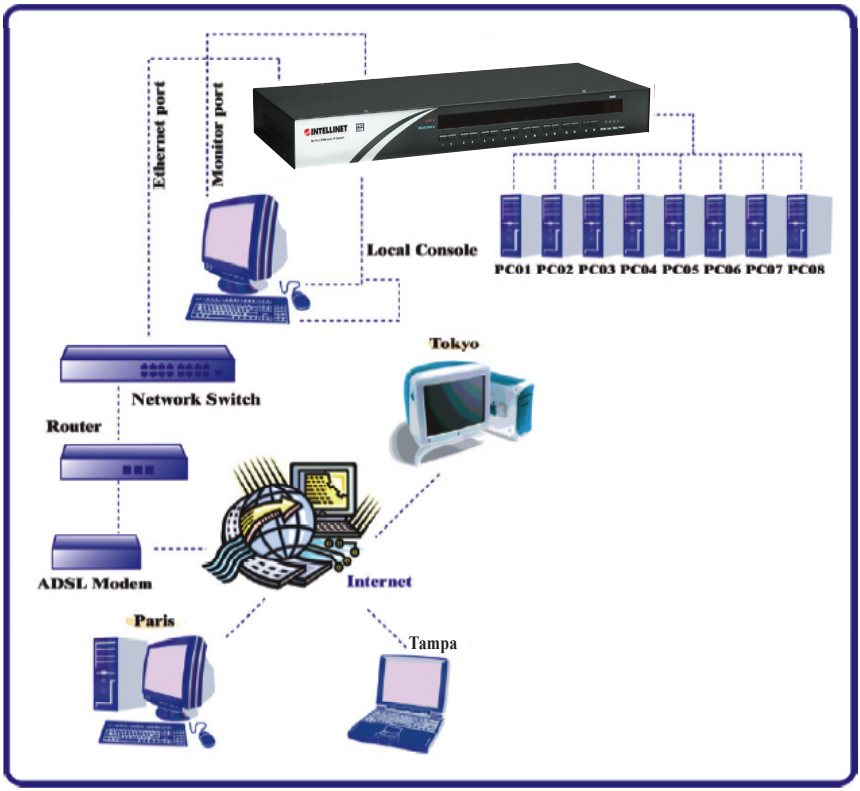
Alarms: E-mails ..... 54
Alarms: SNMP (Traps) ..... 55
Alarms: Selection ..... 56
Maintenance: Software Version ..... 57
Maintenance: Software Upgrade ..... 57
Maintenance: Firmware Upgrade ..... 58
Maintenance: Configuration Save & Restore ..... 59
Maintenance: Reboot ..... 59
Apply Settings: Restart Servers ..... 60
**APPENDIX A ..... 61**
**APPENDIX B ..... 64**
**SPECIFICATIONS ..... 66**

# SYSTEM ARCHITECTURE

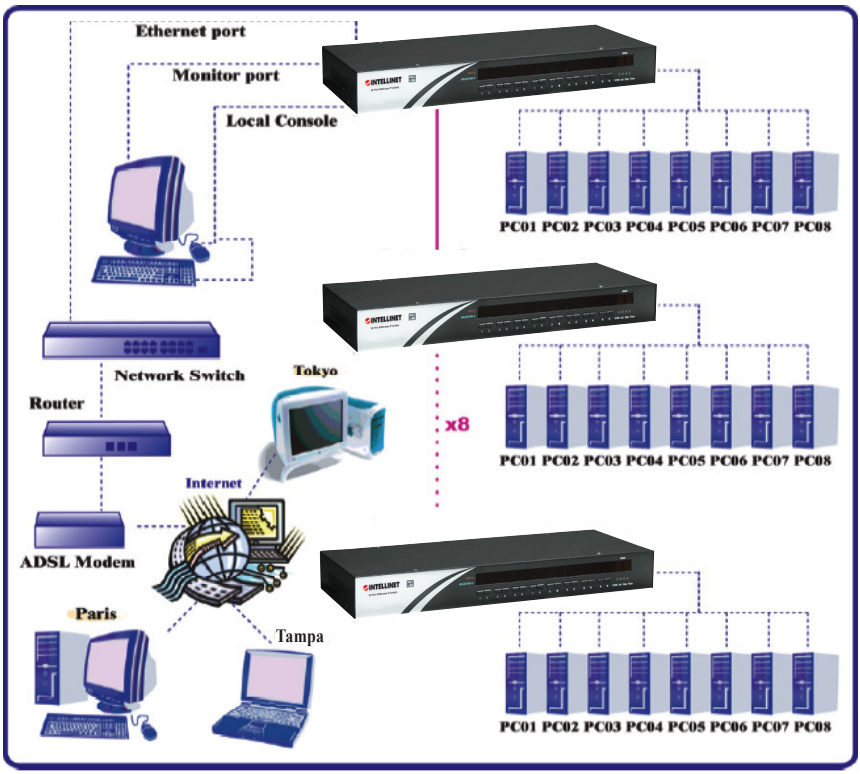
The Digital KVM over IP Switch is based on an embedded Linux platform for computing power and rugged stability. It employs a high-speed processor to ensure excellent video quality and fast keyboard/mouse response across the Internet, even when bandwidth availability is limited.

## LAN/WAN Configurations

***Basic Configuration***

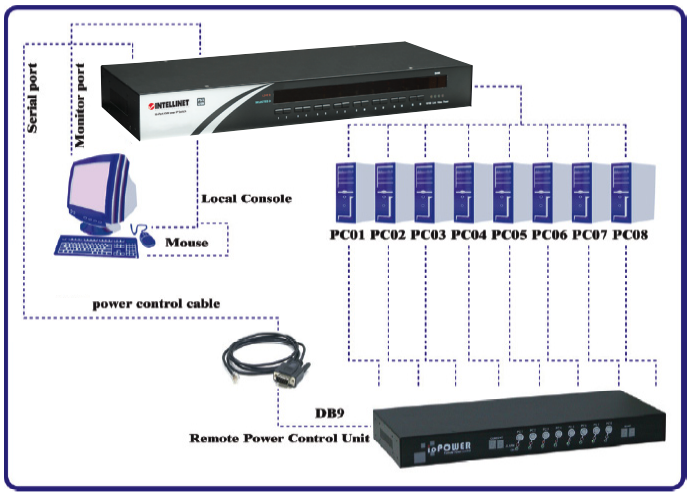


*Daisy-chained (cascaded) with other switches*



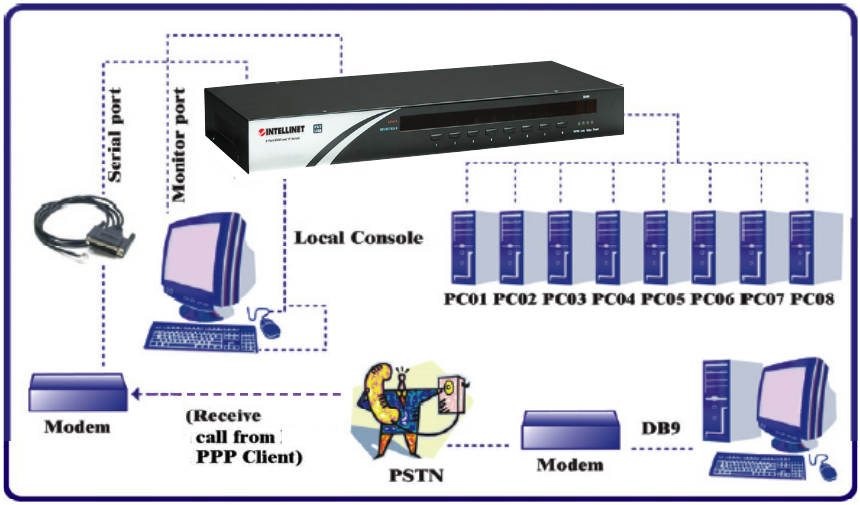

## Power Control Configuration

*Connected to a remote power control device*

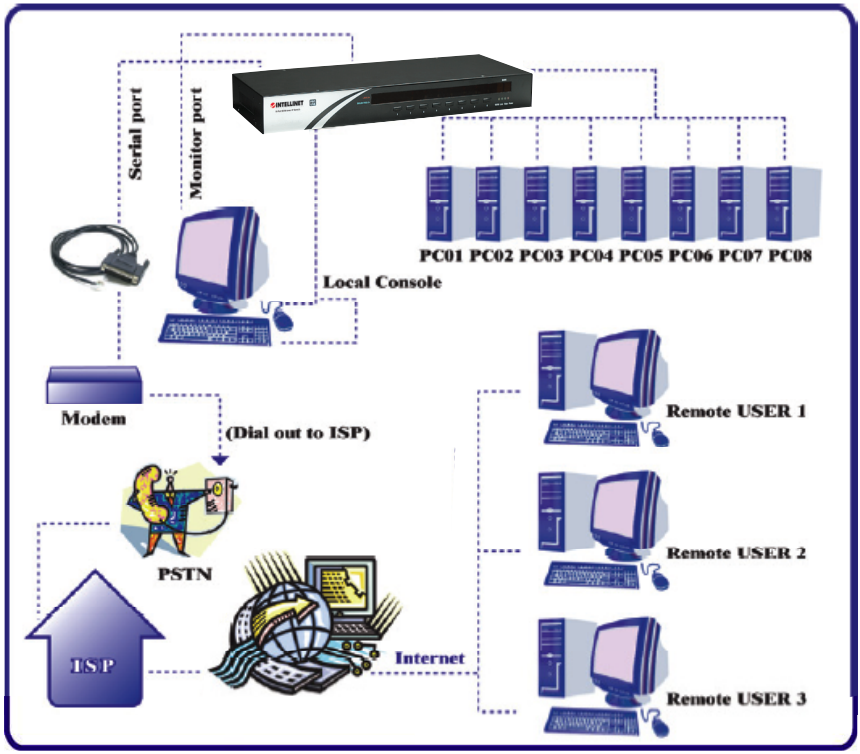


## PPP Configuration

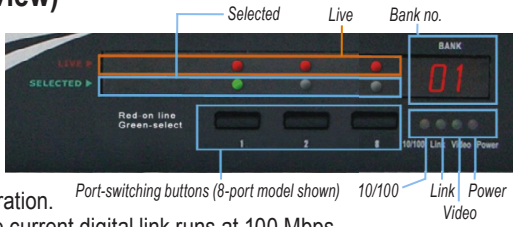
*Set up as a PPP server to accept dial-in requests from a remote PPP client via a modem*




*Set up as a PPP client to dial out to an ISP for remote clients to access via the Internet*



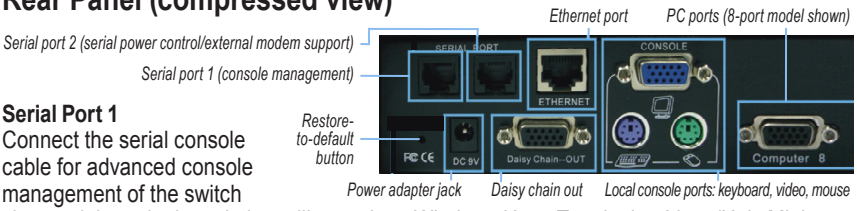
## Front Panel (compressed view)




**Status LEDs**

- Selected identifies a port with a green light.
- Live identifies an on-line port with a red light.
- Bank No. identifies this particular switch within a daisy-chain configuration.
- 10/100 lights solid orange when the current digital link runs at 100 Mbps.
- Link lights solid green when a network link is established; it flashes whenever network transmissions are perceived on the digital port.
- Power lights solid red to indicate the power is on.
- Video blinks orange to indicate the normal functioning of the video server.

## Rear Panel (compressed view)




**Serial Port 1**
Connect the serial console cable for advanced console management of the switch via a serial terminal emulation utility, such as Windows HyperTerminal or Linux/Unix Minicom.

**Serial Port 2**
Connect to either an external modem or a power control unit (or to a cascaded chain of power control units). When an external modem is added to its serial control port (RJ12), the switch can 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 out to an ISP or Enterprise PPP server. Furthermore, through serial commands sent over its serial control port, the switch can perform remote power on/off and power cycling tasks via the (cascaded) power control module(s).

**Ethernet Port**
This digital port (RJ45) offers anytime/anywhere access to the Digital KVM over IP Switch and, subsequently, the conventional KVM switch(es) and servers/computers connected behind it to the remote login clients over the LAN/Internet.

**PC Ports**
Connect to your computer(s) using 3-in-1 connection cable(s).

**Restore-to-Default Button**
Located to the left of the power jack, it's accessed by using a pointed object, such as a pin. To restore the switch to factory defaults (the IP settings and user account settings established before you do any of your own configurations), press the button for 5 seconds or more.

**Power Adapter Jack**
Use only the 9 V DC external power adapter included with the switch to avoid nullifying the warranty.

**Daisy Chain Out**
Connect to additional switches for daisy-chained (cascaded) configurations.

**Console**
Connect the keyboard, mouse and monitor for the local console.

# INSTALLATION

Before installing the Digital KVM over IP Switch, take a moment to make sure you have the following components on hand to ensure a proper setup. (See Appendix B for sample images.)

- Suitable (USB or PS/2) combo KVM cables (or, for added convenience, combo-free cables) to connect the switch to the keyboard, video and mouse ports of each PC.
- Monitor with standard D-sub 15-pin video connector (HDB15) for each PC.
- Standard PS/2 Microsoft or Logitech keyboard.
- Standard PS/2 Microsoft- or Logitech-compatible five-key mouse.
- Daisy chain cable (HDB15 male to HDB15 female) as needed for cascade configurations using conventional 8- or 16-port KVM switches (models 503471 and 503396).
- Terminator (if daisy-chaining) to plug into Daisy Chain Out port of last KVM switch in chain.

## Digital KVM over IP Switch Setup

1. Plug the included power adapter into the switch and an AC source, then turn on the switch.
2. Set up your local console by connecting a keyboard, monitor and mouse to the corresponding Console (keyboard, video and mouse) ports on the switch (see Rear Panel above). ***NOTE:*** Refer to Appendix A for an introduction to basic local console operation.
3. Connect to one or more computers/servers as described below. ***NOTE:*** Make sure that PS/2 computers are turned off before connecting to the switch; otherwise, the non-Plug and Play interfaces may not recognize the PS/2 keyboard and mouse later in the install procedure.
   - **Single Server Mode** (see Page 5 configuration image)**:** To use just one server or computer, simply connect to a PC port with an appropriate (USB or PS/2) combo cable.
   - **Multiple Server Mode** (see Page 6 configuration image)**:** To connect to multiple servers/computers, add a conventional KVM switch to the configuration by connecting the Daisy Chain Out port of the Digital KVM over IP Switch to the Daisy Chain In port of the second KVM switch, which is then connected to additional computers/servers as desired.
4. Boot up connected computers (if not yet powered on and verify the connections. ***NOTE:*** Do not use both USB and PS/2 keyboard connectors on a computer simultaneously.

## Server Configuration

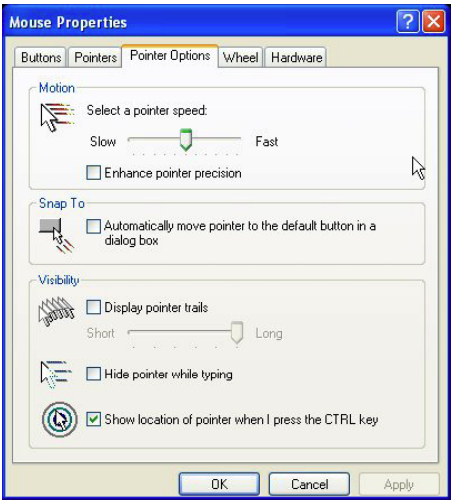
**Mouse Acceleration**

Mouse acceleration is not supported by the Digital KVM over IP Switch, so any such function (including any “Snap To” option) needs to be deactivated on all connected servers.

*Windows XP:*

Go to the Mouse Control Panel, select the Mouse Properties tab, then go to the Pointer Options screen.

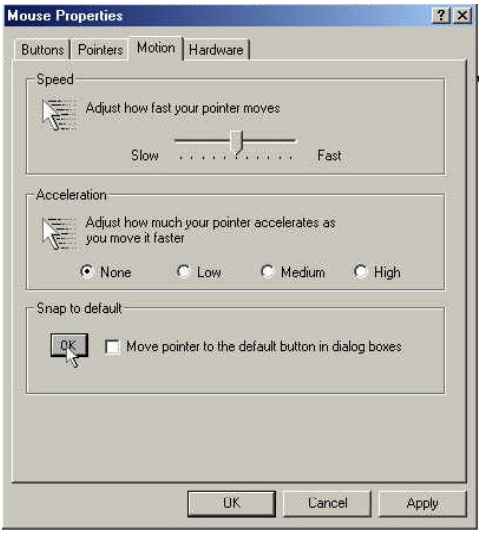
1. Set the pointer speed slide bar to the exact middle.
2. Uncheck the “Enhance pointer precision” option.
3. Uncheck the “Automatically move pointer to the default button in a dialog box” option.
4. Click “OK.”



*Windows 2000:*

Go to the Mouse Control Panel, select the Mouse Properties tab, then go to the Pointer Options screen.

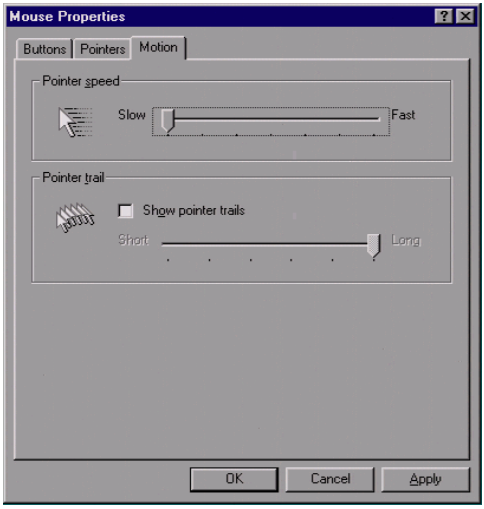
1. Set the pointer speed slide bar to the exact middle.
2. In the Acceleration panel, select "None."
3. Uncheck the "Move pointer to the default button in dialog boxes" option.
4. Click "OK."




*Windows 98:*

Go to the Mouse Control Panel, select the Mouse Properties tab, then go to the Motion screen.

1. Set the pointer speed slide bar to "Slow" (all the way to the left).
2. Click "OK."




***NOTE:*** As shown above, mouse settings differ depending on the operating platform; some presenting mouse acceleration options, some not. If you see any mouse acceleration option, uncheck (deactivate) it. If there is no mouse acceleration available on the Settings screen, adjust the mouse speed slide bar either to x1 or the slowest position (such as on Linux platforms). In some cases, a middle position on the speed slide bar may be required for mouse synchronization on the viewer side (as with Windows XP, for example); or a bit of trial-and-error configuring may be necessary to set your mouse acceleration to Off and the speed to x1.

**Additional Server Configuration Considerations**

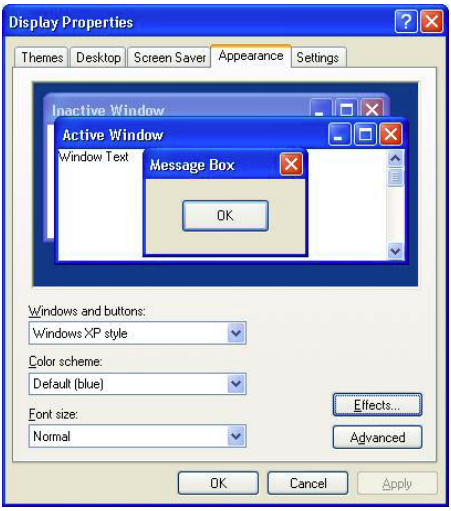
For optimal performance of the Digital KVM over IP Switch and whatever devices it's connected to, keep these configuration points in mind for networked computers and servers.

*Select resolution modes that are within the switch's standard support parameters:*

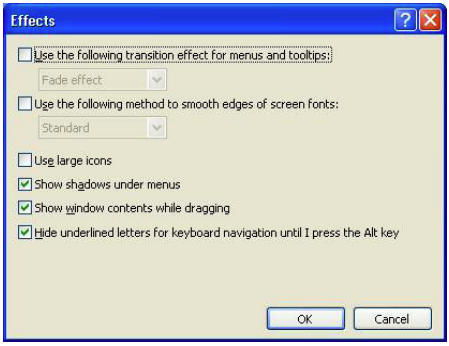
The Digital KVM over IP Switch supports most display modes up to 1600 x 1200. However, you might encounter some display problems when your display card is outputting an unusual display mode, such as no video or an abnormal screen display. To simplify the display factor before connection to the switch, it's recommended that more standard display modes be used (see chart at left). ***NOTE:*** These are suggested display modes for server desktops; however, actual feasible display modes for any particular server desktop will be dependent on its display card. (That is, some display modes listed on the chart might not be feasible with some display cards, and a trial-and-error approach may be more useful in determining the best display mode.)

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

*Disable special transition effects on the screen outputs of your connected servers:* Go to Control Panel → Display → Appearance → Effects. Uncheck any of the selected options (as needed) in order to disable transition effects such as Fade for the menus and tool tips. Perform this same operation on each of your connected servers. ***NOTE:*** On platforms such as Windows 98, 2000, XP and Server 2003, 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 prevent undesirable artifacts from appearing on your screen, deselect the special transition effects.



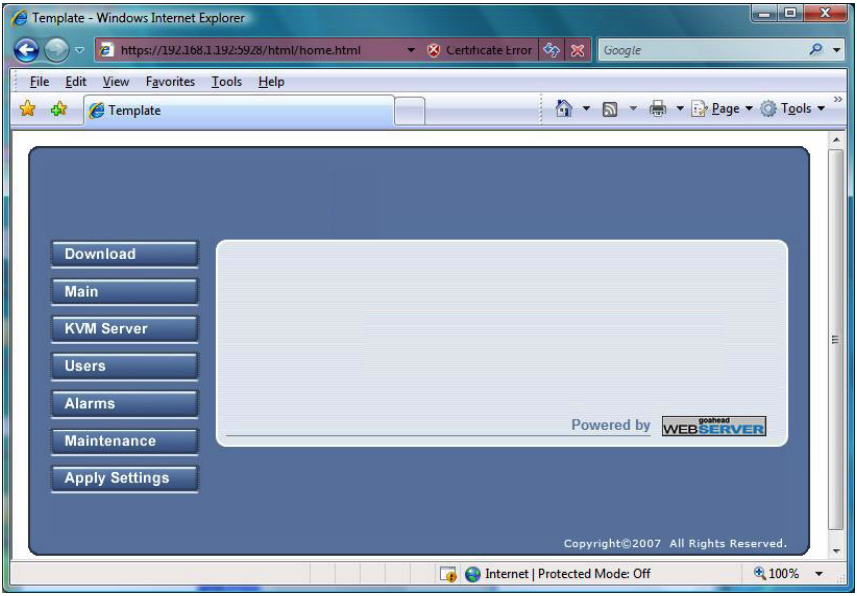

*Choose plain and solid server desktop backgrounds for your connected servers:* To optimize the bandwidth efficiency and speed up video performance across the bandwidth-limited environment, it's recommended that you select a relatively plain server desktop: solid colors or light-colored graphics. Complex patterns or color gradients should be avoided if bandwidth is critical in your application, as they will create more bandwidth demands for their transmission across the Internet.



## Network Settings

1. Connect the Digital KVM over IP Switch to the Ethernet LAN. The factory default network settings for the switch:
   - IP address: 192.168.1.200
   - Net mask: 255.255.255.0
   - Gateway: 192.168.1.254
   - DNS: 192.168.1.254
2. Access the switch's Web Management interface by entering the following in the address bar of your browser window on a remote client: https://192.168.1.200:5908.
3. A login prompt displays for the account name (username) and the password. Use the defaults:
   - Username: superuser
   - Password: superu

   After logging in, you will see the Web Management interface.




4. Go to the LAN TCP/IP page on the switch's Web Management interface and modify your IP settings. (Refer to Unit Management over a Secure HTTPS Browser Connection / Main / TCP/IP Settings – Port and IP Settings.)
5. Click "Apply Settings."
6. Verify the switch's network connection by connecting to the switch through the Web Management interface using the new IP address. ***NOTE:*** The IP address should be followed immediately by a colon and the port base +8 for the port number:

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

   For example, if the IP address is 192.168.1.7 and the port base number is 5970, then you should enter https://192.168.1.7:5978. ***IMPORTANT:*** Remember that it's a secure SSL-encrypted connection, so enter "https" instead of the usual "http." Otherwise, the connection won't be established.

## Port Base Settings

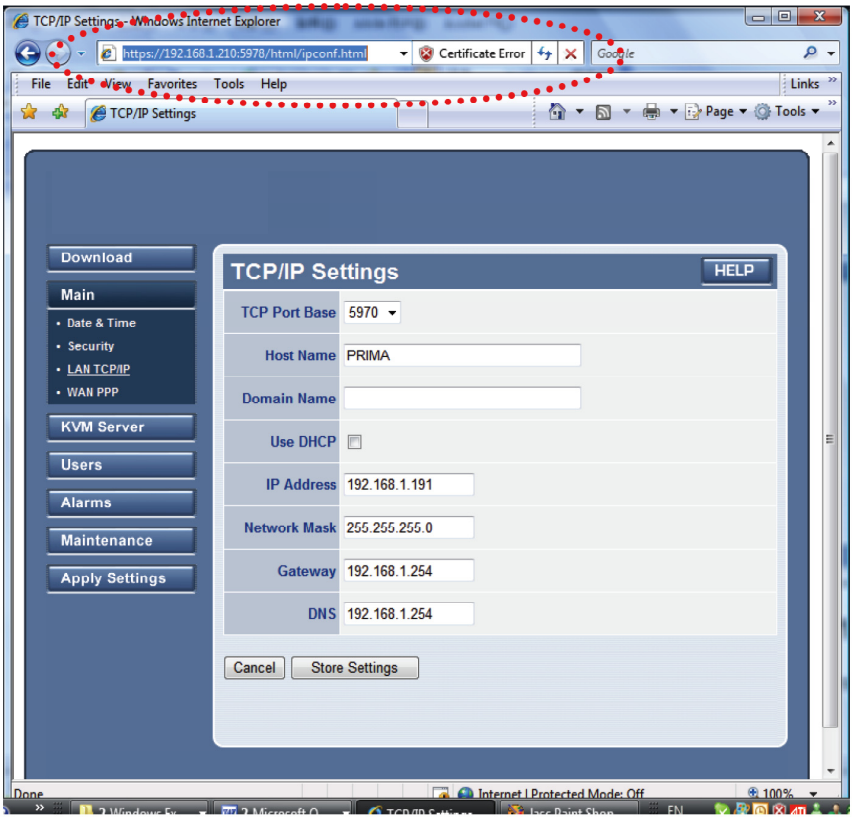
***NOTE:*** If you're satisfied with the default port base setting as 5900, you can skip this section.

The default port base for switch 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.

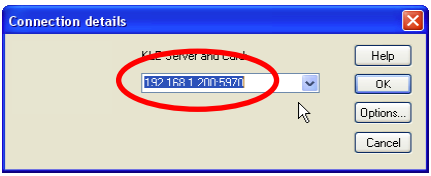
- for viewer connection: <Port base>
- for secure browser connection: <Port base + 8>

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:

- for viewer connection: 5970
- for secure browser connection: 5978




Click "Submit" and "Apply Settings" to validate the new settings. The switch is now installed within your LAN, and you're able to proceed with establishing a remote viewer connection.



## Configuration of the Firewall/Router for Access across the Internet

To allow access to the Digital KVM over IP Switch behind a corporate firewall/router, establish the following settings on your firewall/router (not on your switch).

1. Configure a virtual server on your router (or ask your network administrator to do it) as mapped to the switch's local IP address.
2. Open a port range (<port_base> – <port_base_+_9>) both inbound and outbound for the virtual server according to what has been previously configured as the port base for the switch.

As per the previous example, if the switch is configured with a port base of 5970, then the port range should be opened as 5970–5979 (i.e., <port_base> – <port_base +9>) both for inbound and outbound, in which:

- for the switch's viewer connection port: <port_base> = 5970
- for the browser SSL connection port: <port_base + 8> = 5978
- for viewer internal communication, etc.: <port_base + 9> = 5979

***EXAMPLE:*** Router Internet IP ↔ virtual server (port range open) ↔ switch's local IP 61.232.134.120 ↔ virtual server (port 5970–5979 open) ↔ 192.168.1.7

Once you've configured a virtual server with an appropriate port range open (<port_base> – <port_base_+_9>), you can try to access your switch across the Internet by using a public IP address and designated port number. Based on the previous example settings:

- 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

***NOTE:*** Once you've changed the port base of your switch, you should also modify the open port range on your router accordingly if you want Internet access to come across.

## Installation of Certificates

***NOTE:*** You can use the default set of certificates (on the included CD) to practice making some PKI-authenticated connections as long as your network safety isn't jeopardized. It's recommended that this be done within your local area network, assuming it's well secured with an adequate firewall and other due precautions against network intrusions. Otherwise, anyone who has a copy of the default certificates can establish a connection to your servers. If you have already obtained a set of certificates with the file names and formats required for the switch (which is strongly recommended), you can use them for viewer authentication. You can also generate the certificates using software like XCA. (For certificate generation using XCA, refer to "How to Generate ... Certificates Using XCA" on the included CD.)

First, you need to have these certificates — as mentioned above, if you haven't obtained your own certificates, you can use the default set of certificates — ready on your client computers for uploading to the switch via a Web browser:

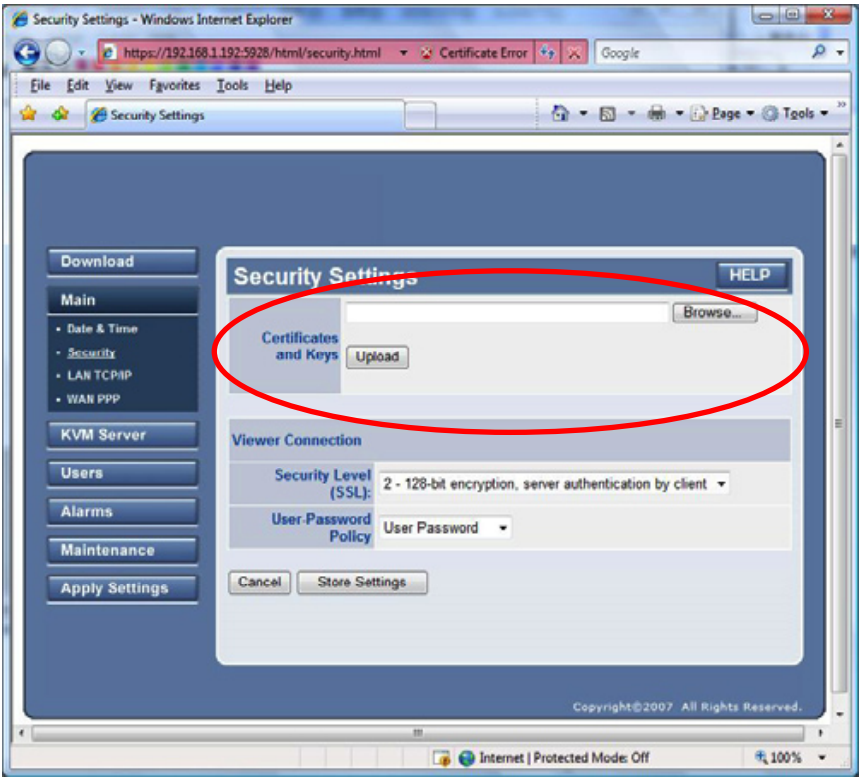
For PKI Authentication to be installed on the Digital KVM over IP Switch —

- root certificate (root.crt)
- server certificate (server.crt), and
- server private key (serverkey.pem)

For LDAP Authentication to be installed on the Digital KVM over IP Switch —

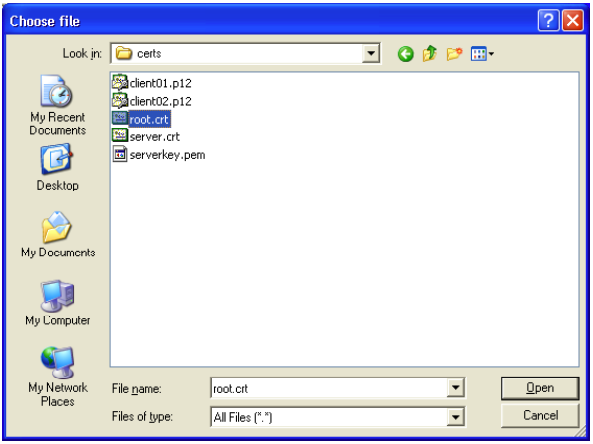
- server LDAP certificate (ldapcert.crt), and
- server LDAP private key (ldapkey.pem)

Once you've located whichever set of certificates is to be used, you can begin the installation.




1. Access the switch's Web Management interface and go to the Security Settings screen.
2. Click "Browse" and use the "Choose File" dialog box to browse and locate your certificate files.
3. Click "Upload" on the Security Settings screen to upload the root certificate to the switch. When the upload is completed, the prompt page for rebooting will display.
4. Click "Reboot." Once the switch has booted back up, continue with the import of the server.crt and the serverkey.pem files.

***NOTE:*** You don't need to reboot each time you finish uploading a certificate: You can do one complete reboot after you finish uploading all of them. To return to the previous Security Settings screen to upload another certificate without immediately going to a reboot, just click "Security Settings" on the left side of the screen.



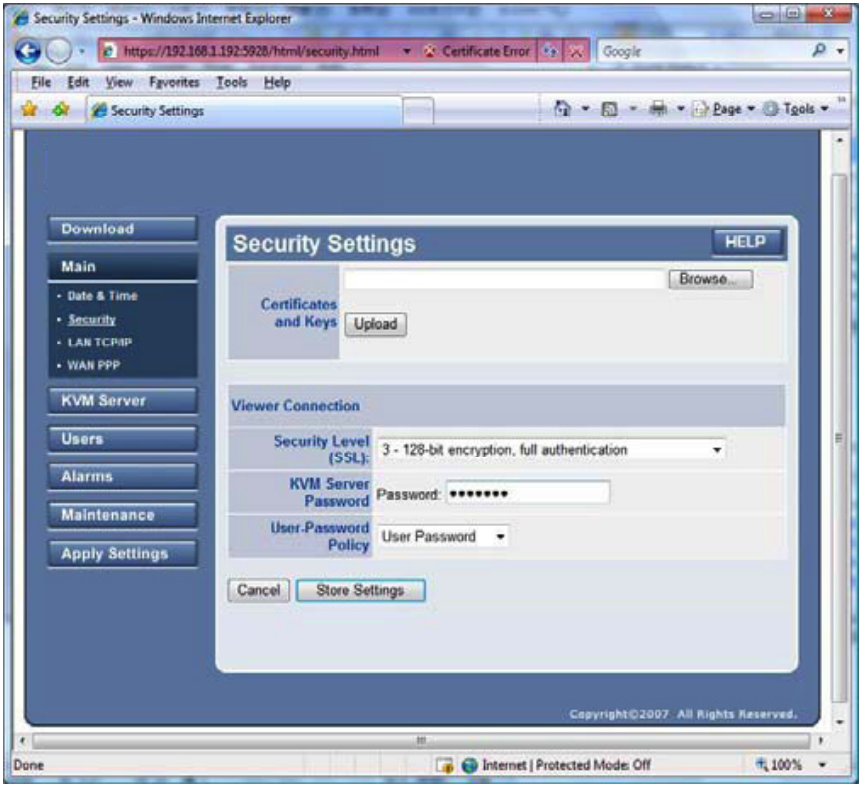
## Selection of a Security Level for Viewer Connection

1. Go to the Security Settings screen on the switch's Web Management interface and make a viewer connection selection from the "Security Level" drop-down menu.
   - 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 the switch is intended to be accessed through an 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.

***IMPORTANT:*** The selection of a security level to be implemented for the switch's viewer connection is of utmost importance, especially when your remote server connections require a high level of security in order to keep your servers safe from unauthorized entry and/or network sniffers.

2. (Optional) If you choose to implement the PKI authentication feature on the switch's viewer, you need to select Level 3 security in the Viewer Connection panel on the Security Settings screen of your Web Management interface.




Then enter the password in the "KVM Server Password" field. ***NOTE:*** You should enter the password that has encrypted the server private key in the server private key file (serverkey.pem)

in order to make a successful viewer connection with the switch in the Level 3 security setting. If you use the standard set of certificates provided on the included support CD, 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 issued those certificates.

3. Go to the Apply Settings screen and click “Restart Servers” to validate your selection.

## Selection of a User Password Policy

1. On the Security Settings screen, select one of three options from the “User Password Policy” drop-down menu.
   - No Password
   - Global Password
   - User Password

   If you select “No Password,” anyone can establish a connection without entering a valid password.

   If you select “Global Password,” the viewer will prompt you for a global password, which is used by all who want to make a viewer connection to the switch.

   If you select “User Password,” the viewer will prompt you for a user-specific password. With this setting, each login user will be checked against his or her corresponding password before being allowed a viewer connection.
2. Go to the Apply Settings screen and click “Restart Servers” to validate your selection..

***NOTE:*** In all, there are nine (3 x 3) possible combinations of Viewer Security Levels / Password Policies, allowing administrators to choose the pairing that best suits their particular needs.

| | 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 U = User-specific Password S = 256-bit SSL Encryption P = 1024-bit PKI Authentication N = Not available

***IMPORTANT:*** User Password Policy and Security Level (SSL/PKI Authentication) settings should be used with caution: If you adopt No Password Policy and No SSL Encryption / No SSL Authentication, anyone with a viewer and knowledge of the access IP and port number of the switch can establish a remote connection.

At this point, your Digital KVM over IP Switch is ready for a PKI-authenticated plus SSL-encrypted viewer connection! All you need to do is to distribute the following to your remote connection client(s):

- Certificates (obtained from your Certification Authority and required only if you selected Level 3 viewer security)
- Certificate password (obtained from your Certification Authority and required only if you selected Level 3 viewer security; if using the default set of certificates, use “clientpwd”)
- Username and password (specified on the Web Management interface/screen and required only if you chose the User Password option; if using defaults, use the username/password combinations Superuser/superu, Admin/123456 or User/123456)
- Global Password (as specified on the Security Settings screen and required only if you chose the Global Password option)

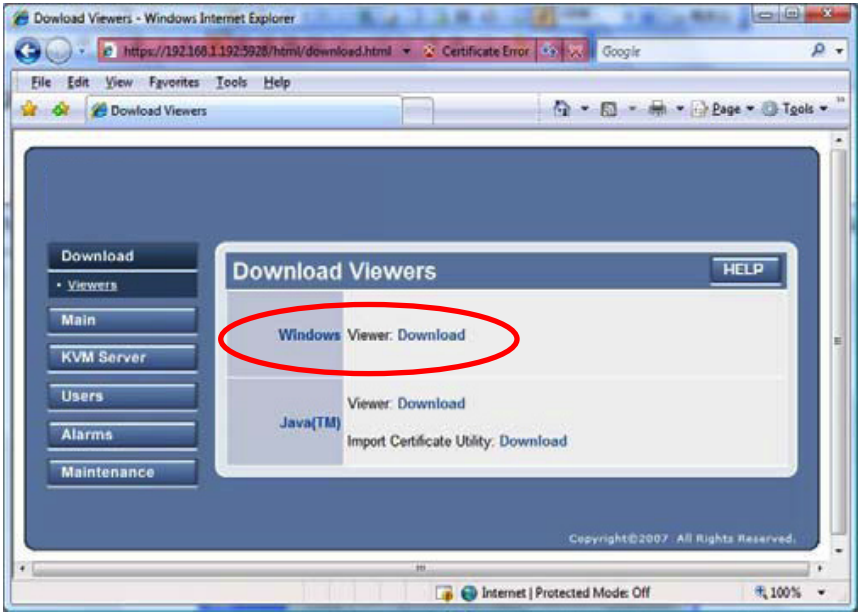
# VIEWER CONNECTION

The Digital KVM over IP Switch provides a Win32 viewer for Windows users and a Java viewer for cross-platform use on any major operating system.

## Installation of a Win32 Viewer

Go to the Download screen to download the Win32 viewer (Kripview_install.exe). Install the viewer program on the client computer that will connect to the switch. After installation, a KLE icon (right) will be created on your client desktop.

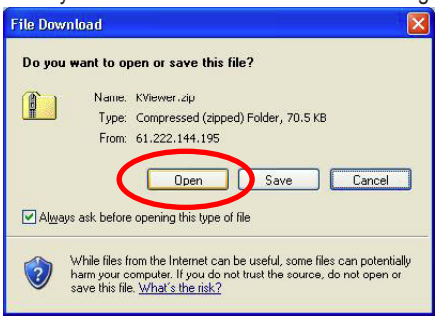



## Installation of a Java Viewer

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 can be downloaded from www.java.com. To download the Java viewer, just go to the Download screen of the Web Management interface. ***NOTE:*** To run the small Java program, you don't have to actually save the Kviewer.jar file to your local hard drive since it isn't that big (only 70 kB): You can open it directly. Note also that on some client platforms — such as Linux — after you have installed the JRE file on your client platform, you need to set the path information in order for the client system to know where the Java compiler program is.



## Importing Certificates to a Viewer on a Client Computer

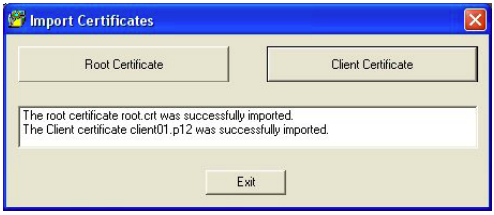
***NOTE:*** If you will be using only the non-PKI-authenticated viewer connections to the switch (such as Level 1 – no encryption/authentication or Level 2 – 256-bit SSL encryption and only server authentication by client), you are not obliged to use or import any certificates and you can skip this section.

To make a fully PKI-authenticated viewer connection with the Digital KVM over IP Switch, you need to import client certificates to the Win32 viewer and Java viewer on the client computer. A default set of certificates is provided on the enclosed CD, or you can use your own set of certificates. If using your own, in addition to importing the client certificates to the Win32/Java viewer on the remote client computer(s), you should import the root certificate, the server certificate and the server private key to the switch on the Web Management interface Security Settings screen. (Refer to Main/Security – Certificate Installation, Viewer Encryption and Password Policies in the next section.)

The file names of the client certificates can vary (client_name1.p12, client_name2.p12, etc.), but the certificates and private key for the switch remain as they are (root.crt, server.crt, serverkey.pem). The client certificates should be imported in the .p12 format, using the import utility of whichever viewer (Win32 or Java) is on the client computer. ***NOTE:*** Make sure you have the certificates ready for import, either on a transfer device or the local computer hard drive. If you copy certificates to the local hard drive, you may need to delete them after finishing the import so others won't have access to the certificate files. Even though they're password-protected, one can never be too careful. Remember, too, that the Win32 and Java viewers require separate certificate import utilities.

### Import a Client Certificate to a Win32 Viewer

Go to Start → Programs → PROSUM → Prima IP Viewer → Import Certificates. Click "Root Certificate" to import the root certificate; click "Client Certificate" to import the client certificate. When the "successfully imported" message appears in the text field, click "Exit" to proceed.




### Import a Client Certificate to a Java Viewer

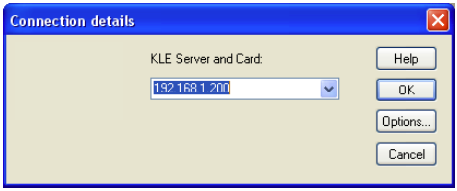
Go to Start → Programs → PROSUM → Prima IP Viewer → Import Certificates. Click "Root Certificate" to import the root certificate; click "Client Certificate" to import the client certificate. When the "successfully imported" message appears in the text field, close the window to proceed.




Once you've imported certificates to the viewers on the client computer(s), you can make your viewer connection(s).

# Viewer Connection Options

The viewer connection option interface presents several options that can be combined in various ways to optimize your viewer connection. In the Connection Details window, click "Options" (represented by the top two screen images at right for Win32; by bottom two images for Java).



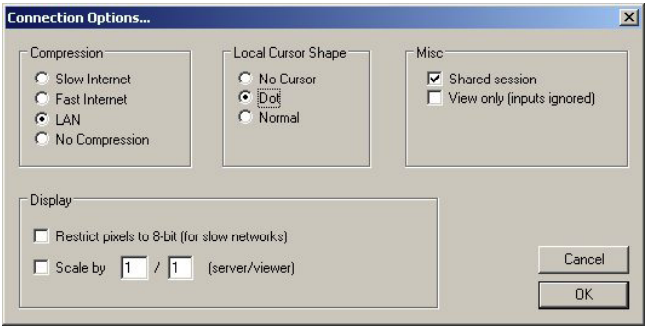

### Compression

*Slow Internet:* Video quality is optimized viewer connection with slower Internet bandwidth.

*Fast Internet:* Video quality is optimized for connection with better Internet bandwidth.

*LAN:* High video quality for connection over the LAN.

*No Compression:* Best video quality with no compression.

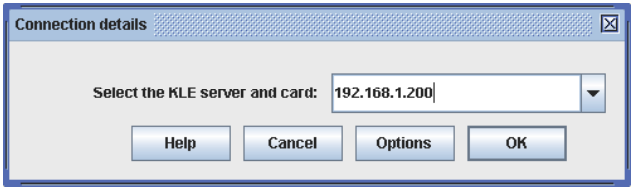



### Local Cursor Shape

*No Cursor:* The local cursor is invisible on the viewer.

*Dot:* A dot shape used for the viewer cursor.

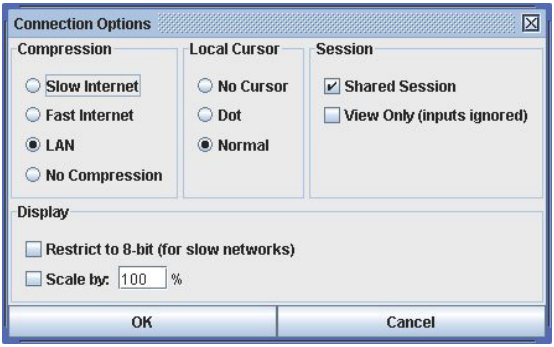
*Normal:* An arrow shape is used for the local viewer cursor.




### Misc/Session

*Shared Session:* Multiple users access the same server desktop.

*View Only (inputs ignored):* Keyboard and mouse inputs are ignored (but not restricting keyboard and mouse access for other users).

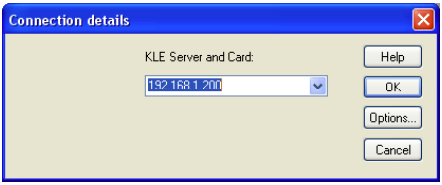



### Display

*Restrict pixels to 8-bit (for slow networks):* Color is reduced to 256 colors for slow connection.

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

## Establishing the Viewer Connection

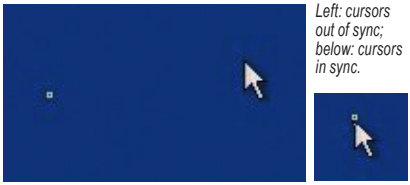



To use the Win32 viewer for connection, run the viewer program, entering the access address and port number for the switch in login window (as shown at right with default IP address). ***NOTE:*** You can enter access IP address without specifying the port number (as shown), but only when the port number is defaulted to 5900. (You can also enter the full default address: 192.168.1.200:5900.) If the port setting on the switch has been changed, the IP address needs to reflect this by specifying the port number at the end. To connect to port 5910 on the server, for example, enter 192.168.1.200:5910. (Refer to Main/LAN TCP/IP – Port and IP Settings for details.)

When prompted for a password or private path phrase, enter the username and password previously established. The default username/password = superuser/superu; the default global password (if using the Global Password policy setting) = 123456; the default private path phrase (if using the Level 3 security setting) = clientpwd. Once these entries have been made, a viewer connection will be established.

***NOTE:*** If you are using a dial-up modem and experiencing slow keyboard/mouse movement and response, it could be due to your 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 could be a network bottleneck somewhere between the switch and your client desktop.

## Cursor Settings/Synchronization

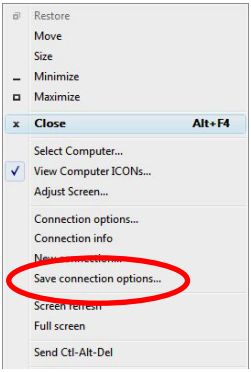


*Left: cursors out of sync; below: cursors in sync.*

Normally, you will see both the local cursor and the remote cursor in the view area. You can specify the shape of the local cursor as seen within the view window: as a dot, an arrow or none (not showing any local cursor within the viewer area). If the two cursors become out of sync, simply press the mouse synchronization hotkey sequence (right Control, right Control, Home) to re-synchronize them.

***NOTE:*** 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: You can click the target just using the local cursor well before your remote cursor catches up with the target.

## Saving Connection Settings

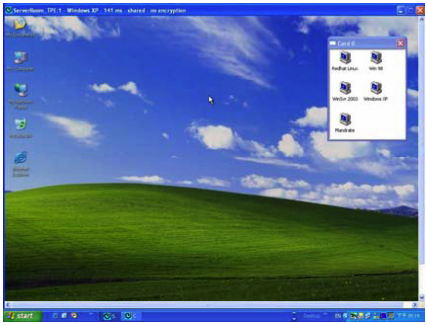


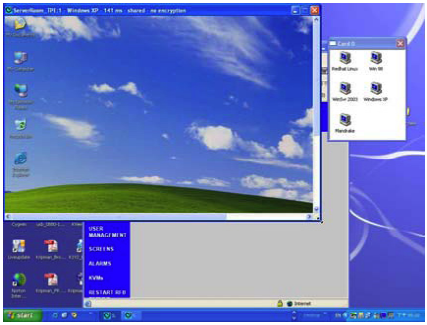

Once you have optimized your viewer connection, you might want to save the selected connection options. This way, the next time you log in with the viewer, that specific client computer will use the stored connection parameters as well as the password (but not the private path phrase, which is not saved since it is used by a secured/PKI-authenticated connection) for connection with the switch. To save connection options, click the icon on the viewer title bar to display the viewer's Quick Menu and select "Save connection options."

# Win32 Viewer Settings

### Window Size Adjustment

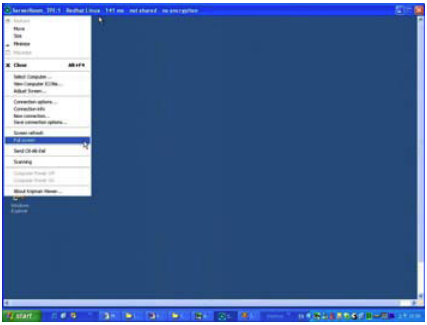
The size of the viewer window can be adjusted by dragging the border of the viewer windows.





### Full Screen Mode

For a full-screen display, click the viewer icon on the title bar of the viewer window to display the Quick Menu (shown on the left-hand side of the image at right), then select “Full Screen.”

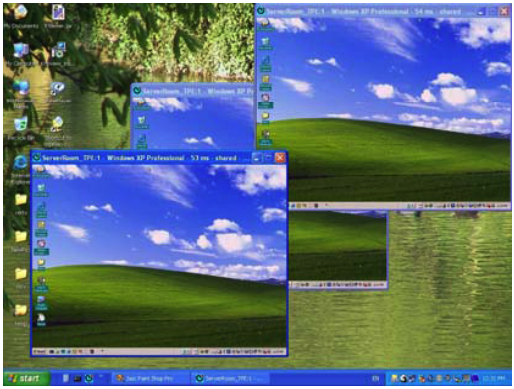





A message prompt will display as a reminder of how to exit the Full-Screen mode. Click “OK” and the viewer will present Full-Screen mode. To exit Full-Screen mode, press Ctrl-Esc-Esc to bring up the local task bar, then right-click the viewer taskbar icon to bring up the Quick Menu again. Click to de-select Full-Screen and restore the display to the normal window mode. ***NOTE:*** Only the Win32 viewer supports Full-Screen mode — the Java viewer doesn’t.

### Window Size Scaling

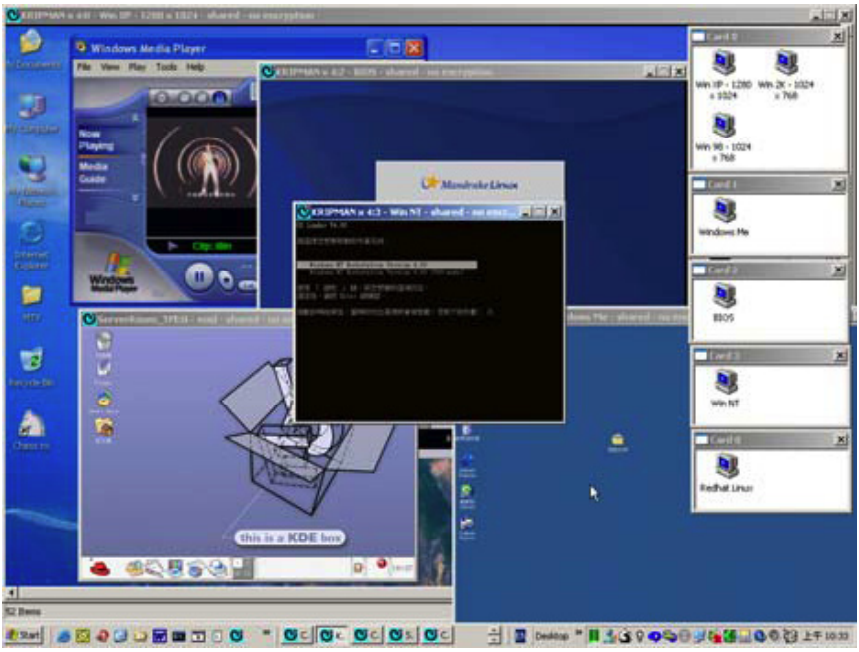
To scale the viewer display, click the viewer icon on the title bar of the viewer window to display the Quick Menu, then select “Connection Options.” With the Connection Options screen displayed, specify the proportions of the viewer window that you want, then select the option. Click “OK” to scale the window. (In the example at right, “1/2” is the specified proportion.)



### Centralization of Remote Server Control

If you have multiple units installed in a distributed manner among your global branch offices, you can simultaneously monitor different remote servers distributed over this Digital KVM over IP

Switch infrastructure using a single client desktop. (Shown below: The upper image presents five Win32 viewers on a Windows client desktop, each showing a different remote server desktop; the lower image presents four Java viewers on a Linux client desktop, each showing a different remote server desktop.)






## Title Bar Information




*ServerRoom_TPE:* This is the name specified for your video server.
*Windows XP Professional:* This is the name you specified for this connected computer.
*54 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. ("not shared" indicates a session that blocks others from subsequent logins.)
*Optimizing:* Indicates the video server is optimizing the video capture from the server desktop.
*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). ("no encryption" indicates no encryption for signal transmission [Level 1].)

## Select Computer Box




**Win32 Viewer**
The Select Computer box allows you to perform intuitive click-and-switch operations without memorizing the varied port-switching hotkey commands that could exist on different kinds of switches installed with this device. To use the click-and-switch feature, first configure the KVM switching hotkey commands for any connected KVM switch(es) by using the Web Management interface. (Refer to KVM Server/KVM Switch Database – Keeping and Adding Your KVM Database in the next section.)

The Select Computer box always displays at the top of your screen once a proper viewer connection is made. In the box, you can see the computer icons together with the computer names already specified for each of them using the Web Management interface. To switch to a computer, just click its icon in the box. ***NOTE:*** These icons only represent what's already been registered using the Web Management interface, and don't indicate the status of a connection or whether or not the computer is on.

**Java Viewer**
To display 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.) To switch to a specific computer, click/select any item on the list.



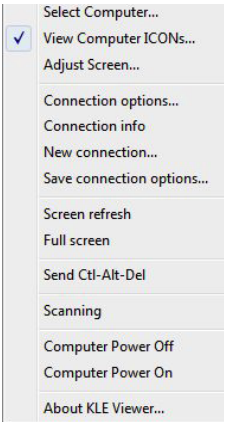

## Viewer Quick Menu

The Quick Menu on the Win32 viewer can be displayed by clicking the program icon at the upper-left of the title bar or by right-clicking anywhere on the title bar. If using a Java viewer, just select a menu option from "Actions," "Settings" or "Information" right below the title bar. ***NOTE:*** The following operations and screen images represent the Win32 viewer. Although the Java viewer has a slightly different menu arrangement, you should find it just as easy to use (except that the "Full screen" option is unavailable on Java).

*Select Computer:* Select a remote computer using the drop-down combo box (as shown below).
*View Computer Icons:* Open the "Select Computer" box make a selection by clicking an icon.
*Adjust Screen:* Fine-tune the screen area by pixel shifts.

*Connection options:*
Click to display the "Connection Options" window (below).

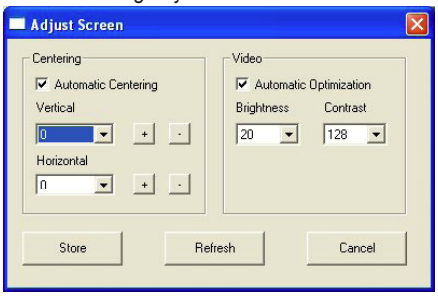


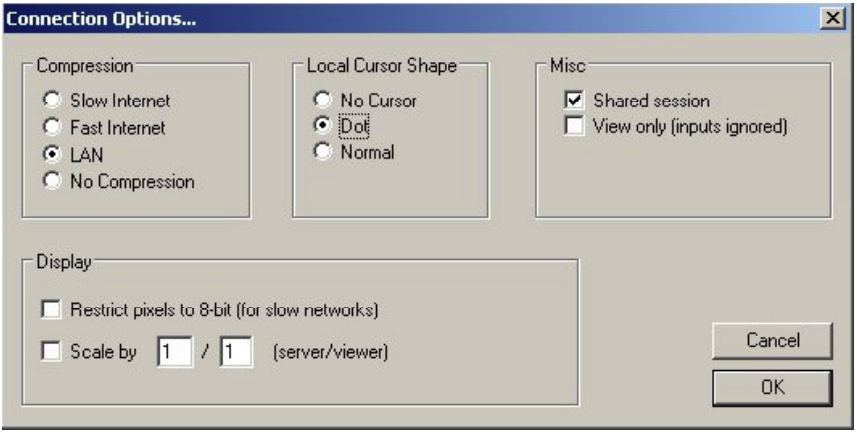

*Connection info:*
This displays the server connection information as it relates to the viewer session.

*New connection:* Make another new connection using the viewer.

*Save connection options:* Save the settings (such as those connection parameters specified in the "Connection Options" window) and also the password within the registry of the client computer.
***NOTE:*** By selecting this option, you can save your session password as well as other connection parameters in the registry of your client computer, so the next time you log in to the viewer for a new session, you won't be prompted for the password again. However, the client path phrase required in the connection of Level 3 security (256-bit SSL encryption and PKI Authentication) won't be saved and will be requested every time you log in with the Level 3 security setting.




*Screen refresh:* Force-update the viewer screen output.




*Full screen:* Change the viewer screen to Full Screen mode. (Only the Win32 viewer supports this 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 command with a delay time to a conventional KVM switch.




*Computer Power Off/On:* Send a Power Off (or On) serial port command to the remote power control unit (only SUPERADMIN or ADMIN is authorized).

## Video Display Troubleshooting

The video server supports most major display modes up to 1600 x 1200. Some display problems can occur, however, such as when there is abnormal or unusual display output from your server, when the display resolution is beyond the maximum support level of 1600 x 1200, or when the display vertical frequency is beyond the support range in that pixel dimension. A few of the more common issues are addressed below.

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

- The video filter may be set at either the Medium or Low quality level. These two levels are for faster response than is provided by the High setting in order to increase the response speed in limited bandwidth conditions. If your bandwidth allows — or if you need higher video quality in lieu of higher speed — just change the video filter from Low to Medium (or even High). To raise the video filter level, go to the Main Settings screen (in the KVM Server submenu) and select the filter as either Medium or High Quality. Note that a High Quality video filter setting provides results at the expense of video response speed on the viewer screen.
- The transition effects in Windows XP are enabled, which will cause refreshing problems in Low/Medium Video Filter settings. Thus, if you are using a Low/Medium Quality level of the video filter, either try to raise the video filter level to High Quality (at the expense of response speed) or just turn off the transition effects in Windows XP. To turn off the transition effects in Windows XP, see Additional Server Configuration Considerations, P. 11. Also note that the local console is not affected at all by the Video Filter settings or by the transition effects in Windows XP.

***The switch's booting time has become unduly long. What's wrong?***

- Make sure that the external authentication, PPP server/client, time server and power control settings are correct. If you don't use all these features or the authentication/time servers are not available, just try disabling them to save booting time; otherwise, the switch will try to look for them till timeout.

***Video response seems slower under limited bandwidth conditions. Are there ways to increase the response speed?***

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

- Under bandwidth limited conditions, you should select a more economical encoding scheme, such as Slow Internet or Fast Internet Encoding instead of the LAN or No Compression options from the viewer connection menu. However, if the connection is made only within the LAN with plenty of connection bandwidth, LAN or No Compression encoding schemes should be (paradoxically) quicker than the Internet scheme – since your client computer won't dissipate extra computing power for decoding the more compressed Internet scheme.
- Use 8-bit color reduction (with only 256 colors instead of the 65K colors in 16-bit settings).
- You can enable Automatic Filter Adjustment (Web Management/Video Server screen) for automatic video optimization based on different bandwidth conditions.
- If you don't want to use Automatic Filter Adjustment, you could always select either Medium Quality or Low Quality for more speed as your Video Filter setting. You could also use a server desktop with smaller resolution (such as 800 x 600) and use a solid, plain-color background for server desktops.
- Also, check the networking environment to see if there is any bottleneck that can be improved or eliminated for more bandwidth throughput.

***When a connection is first made, the viewer screen display doesn't appear to be centered correctly, and there is a black margin on the edge. How can the black strip be removed?***

The black strip is the offset that'll be seen when the display on a viewer screen isn't centered correctly because the switch's automatic centering option isn't enabled. When the viewer

connection is made, select the Adjust Screen option on the viewer's Quick Menu to display the Adjust Screen window (as shown on Page 25). Check whether or not you have Automatic Centering enabled. If it is not yet enabled, select/enable it. If it is already checked, uncheck it, wait at least 15 seconds, then check the option again to force the video server to align (center) the display on the viewer screen.

***I can log in and make a successful browser connection with the switch, but I can't make a valid viewer connection or the switch doesn't respond to my viewer connection request.***

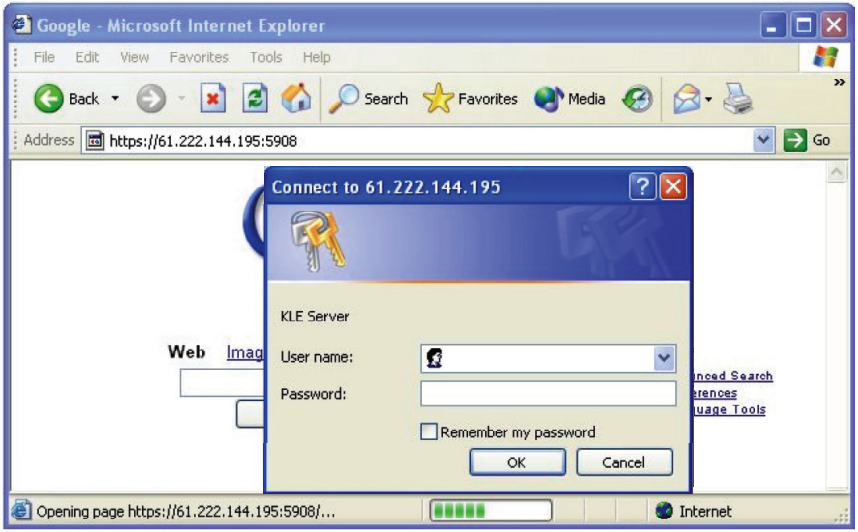
- The switch's video server may not be functioning properly. First, make sure your account has the SUPERADMIN privilege. If not, you should request one that has the SUPERADMIN privilege to do the troubleshooting job for you. Next, go to the Apply Settings screen on the Web Management interface and click "Restart Servers" to restart the switch. Wait at least 10 more seconds for it to start completely, then try to make the viewer connection again to see if it is back to normal. Second, If clicking "Restart Servers" doesn't solve the problem, click "Emergency Reboot" on the Maintenance screen of the Web Management interface for a complete start from ground level. An emergency reboot is a clean reboot, and it takes longer for the switch and video server to load; thus, you need 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's been brought back to normal. ***NOTE:*** A cold boot is always a last resort to bring the switch back: Disconnect the power adapter from the switch and wait about 30 seconds before plugging it back in and restarting.

# MANAGEMENT OVER A SECURE HTTPS BROWSER

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

## Web-Based Management Interface

Enter a correct IP address and port number in the address field:
https://<IP_address>:<port_number> → https://61.222.144.195:5908

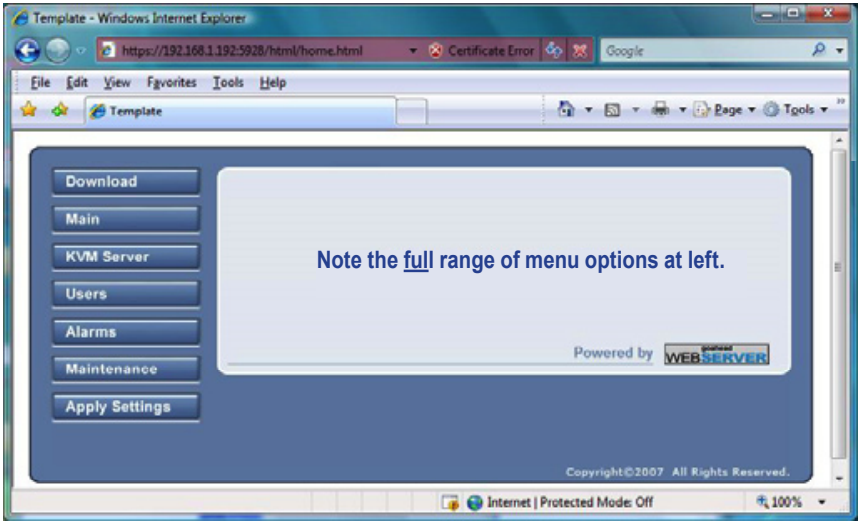


***NOTE:*** Remember that it's a secure SSL-encrypted connection, so you should enter "https" instead of the usual "http"; otherwise, the connection will not be established. The port number may vary according to its setting on the server. By default, the browser connection uses port 5908. Both the username and password are case-sensitive.

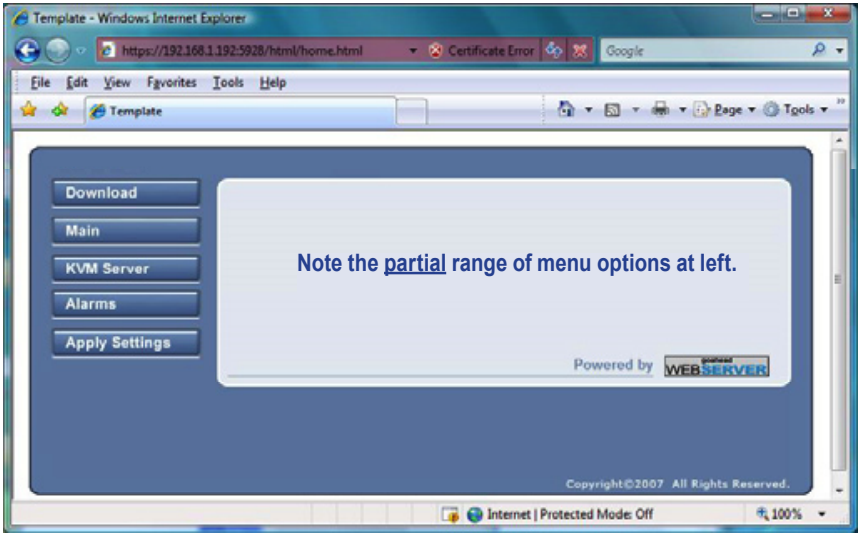
**User Privileges: SUPERADMIN, ADMIN, USER**

The switch offers three categories of user privileges for Web Management (as indicated by the varied range of menu listings on the screen images below and the table that follows).

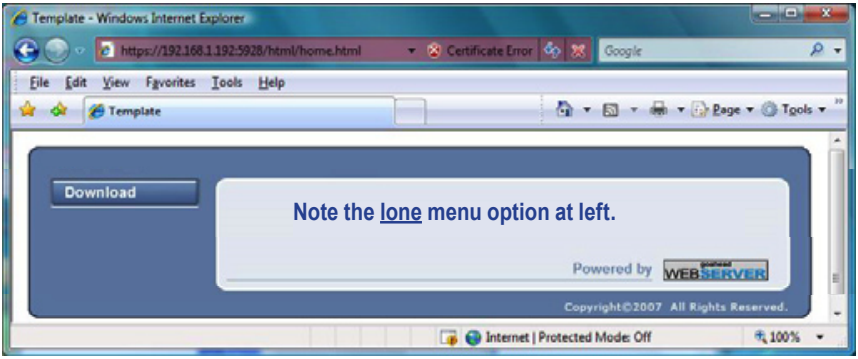
*SUPERADMIN:* Provides full access to Web Management features (and the Power On/Off feature on the viewer).




*ADMIN:* Provides partial access to Web Management features (and the Power On/Off feature on the viewer).



*USER:* Provides only minimal access to Web Management features (only the Download screen).

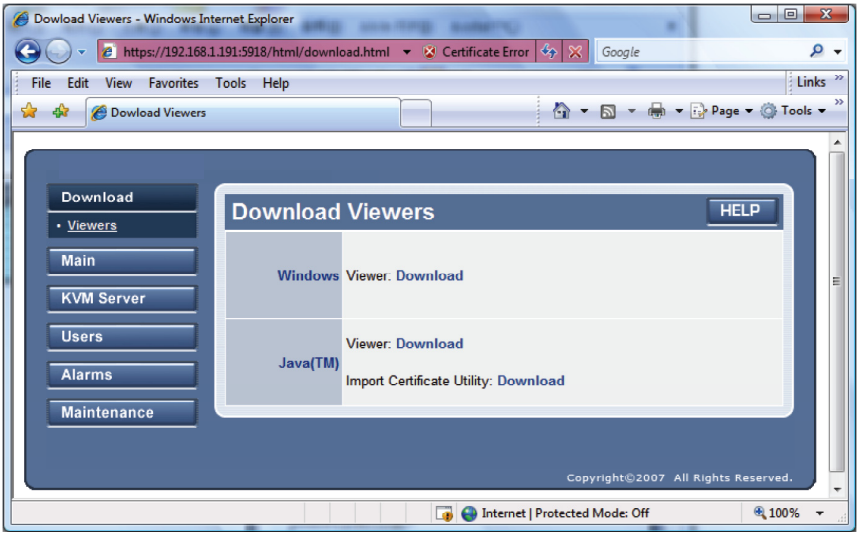



| Browser Management Access Privilege | | | |
|---|---|---|---|
| **Feature Page** | **SUPERADMIN** | **ADMIN** | **USER** |
| Download | √ | √ | √ |
| Main | √ | √ | × |
| KVM Servers | √ | √ | × |
| Users | √ | × | × |
| Alarms | √ | √ | × |
| Maintenance | √ | × | × |
| Apply Settings | √ | √ | × |

## Download

### Viewers

The Download menu option lets you download both the Windows and Java viewers.



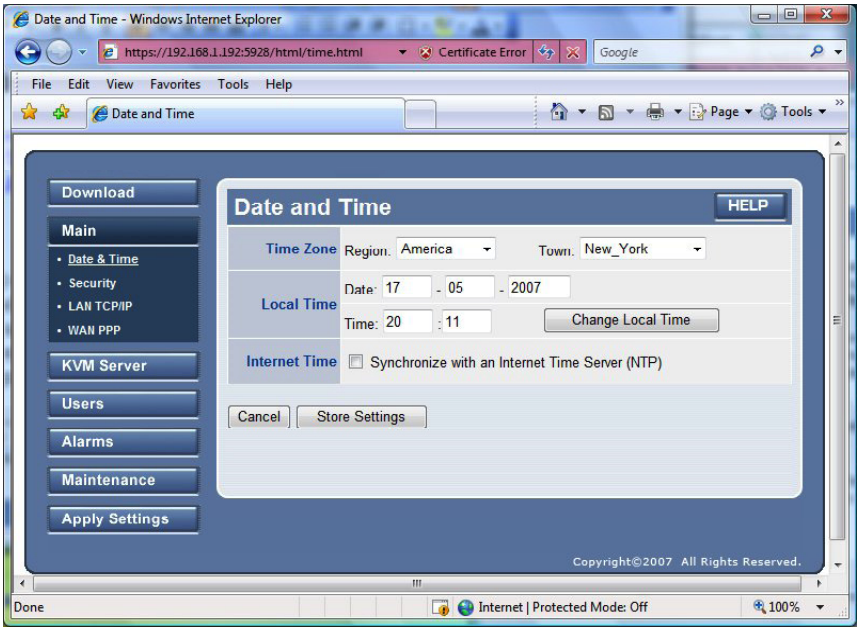
The viewer for Windows can run on most Windows platforms: 98/Me/NT/2000/XP/Server 2003/ Vista. Click “Download” and follow the installation instructions. ***NOTE:*** To use the secure full-SSL connection (Level 3 security), obtain a set of certificates from your administrator. Install the certificates on your computer by running the Import Certificate utility provided with this viewer. Refer to the Security section.

The viewer for Java is truly cross-platform for all major operating systems, including Windows, Linux and Mac OS. 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 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 (*not* javaws.exe). On other machines, download the KViewer.jar file into a folder; then enter: java -jar KViewer.jar. ***NOTE:*** Some browsers will automatically change the file extension from .jar to .zip while you are downloading the file. If this is the case, change the file extension back to .jar so that you can run it properly. ***NOTE:*** To use the secure full-SSL connection (Level 3 security) with the Java viewer, obtain a set of certificates from your administrator, download the Import Certificate utility Impcert.jar file into a folder, then enter: java -jar Impcert.jar. Refer to the Security section.

## Main: Date & Time

This screen allows you to configure the time-related settings of your switch, including time zone, local time and Internet time. After you have made all modifications, click “Store Settings” to save your settings, then click “Apply Settings”/”Restart Servers” to validate these new settings. ***NOTE:*** No change made on this screen will take effect until you click “Apply Settings”/“Restart Servers.”




### Time Zone

Select the time zone/region and city/town from the available list as seen in the drop-down menus. For example: If the switch is located in Los Angeles, you can choose “America” as your time

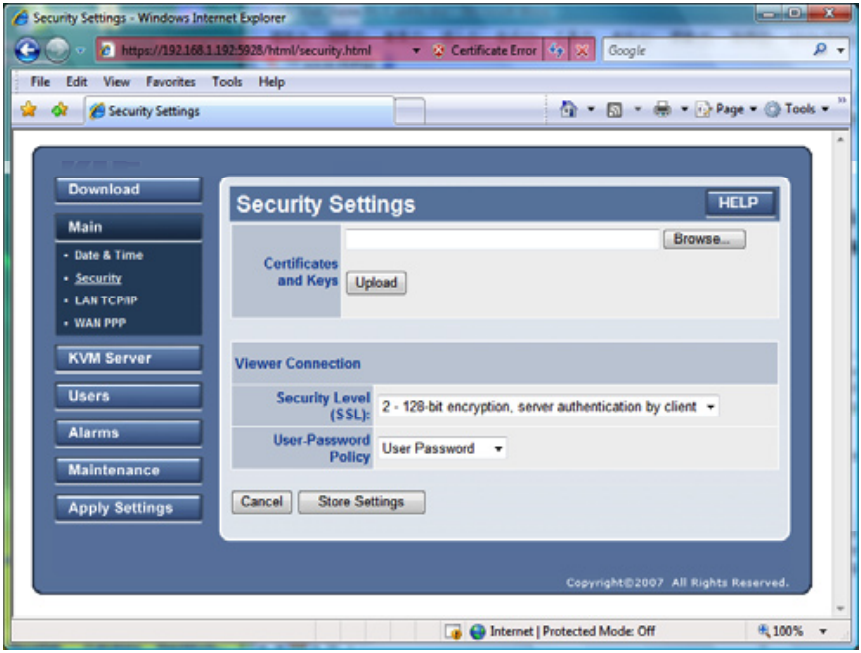
zone and “Los Angeles” as your region. The advantage of setting up the correct time zone is that you don’t have to change your local time setting every time you relocate the switch to a different time zone. Instead, you just change the “Time Zone” settings and let the switch readjust the local time for you.

**Local Time**
Enter the correct date (dd-mm-yyyy) and time (hh:mm) here and click “Change Local Time” to set the current system time on the switch.

**Internet Time**
If you check the option “Synchronize with an Internet Time Server (NTP),” the time setting will be periodically synchronized to the time of the NTP server specified on each restart of the switch and every hour. NTP Server1 is the server the switch will first try to synchronize with; NTP Server2 is the backup time server, which the switch will synchronize with 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 local date and time settings you manually entered will be refreshed with the time provided bythe Internet time server. There are many Internet time servers available: Search the Internet for those nearest your switch installation, as a time server nearer to you will reduce time latency in synchronization.

## Main: Security

This screen lets you to configure and implement security-related settings of your switch, such as uploading your certificates for the server side, selecting the security level of the viewer connections, and establishing the password policy for the viewer and browser connections. After you have made all modifications, click “Store Settings” to save your settings, then click “Apply Settings”/”Restart Servers” to validate these new settings. ***NOTE:*** No change made on this screen will take effect until you click “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 is a default set of certificates on your support CD. You can use them to practice the certificate uploads. In a real-world scenario, you can generate the certificates by yourself (there is some freeware or shareware, such as XCA, for this purpose); or you can buy certificates from companies that provide authentication services. The valid file names and formats of the certificates and keys to be uploaded to the switch should be exactly as shown here: root.crt, server.crt, serverkey.pem, ldapcert.crt and ldapkey.pem.

**Viewer Connections**

The browser connections to the Web Management interface are always using SSL connections. The viewer connections can use different levels of security.

*Security Level (SSL):* The switch offers three levels of security for viewer connections. From the drop-down menu, select the level appropriate for your real demands on viewer connection security: "Level 1," "Level 2" or "Level 3."

- Level 1 uses no SSL data encryption and no authentication. It's the most straightforward setting and offers the most convenience if there are no security concerns. Anyone who has a viewer and an Internet connection can easily connect to the switch as long as the user fulfills the password policy requests.
- Level 2 uses SSL encryption for viewer connection, but only requires server authentication by the viewer client. Remote users are not required 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 is protected, including keyboard, mouse and video signals.
- Level 3 uses 256-bit encryption and a bi-directional PKI authentication between the 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 the switch.

In all, there are nine possible combinations of viewer security levels and password policies available for the flexibility to adapt to your specific security needs.

*KVM Server Password:* This field will only appear if you choose to implement Level 3 security. **See Page 16**. Enter the password that has encrypted the server private key in the server private key file (serverkey.pem) in order to make a successful viewer connection with the switch in the Level 3 security setting. If you use the standard set of certificates provided on the included support CD, the password that encrypts the server private key is "serverpwd." However, if you use your own set of certificates (as you should for a genuinely secure installation), you need to get the correct server password from the Certificate Authority that issued those certificates.

First, you should obtain a set of certificates from your administrator. If your certificate files have different names, change them to the valid names before uploading. To upload the certificates, click "Browse" to go to the location where your certificates reside. Select a certificate file, then click "Upload" to upload your certificates, one at a time, to the switch. After the uploading is completed, you should see the prompt page for a reboot. However, you don't have to reboot before you have uploaded all the necessary certificates: Just reboot once after you've uploaded all necessary certificates: root.crt, server.crt and serverkey.pem. If you need to SSL-encrypt the LDAP connection for user remote authentication, you must upload two extra certificates: ldapcert.crt and ldapkey.pem.

*User-Password Policy:* The switch offers three types of password policies for selection from the drop-down menu: "No Password," "Global Password" and "User Password."

- No Password means the viewer will not prompt you for any user password: The door is open unless you are using Level 3 security.

- Global Password means the viewer will prompt you for a global user password, which is used by all users (a sort of building door code).
- User Password means the viewer will prompt you for your user-specific password (a sort of apartment door code).

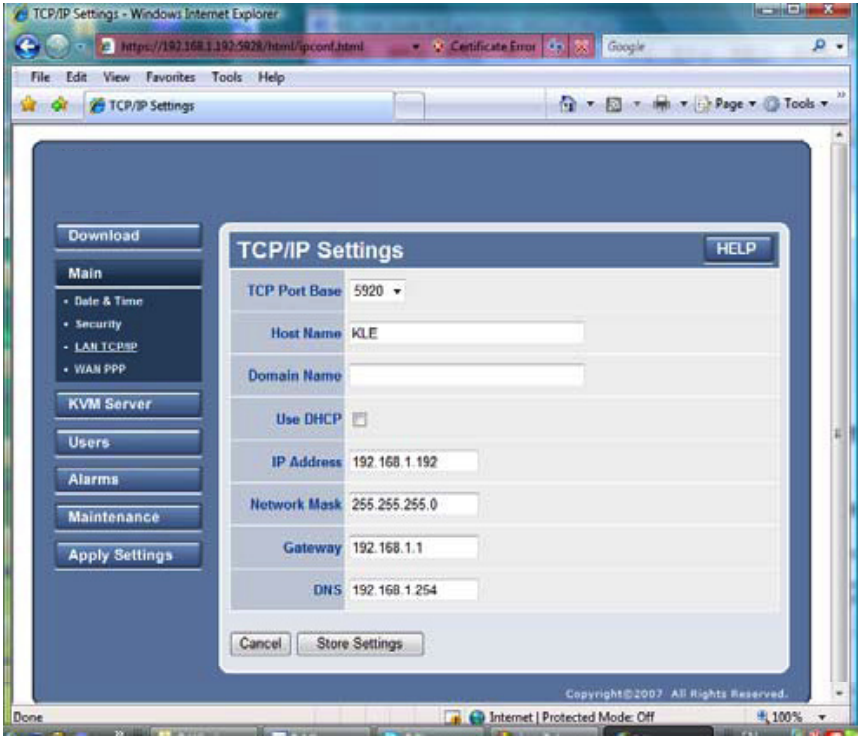
***NOTE:*** The viewer can also prompt you for the client certificate password if you are using Level 3 security.

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

***NOTE:*** Password and security (SSL/PKI authentication) settings should be used with caution. If the switch's 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 the switch can establish a remote connection. With these settings, there is no password protection and no data encryption. ***IMPORTANT:*** It's highly recommended that you (or your network administrator) establish and maintain the proper security for your switch.

## Main: LAN TCP/IP

This screen lets you set up the TCP/IP settings of your switch, including whether or not you want to use DHCP. Before you proceed with the various settings on this screen, however, you may first need to check with your network administrator for proper settings, as improper TCP/IP settings will result in invalid connections to the switch. After you have made all modifications, click "Store Settings" to save your settings, then click "Apply Settings"/"Restart Servers" to validate these new settings. ***NOTE:*** No change made on this screen will take effect until you click "Apply Settings"/"Restart Servers."



**TCP/IP Settings**

*TCP Port Base:* You can freely specify the port base for viewer connection with the server. Choose any available port base, starting from the lowest alternative of Port 5900 in increments of 10 up to Port 6090. The port base you choose is exactly the port number the switch uses for viewer connection. Also, "port base + 8" is the exact port number you'll use for secure http connection to the browser. After you have made the port base modification, click "Store Settings" and then click "Apply Settings"/"Restart Servers" to effect changes.

*Host Name:* This is the name the switch will assume on your local area network.

*Domain Name:* Specify the domain name for your switch as it appears on your LAN. (Leave it empty if you don't know.)

*Use DHCP:* This allows the switch 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 switch in your LAN.

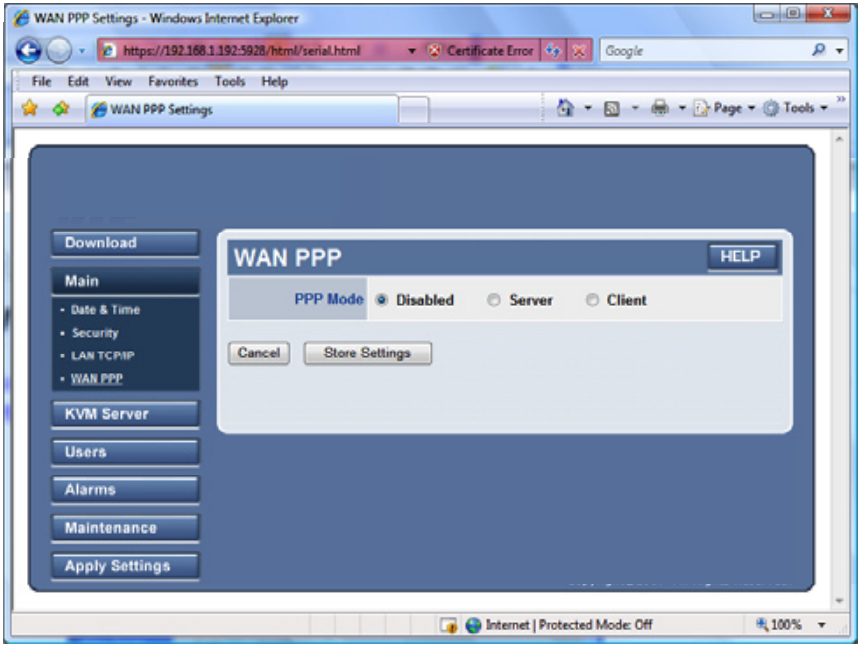
*Network Mask:* Enter a net mask value (in dotted decimal format, such as 255.255.255.0) that will be used by the switch in your LAN.

*Gateway:* Enter the fixed IP address (in dotted decimal format, such as 192.168.1.254) of the gateway (e.g., router) to access the Internet.

*DNS:* Enter the IP address (in dotted decimal format, such as 80.10.246.30) of the DNS server used by the switch for domain name resolution. (Ask your administrator if you don't know.)
***NOTE:*** You must enter a valid DNS server IP address for the e-mail alert to be effective.

## Main: WAN PPP

This screen lets you set the PPP server/client mode of your switch: to serve either as a PPP server for the remote computers to dial in for connection or as a PPP client to dial in to a PPP server to connect to a network or the Internet. The PPP connection can also serve as a backup connection mode when a direct network connection is not available. The switch's high-speed serial interface can offer excellent bandwidth to PPP connections. After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers."



**PPP Mode**

There are three PPP options: “Disabled,” “Server” and “Client.”

- Disabled is the default setting.
- Server is for a connection request from a peer computer. It allows users to connect to your servers without the Internet understructure, and 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.
- Client is for a dial-in connection to a PPP server (your ISP or an Enterprise PPP server). It can be used when there is no LAN or router available for direct Internet access using a modem.

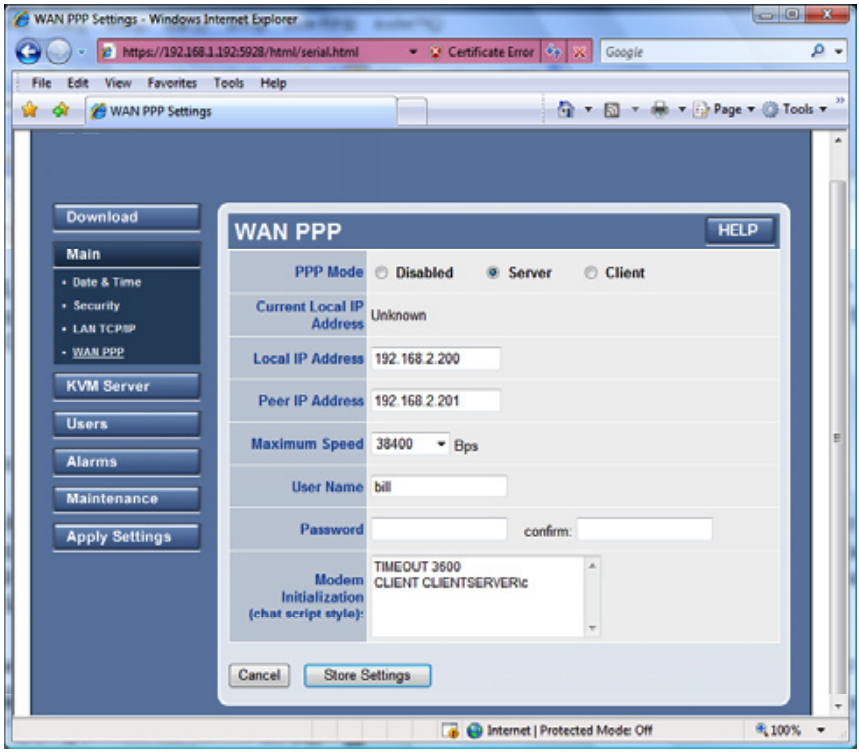
***NOTE 1:*** The PPP connection can work simultaneously with the LAN connection. ***NOTE 2:*** The PPP connection uses the same serial interface as Power Management: As these two features are mutually exclusive, by enabling the PPP you automatically disable Power Management and vice versa.

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, you can 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 displays the IP address of the switch when a PPP connection is established. If the PPP connection is not yet established, however, the IP address will show as “Unknown.” ***NOTE:*** This address is normally the same as the Local IP Address entry, but must be distinct from the one that is used by the switch on the LAN.

*Local IP Address:* Enter the IP address (default = 192.168.2.200) to be used by the switch in the PPP connection. This IP address will be used only in PPP connections by the switch alone, and should be distinct from the IP address (default = 192.168.1.200) that is specified on the LAN TCP/IP screen 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 the switch to the peer client at connection time.

*Maximum Speed:* Specify the modem connection speed. The switch 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 username 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 enter the same password in the next entry field to confirm the password. ***NOTE:*** The switch can support only one User Name / Password combination and one PPP connection at a time.

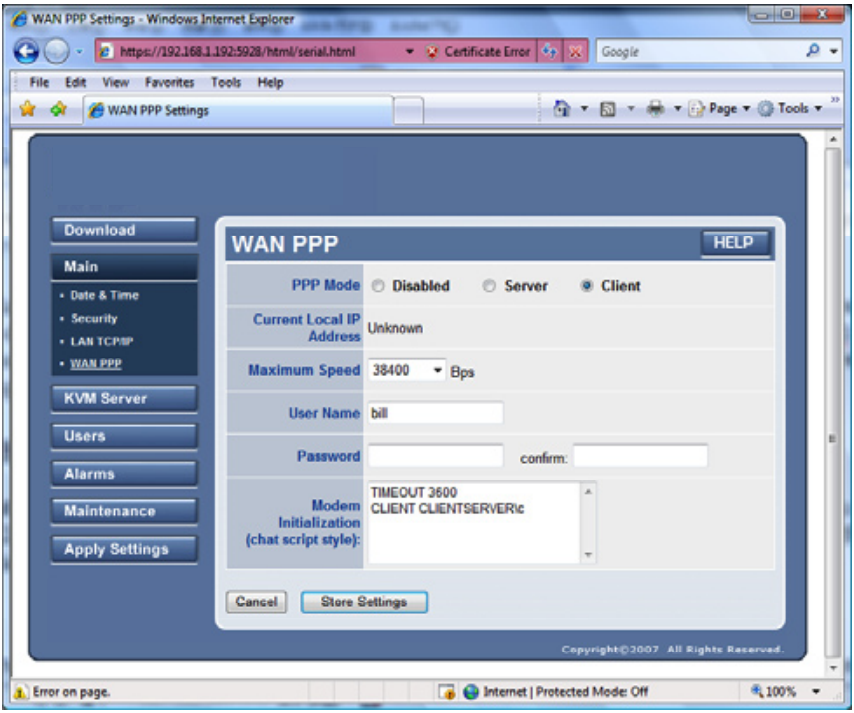
*Modem Initialization (chat script style):* The modem initialization script is a chat script that will initialize the modem to be ready for connection. The standard script provided by default permits you to connect a Windows client to the switch in Server mode over a direct serial cable (null modem). As shown:

TIMEOUT 3600
CLIENT CLIENTSERVER\c

In other words: Wait for "CLIENT" one hour before timeout, and respond "CLIENTSERVER" without a carriage (hard) return. ***NOTE:*** Refer to the Power Management screen for more details about the chat program. Also refer to your modem documentation; for Linux users, to the standard manual pages of pppd and chat programs. In Server mode, the modem should be set to wait and automatically connect when receiving remote calls.

**PPP Client Settings**

*Current Local IP Address:* This displays the dynamic IP address assigned to the switch by the



PPP server at connection time; for example, 62.147.111.39. If the PPP connection is not yet established, however, the IP address will show as "Unknown." ***NOTE:*** This address is used by the switch as a PPP client, and thus is distinct from the one that is used by the switch on the LAN.

*Maximum Speed:* Specify the modem connection speed. The switch 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 username that will be used by the switch to connect to the PPP server.

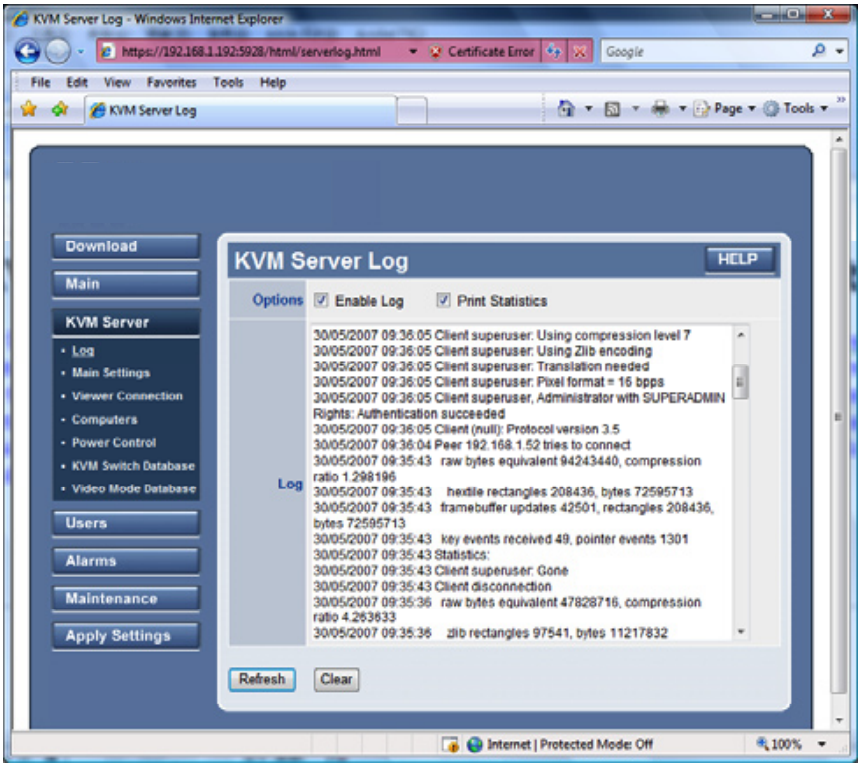
*Password:* Specify the password that will be used by the switch to connect to the PPP server.

***NOTE:*** The username and password are normally provided by the ISP at subscription time.

*Modem Initialization (chat script style):* 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 the Power Management screen for more details about the chat program. Also refer to your modem documentation; for Linux users, refer to the standard manual pages of pppd and chat programs. In Client mode, the modem should be set to dial automatically at start time.

## KVM Server: Log

This screen presents a detailed record of events — beginning from each restart — of each user's login, port switching actions and video modes. It also records each login attempt and the IP



address from which the login attempt originated, even when the attempt was 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 screen you should view first if you want to know the usage/"health" conditions of your switch.

*Enable Log:* Select to enable the logging of switch server events. If you choose to not enable this option, no logging will be done.

*Print Statistics:* If you need to know more about the switch's server statistics — such as the compression ratio, bytes transmitted, rectangles drawn, frame buffer updates and key events received — select 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 the switch's remote users, select this option to print statistics to the server log file.

Each log entry is preceded by a date code, time stamp and description of the specific log event. Look here for the IP address that is assumed by login users when they made the login attempt, and for 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 its maximum size while newer logging events keep coming in. Click "Refresh" to update the screen output of the log file. Since newer server log events may have occurred and been logged to the database after your previous access of this server log page, click "Refresh" to reload the log messages. Click "Clear" 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 "Reboot" on the Maintenance/Reboot screen or when the switch suffers a power loss.

## KVM Server: Main Settings

This screen allows you to set up the KVM server operation: video quality and optimization, KVM switch model and the auto scanning function. After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers."

**Video Quality**

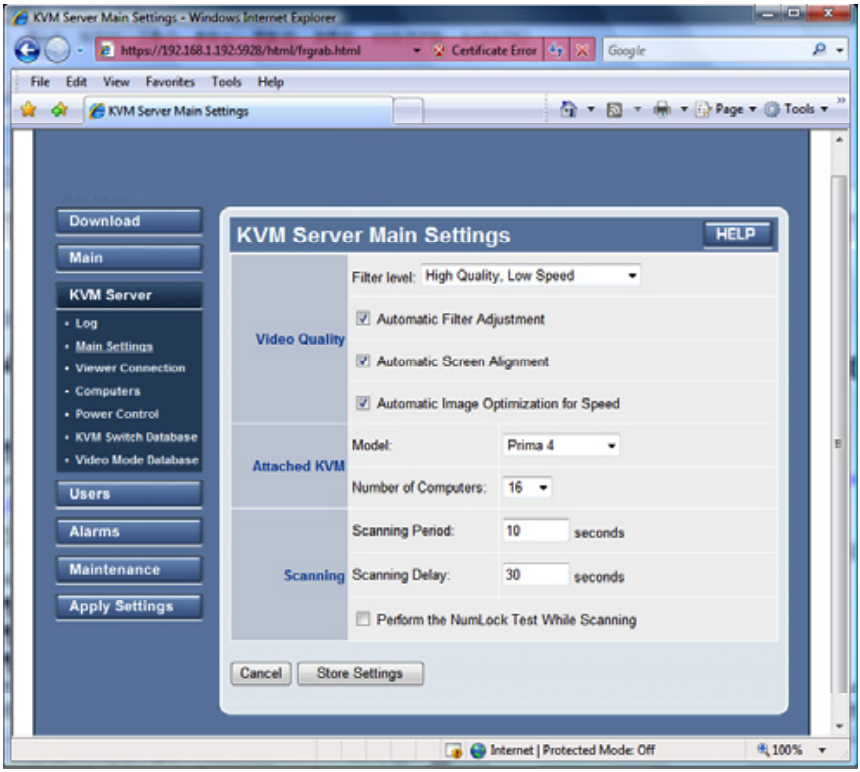
*Filter Level:* Based on the desired (or required) combination of video quality and available bandwidth, select one of three video filter levels for the switch's video server: "High Quality, Low Speed," "Medium Quality, Medium Speed" or "Low Quality, High Speed." Understand that there's always a trade-off between video quality and response speed when constrained by limited network bandwidth availability.

- High Quality, Low Speed (light filter) is recommended for high bandwidth networks such as a LAN or broadband Internet. It requires more bandwidth than the other two filter levels and video refresh speed is slower (only noticeable, though, when bandwidth is very limited). This filter provides the best image quality.
- Medium Quality, Medium Speed (medium filter) is recommended for Internet connections. It requires more bandwidth than the "Low Quality, High Speed" option, but is most often the best speed/bandwidth compromise.
- Low Quality, High Speed (strong filter) 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 selected, the switch can tune the video filter automatically for optimized performance according to the current bandwidth availability.

*Automatic Screen Alignment:* When this option is selected, the switch tries to center the view screen automatically to eliminate the offsets sometimes seen on the viewer screen as black gaps.

*Automatic Image Optimization for Speed:* When this option is selected, the switch 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 this Digital KVM over IP Switch for connection with multiple computers, you should select the model of that KVM switch. If the KVM switch model does not appear on the list, you can always add it or even add more KVM switch models to augment the list so that your computer icons can support the port switching hotkeys of that specific KVM switch when they're clicked. (For details about adding a KVM switch model to the KVM switch database, go to the KVM Switch Database section; for details about naming a computer as it appears on the computer icon of the Select Computer box, go to the Computers section.)

*Number of Computers:* Specify a maximum allowable number of connected PCs for the KVM switch attached behind this Digital KVM over IP Switch. The maximum is 256 computers, as you might have with a configuration of several cascadable KVM switches behind this Digital KVM over IP Switch.

**Scanning**

*Scanning Period:* This 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 a video resolution change, the scanning will be temporarily paused until it reaches the timeout of the scanning delay, then continue. Specify the scanning period in seconds.

*Scanning Delay:* This is the time that the switch will wait after it last perceives a KVM (keyboard/video/mouse) event before it switches to the next connected PC.

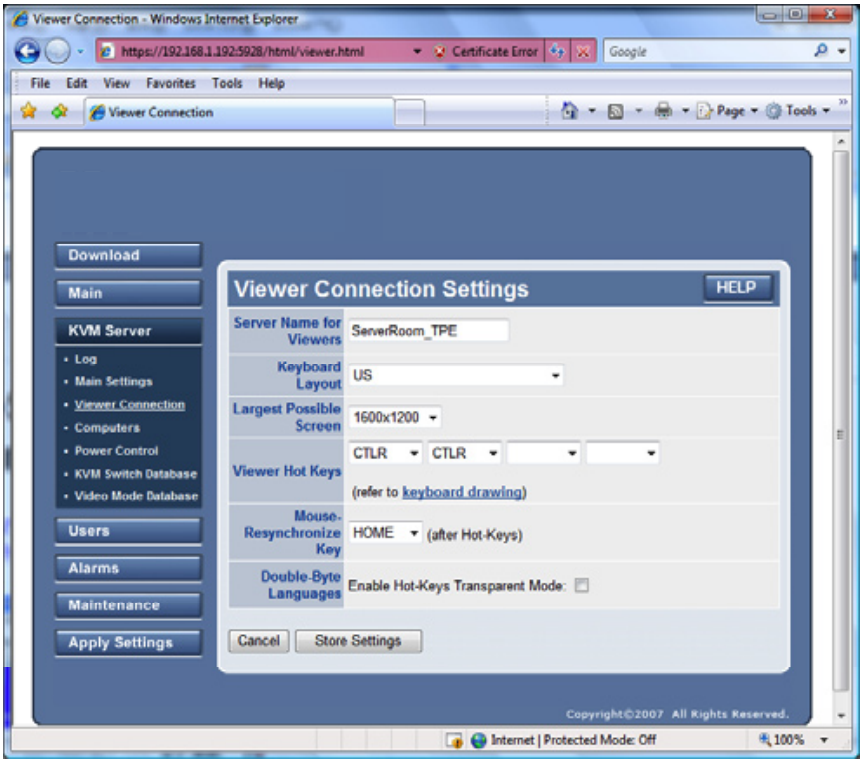
*Performing the NumLock Test While Scanning:* The NumLock test is a way to detect whether

or not a computer is still responding to keyboard actions. If you select this option, the switch will send a NumLock signal to the PC while scanning. If the PC sends a response, then the NumLock LED will light. The NumLock test can determine if the connected PC is still responsive to keyboard events. Additionally, 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. Select this option if you want to use auto-scanning to monitor whether or not each of your computers has stayed alive. You can also specify which computer will be included in the auto-scanning process. (For details about adding/removing computers from the auto-scanning list, go to the Computers section.)

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 either send an alert e-mail or SNMP message or send power cycling commands to a serial power control device to power cycle the server with the problem. (For details about configuring the alarm features of the switch, go to the Alarms section.)

## KVM Server: Viewer Connection (Settings)

This screen 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 the switch will assume so as to be consistent with the one you use on the client side, the biggest resolution support, the mouse re-sync hot key sequence, and the very convenient and useful feature for anyone using a double-byte language such as Chinese, Japanese or Korean (the CJK languages) and some other languages. After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers."



**Server Name for Viewers**
Enter the server name you chose for the video server on the switch, and it will appear on the title bar of your switch's viewer window.

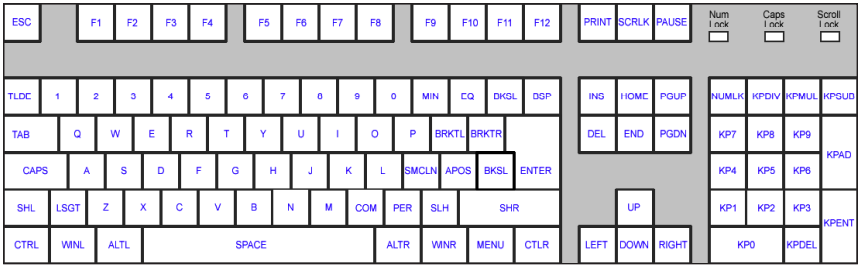
**Keyboard Layout**
Choose the keyboard layout for the switch according to the real keyboard you're using on the remote login client. Choosing the correct keyboard layout for your keyboard is very important since some key codes are represented by different keys, depending on the keyboard layout. Also, a correct keyboard layout setting ensures that you'll have a key code output on the server side that matches what you've input on the physical keyboard from the client computer side. The default keyboard layout is the U.S. keyboard, though the switch supports more than 60 types of keyboards used all over the world.

**Largest Possible Screen**
The switch supports a maximum resolution of up to 1600 x 1200 pixels. Normally, the greatest resolution support (1600 x 1200) will be the setting that is 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, be aware that any screen larger than what you specify here will not be shown on the viewer. The switch supports the following resolutions:
• 640 x 400 • 640 x 480 • 800 x 600 • 1024 x 768 • 1152 x 864 • 1280 x 1024 • 1600 x 1200
(For details about the refresh rate support, go to the Video Mode Database section.)

**Hot Keys**
The Digital KVM over IP Switch can detect a special sequence of keystrokes when you type on your remote keyboard. This special sequence is used to ask the switch to resynchronize the local and remote mouse cursors in a fast and convenient way. For example, it's faster to press CTLR–CTLR–Home on the keyboard than to use the mouse and select a command in a menu. For compatibility with higher devices, this command is divided in two parts: viewer hot keys and a mouse resynchronization key.

The viewer hot keys are transmitted to the switch or server attached to the switch, whereas the mouse resynchronization key is filtered out by the switch. 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 other hand, the mouse resynchronization key can be anything since it is not transmitted by TKIP-101.

Hot keys can be configured to fit your needs, as well, based on the key positions on a standard keyboard, as shown below. ***NOTE 1:*** The viewer hot keys are transmitted to the switch that's attached, thus they must be chosen so that they don't interfere with the switch's hot keys. ***NOTE 2:*** If you're running the Java viewer on a Mac OS, you may find that the default mouse resynchronization sequence — CTLR–CTLR–Home — doesn't work. This is because the Right Control key on a Mac keyboard sends out a different key code than a PC keyboard does. If this is the case, consider configuring your hot keys differently (CTLL-CTLL and S, as an example).



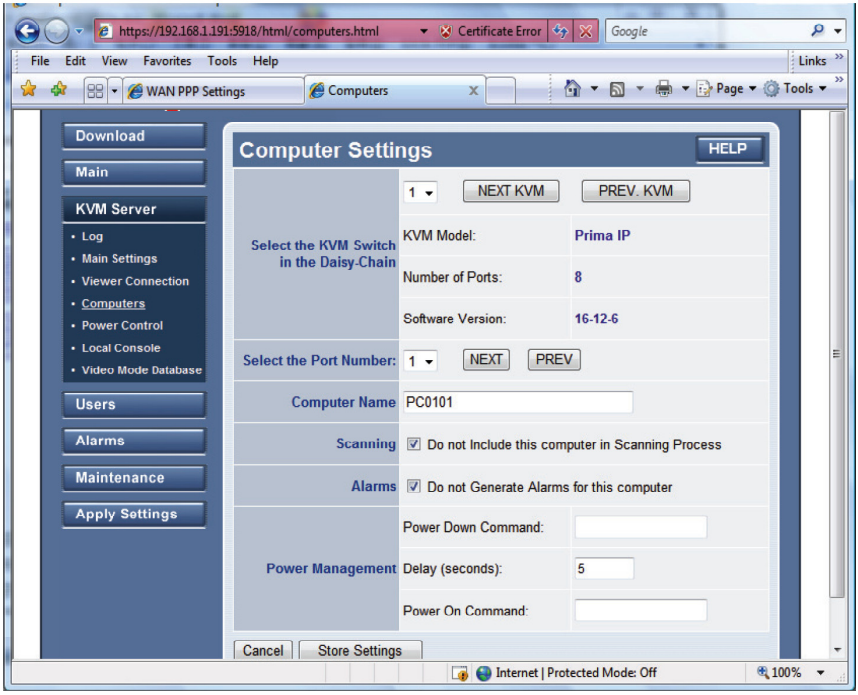
**Viewer Hot Keys**
Enter your preferred keystroke sequence that will serve as viewer hot keys. By default, this is CTLR–CTLR (two consecutive keystrokes of the Right Ctrl key: CTLR). Note that this is *not* the Left Control key (CTLL).

**Mouse Resynchronize Key**
This is the only command supported by TKIP-101. It permits synchronization of the local and 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 the switch compatible with double-byte languages such as Chinese, Japanese and Korean. When using the viewer, if the remote computer and/or your local computer is running a double-byte system, just hit Alt and then Shift or Ctrl and then Shift sequentially (instead of simultaneously) to produce the same effects.
*Enable Hot-Keys Transparent Mode:* Select 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 languages.

## KVM Server: Computers

This screen lets you provide the switch with information about all KVM-attached computers, which allows various actions to be performed more readily, if not automatically:
- Work with computer names instead of switch port numbers.
- Generate automatically the KVM switch hot keys to select computers so you can select a computer with a simple mouse click or by using the computer name.
- Generate automatically (or upon request) the power-down and power-on cycling if a power



control unit is connected.
- Exclude some computers from the auto-scanning process.
- Refrain from generating alarms for some computers.

***NOTE:*** You can also work without supplying any computer information. In this case, just keep the values by default. You'll have to remember on which KVM port your computers are attached and generate the specific KVM hot keys by hand. (This is the way most low-end IP KVM extenders work.) After you've made all modifications, click "Store Settings," then "Apply Settings"/ "Restart Servers."

**Select the KVM Switch in the Daisy Chain**

The various settings on this screen 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 configuring any port-specific settings, choose the KVM switch on which you will configure these settings.

**Select the Port Number**

Select the KVM port on which your subsequent settings on this screen are directed. You can use the drop-down menu as well as use the "Previous" and "Next" buttons to navigate to a specific port.

**Computer Name**

Enter a character string (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 don't want a computer included in auto-scanning, select "Do not include in Scanning Process." Thus, you can place a specific computer "off your radar screen" if it is of no monitoring importance.

**Alarms**

If you don't want the scanning process to generate alarms or SNMP messages for this specific (selected) computer, select "Do not Generate Alarms" to exclude it.

**Power Management**

If you require power control for your connected computers, you can connect a serial power control (SPC) device to the serial port on the rear panel of the switch, and then enable the switch's power control feature. By doing so, remote users can perform power on/off and power cycling either via the viewer interface or by a pre-defined alarm-triggered action. The switch can support most standard serial power control devices via its serial port (RJ12) on the rear panel. (For details about enabling the switch's power control feature, refer to the Power Control section below.)

***IMPORTANT:*** When using a power control device, note that some newer computers will require some BIOS option adjustment to restart when power is coming back; otherwise, they will not restart without pressing 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 Down Command:* Specify 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 Java viewers, switch to this computer and then click "Power off" in the viewer menu. The command specified here will be sent automatically by the switch to the power control unit.

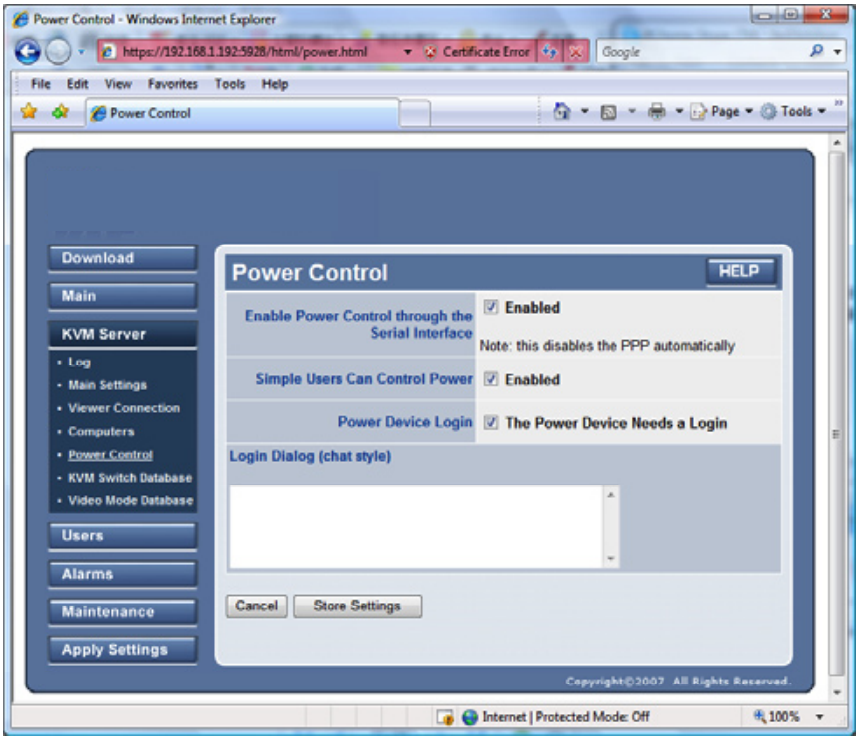
*Delay:* Specify the delay time between the sending of power-down and power-on commands to complete a power cycling. A power cycling is processed only if you've selected "Restart Computer" on the Alarms screen. By default, this delay is 5 seconds.

*Power On Command:* Specify the command that must be sent to the power control unit to power on the computer. (Refer to your power control unit documentation.) ***NOTE:*** To remotely power on this computer from the Windows or Java viewers, switch to this computer and then click "Power on" in the viewer menu. The command specified here will be sent automatically by the switch to the power control unit.

## KVM Server: Power Control

This screen lets you enable or disable the power control feature via the serial port on the rear panel of your switch. You can also specify the login script of your power control device (if it requires a login script). After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers."

**Enable Power Control through the Serial Interface**
Select "Enabled" to activate the remote power control support feature of the rear panel serial port of the switch. Once this option is selected, a subsequent Power Device Login screen will appear for you to decide whether or not to enter the login script.




**Simple Users Can Control Power**
Select/check this box if you want simple users to be able to power the computers on and off. By default, the switch allows only users designated as SUPERADMIN or ADMIN the right to power on/off the computer from the viewer Quick Menu.

**Power Device Login**
Depending on the serial power control device you've installed behind the switch, you may need a login script to log in or initialize your power control device. If this is the case, just select the

“Power Device Needs a Login” option to display a Login Dialog field for entering your login script.

**Login Dialog (chat style)**
This editable field is where you should enter the login script for your power control device, if the device requires it. (Refer to the user guide of your power control device for specifics.) 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 switch should expect the string “login:” and, once it’s received the “login:” prompt, the switch will send the string “myid” and then expect the “password:” prompt. When it receives the prompt for the password, it will send the password “mypass.” A carriage return — normally sent following the reply string — 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 single quotes with no space in between) as the expect string:
‘’ restart
login: myid
password: mypass
In other words, send “restart” and then expect “login:” and then send “myid” and then expect “password” and then send “mypass.” The expect sequence should contain only what’s 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:” to see if the initial letter (“l”) was received in error. You may never find the string even though it was sent by the power device, so, for this reason, the script should look for “ogin:” rather than “login:” and “ssword:” rather than “password:” — like this:
ogin: myid
ssword: mypass
Again, in other words, expect “ogin:” and then send “myid” and then expect “ssword:” and then send “mypass.”

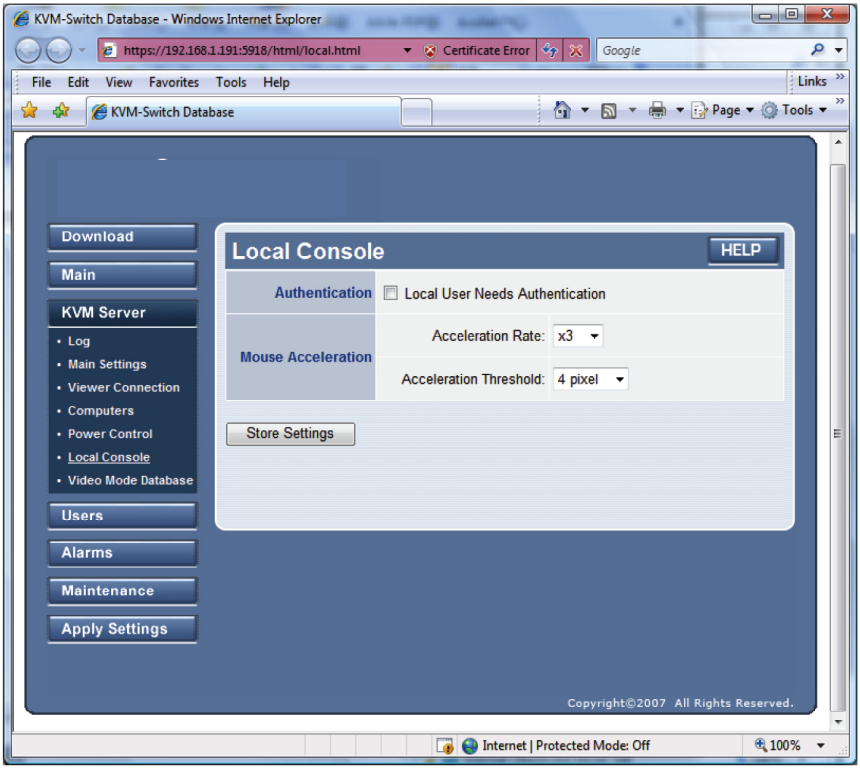
**Comments**
A comment is a line that starts with the pound sign (“#”) in column 1. Such comment lines are just ignored. If a “#” character is to be expected as the first character of the expect sequence, you should set the expect string in single quote marks (‘’). If you want to wait for a prompt that starts with a pound sign, you would need 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 not valid in the expect sequence are so indicated.
A pair of single quotes or apostrophes (‘’ or ’’) — Expects or sends a null string. If you send a null string, then it will still send the return character.
\b — Represents a backspace character.
\c — Suppresses the new line at the end of the reply string. This is the only way 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 letters “h,” “e,” “l,” “l,” “o” (not valid in expect).
\d — Delays for one second (not valid in expect).
\n — Sends a new line or linefeed character.
\N — Sends a null character. The same sequence may be represented by “\0” (not valid in expect).

\p — Pauses for a fraction of a second. The delay is 1/10th of a second (not valid in expect).
\r — Sends or expects 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 — Sends or expects a tab character.
\\ — Sends or expects a backslash character.
For more detailed information, refer to the Linux chat program man page (man 8 chat).

## KVM Server: Local Console

This screen allows you to enable or disable the user password authentication feature and adjust the mouse acceleration on the local console. After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers."




**Authentication**

*Local User Needs Authentication:* Enable/disable password authentication on the local console. To enable the password authentication on the Digital KVM over IP Switch local console, you must select this option.

**Mouse Acceleration**

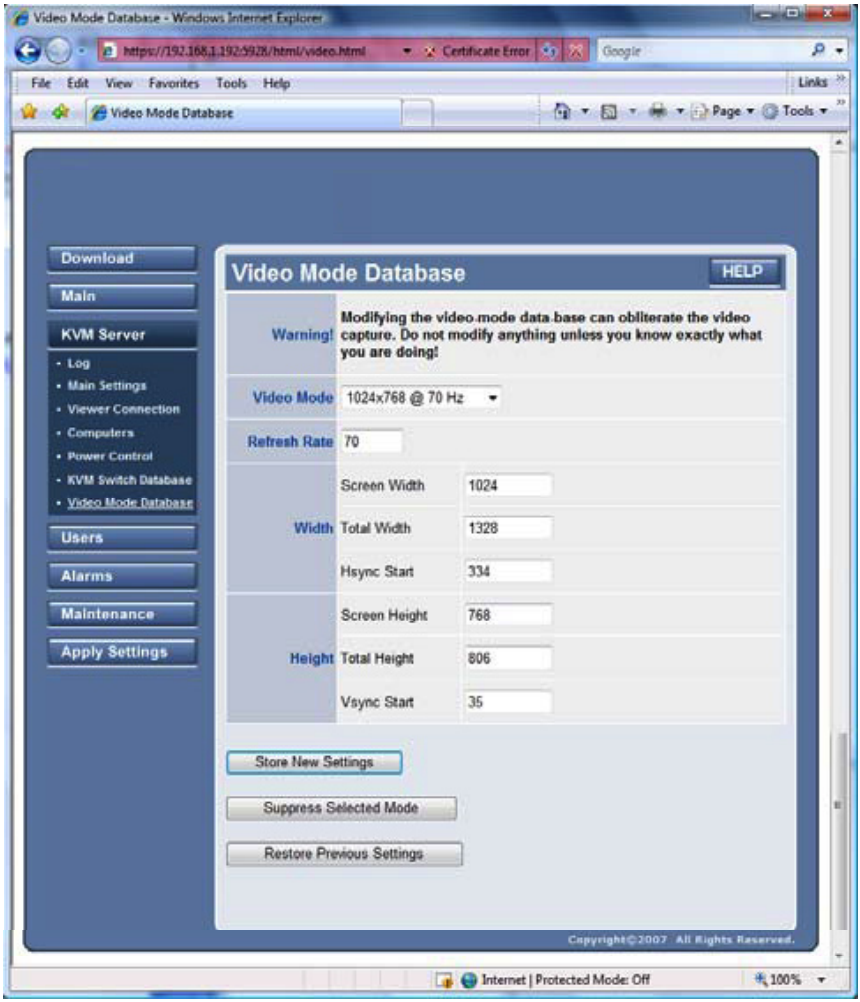
*Acceleration Rate:* From the drop-down menu, select the mouse acceleration factor (x1 to x20) for the local console.

*Acceleration Threshold:* This is the point (a value in pixels) at which the local console mouse acceleration factor goes into effect. ***NOTE:*** In order for the mouse resynchronization to work properly on the viewer, the mouse acceleration on each of the connected servers or computers

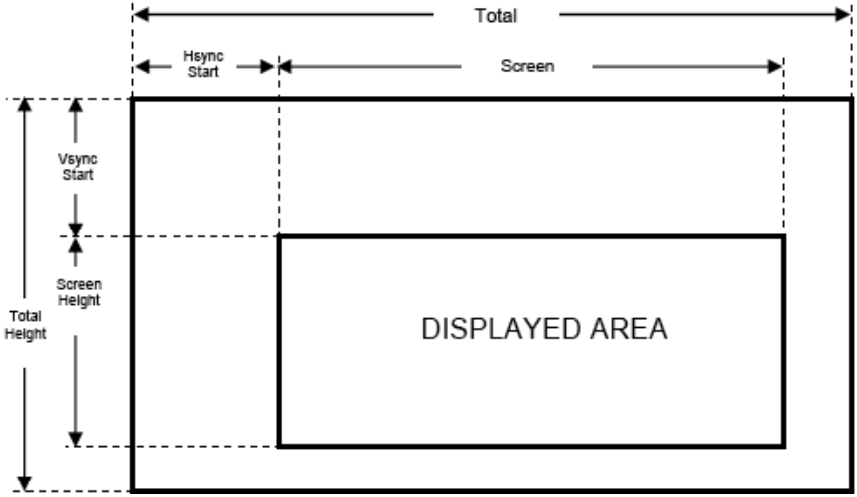
has to be turned off. A zero-acceleration mouse on a remote server will not reflect on the viewer since the mouse cursor on the remote server should catch up with the mouse on the viewer side, which could use any acceleration factor. However, on the local console of the Digital KVM over IP Switch you'll experience zero mouse acceleration and reduced efficiency when trying to move your mouse. Enabling the mouse acceleration on the local console can provide more effective mouse maneuvering, yet won't affect the mouse acceleration on the connected server since it is only imposed atop its original zero acceleration on the local console.

## KVM Server: Video Mode Database

This screen allows you to modify, create and suppress the VGA modes supported by the device. After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers." ***CAUTION:*** Carelessly modifying a video mode in this video database might obliterate the video capture: *Don't modify anything* unless you know exactly what you are doing.



**Video Mode**
Use the drop-down menu 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; for example, 1024 x 768 @ 60 Hz. As with the refresh rate and the pixel dimensions, video mode parameters — screen width, total width, Hsync start and screen height, total height, Vsync start — can be adjusted. The following diagram demonstrates the geometric relations between the VGA parameters.




**Refresh Rate**
Modify the refresh rate of the target VGA mode as needed.

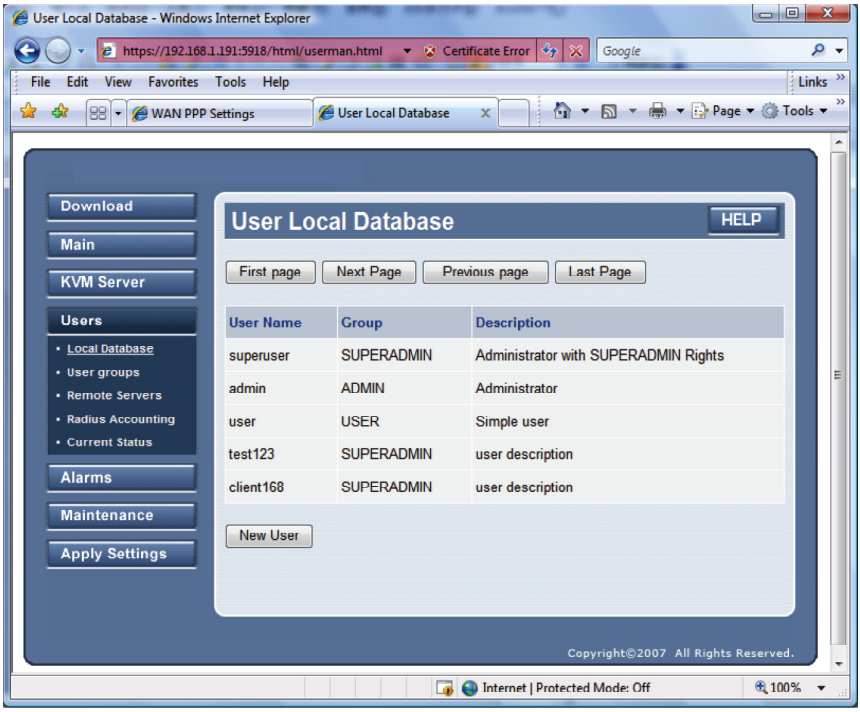
**Width**
*Screen Width:* Specify the width of the visible part of the screen.
*Total Width:* Specify the total width of the screen (active + hidden).
*Hsync Start:* Specify where the VGA horizontal synchronization should start with reference to the beginning of the line.

**Height**
*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.
Click “Store New Settings” to save your modifications/additions to the video mode database. Click “Suppress Selected Mode” to remove the selected video mode from the video mode database. Click “Restore Previous Settings” to undo the previous addition or elimination of a video mode. ***NOTE:*** You can only undo one move.

## Users: Local Database

This screen is for user account management for the switch. You can see the listing of the existing user entries together with the user group that 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” and “Last Page” to navigate through the user database listing.

To modify, add or delete an entry, select the target user name in the listing to display a User Edit screen to make further modifications or to create a new user entry. After you’ve made necessary modifications, click “Store User” to save into the user account database.



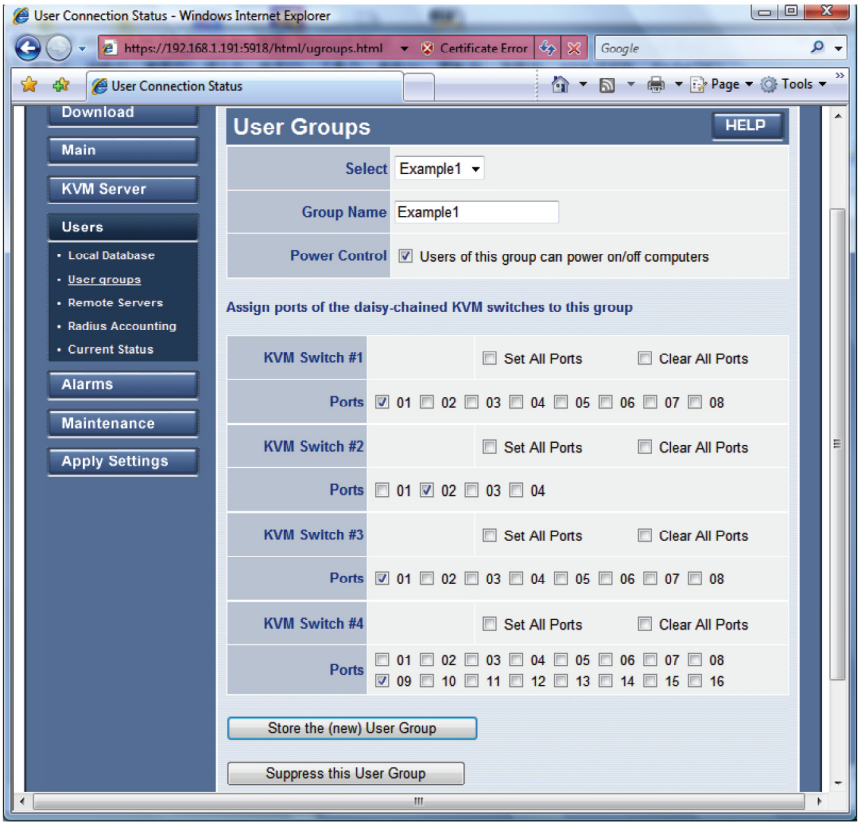

Each of the three user groups — SUPERADMIN, ADMIN and USER — has different rights regarding the Web Management interface and the viewers.

***NOTE:*** Only SUPERADMIN users can manage user accounts.

| 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/KVM switch database | x | x | - |
| KVM Server/Video Mode database | x | x | - |
| Users/local database | x | - | - |
| 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/Config. Save/Restore | x | - | - |
| Maintenance/Reboot | x | - | - |
| Apply Settings/Restart Servers | x | x | - |

## Users: User Groups

This screen allows you to modify, create or suppress user groups, each of which is listed in the Select drop-down menu as detailed below. After you've made all modifications, click "Store the (new) User Group," then "Apply Settings"/"Restart Servers."




Up to 64 user groups can be defined, each having 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. When modifying or creating a new user, you must select which user group he will belong to (see Users: Local Database above). When implementing the user-password policy, users are identified at connection time, their group is retrieved and the group properties are applied.

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 "Local User Needs Authentication" is enabled (see KVM Server: Local Console), the local user cannot select the prohibited ports, but can still access a computer that would be selected by a remote authorized user. Also, user groups have no effect if the password policy is not set to User Password. If you're using other password policies (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.

**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* make changes in this field if you only want to change the port list of the current user group.

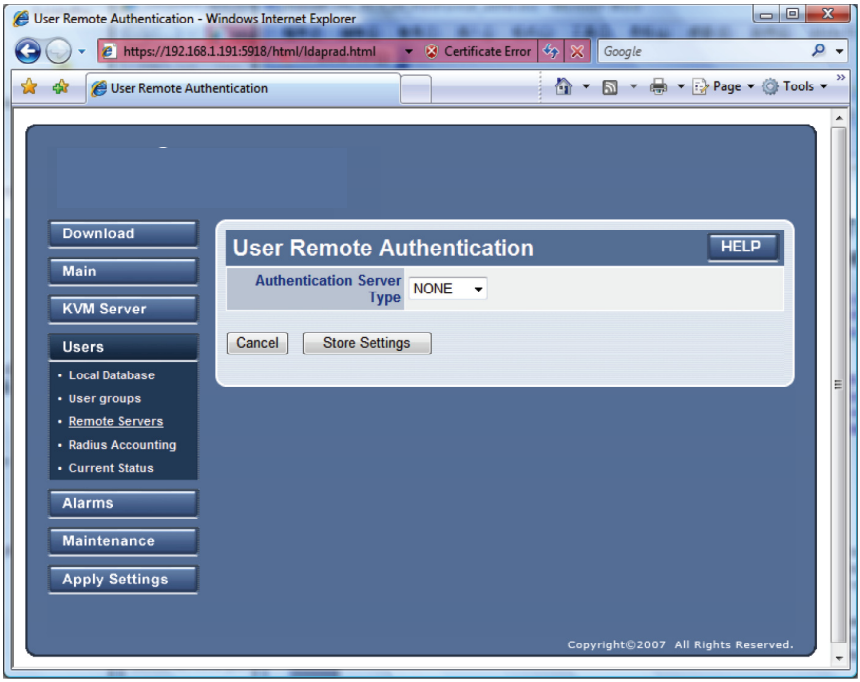
**Power Control**
Select "Users of this group can power on/off computers" to allow these users to "manually" power on and power off the computers they can access through the viewers. ***NOTE:*** A power control device is required to do this.

In the section "Assign ports of the daisy-chained KVM switches to this group," 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; check specific port numbers to select each KVM port individually.

## Users: Remote Servers (User Remote Authentication)

This screen allows you to authenticate the users that attempt to connect to the switch from centralized servers running a RADIUS service or hosting a directory that can be accessed through the LDAP protocol (Active Directory, for example). User Remote Authentication lets you integrate the switch into your global enterprise user management.

By default, Remote Authentication is configured as "None"; i.e., all remote authentications are disabled, in which case the authentication is all done locally by using the database on the switch only. After you've made all modifications, click "Store Settings," then "Apply Settings"/ "Restart Servers."

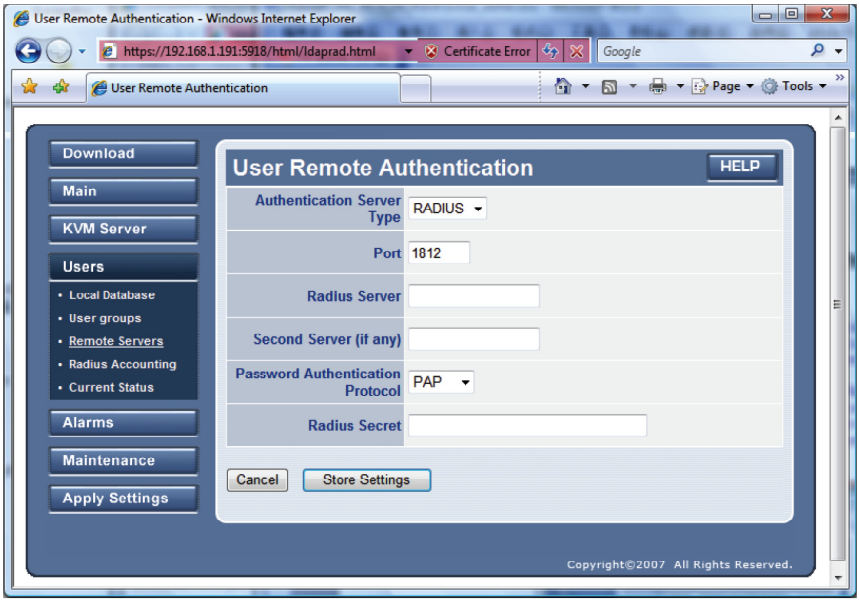


**Authentication Server Type**
From the drop-down menu, enable the remote server authentication either by LDAP or the RADIUS server (or select "None" to disable the remote authentication support). Before proceeding with subsequent settings on this screen, check with your network administrator for the availability of either an LDAP server or a RADIUS server.

**Directory Server Using LDAP**
*SSL Access:* Select to enable SSL access of the LDAP authentication. ***NOTE:*** Make sure your LDAP server supports SSL, and remember, too, that you need to install a distinct set of certificates — ldapcert.crt and ldapkey.pem — on the switch by uploading them through the Security screen. Normally these certificates are generated by the directory server itself.
*Port:* Enter the port number used in LDAP authentication. By default, it is set to Port 389.
*LDAP Server:* Enter 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:* Make an appropriate entry here, which is characteristic of the LDAP server you use for authentication. The default is cn=users, dc=abc, dc=kle, dc=com, but you should enter your own. (If unsure what to enter, contact your LDAP server administrator.)

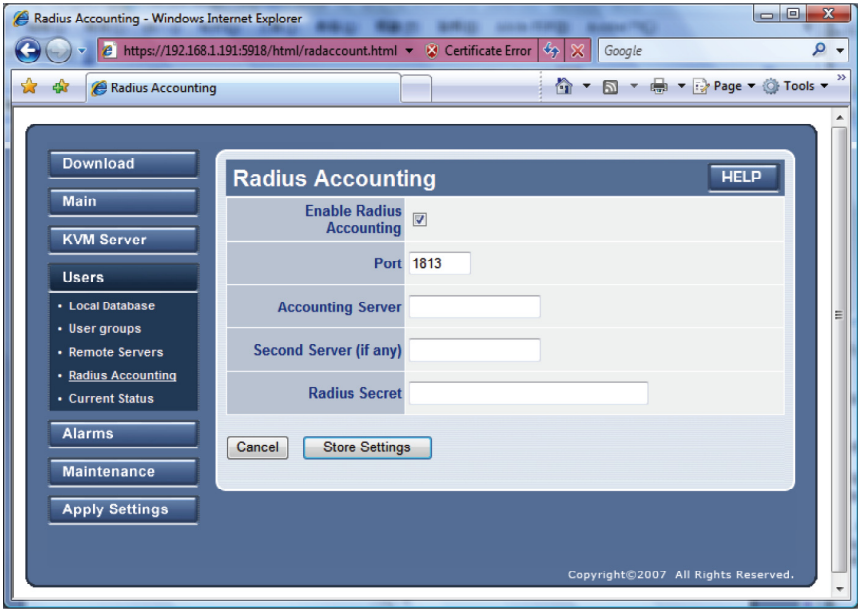



**RADIUS Server**
*Port:* Enter the port number used in RADIUS authentication. By default, it is set to Port 1812.
*RADIUS Server:* Enter the IP address of the RADIUS server.
*Second Server (if any):* If there is a second RADIUS server available for authentication, enter its IP address here.
*Password Authentication Protocol:* Select either "CHAP" or "PAP."
*RADIUS Secret:* Specify the RADIUS secret (or Shared Secret) between the switch and the RADIUS server. The RADIUS secret is a text string used as a password between the RADIUS client and the RADIUS server. Request the RADIUS secret from your server administrator.




## Users: RADIUS Accounting

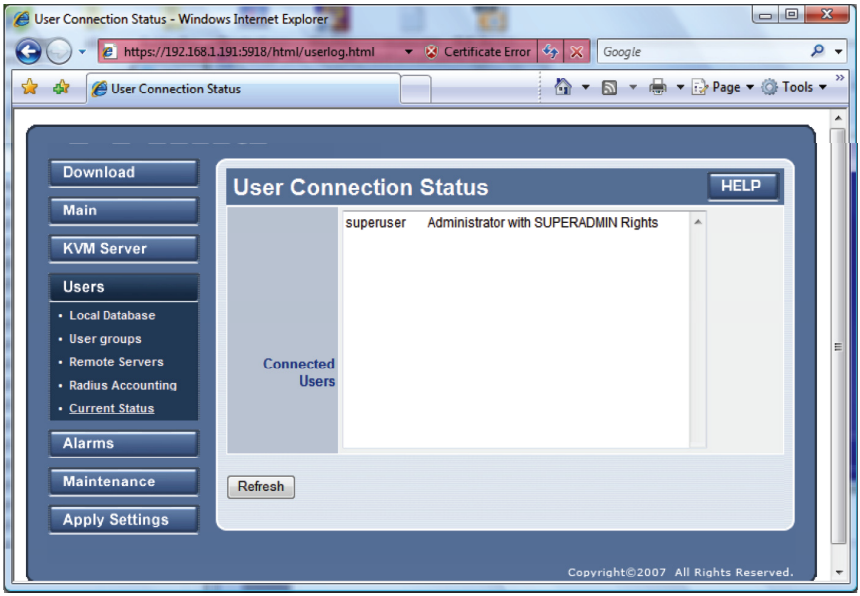
Normally, RADIUS accounting is disabled by default. However, if you have RADIUS accounting enabled on a RADIUS or LDAP server, you can enable it here and subsequently configure its relevant settings to take advantage of this feature. After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers."



**Enable RADIUS Accounting**
Select to enable RADIUS accounting support and modify the settings.
*Port:* Specify the port used for RADIUS accounting. By default, it's set to 1813.
*Accounting Server:* Enter the IP address of the server offering the RADIUS accounting service.
*Second Server (if any):* Enter the IP address of the secondary server, if you've got any backup RADIUS accounting server that offers RADIUS accounting service.
*RADIUS Secret:* Specify the RADIUS secret (or Shared Secret) between the RADIUS client (e.g., IP KVM) and the RADIUS server. The RADIUS secret is a shared text string used as a password between the RADIUS client and RADIUS server.

## Users: Current Status

This screen displays the remote users currently connected. ***NOTE:*** This screen doesn't refresh automatically, so to see whether there's any change, click "Refresh" to update the information.



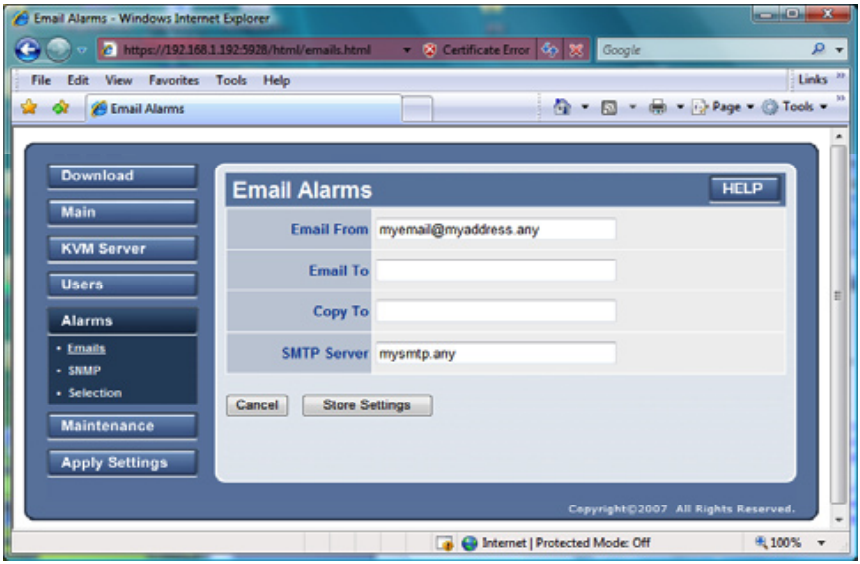

***IMPORTANT:*** Only when "User Password" has been selected as your password policy will the currently connected users be registered and shown on this screen. If you're using another password policy (No Password or Global Password), connected users won't show on this screen since these policies imply that the distinction of user identities is not necessary.

## Alarms: E-mails

This screen allows you to set up the e-mail notification for alarm events. After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers."

**E-mail From**
Sender e-mail address used by the switch for alarm e-mails. This address can help identify which switch is the sender, and must be accepted by the SMTP server.

**E-mail To**
The e-mail address(es) of any switch alarm e-mail addressee(s). ***NOTE:*** You can use commas for multiple recipients: support@myaddress.net, emma@international.com, joe@netview.co.jp.

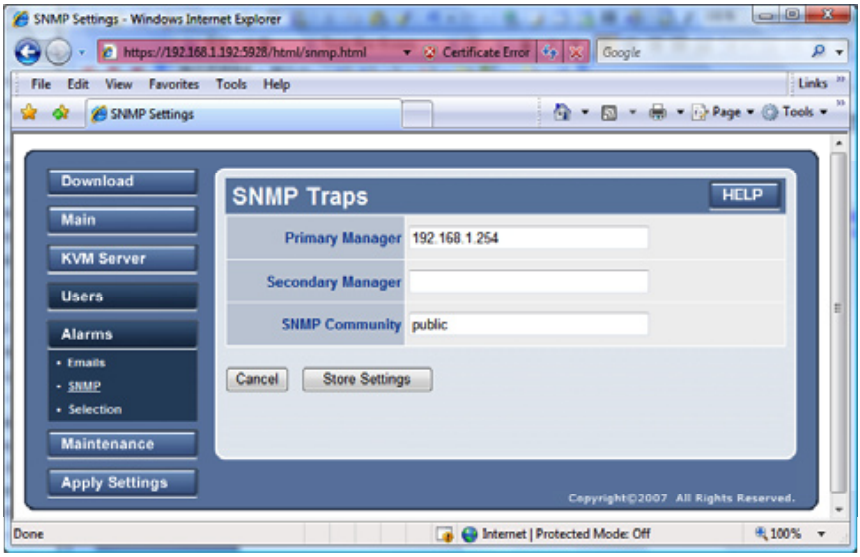



**Copy To:**
The e-mail address of addressees who should get a courtesy copy of alarm e-mails.

**SMTP Server:**
Enter the name or IP address of the SMTP server (mail server) that will route the switch's e-mail alarms to recipients.

## Alarms: SNMP (Traps)

This screen allows you to set up the e-mail notification for alarm events. After you've made all modifications, click "Store Settings," then "Apply Settings"/"Restart Servers."



**Primary Manager**
Specify the IP address of the primary SNMP manager device on your network.

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

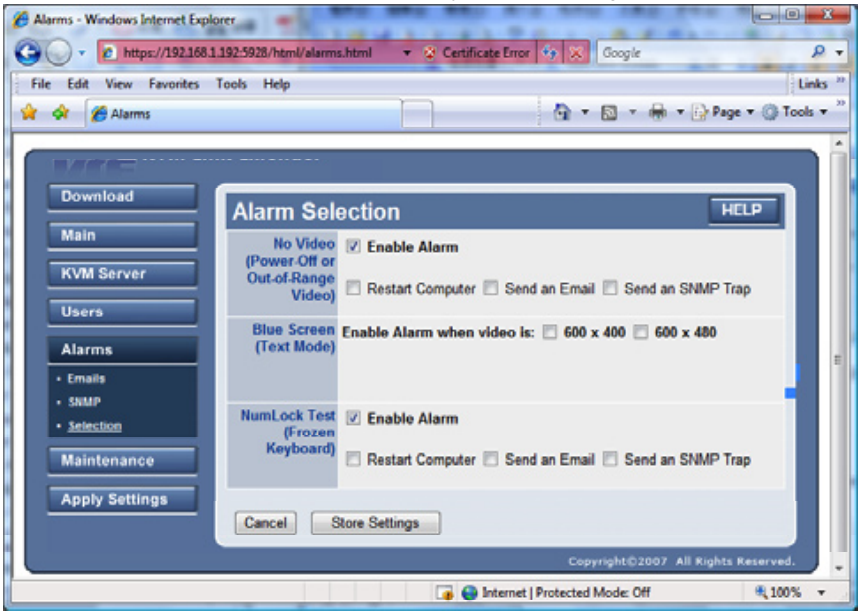
**SNMP Community**
Specify the name of the SNMP community to which your SNMP management host and SNMP agent should belong. ***NOTE:*** The SNMP manager and agents must belong to an SNMP community identified by its name, which is a collection of hosts grouped together for administrative purposes.

## Alarms: Selection

The switch can be configured to send three types of immediate alerts — e-mails, SNMP traps or automatic power cycling — in response to three alarm-triggering events: blue screen, no video or NumLock test failure from a remote computer. This feature should be used in conjunction with the auto-scan function so that the switch will help carry on a constant surveillance on the "health" conditions of your connected servers. ***NOTE:*** This screen is where you can select which action the switch is to perform when it detects an event. This is *not* the screen where you specify *how* the action is to be implemented. For this, refer to the SNMP options above.

**No Video**
This alarm could result from power failure or an unsupported video mode; e.g., an out-of-range video mode or, most often, a video mode not yet set up in the video database. If you want the switch to respond immediately to this sort of event, select "Enable Alarm" and which action(s) you want as a response: restart the computer, send an e-mail and/or send an SNMP trap.

**Blue Screen (Text Mode)**
A blue screen is the result of a Windows operating system fatal error. It can be detected by its low resolution video mode. If you want the switch to respond immediately to this event, select "Enable Alarm" and choose thr screen resolution you want to be regarded as a "blue screen":

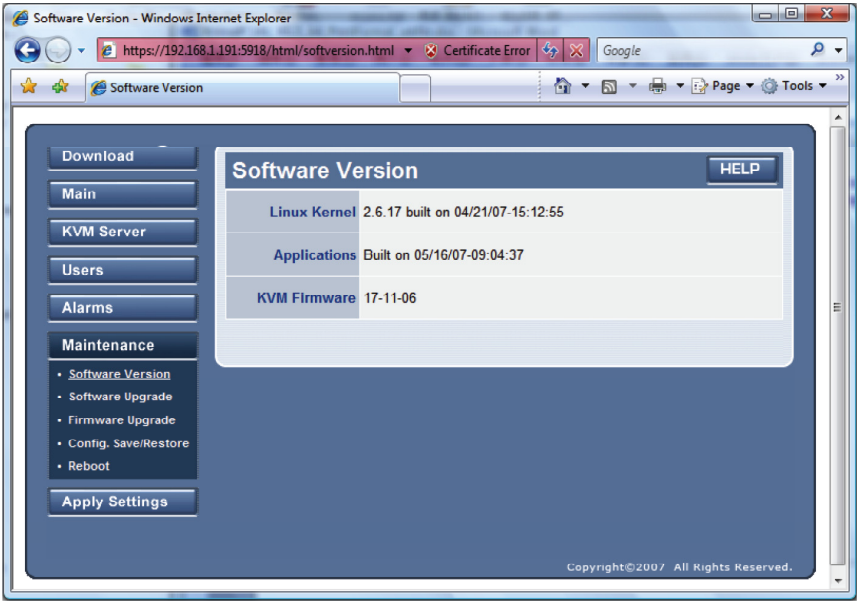


600 x 400 or 600 x 480. Then select a response action: “Restart Computer,” “Send an E-mail” or “Send an SNMP Trap.”

**NumLock Test Alarm (Frozen Keyboard)**
The NumLock test sends a NumLock signal to the computer, to which the computer normally returns an immediate response 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 the least, a keyboard failure to respond to this NumLock signal; otherwise, it could indicate a bigger problem (such as system failure) or simply a powered-off state. If you want the switch to respond to this alarm-triggering event, select “Enable Alarm” and which action or actions you want as a response: restart the computer, send an e-mail or send an SNMP trap.

## Maintenance: Software Version

This screen displays the current resident software version information.

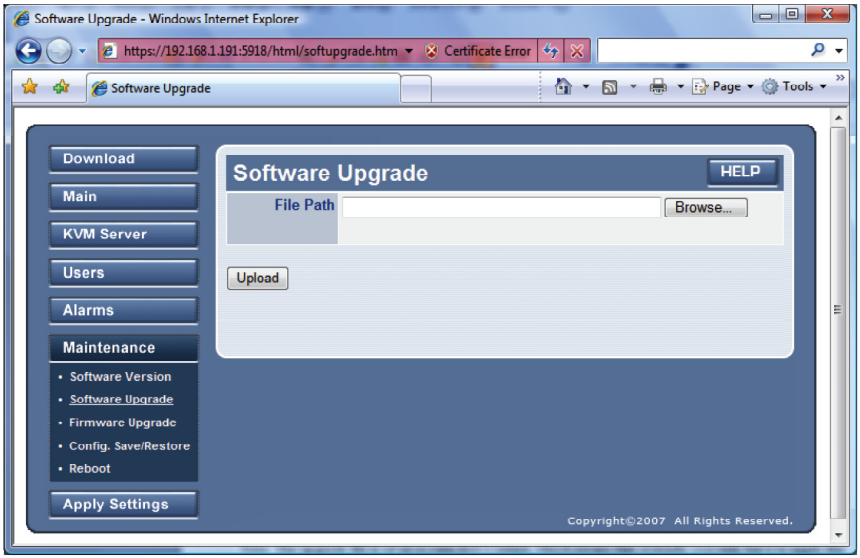



## Maintenance: Software Upgrade

This screen allows you to browse to the path location of the software upgrade file and upload the file to the switch across the LAN or Internet. ***NOTE:*** The switch upgrade file must have a name starting with “tkip101” followed by the date: tkip101-yy-mm-dd.

The upgrade file is of an accumulative nature, which means that normally you need only apply the single latest upgrade patch to keep your switch up to date. When you receive the upgrade file, you must first copy it to a local computer, then use the switch’s Web Management interface to perform the update across your LAN or the Internet.

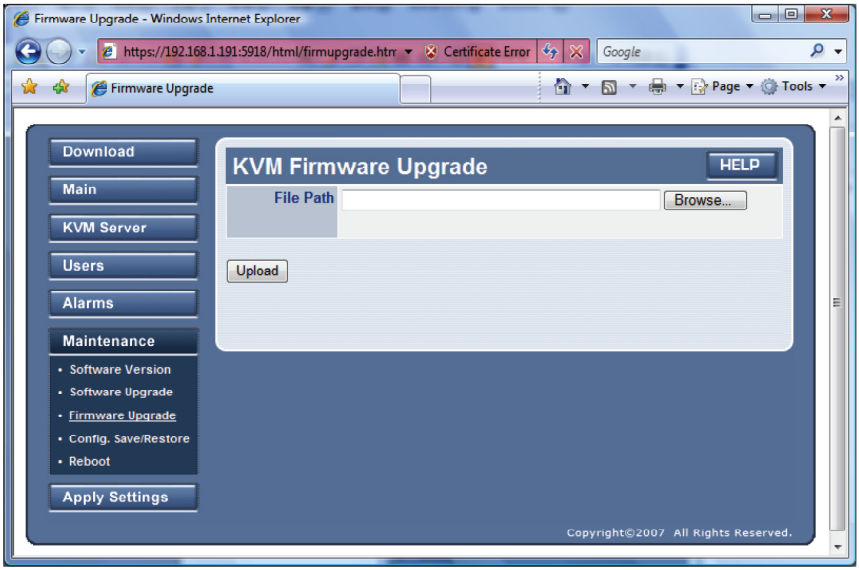
To perform a software upgrade, click “Browse” to browse to the location of the update file, then click “Upload.” A running progress indicator bar indicates the ongoing upload process. Depending on the upgrade file size and the bandwidth availability across the network, the file upload time can vary from one to 20 minutes. When the upload process is complete, the switch will reboot by itself. Once the reboot is completed, the switch should work right away.




## Maintenance: Firmware Upgrade

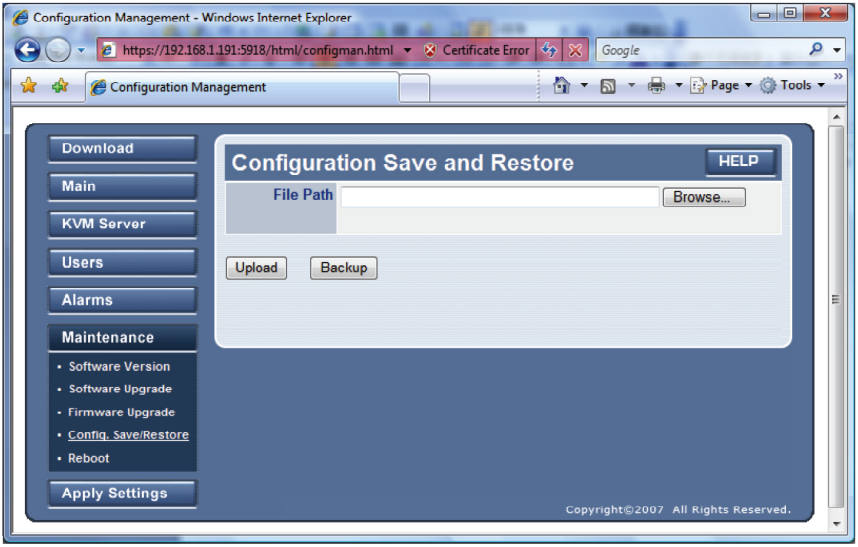
This screen allows you to browse to the path location of a firmware upgrade file and upload it to the Digital KVM over IP Switch across a LAN or the Internet.

Generally, the upgrade file comes with a filename formatted as kvmfirm-yy-mm-dd, and is accumulative: You can upgrade the KVM part of the file just as you upgrade the firmware of its IP module. Just browse to the location of the upgrade file and click “Upload.” A progress status bar will indicate one to 20 minutes, depending on the file size and bandwidth availability across the network. When the upload is complete, the switch will reboot by itself.



## Maintenance: Configuration Save and Restore

This screen allows you to save your current switch settings to a single .tgz file for more portability and usability. You can also set up several switches with the same or similar configurations.




To back up the configuration file, click “Backup”; choose a location for saving the configuration file (*.tgz); then click “Save.” The filename format is kconfig-yyyymmdd.tgz, with a timestamp in it.

To upload the configuration file, click “Browse” to browse to the location of the update file (kconfig-yyyymmdd.tgz); then click “Upload.” You’ll be prompted for a reboot when the upload process is complete. Reboot to validate the new configuration.

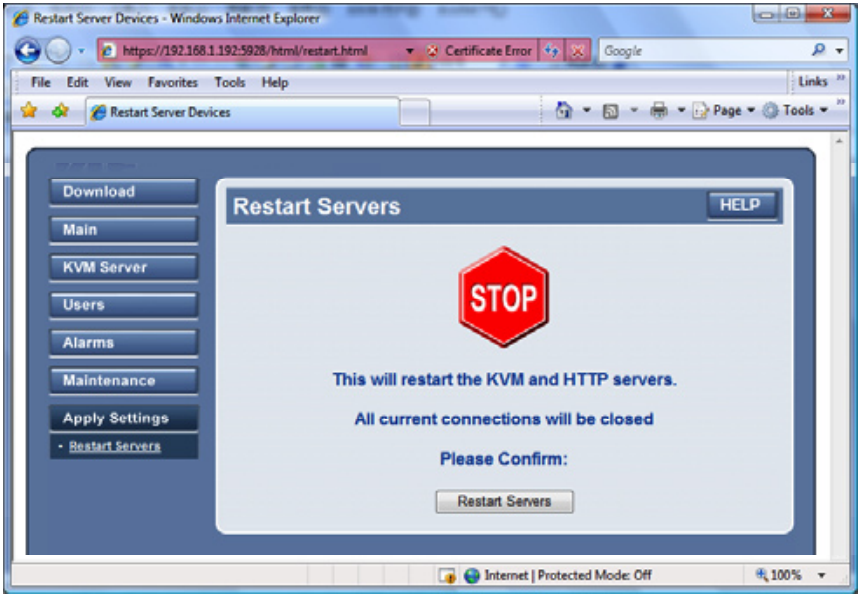
## Maintenance: Reboot



If your switch has crashed and simply clicking “Apply Settings”/“Restart Servers” has no effect on your restoration effort, a last resort is to completely reboot the switch by clicking “Reboot Device.” ***NOTE:*** The reboot brought about by clicking “Reboot Device” is a total reboot and takes longer to boot up completely, while clicking “Restart Servers” is much quicker (just few seconds) since it restarts only the server programs on the switch.

## Apply Settings: Restart Servers

Any new settings are only committed to the switch’s database by clicking “Store Settings,” “Store” or “Store User” on each setting screen. However, just clicking any of these buttons won’t immediately validate these new settings: You should click “Restart Servers” so that new settings can be put into use at once. ***NOTE:*** Clicking “Restart Servers” will disconnect all current viewer connections. As mentioned above in Maintenance: Reboot, clicking “Reboot” is an option if clicking “Restart Servers” provides no results, but, as a total reboot, will require more time.



# APPENDIX A: LOCAL CONSOLE OPERATION

If you're unfamiliar with local console operation, this section serves as an introduction to its controls. Additionally, Appendix B features the cable components needed for initial setup of the Digital KVM over IP Switch.

There are three ways to operate the Digital KVM over IP Switch: using the front-panel buttons, keyboard hotkeys and the on-screen display (OSD) menus.

## 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 button during normal operation will cause the corresponding channel to be selected.

## Keyboard Hotkeys

Hotkey control is usually considered the most convenient and quickest way to operate the Digital KVM over IP Switch on the local console. Most of the hotkey control commands are preceded by two consecutive Scroll Lock keystrokes (done within 2 seconds) and followed by a specific command key or key sequence:

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

In most cases, it will take at least three keystrokes to complete a command; in some cases, it will require six (as when selecting a specific bank and port number as an active channel). All the available hotkey commands and OSD menu options are summarized in the chart below.

| Command | Hotkeys / OSD Menu option |
|---|---|
| Select PC | ScrLk + ScrLk + (a) + (b) + (y) + (z) [1]<br>*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]* |

*1* a, b, y and z each denote a number key.
(ab) = 01 – 16; (yz) = 01 – 08 or 01 – 16, depending on the model.

## On-Screen Display (OSD)

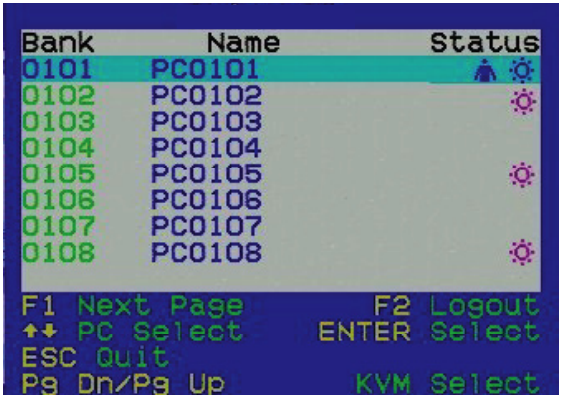
To activate the OSD menu — which will be superimposed on your current screen display — use the hotkey sequence ScrLk, ScrLk, Space Bar. The menu presents a listing of available banks and channels and the current online status of each channel. It also allows you to rename your computer (up to eight characters), to find a specific computer by name and to password-protect your switch system. ***NOTE:*** While the OSD is activated, all front-panel buttons and mice are rendered inactive.

**Main Menu**


Indicates that the corresponding computer is currently the active channel that can be monitored on your local console.


Indicates that the corresponding computer is currently connected to the switch via a PS/2 interface and is feeding power to the switch.

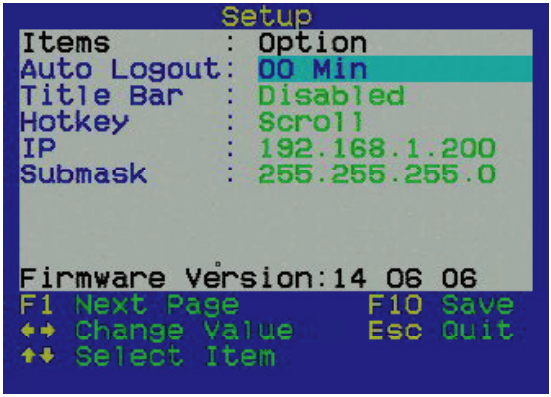

Indicates that the corresponding computer is currently connected to the switch via a USB interface and is feeding power to the switch. ***NOTE:*** Computers listed without any of the above symbols in the Status column either are not currently connected or are not feeding power to the switch.




As shown in the image above, the bottom of the menu screen displays various key controls. Use the left, right, up and down cursor keys to navigate within the menu; use the Insert key to edit; use F1 to move to the next menu screen.

**Setup Menu**

*Auto Logout:* Specify the amount of time (00 – 99 minutes).
*Title Bar:* Specify the position of the OSD title bar (or disable it).
*Hotkey:* Specify the hotkey preceding sequence.
*IP:* Specify the local IP address for the Digital KVM over IP Switch.
*Submask:* Specify the submask for the Digital KVM over IP Switch.
*Firmware Version:* Display the current firmware version.




## Local Console Control Options

Some common commands are listed below with the three control options (when applicable) that can be used to execute each of them: front-panel buttons, keyboard hotkeys and the OSD.

**Select PC**

- Front-panel buttons: Press the corresponding button on the switch that PC is connected to.
- Hotkeys: ScrLk, ScrLk, (a), (b), (y), (z). In a cascaded (daisy-chained) configuration, for

example, ScrLk, ScrlLk, 0, 3, 0, 7 would select the computer connected to Bank 3, Port 7. In a single-switch configuration, however, enter “01” as the bank number — (a) and (b) — in the hotkey sequence, as this is the default for each individual (and in this case, single) switch.
- OSD: With the OSD menu activated (ScrLk, ScrLk, Space Bar), use the cursor keys to navigate to the desired channel and press Enter. In a daisy-chain configuration, first select the correct bank using the Page Up or Page Down keys.

**Next Lower Channel**
- Front-panel buttons: Press the corresponding button.
- Hotkeys: ScrLk, ScrLk, Up arrow (since the lower-numbered channel would be in a “higher” position if displayed in a list).
- OSD: Navigate to and select the corresponding item on the menu.

**Next Higher Channel**
- Front-panel buttons: Press the corresponding button.
- Hotkeys: ScrLk, ScrLk, Down arrow (since the higher-numbered channel would be in a “lower” position if displayed in a list).
- OSD: Navigate to and select the corresponding item on the menu.

**Next Lower Bank (within a daisy-chain)**
- Front-panel buttons: Press the corresponding Port-Switching button on the appropriate cascaded switch in the configuration.
- Hotkeys: ScrLk, ScrLk, Page Down.
- OSD: Press Page Up.

**Next Higher Bank (within a daisy-chain)**
- Front-panel buttons: Press the corresponding Port-Switching button on the appropriate cascaded switch in the configuration.
- Hotkeys: ScrLk, ScrLk, Page Up.
- OSD: Press Page Down.

**Beep On/Off**
While autoscanning, port-switching or issuing a hotkey command, a beep will sound. If you want to turn this beeping on or off, use the hotkey sequence ScrLk, ScrLk, B.

**OSD Title Bar On/Off**
The OSD title bar, which displays the computer name, can be toggled on or off by using the hotkey sequence ScrLk, ScrLk, T.

**OSD Title Bar Position**
The OSD title bar can be positioned on either the left or right side of the screen. On the Setup menu, navigate to the Title Bar option, press Enter to select, then use the cursor keys to position. The default position is the left side.

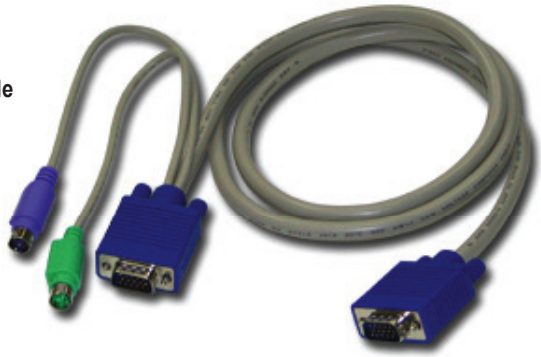
**Auto Logout**
On the OSD Setup menu, navigate to the Auto Logout option, press Enter to select, then make the desired change to the value (0 - 99 minutes. Auto Logout is disabled by default, indicated by 00.

# APPENDIX B: INSTALLATION COMPONENTS



3-in-1 USB Combo KVM cable

3-in-1 PS/2 Combo KVM cable





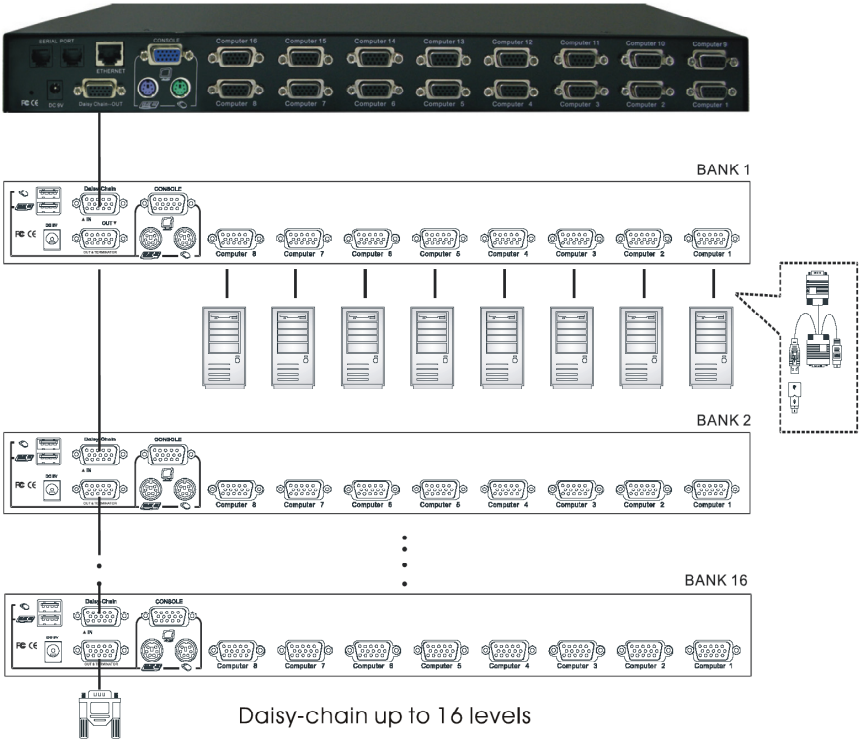
Combo-Free USB PS/2 KVM cable



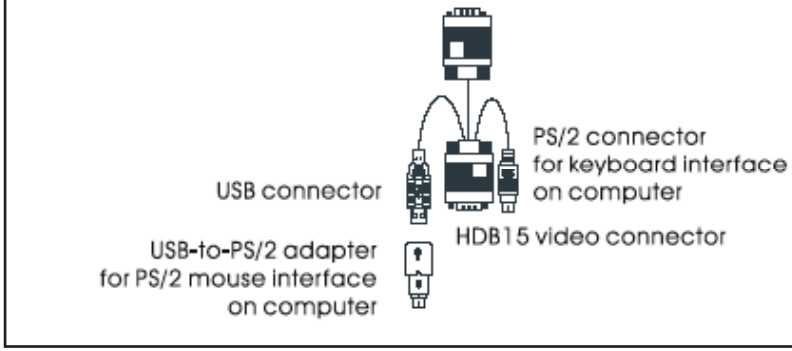
Daisy-Chain cable (HDB15 male to HDB15 female



Daisy-Chain terminator




**Combo-Free USB PS/2 KVM cable**



# SPECIFICATIONS

**Standards**
- IEEE 802.1X (Network Access Control)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3u (100Base-TX Fast Ethernet)

**General**
- 10/100 Mbps LAN port
- Local console: 1 VGA and 2 PS/2 ports (1 mouse, 1 keyboard)
- PC connection ports:
  - Model 503723: 8 HD15 female connections for use with 3-in-1 connection cables (375382, 375399)
  - Model 503730: 16 HD15 female connections for use with 3-in-1 connection cables (375382, 375399)
- RJ12 console management port
- RJ12 serial control port
- DC In connector
- Protocols supported:
  - SSH
  - RADIUS
  - HTTP
  - HTTPS
  - SNMP
- Access via Win32 or Java viewer
- Alert e-mail notification and SNMP trap messages for critical server events (“no video,” “blue screen of death” and “NumLock test failure”
- Certifications: FCC Class B

**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 SSL-secured 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 SSL password security levels:
  - No password
  - 1 global password for all users
  - Different password for each user

**User Management**
- 3 user levels: Superadmin, Admin, User
- Local user database
- Authentication to remote LDAP or RADIUS server
- User groups with access rights to specific connected computers

**Video**
- Supported resolutions:
  - 640 x 480 @ 60 Hz / 72 Hz / 75 Hz / 85 Hz / 100 Hz
  - 800 x 600 @ 60 Hz / 72 Hz / 75 Hz / 85 Hz / 100 Hz
  - 1024 x 768 @ 60 Hz / 72 Hz / 75 Hz /76 Hz / 85 Hz / 100 Hz
  - 1152 x 864 @ 60 Hz / 70 Hz / 78 Hz
  - 1280 x 1024 @ 60 Hz / 70 Hz
  - 1600 x 1200 @ 60 Hz / 70 Hz
- Color depth: 8 and 16 bit
- Quality settings: 3
- Video compression schemes: 4

**LEDs**
- Link
- 10/100 Mbps
- Power
- Video
- Selected (per port)
- Live (per port)
- Bank number

**Environmental**
- Dimensions: 410 (W) x 165 (L) x 44.5 (H) mm (16 x 6.5 x 1.7 in.)
- Weight: 3.6 kg (7.9 lbs.)
- Operating temperature: 0 – 50°C (32 – 122°F)
- Storage temperature: -20 – 60°C (-4 – 140°F)
- Humidity: 0 to 90% RH, non-condensing

**External Power Adapter**
- Input: 110 - 240 V AC, 50 / 60 Hz
- Output: 9 V DC, 2.0 A

**Package Contents**
- Digital KVM over IP switch
- Console management cable
- Modem serial cable
- External power adapter
- User manual
- Software CD
- 19” rackmount brackets




BRINGING NETWORKS TO LIFE

INTELLINET NETWORK SOLUTIONS™ offers a complete line of active and passive networking products. Ask your local computer dealer for more information or visit

**www.intellinet-network.com**.

Copyright © INTELLINET NETWORK SOLUTIONS
All products mentioned are trademarks or registered trademarks of their respective owners.