Contents

Chapter 1  Introduction ................................................................. 1
  Package Contents ............................................................................. 1
  Hardware .......................................................................................... 1
  Software .......................................................................................... 2
  ThinkSystem Digital KVM Switch Photos and Features ................ 3
  Remote and Local Console Interfaces ........................................... 3
  KVM Client Applications .................................................................. 4

Chapter 2  Get Started Using ThinkSystem Digital KVM Switch .......... 5
  Allow Pop-Ups ................................................................................. 5
  Appendix A  Security Warnings and Validation Messages ............. 6
    Java Validation and Access Warning ............................................ 7
    Additional Security Warnings ....................................................... 8
  Installing a Certificate ................................................................... 8
    Example 1: Import the Certificate into the Browser ................. 9
    Example 2: Add the ThinkSystem Digital KVM Switch to Trusted Sites and Import the Certificate ................. 10
  Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional) ......................................................... 12
  Logging In ....................................................................................... 14

Chapter 3  ThinkSystem Digital KVM Switch Interface and Navigation .... 15
  Overview ........................................................................................ 15
  ThinkSystem Digital KVM Switch Remote Console Interface .......... 16
    Port Access Page (Remote Console Display) ............................. 17
    Port Action Menu ....................................................................... 20
    Left Panel .................................................................................. 23
  ThinkSystem Digital KVM Switch Local Console Interface .......... 25

Chapter 4  Virtual Media ................................................................. 26
  Overview ....................................................................................... 26
  Prerequisites for Using Virtual Media .......................................... 27
    ThinkSystem Digital KVM Switch Virtual Media Prerequisites .... 27
    Remote PC VM Prerequisites ....................................................... 27
    Target Server VM Prerequisites .................................................. 27
    CIMs Required for Virtual Media ................................................ 27
## Contents

- Mounting Local Drives .................................................................................................................... 28
  - Notes on Mounting Local Drives ........................................................................................................ 28
- Supported Tasks Via Virtual Media ......................................................................................................... 28
- Supported Virtual Media Types .................................................................................................................. 29
  - Conditions when Read/Write is Not Available ............................................................................. 29
- Supported Virtual Media Operating Systems ........................................................................................... 29
- Number of Supported Virtual Media Drives ............................................................................................... 30
- Connecting and Disconnecting from Virtual Media .................................................................................. 30
  - Access a Virtual Media Drive on a Client Computer ........................................................................ 30
  - Mounting CD-ROM/DVD-ROM/ISO Images ...................................................................................... 31
  - Disconnect from Virtual Media Drives ............................................................................................... 32
- Virtual Media in a Windows XP Environment ............................................................................................ 32
- Virtual Media in a Linux Environment ......................................................................................................... 33
  - Active System Partitions ..................................................................................................................... 33
  - Mapped Drives .................................................................................................................................... 33
  - Drive Partitions ................................................................................................................................... 33
  - Root User Permission Requirement ................................................................................................. 33
  - Connect Drive Permissions (Linux) ...................................................................................................... 34
- Virtual Media in a Mac Environment ............................................................................................................. 35
  - Active System Partition ...................................................................................................................... 35
  - Drive Partitions ................................................................................................................................... 35
  - Connect Drive Permissions [Mac] ........................................................................................................ 36
- Virtual Media File Server Setup (File Server ISO Images Only) .................................................................. 36

## Chapter 5  KVM Clients

- KVM Client Launching ......................................................................................................................... 38
- Virtual KVM Client (VKC and VKCs) Help ............................................................................................... 39
  - Overview ........................................................................................................................................... 39
  - Recommended Minimum Virtual KVM Client (VKC) Requirements ................................................. 39
  - Virtual KVM Client Java Requirements ......................................................................................... 40
  - Proxy Server Configuration for Use with VKC, VKCS, and AKC ................................................... 41
  - Connect to a Target from Virtual KVM Client (VKC), Standalone VKC [VKCs], or Active KVM Client [AKC] ......................................................................................................................... 42
  - Configuring Connection Properties ................................................................................................. 43
  - Connection Information ..................................................................................................................... 47
  - USB Profiles ....................................................................................................................................... 48
  - Keyboard ............................................................................................................................................ 49
  - Video Properties ............................................................................................................................... 53
  - Mouse Options ................................................................................................................................... 57
  - Tool Options ...................................................................................................................................... 61
  - View Options ...................................................................................................................................... 70
  - Connect to Virtual Media .................................................................................................................... 71
  - Smart Cards ....................................................................................................................................... 72
  - Digital Audio ...................................................................................................................................... 74
Contents

Dual Power Supplies .......................................................................................................... 169

Index ................................................................................................................................ 175
Chapter 1 Introduction

The ThinkSystem Digital KVM Switch is an enterprise-class, secure, KVM-over-IP switch that provides multiple users with remote BIOS-level control of servers.

In This Chapter

Package Contents........................................................................................ 1
Hardware ..................................................................................................... 1
Software ....................................................................................................... 2
ThinkSystem Digital KVM Switch Photos and Features ............................. 3
Remote and Local Console Interfaces ....................................................... 3
KVM Client Applications ............................................................................ 4

Package Contents

Each ThinkSystem Digital KVM Switch ships as a fully-configured stand-alone product in a standard 1U or 2U form with 19” rackmount chassis.

- 1 - ThinkSystem Digital KVM Switch device
- 1 - Quick Setup Guide
- 1 - Rackmount kit
- 2 - AC power cords
- 1 - Set of 4 rubber feet (for desktop use)
- 1 - Application note
- 1 - Warranty card

Hardware

- Integrated KVM-over-IP remote access
- 1U or 2U rack-mountable (brackets included)
- Dual power supplies with failover; autoswitching power supply with power failure warning
- Support for the following CIMs:
  - ThinkSystem S-USB cable for Digital KVM: SC17A30053
  - ThinkSystem D-USB cable for Digital KVM: SC17A30049
- DVI monitor support from the DVI local port
  - VGA support via a DVI to VGA converter
  - DVI support via a standard DVI cable
Remote access from an iPhone® or iPad®
Support for tiering in which a base ThinkSystem Digital KVM Switch device is used to access multiple other tiered devices
Multiple user capacity (1/2/4/8 remote users; 1 local user)
UTP (Cat5/5e/6) server cabling
Dual Ethernet ports (10/100/1000 LAN) with failover or isolation mode support
Field upgradeable
Local USB User port for in-rack access
  • USB Keyboard/mouse ports, or connect to a cellular modem
  • One front and three back panel USB ports for supported USB devices
  • Fully concurrent local and remote user access
  • Local graphical user interface (GUI) for administration
Serial port to connect to an external telephone modem
Centralized access security
LED indicators for dual power status, network activity, and remote user status
Hardware Reset button

Software

Virtual media support in Windows®, Mac® and Linux® environments
Absolute Mouse Synchronization
Support for digital audio over USB
Port scanning and thumbnail views within a configurable scan set
Web-based access and management
Intuitive graphical user interface (GUI)
Support for dual port video output
256-bit encryption of complete KVM signal, including video and virtual media
LDAP, Active Directory®, RADIUS, or internal authentication and authorization
DHCP or fixed IP addressing
Smart card/CAC authentication
SNMP, SNMPv3, SMTP, and Syslog management
IPv4 and IPv6 support
ThinkSystem Digital KVM Switch Photos and Features

ThinkSystem Digital 2x1x16 KVM Switch

Diagram key

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Dual Power AC 100V/240V</td>
</tr>
<tr>
<td>B</td>
<td>Dual 10/100/1000 Ethernet access</td>
</tr>
<tr>
<td>C</td>
<td>Local USB ports</td>
</tr>
<tr>
<td>D</td>
<td>DVI-D port</td>
</tr>
<tr>
<td>E</td>
<td>Modem port for external modems</td>
</tr>
<tr>
<td>F</td>
<td>Tier port for tiering devices</td>
</tr>
<tr>
<td>G</td>
<td>KVM ports for UTP Cabling (Cat5/5e/6)</td>
</tr>
</tbody>
</table>

Remote and Local Console Interfaces

Use the Remote Console interface to configure and manage the ThinkSystem Digital KVM Switch over a network connection.

Use the Local Console interface to access the ThinkSystem Digital KVM Switch while at the rack.

See *ThinkSystem Digital KVM Switch Remote Console* (on page 115).

See *ThinkSystem Digital KVM Switch Local Console* (on page 121).
KVM Client Applications

ThinkSystem Digital KVM Switch works with -

- Active KVM Client (AKC) - Default client, Windows only. Microsoft .NET® 4.0 (or later) is required to use ThinkSystem Digital KVM Switch with the Microsoft Windows®-based Active KVM Client (AKC). See Active KVM Client (AKC) Help (on page 81)

- Virtual KVM Client (VKC) -Java™ 1.8 is required to use the Java-based Virtual KVM Client (VKC). Java 1.8.0_40 or higher is required to use the VKCS. Also available in a Standalone version for the Chrome browser. Java is required. See Virtual KVM Client (VKC) Help (see "Virtual KVM Client (VKC and VKCs) Help" on page 39)

- HTML KVM Client (HKC) - Runs on Linux, Mac, and Windows without .NET, in IE, Edge, Firefox, Chrome and Safari. No Java. Basic KVM features are supported. See HTML KVM Client (HKC) Help.
Chapter 2  Get Started Using ThinkSystem Digital KVM Switch

This section walks you through high-level tasks to start using ThinkSystem Digital KVM Switch.

In This Chapter
Allow Pop-Ups .................................................................................................................. 5
Security Warnings and Validation Messages .................................................................. 6
Installing a Certificate ..................................................................................................... 8
Converting a Binary Certificate to a Base64-Encoded DER Certificate [Optional] .................. 12
Logging In ......................................................................................................................... 14

Allow Pop-Ups

Regardless of the browser you are using, you must allow pop-ups in order to launch the ThinkSystem Digital KVM Switch Remote Console.
Appendix A

Security Warnings and Validation Messages

When logging in to ThinkSystem Digital KVM Switch using RSC, security warnings and application validation message may appear.

These include -

- Java™ security warnings and requests to validate ThinkSystem Digital KVM Switch
  See Java Validation and Access Warning (on page 7) and Installing a Certificate (on page 8)
- Additional security warnings based on your browser and security settings
  See Additional Security Warnings (on page 8)

In This Chapter

Java Validation and Access Warning .......................................................... 7
Additional Security Warnings ........................................................................ 8
Java Validation and Access Warning

When logging in to ThinkSystem Digital KVM Switch, Java prompts you to validate ThinkSystem Digital KVM Switch, and to allow access to the application.

Installing an SSL certificate in each ThinkSystem Digital KVM Switch device is recommended to reduce Java warnings, and enhance security.

See SSL Certificates
Appendix A: Get Started Using ThinkSystem Digital KVM Switch

Additional Security Warnings

Even after an SSL certificate is installed in the ThinkSystem Digital KVM Switch, depending on your browser and security settings, additional security warnings may be displayed when you log in to ThinkSystem Digital KVM Switch.

It is necessary to accept these warnings to launch the ThinkSystem Digital KVM Switch Remote Console.

Reduce the number of warning messages during subsequent log ins by checking the following options on the security and certificate warning messages:

- In the future, do not show this warning
- Always trust content from this publisher

Installing a Certificate

You may be prompted by the browser to accept and validate the ThinkSystem Digital KVM Switch’s SSL certificate.

Depending on your browser and security settings, additional security warnings may be displayed when you log in to ThinkSystem Digital KVM Switch.

It is necessary to accept these warnings to launch the ThinkSystem Digital KVM Switch Remote Console. For more information, see Security Warnings and Validation Messages (on page 6).

Two sample methods on how to install an SSL Certificate in the browser are provided here, both using Microsoft Internet Explorer 8® and Windows 7®.

Specific methods and steps depend on your browser and operating system. See your browser and operating system help for details.
Example 1: Import the Certificate into the Browser

In this example, you import the Certificate into the browser.

1. Open an IE browser, then log in to ThinkSystem Digital KVM Switch.
2. Click More Information on the first Java™ security warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

*Note: If you are not prompted by the browser, manually select Tools > Internet Options to open the Internet Options dialog.*

1. Click the Content tab.
2. Click Certificates.
The Certificate Import Wizard opens and walks you through each step.

- File to Import - Browse to locate the Certificate
- Certificate Store - Select the location to store the Certificate

3. Click Finish on the last step of the Wizard.

The Certificate is imported. Close the success message.

4. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

Example 2: Add the ThinkSystem Digital KVM Switch to Trusted Sites and Import the Certificate

In this example, the ThinkSystem Digital KVM Switch’s URL is added as a Trusted Site, and the Self Signed Certificate is added as part of the process.

1. Open an IE browser, then select Tools > Internet Options to open the Internet Options dialog
2. Click the Security tab.
3. Click on Trusted Sites.
4. Disable Protected Mode, and accept any warnings.
5. Click Sites to open the Trusted Sites dialog.
6. Enter the ThinkSystem Digital KVM Switch URL, then click Add.
7. Deselect server verification for the zone (if applicable).
8. Click Close.
9. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser. Next, import the Certificate.

1. Open an IE browser, then log in to ThinkSystem Digital KVM Switch.
2. Click More Information on the first Java™ security warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

For details see, Example 1: Import the Certificate into the Browser (on page 9).
Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)

ThinkSystem Digital KVM Switch requires an SSL certificate in either Base64-Encoded DER format or PEM format. If you are using an SSL certificate in binary format, you cannot install it. However, you can convert your binary SSL certificate.

2. Click the Detail tab.
3. Click "Copy to File...".

4. The Certificate Export Wizard opens. Click Next to start the Wizard.

5. Select “Base-64 encoded X.509” in the second Wizard dialog.

6. Click Next to save the file as a Base-64 encoded X.509.

You can now install the certificate on your ThinkSystem Digital KVM Switch.
Logging In

Log in to your ThinkSystem Digital KVM Switch Remote Console from any workstation with network connectivity. Java™ 1.8 is required to use the Java-based . Java 1.8.0_40 or higher is required to use the VKCS. Alternatively, Microsoft .NET® 4.0 (or later) is required to use ThinkSystem Digital KVM Switch with the Microsoft Windows®-based Active KVM Client (AKC).

Logging in and using ThinkSystem Digital KVM Switch requires you to allow pop-ups.

For information on security warnings and validation messages, and steps to reduce or eliminate them, see Security Warnings and Validation Messages (on page 6).

To log in via Remote Console:

1. Launch a supported web browser, and enter the IP address assigned to the ThinkSystem Digital KVM Switch.

2. A default client is launched based on your PC and browser settings. See KVM Client (see "KVM Clients" on page 38). You can also choose a client by entering the URL directly. See KVM Client Launching.

3. Enter your username and password, then click Login.

4. Accept the user agreement (if applicable). If security warnings appear, click to accept.
Chapter 3  ThinkSystem Digital KVM Switch Interface and Navigation

The ThinkSystem Digital KVM Switch Remote Console and the ThinkSystem Digital KVM Switch Local Console are web-based graphical user interfaces.

Use the Remote Console interface to configure and manage the ThinkSystem Digital KVM Switch over a network connection.

Use the Local Console interface to access the ThinkSystem Digital KVM Switch while at the rack.

Access targets from either the Remote or Local console from one of the supported KVM clients.

In This Chapter

Overview .................................................................................................... 15
ThinkSystem Digital KVM Switch Remote Console Interface ................... 16
ThinkSystem Digital KVM Switch Local Console Interface ...................... 25

Overview

The ThinkSystem Digital KVM Switch Remote Console and the ThinkSystem Digital KVM Switch Local Console interfaces provide a web-based interface for device configuration and administration, as well as target server list and selection.
ThinkSystem Digital KVM Switch Remote Console Interface

The ThinkSystem Digital KVM Switch Remote Console is a browser-based graphical user interface that allows you to log in to KVM target servers and serial targets connected to the ThinkSystem Digital KVM Switch and to remotely administer the ThinkSystem Digital KVM Switch.

The ThinkSystem Digital KVM Switch Remote Console provides a digital connection to your connected KVM target servers. When you log into a KVM target server using the ThinkSystem Digital KVM Switch Remote Console, a Virtual KVM Client window opens.

There are many similarities among the ThinkSystem Digital KVM Switch Local Console and the ThinkSystem Digital KVM Switch Remote Console graphical user interfaces, and where there are differences, they are noted in the user manual. The following options are available in the ThinkSystem Digital KVM Switch Remote Console but not the ThinkSystem Digital KVM Switch Local Console:

- Virtual Media
- Backup/Restore
- Firmware Upgrade
- SSL Certificates
- Audio
Chapter 3: ThinkSystem Digital KVM Switch Interface and Navigation

Port Access Page [Remote Console Display]

After a successful login, the Port Access page opens listing all ports along with their status and availability.

Ports connected to KVM target servers (blades and standard servers) are displayed in blue. Right-click on any of these ports to open the Port Action menu. For more information, see Port Action Menu [on page 20].

If a ThinkSystem Digital KVM Switch port has no CIM connected or is connected to a CIM with no name, a default port name of KVM_SWITCH_PORT# is assigned to the port.

- KVM_SWITCH is the model of the KVM switch.
- Port# is the number of the ThinkSystem Digital KVM Switch physical port.

Tabs above the port list allow you to view by port, view by group, view by search and scan ports.

Sort by Port Number, Port Name, Status [Up and Down], and Availability [Idle, Connected, Busy, Unavailable, and Connecting] by clicking on the column heading.

Use the Set Scan tab to scan for targets that are connected to the ThinkSystem Digital KVM Switch. See Scanning Ports - Remote Console [on page 116]
Chapter 3: ThinkSystem Digital KVM Switch Interface and Navigation

**Tiered Devices - Port Access Page**

If you are using a tiered configuration in which a base ThinkSystem Digital KVM Switch device is used to access multiple other tiered devices, the tiered devices are viewed on the Port Access page by clicking on the Expand Arrow icon to the left of the tier device name.

**Blade Chassis - Port Access Page**

The blade chassis is displayed in an expandable, hierarchical list on the Port Access page, with the blade chassis at the root of the hierarchy and the individual blades labeled and displayed below the root. Use the Expand Arrow icon next to the root chassis to display the individual blades.

*Note: To view the blade chassis in a hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.*

**Dual Port Video Groups - Port Access Page**

Dual video port groups appear on the Port Access page as Dual Port types.

The primary and secondary ports that are a part of the port group appear on the Port Access page as Dual Port(P) and Dual Port(S), respectively.

When you access a dual port video group from the remote client, you connect to the primary port, which opens a KVM connection window to both the primary and secondary ports of the dual port group.

*Note: The dual video primary port is defined when the port group is created.*

*Note: You cannot remotely connect to the dual video port group by clicking on a primary port unless two KVM channels are available. If two channels are not available, the Connect link is not displayed.*

*Note: The Action menu is not displayed when you click on a secondary port in a dual video port group.*

*Note: You cannot connect to the primary port and secondary port at the same time from the Local Port.*
View by Group Tab

The View by Group tab displays blade chassis, ‘standard’ port groups, and dual video port groups. Click the Expand Arrow icon next to a group to view the ports assigned to the port group.

<table>
<thead>
<tr>
<th>View By</th>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WinXP Group</td>
<td>Dual Video Port Group</td>
</tr>
<tr>
<td>2</td>
<td>WinXP primary</td>
<td>Dual-VM Dual Port (P)</td>
</tr>
<tr>
<td>3</td>
<td>WinXP secondary</td>
<td>Dual-VM Dual Port (S)</td>
</tr>
<tr>
<td>3</td>
<td>win1-direct-video</td>
<td>Dual Video Port Group</td>
</tr>
</tbody>
</table>

View by Search Tab

The View by Search tab allows you to search by port name. The search feature supports the use of an asterisk (*) as a wildcard, and full and partial names.

Set Scan Tab

The port scanning feature is accessed from the Set Scan tab on the Port Access page. The feature allows you to define a set of targets to be scanned. Thumbnail views of the scanned targets are also available. Select a thumbnail to open that target in its Virtual KVM Client window.

See Scanning Ports - Remote Console (on page 116) for more information.
Port Action Menu
When you click a Port Name in the Port Access list, the Port Action menu appears.

Choose the desired menu option for that port to execute it. Note that only currently available options, depending on the port’s status and availability, are listed in the Port Action menu.

Port Access

Click on the individual port name to see allowable operations. 0 / 4 Remote KVM channels currently in use.

<table>
<thead>
<tr>
<th>View By Port</th>
<th>View By Group</th>
<th>View By Search</th>
<th>Set Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>▲ No.</td>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>HDMI Target</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Generic KVM Port 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Low Cost [PQ20540016]</td>
<td>Connect</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Windows XP SP3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Low Cost [PQ20540016]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Low Cost [PQ20540016]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Connect

- Connect - Creates a new connection to the target server

For the ThinkSystem Digital KVM Switch Remote Console, a new Virtual KVM Client page appears.

For the ThinkSystem Digital KVM Switch Local Console, the display switches to the target server, and switches away from the local user interface.

On the local port, the ThinkSystem Digital KVM Switch Local Console interface must be visible in order to perform the switch.

Hot key switching is also available from the local port.

Note: This option is not available from the ThinkSystem Digital KVM Switch Remote Console for an available port if all connections are busy.
Chapter 3: ThinkSystem Digital KVM Switch Interface and Navigation

Switch From

- **Switch From** - Switches from an existing connection to the selected port (KVM target server)

  This menu item is available only for KVM targets, and only when a Virtual KVM Client is opened.

  *Note: This menu item is not available on the ThinkSystem Digital KVM Switch Local Console.*

---

**Port Access**

*Click on the individual port name to see allowable operations. 1/4 Remote KVM channels currently in use.*

<table>
<thead>
<tr>
<th>View By Port</th>
<th>View By Group</th>
<th>View By Search</th>
<th>Set Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Switch From HDMI Target</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Low Cost DVM [PQ20540018]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Disconnect

- **Disconnect** - Disconnects this port and closes the Virtual KVM Client page for this target server

  This menu item is available only when the port status is up and connected, or up and busy.
Note: This menu item is not available on the ThinkSystem Digital KVM Switch Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.

Port Access

Click on the individual port name to see allowable operations.

1 / 4 Remote KVM channels currently in use.

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>View By Port</th>
<th>View By Group</th>
<th>View By Search</th>
<th>Set Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disconnect</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Dominion-KQ2_Port2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ThinkSystem Digital KVM [FC0540016]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Left Panel**

The left panel of the ThinkSystem Digital KVM Switch interface contains the following information.

Note that some information is conditional - meaning it is displayed based on your role, features being used and so on. Conditional information is noted here.

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
<th>When displayed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time &amp; Session</td>
<td>The date and time the current session started</td>
<td>Always</td>
</tr>
<tr>
<td>User</td>
<td>Username</td>
<td>Always</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the application, either idle or active. If idle, the application tracks and displays the time the session has been idle.</td>
<td>Always</td>
</tr>
<tr>
<td>Your IP</td>
<td>The IP address used to access the ThinkSystem Digital KVM Switch</td>
<td>Always</td>
</tr>
<tr>
<td>Last Login</td>
<td>The last login date and time</td>
<td>Always</td>
</tr>
</tbody>
</table>
### Information Description When displayed?

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
<th>When displayed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td>Information specific to the ThinkSystem Digital KVM Switch you are using</td>
<td>Always</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name assigned to the device</td>
<td>Always</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the ThinkSystem Digital KVM Switch</td>
<td>Always</td>
</tr>
<tr>
<td>Firmware</td>
<td>Current version of firmware</td>
<td>Always</td>
</tr>
<tr>
<td>Device Model</td>
<td>Model of the ThinkSystem Digital KVM Switch</td>
<td>Always</td>
</tr>
<tr>
<td>Serial number</td>
<td>Serial number of the ThinkSystem Digital KVM Switch</td>
<td>Always</td>
</tr>
<tr>
<td>Network</td>
<td>The name assigned to the current network</td>
<td>Always</td>
</tr>
<tr>
<td>PowerIn1</td>
<td>Status of the power 1 outlet connection. Either on or off, or Auto-detect off</td>
<td>Always</td>
</tr>
<tr>
<td>PowerIn2</td>
<td>Status of the power 2 outlet connection. Either on or off, or Auto-detect off</td>
<td>Always</td>
</tr>
<tr>
<td>Configured As Base or Configured As Tiered</td>
<td>If you are using a tiering configuration, this indicates if the ThinkSystem Digital KVM Switch you are accessing is the base device or a tiered device.</td>
<td>When the ThinkSystem Digital KVM Switch is part of a tiered configuration</td>
</tr>
<tr>
<td>Port States</td>
<td>The statuses of the ports being used by the ThinkSystem Digital KVM Switch</td>
<td>Always</td>
</tr>
</tbody>
</table>
Chapter 3: ThinkSystem Digital KVM Switch Interface and Navigation

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
<th>When displayed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Users</td>
<td>The users, identified by their username and IP address, who are currently connected to the ThinkSystem Digital KVM Switch</td>
<td>Always</td>
</tr>
<tr>
<td>FIPS Mode</td>
<td>FIPS Mode: EnabledSSL Certificate: FIPS Mode Compliant</td>
<td>When FIPS is enabled</td>
</tr>
</tbody>
</table>

**ThinkSystem Digital KVM Switch Local Console Interface**

There are many similarities among the ThinkSystem Digital KVM Switch Local Console and the ThinkSystem Digital KVM Switch Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

For details on using the Local Console see *ThinkSystem Digital KVM Switch Local Console* (on page 121).
Chapter 4  Virtual Media

In This Chapter

Overview .................................................................................................... 26
Prerequisites for Using Virtual Media ...................................................... 27
Mounting Local Drives ............................................................................... 28
Supported Tasks Via Virtual Media ........................................................... 28
Supported Virtual Media Types ................................................................. 29
Supported Virtual Media Operating Systems ............................................ 29
Number of Supported Virtual Media Drives .............................................. 30
Connecting and Disconnecting from Virtual Media .................................. 30
Virtual Media in a Windows XP Environment ............................................ 32
Virtual Media in a Linux Environment ....................................................... 33
Virtual Media in a Mac Environment ......................................................... 35
Virtual Media File Server Setup (File Server ISO Images Only)................. 36

Overview

All ThinkSystem Digital KVM Switch models support virtual media. Virtual media extends KVM capabilities by enabling target servers to remotely access media from a client PC and network file servers.

With this feature, media mounted on client PCs and network file servers are essentially “mounted virtually” by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself.

Each ThinkSystem Digital KVM Switch comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, audio playback and record devices, internal and remote drives, and images.

Virtual media sessions are secured using 128 or 256 bit AES encryption.
Prerequisites for Using Virtual Media

ThinkSystem Digital KVM Switch Virtual Media Prerequisites

- For users requiring access to virtual media, the ThinkSystem Digital KVM Switch permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level.
- A USB connection must exist between the device and the target server.
- If you want to use PC-Share, Security Settings must also be enabled in the Security Settings page. **Optional**
- You must choose the correct USB profile for the KVM target server you are connecting to.

Remote PC VM Prerequisites

- Certain virtual media options require administrative privileges on the remote PC (for example, drive redirection of complete drives).

  **Note:** If you are using Microsoft Vista or Windows 7, disable User Account Control or select Run as Administrator when starting Internet Explorer. To do this, click the Start Menu, locate IE, right-click and select Run as Administrator.

Target Server VM Prerequisites

- KVM target servers must support USB connected drives.
- USB 2.0 ports are faster and preferred.

CIMs Required for Virtual Media

You must use one of the following CIMs to use virtual media:

- ThinkSystem S-USB cable for Digital KVM: SC17A30053
- ThinkSystem D-USB cable for Digital KVM: SC17A30049

The black USB connector on the dual USB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media. Keep both USB plugs of the CIM connected to the device. The device may not operate properly if both plugs are not connected to the target server.
Mounting Local Drives

This option mounts an entire drive, which means the entire disk drive is mounted virtually onto the target server.

Use this option for hard drives and external drives only. It does not include network drives, CD-ROM, or DVD-ROM drives.

Notes on Mounting Local Drives

KVM target servers running the Windows XP operating system may not accept new mass storage connections after an NTFS-formatted partition (for example, the local C drive) has been redirected to them.

If this occurs, close the Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.

Supported Tasks Via Virtual Media

Virtual media provides the ability to perform tasks remotely, such as:

• Transferring files
• Running diagnostics
• Installing or patching applications
• Complete installation of the operating system
• Record and playback of digital audio

Important: Once you are connected to a virtual media drive, do not change mouse modes in the KVM client if you are performing file transfers, upgrades, installations or other similar actions. Doing so may cause errors on the virtual media drive or cause the virtual media drive to fail.
Supported Virtual Media Types

The following virtual media types are supported for Windows®, Mac® and Linux™ clients:

- Internal and external hard drives
- Internal and USB-mounted CD and DVD drives
- USB mass storage devices
- PC hard drives
- ISO images (disk images)
  ISO9660 is the standard supported. However, other ISO standards can be used.
- Digital audio devices*

Conditions when Read/Write is Not Available

Virtual media Read/Write is not available in the following situations:

- For Linux® and Mac® clients
- When the drive is write-protected
- When the user does not have Read/Write permission:
  - Port Permission Access is set to None or View
  - Port Permission VM Access is set to Read-Only or Deny

Supported Virtual Media Operating Systems

The following client operating systems are supported:

- Windows® 7 operating system
- Windows 8 operating system
- Windows XP® operating system
- openSUSE® 11.4 Celadon (x86_64)
- Fedora® 18
- RHEL® 6.4
- OSX Mountain Lion® 10.7 (and later)
- Solaris® 10

The Active KVM Client (AKC) can be used to mount virtual media types but only for Windows operating systems.
Number of Supported Virtual Media Drives

With the virtual media feature, you can mount up to two drives [of different types] that are supported by the USB profile currently applied to the target. These drives are accessible for the duration of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then disconnect it when you are done. The CD-ROM virtual media “channel” will remain open, however, so that you can virtually mount another CD-ROM. These virtual media “channels” remain open until the KVM session is closed as long as the USB profile supports it.

To use virtual media, connect/attach the media to the client or network file server that you want to access from the target server.

This need not be the first step, but it must be done prior to attempting to access this media.

Connecting and Disconnecting from Virtual Media

Access a Virtual Media Drive on a Client Computer

Important: Once you are connected to a virtual media drive, do not change mouse modes in the KVM client if you are performing file transfers, upgrades, installations or other similar actions. Doing so may cause errors on the virtual media drive or cause the virtual media drive to fail.

To access a virtual media drive on the client computer:

1. From the KVM client, choose Virtual Media > Connect Drive, or click the Connect Drive... button. The Map Virtual Media Drive dialog appears.

2. Choose the drive from the Local Drive drop-down list.
If you want Read and Write capabilities, select the Read-Write checkbox.

This option is disabled for nonremovable drives. See the Conditions when Read/Write is Not Available (on page 29) for more information.

When checked, you will be able to read or write to the connected USB disk.

WARNING: Enabling Read/Write access can be dangerous! Simultaneous access to the same drive from more than one entity can result in data corruption. If you do not require Write access, leave this option unselected.

3. Click OK. The media will be mounted on the target server virtually. You can access the media just like any other drive.

Mounting CD-ROM/DVD-ROM/ISO Images

This option mounts CD-ROM, DVD-ROM, and ISO images.

Note: ISO9660 format is the standard supported. However, other CD-ROM extensions may also work.

To access a CD-ROM, DVD-ROM, or ISO image:

1. From the KVM client, choose Virtual Media > Connect CD-ROM/ISO Image, or click the Connect CD ROM/ISO button. The Map Virtual Media CD/ISO Image dialog appears.

2. For internal and external CD-ROM or DVD-ROM drives:
   a. Choose the Local CD/DVD Drive option.
   b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.
   c. Click Connect.

3. For ISO images:
   a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
   b. Click Browse.
   c. Navigate to the path containing the disk image you want to use and click Open. The path is populated in the Image Path field.
   d. Click Connect.

4. For remote ISO images on a file server:
b. Choose Hostname and Image from the drop-down list. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the File Server Setup page will be in the drop-down list.

c. File Server Username - User name required for access to the file server. The name can include the domain name such as mydomain/username.

d. File Server Password - Password required for access to the file server (field is masked as you type).

e. Click Connect.

The media will be mounted on the target server virtually. You can access the media just like any other drive.

*Note: If you are working with files on a Linux® target, use the Linux Sync command after the files are copied using virtual media in order to view the copied files. Files may not appear until a sync is performed.*

*Note: If you are using the Windows 7® operating system®, Removable Disk is not displayed by default in the Window’s My Computer folder when you mount a Local CD/DVD Drive or Local or Remote ISO Image. To view the Local CD/DVD Drive or Local or Remote ISO Image in this folder, select Tools > Folder Options > View and deselect “Hide empty drives in the Computer folder”.*

*Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to third-party software technical limitations.*

### Disconnect from Virtual Media Drives

- **To disconnect the virtual media drives:**
  - For local drives, choose Virtual Media > Disconnect Drive.

*Note: In addition to disconnecting the virtual media using the Disconnect command, simply closing the KVM connection closes the virtual media as well.*

### Virtual Media in a Windows XP Environment

If you are running the Virtual KVM Client or Active KVM Client in a Windows® XP environment, users must have Administrator privileges to access any virtual media type other than CD-ROM connections, ISOs and ISO images.
Virtual Media in a Linux Environment

Active System Partitions
You cannot mount active system partitions from a Linux client.
Linux Ext3/4 drive partitions need to be unmounted via umount
/dev/<device label> prior to a making a virtual media connection.

Mapped Drives
Mapped drives from Linux clients are not locked when mounted onto
connected targets. This applies only to ThinkSystem Digital KVM Switch
2.4.0 (and later).

Drive Partitions
The following drive partition limitations exist across operating systems:
• Windows® and Mac targets are not able to read Linux formatted
  partitions
• Windows and Linux cannot read Mac formatted partitions
• Only Windows Fat partitions are supported by Linux

Root User Permission Requirement
Your virtual media connection can be closed if you mount a CD ROM from
a Linux client to a target and then unmount the CD ROM.
To avoid these issues, you must be a root user.
Connect Drive Permissions (Linux)

Users must have the appropriate access permissions in order to connect the Drive/CD-ROM to the target. This can be checked using:

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0
brw-rw---- 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

In the above example, the permission must be changed to allow read access.

On a system that supports ACLs in its file utilities, the `ls` command changes its behavior in the following way:

- For files that have a default ACL or an access ACL that contains more than the three required ACL entries, the `ls(1)` utility in the long form produced by `ls -l` displays a plus sign (+) after the permission string.

This is indicated in the example provided here for `/dev/sr0`, use `getfacl -a /dev/sr0` to see if the user has been provided access as part of an ACL. In this case they have and are therefore able to connect the cd-rom onto the target even though the output of the `ls -l` command may indicate otherwise.

```
guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl: Removing leading '/' from absolute path names
# file: dev/sr0
# owner: root
# group: cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---
```

A similar check of the permissions for a removable device shows:
guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

getfacl -a /dev/sdb1
getfacl: Removing leading '/' from absolute path names
# file: dev/sdb1
# owner: root
# group: disk
user::rw-
group::rw-
other::---

This requires that the user is provided read-only permissions for the removable device:

root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

The drive is then available to connect to the target.

Virtual Media in a Mac Environment

Active System Partition
You cannot use virtual media to mount active system partitions for a Mac client.

Drive Partitions
The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows cannot read Mac formatted partitions
- Windows FAT and NTFS are supported by Mac
- Mac users must unmount any devices that are already mounted in order to connect to a target server. Use `diskutil umount /dev/disk1s1` to unmount the device and `diskutil mount /dev/disk1s1` to remount it.
Connect Drive Permissions (Mac)

In order for a device to be available to connect to a target from a Mac® client, you must have read-only permissions to the removable device:

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw----r----- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

Virtual Media File Server Setup (File Server ISO Images Only)

This feature is only required when using virtual media to access file server ISO images. ISO9660 format is the standard supported. However, other CD-ROM extensions may also work.

*Note: SMB/CIFS support is required on the file server.*


To designate file server ISO images for virtual media access:

2. Check the Selected checkbox for all media that you want accessible as virtual media.
3. Enter information about the file server ISO images that you want to access:
   - IP Address/Host Name - Host name or IP address of the file server.
   - Image Path - Full path name of the location of the ISO image. For example, /sharename0/path0/image0.iso, \sharename1\path1\image1.iso, and so on.

   *Note: The host name cannot exceed 232 characters in length.*
4. Click Save. All media specified here are now available for selection in the Map Virtual Media CD/ISO Image dialog.
Note: If you are connecting to a Windows 2003® server and attempt to load an ISO image from the server, you may receive an error stating “Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password”.

If this occurs, disable “Microsoft Network Server: Digitally Sign Communications” option on the server under the Domain Controllers policies.
Chapter 5  KVM Clients

<table>
<thead>
<tr>
<th>KVM Client</th>
<th>Name</th>
<th>Platform</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active KVM Client</td>
<td>AKC</td>
<td>Windows Platforms</td>
<td>Full-featured KVM Client Java-Free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires Microsoft .NET</td>
<td></td>
</tr>
<tr>
<td>Virtual KVM Client</td>
<td>VKC</td>
<td>Linux &amp; Mac</td>
<td>Full-featured KVM Client Java</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires Java</td>
<td></td>
</tr>
<tr>
<td>HTML KVM Client</td>
<td>HKC</td>
<td>Linux &amp; Mac</td>
<td>Basic KVM Access Only Java-Free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows w/o .NET</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTML &amp; Javascript</td>
<td></td>
</tr>
</tbody>
</table>

- AKC is best for Windows Platforms
- VKC is best for Linux and Mac users with Java
- HKC is best for Linux and Mac users without Java

Note: Many features are supported on HKC. See HTML KVM Client (HKC) Help for details.

In This Chapter

KVM Client Launching ............................................................................... 38
Virtual KVM Client (VKC and VKCs) Help ........................................... 39
Active KVM Client (AKC) Help ................................................................... 81
HTML KVM Client (HKC) Help ................................................................... 85

KVM Client Launching

<table>
<thead>
<tr>
<th>KVM Client</th>
<th>Name</th>
<th>Underlying Technology</th>
<th>Automatically Launched For</th>
<th>URL to Force Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active KVM Client</td>
<td>AKC</td>
<td>Microsoft .NET Framework</td>
<td>Windows and .NET Framework</td>
<td>&lt;ThinkSystem IP Address&gt;/akc</td>
</tr>
<tr>
<td>Virtual KVM Client</td>
<td>VKC</td>
<td>Oracle Java</td>
<td>Non-Windows with Java</td>
<td>&lt;ThinkSystem IP Address&gt;/vkc</td>
</tr>
<tr>
<td>HTML KVM Client</td>
<td>HKC</td>
<td>Browser HTML and Javascript</td>
<td>Non-Windows</td>
<td>&lt;ThinkSystem IP Address&gt;/hkc</td>
</tr>
</tbody>
</table>
Virtual KVM Client [VKC and VKCs] Help

Overview

VKC is the default client for Non-Windows platform clients with Java. Whenever you access a target server from the Port Access page of ThinkSystem Digital KVM Switch the Remote Console, a Virtual KVM Client [VKC] window opens.

There is one Virtual KVM Client for each target server connected. Virtual KVM Client windows can be minimized, maximized, and moved around your computer desktop.

IMPORTANT: Refreshing your browser closes the Virtual KVM Client connection.

Recommended Minimum Virtual KVM Client [VKC] Requirements

It is recommended that the Virtual KVM Client [VKC] machines meet the following minimum requirements.

- Client machine with either a -
  - ‘modern’ dual-core CPU for a single connections, or
  - ‘modern’ quad core CPU for two or more simultaneous connections
- 4GB of RAM
  - VKC requires 50MB of RAM per connection
Virtual KVM Client Java Requirements

Java™ 1.8 is required to use the Java-based Virtual KVM Client (VKC). Java 1.8.0_40 or higher is required to use the VKCS.

Java 7 is not supported, and a Java error displays if you attempt to launch VKCS with JRE 1.7.

If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

*Note:* VKC cannot be launched from Edge, Chrome 45 or later, Firefox 42 or later. VKCS is recommended for these browsers.

**VKCS Launching:**

For all browsers, the VKCS standalone application needs to be downloaded every time you use it.

- Chrome: The downloaded VKCS jnlp file must always be clicked at bottom left corner of browser window to launch.
• Edge: You must click Open at the bottom of the browser to launch.
• Internet Explorer: Launches automatically.
• Firefox: Use the option "Do this automatically for files like this from now on", when the vkcs.jnlp file downloads, and it will launch automatically in future.

Proxy Server Configuration for Use with VKC, VKCS, and AKC
When the use of a Proxy Server is required, a SOCKS proxy must also be provided and configured on the remote client PC.

Note: If the installed proxy server is only capable of the HTTP proxy protocol, you cannot connect.

► To configure the SOCKS proxy:
1. On the remote client PC, select Control Panel > Internet Options.
   b. Select ‘Use a proxy server for your LAN’.
   c. Click Advanced. The Proxy Settings dialog opens.
   d. Configure the proxy servers for all protocols.
      IMPORTANT: Do not select ‘Use the same proxy server for all protocols’.
Chapter 5: KVM Clients

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

e. Click OK at each dialog to apply the settings.

2. Next, configure the proxy settings for the Java™ applets:
   a. Select Control Panel > Java.
   c. Select “Use Proxy Server”.
   d. Click Advanced. The Advanced Network Settings dialog opens.
   e. Configure the proxy servers for all protocols.

   **IMPORTANT:** Do not select ‘Use the same proxy server for all protocols’.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

---

**Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC)**

Once you have logged on to the ThinkSystem Digital KVM Switch Remote Console, access target servers via the Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC).

▶ **To connect to an available server:**

1. On the Port Access page, click on the port name of the target server you want to connect to. The Port Action menu opens.

2. Click Connect.

   ![Port Access](image)

   See **Port Action Menu** (on page 20) for details on additional available menu options.
Configuring Connection Properties

Connection properties manage streaming video performance over remote connections to target servers.

The properties are applied only to your connection - they do not impact the connection of other users accessing the same target servers.

If you make changes to connection properties, they are retained by the client.

Access Connection Properties

To access connection properties:

Click Connection > Properties, or click the Connection... icon to open the Connection Properties dialog.

Default Connection Property Settings - Optimized for Best Performance

The ThinkSystem Digital KVM Switch comes configured to provide optimal performance for the majority of video streaming conditions.

Default connection settings are:

- Optimized for: Text Readability - video modes are designed to maximize text readability.
  
  This setting is ideal for general IT and computer applications, such as performing server administration.
• Video Mode - defaults to Full Color 2.
  Video frames transmit in high-quality, 24-bit color. This setting is suitable where a high-speed LAN is used.
• Noise Filter - defaults to 2.
  The noise filter setting does not often need to be changed.

Click Reset on the Connection Properties dialog at any time to return to the default settings.

Tip: Use the Connection Information dialog to monitor the connection in real-time. See Access and Copy Connection Information (on page 47)

Optimize for: Selections

Text Readability
Text Readability is designed to provide video modes with lower color depth but text remains readable. Greyscale modes are even available when applying lower bandwidth settings.

This setting is ideal when working with computer GUls, such as server administration.

When working in full color video modes, a slight contrast boost is provided, and text is sharper.

In lower quality video modes, bandwidth is decreased at the expense of accuracy.

Color Accuracy
When Color Accuracy is selected, all video modes are rendered in full 24-bit color with more compression artifacts.

This setting applies to viewing video streams such as movies or other broadcast streams.

In lower quality video modes, sharpness of fine detail, such as text, is sacrificed.
Video Mode

The Video Mode slider controls each video frame’s encoding, affecting video quality, frame rate and bandwidth.

In general, moving the slider to the left results in higher quality at the cost of higher bandwidth and, in some cases, lower frame rate.

Moving the slider to the right enables stronger compression, reducing the bandwidth per frame, but video quality is reduced.

In situations where system bandwidth is a limiting factor, moving the video mode slider to the right can result in higher frame rates.

When Text Readability is selected as the Optimized setting, the four rightmost modes provide reduced color resolution or no color at all.

These modes are appropriate for administration work where text and GUI elements take priority, and bandwidth is at a premium.

Click Reset on the Connection Properties dialog at any time to return to the default settings.
Chapter 5: KVM Clients

Noise Filter

Unless there is a specific need to do so, do not change the noise filter setting. The default setting is designed to work well in most situations.

The Noise Filter controls how much interframe noise is absorbed by the ThinkSystem Digital KVM Switch.

Moving the Noise Filter slider to the left lowers the filter threshold, resulting in higher dynamic video quality. However, more noise is likely to come through, resulting in higher bandwidth and lower frame rates.

Moving the slider to the right raises the threshold, allows less noise and less bandwidth is used. Video artifacts may be increased.

Moving the noise filter to the right may be useful when accessing a computer GUI over severely bandwidth-limited connections.

Click Reset on the Connection Properties dialog at any time to return to the default settings.
Connection Information
Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See Configuring Connection Properties (on page 43)

- Current connection information:
  - Name of the ThinkSystem Digital KVM Switch
  - IP address of the ThinkSystem Digital KVM Switch
  - Port - The KVM communication TCP/IP port used to access ThinkSystem Digital KVM Switch.
  - Data In/Second - Data rate received from the ThinkSystem Digital KVM Switch
  - Data Out/Second - Data rate sent to the ThinkSystem Digital KVM Switch.
  - Connect Time - The duration of the current connection.
  - FPS - Video frames per second transmitted received from the ThinkSystem Digital KVM Switch.
  - Horizontal Resolution - The target server horizontal resolution.
  - Vertical Resolution - The target server vertical resolution.
  - Refresh Rate - Refresh rate of the target server.
  - Protocol Version - Communications protocol version.

Access and Copy Connection Information
Steps

1. Click Connection > Info... to open the Connection Info dialog.
2. Click Copy to Clipboard. Paste the information as needed.

USB Profiles

Select a USB profile that best applies to the KVM target server. For example, if the server is running Windows® operating system, it would be best to use the Generic profile.

Or, to change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

- **To set a USB profile for a target server:**
  - Choose USB Profile, then choose Generic, or choose Other Profiles to select from a menu.

- **To view details on USB profiles:**
  - Choose USB Profile > Help on USB Profiles.
Keyboard

Send Ctrl+Alt+Del Macro
Due to its frequent use, a Ctrl+Alt+Delete macro is preprogrammed. Selecting Keyboard > Send Ctrl+Alt+Del, or clicking on the Ctrl+Alt+Delete button in the toolbar sends this key sequence to the server or to the KVM switch to which you are currently connected. In contrast, if you were to physically press the Ctrl+Alt+Del keys, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Send LeftAlt+Tab (Switch Between Open Windows on a Target Server)
Select Keyboard > Send LeftAlt + Tab to switch between open windows on the target server or KVM switch you are connected to.

Send Text to Target

To use the Send Text to Target function for the macro:
1. Click the Keyboard > Send Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target.
   
   Note: Non-English characters are not supported by the Send Text to Target function.
3. If the target uses a US/International keyboard layout, select the “Target system is set to the US/International keyboard layout” checkbox.
4. Click OK.

Keyboard Macros
Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by your client PC.

Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.
Build a New Macro

▲ To build a macro:

1. Click Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Click Add. The Add Keyboard Macro dialog appears.
3. Type a name for the macro in the Keyboard Macro Name field. This name appears in the Keyboard menu after it is created.
4. From the Hot-Key Combination field, select a keyboard combination from the drop-down list. This allows you to execute the macro with a predefined keystroke. Optional
5. In the Keys to Press drop-down list, select each key you would like to use to emulate the keystrokes that is used to perform the command. Select the keys in the order by which they are to be pressed. After each selection, select Add Key. As each key is selected, it appears in the Macro Sequence field and a Release Key command is automatically added after each selection.
   
   For example, create a macro to close a window by selecting Left Ctrl + Esc. This appears in the Macro Sequence box as follows:
   
   Press Left Alt
   Press F4
   Esc
   Release F4
   Esc
   Release Left Alt
6. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
   a. To remove a step in the sequence, select it and click Remove.
   b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.
7. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.
8. Click Close to close the Keyboard Macros dialog. The macro now appears on the Keyboard menu in the application.
9. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.
Importing and Exporting Macros

Macros created in VKC cannot be used in AKC or vice versa. Macros created on HKC are only compatible with HKC, and cannot be used on AKC or VKC. Likewise, macros created on VKC or AKC cannot be used on HKC.

Import Macros

To import macros:
1. Choose Keyboard > Import Keyboard Macros to open the Import Macros dialog. Browse to the folder location of the macro file.
2. Click on the macro file and click Open to import the macro.
   a. If too many macros are found in the file, an error message is displayed and the import terminates once OK is selected.
   b. If the import fails, an error dialog appears and a message regarding why the import failed is displayed. Select OK to continue the import without importing the macros that cannot be imported.
3. Select the macros to be imported by checking their corresponding checkbox or using the Select All or Deselect All options.
4. Click OK to begin the import.
   a. If a duplicate macro is found, the Import Macros dialog appears. Do one of the following:
Chapter 5: KVM Clients

- Click Yes to replace the existing macro with the imported version.
- Click Yes to All to replace the currently selected and any other duplicate macros that are found.
- Click No to keep the original macro and proceed to the next macro.
- Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are skipped as well.
- Click Cancel to stop the import.
- Alternatively, click Rename to rename the macro and import it. If Rename is selected, the Rename Macro dialog appears. Enter a new name for the macro in the field and click OK. The dialog closes and the process proceeds. If the name that is entered is a duplicate of a macro, an alert appears and you are required to enter another name for the macro.

b. If during the import process the number of allowed, imported macros is exceeded, a dialog appears. Click OK to attempt to continue importing macros or click Cancel to stop the import process.

The macros are then imported. If a macro is imported that contains a hot key that already exists, the hot key for the imported macro is discarded.

Export Macros

1. Choose Tools > Export Macros to open the Select Keyboard Macros to Export dialog.

2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.

3. Click Ok. An “Export Keyboard Macros to” dialog is displayed. Locate and select the macro file. By default, the macro exists on your desktop.
4. Select the folder to save the macro file to, enter a name for the file and click Save. If the macro already exists, you receive an alert message.
5. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.

### Video Properties

#### Refreshing the Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:
- The Refresh Screen command forces a refresh of the video screen.
- The Auto-sense Video Settings command automatically detects the target server’s video settings.
- The Calibrate Color command calibrates the video to enhance the colors being displayed.

In addition, you can manually adjust the settings using the Video Settings command.

> **To refresh the video settings, do one of the following:**
> - Choose Video > Refresh Screen, or click the Refresh Screen button in the toolbar.

#### Auto-Sense Video Settings

The Auto-sense Video Settings command forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.

> **To automatically detect the video settings:**
> - Choose Video > Auto-sense Video Settings, or click the Auto-Sense Video Settings button in the toolbar.
>
A message stating that the auto adjustment is in progress appears.
Calibrating Color

Use the Calibrate Color command to optimize the color levels (hue, brightness, saturation) of the transmitted video images.

The color settings are on a target server-basis.

Note: When color is successfully calibrated, the values are cached and reused each time you switch to the target. Changes to the brightness and contrast in Video Settings are not cached. Changing resolution resets the video to the cached values again. You can clear the cached values in Video > Clear Video Settings Cache. See Clear Video Settings Cache (on page 54).

To calibrate the color:

- Choose Video > Calibrate Color, or click the Calibrate Color button in the toolbar.

  The target device screen updates its color calibration.

Clear Video Settings Cache

You can clear the video settings cache to delete old settings that do not apply anymore, such as when a target server is replaced. When you clear the video settings cache, the server automatically does a video auto-sense and color calibration. The new values are cached and reused when the target is accessed again.

To clear the video settings cache:

- Choose Video > Clear Video Settings Cache in the toolbar.

Adjusting Video Settings

Use the Video Settings command to manually adjust the video settings.

To change the video settings:

1. Choose Video > Video Settings to open the Video Settings dialog.
2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:
   a. PLL Settings
      
      Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances, this setting should not be changed because the autodetect is usually quite accurate.
Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

b. Brightness: Use this setting to adjust the brightness of the target server display.

c. Brightness Red - Controls the brightness of the target server display for the red signal.

d. Brightness Green - Controls the brightness of the green signal.

e. Brightness Blue - Controls the brightness of the blue signal.

f. Contrast Red - Controls the red signal contrast.

g. Contrast Green - Controls the green signal.

h. Contrast Blue - Controls the blue signal.

If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

**Warning:** Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Technical Support before making any changes.

i. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.

j. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.

3. Select Automatic Color Calibration to enable this feature.

4. Select the video sensing mode.
   - Best possible video mode
     The device will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
   - Quick sense video mode
     With this option, the device will use a quick video Auto Sense in order to show the target’s video sooner. This option is especially useful for entering a target server’s BIOS configuration right after a reboot.

5. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.
Note: Some Sun background screens, such as screens with very dark borders, may not center precisely on certain Sun servers. Use a different background or place a lighter colored icon in the upper left corner of the screen.

Screenshot from Target Command (Target Screenshot)

Take a screenshot of a target server using the Screenshot from Target server command. If needed, save this screenshot to a file location of your choosing as a bitmap, JPEG or PNG file.

To take a screenshot of the target server:
1. Select Video > Screenshot from Target, or click the Target Screenshot button on the toolbar.
2. In the Save dialog, choose the location to save the file, name the file, and select a file format from the 'Files of type' drop-down.
3. Click Save to save the screenshot.
Mouse Options

You can operate in either single mouse mode or dual mouse mode.

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

When controlling a target server, the Remote Console displays two mouse cursors - one belonging to your ThinkSystem Digital KVM Switch client workstation, and the other belonging to the target server.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

On fast LAN connections, you can use single mouse mode, and view only the target server’s pointer.

You can toggle between these two modes (single mouse and dual mouse).
Chapter 5: KVM Clients

**Dual Mouse Modes**

**Absolute Mouse Synchronization**

In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed.

This mode is supported on servers with USB ports and is the default mode for virtual media CIMs.

Requires the use of a virtual media CIM -
- ThinkSystem S-USB cable for Digital KVM: SC17A30053
- ThinkSystem D-USB cable for Digital KVM: SC17A30049

**To enter Absolute Mouse Synchronization:**
- Choose Mouse > Absolute from the KVM client.

Use the black USB connector on the CIM for the keyboard and mouse.
Use the gray connector for virtual media.
Keep both USB plugs of the CIM connected to the device.
The device may not operate properly if both plugs are not connected to the target server.

**Intelligent Mouse Mode**

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

**Enter Intelligent Mouse Mode**

**To enter intelligent mouse mode:**
- Choose Mouse > Intelligent.
Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as “Enhanced pointer precision” or “Snap mouse to default button in dialogs” should be disabled.
- Choose “Best Possible Video Mode” in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.
**Standard Mouse Mode**

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target server.

In order for the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

► To enter Standard Mouse mode:
  - Choose Mouse > Standard.

**Mouse Synchronization Tips**

If you have an issue with mouse synchronization:

1. Verify that the selected video resolution and refresh rate are among those supported by the device. The KVM Client Connection Info dialog displays the actual values that the device is seeing.
2. Force an auto-sense by clicking the KVM Client auto-sense button.
3. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
   a. Open a terminal window.
   b. Enter the following command: `xset mouse 1 1`
   c. Close the terminal window.
4. Click the “KVM Client mouse synchronization” button.

**Synchronize Your Mouse**

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse cursor with the client mouse cursor.

► To synchronize the mouse cursors, do one of the following:
  - Click the Synchronize Mouse button in the KVM client toolbar, or select Mouse > Synchronize Mouse from the menu bar.

*Note: This option is available only in Standard and Intelligent mouse modes.*
**Single Mouse Mode**

Single Mouse mode uses only the target server mouse cursor; the client mouse cursor no longer appears onscreen.

*Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine.*

- **To enter single mouse mode, do one the following:**
  - Choose Mouse > Single Mouse Cursor.
  - Click the Single/Double Mouse Cursor button in the toolbar.

- **To exit single mouse mode:**
  1. Press Ctrl+Alt+O on your keyboard to exit single mouse mode.

**Tool Options**

**General Settings**

- **To set the tools options:**
  1. Click Tools > Options. The Options dialog appears.
  2. Select the Enable Logging checkbox only if directed to by Technical Support.
     This option creates a log file in your home directory.
  3. Choose the Keyboard Type from the drop-down list (if necessary).

The options include:
- US/International
- French (France)
- German (Germany)
- Japanese
- United Kingdom
Chapter 5: KVM Clients

- Korean (Korea)
- French (Belgium)
- Norwegian (Norway)
- Portuguese (Portugal)
- Danish (Denmark)
- Swedish (Sweden)
- German (Switzerland)
- Hungarian (Hungary)
- Spanish (Spain)
- Italian (Italy)
- Slovenian
- Translation: French - US
- Translation: French - US International

In AKC, the keyboard type defaults to the local client, so this option does not apply.

4. Configure hotkeys:
   - Exit Full Screen Mode - Hotkey.
     When you enter Full Screen mode, the display of the target server becomes full screen and acquires the same resolution as the target server.
     This is the hot key used for exiting this mode.
   - Exit Single Cursor Mode - Hotkey.
     When you enter single cursor mode, only the target server mouse cursor is visible.
     This is the hot key used to exit single cursor mode and bring back the client mouse cursor.
   - Disconnect from Target - Hotkey.
     Enable this hotkey to allow users to quickly disconnect from the target.

For hotkey combinations, the application does not allow you to assign the same hotkey combination to more than one function.

For example, if Q is already applied to the Disconnect from Target function, it won’t be available for the Exit Full Screen Mode function.

Further, if a hotkey is added to the application due to an upgrade and the default value for the key is already in use, the next available value is applied to the function instead.
5. Click OK.

**Keyboard Limitations**

**Turkish Keyboards**
Turkish keyboards are only supported on Active KVM Client (AKC).

**Slovenian Keyboards**
The `<` key does not work on Slovenian keyboards due to a JRE limitation.

**Language Configuration on Linux**
Because the Sun JRE on Linux has problems generating the correct Key Events for foreign-language keyboards configured using System Preferences, configure foreign keyboards using the methods described in the following table.

<table>
<thead>
<tr>
<th>Language</th>
<th>Configuration method</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Intl</td>
<td>Default</td>
</tr>
<tr>
<td>French</td>
<td>Keyboard Indicator</td>
</tr>
<tr>
<td>German</td>
<td>System Settings (Control Center)</td>
</tr>
<tr>
<td>Japanese</td>
<td>System Settings (Control Center)</td>
</tr>
<tr>
<td>UK</td>
<td>System Settings (Control Center)</td>
</tr>
<tr>
<td>Korean</td>
<td>System Settings (Control Center)</td>
</tr>
<tr>
<td>Belgian</td>
<td>Keyboard Indicator</td>
</tr>
</tbody>
</table>
Chapter 5: KVM Clients

<table>
<thead>
<tr>
<th>Language</th>
<th>Configuration method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norwegian</td>
<td>Keyboard Indicator</td>
</tr>
<tr>
<td>Danish</td>
<td>Keyboard Indicator</td>
</tr>
<tr>
<td>Swedish</td>
<td>Keyboard Indicator</td>
</tr>
<tr>
<td>Hungarian</td>
<td>System Settings [Control Center]</td>
</tr>
<tr>
<td>Spanish</td>
<td>System Settings [Control Center]</td>
</tr>
<tr>
<td>Italian</td>
<td>System Settings [Control Center]</td>
</tr>
<tr>
<td>Slovenian</td>
<td>System Settings [Control Center]</td>
</tr>
<tr>
<td>Portuguese</td>
<td>System Settings [Control Center]</td>
</tr>
</tbody>
</table>

*Note: The Keyboard Indicator should be used on Linux systems using Gnome as a desktop environment.*

**Client Launch Settings**

Configuring client launch settings allows you to define the screen settings for a KVM session.

- **To configure client launch settings:**
  1. Click Tools > Options. The Options dialog appears.
  2. Click on the Client Launch Settings tab.
     - To configure the target window settings:
       a. Select ‘Standard - sized to target Resolution’ to open the window using the target’s current resolution. If the target resolution is greater than the client resolution, the target window covers as much screen area as possible and scroll bars are added (if needed).
       b. Select ‘Full Screen’ to open the target window in full screen mode.
     - To configure the monitor on which the target viewer is launched:
       a. Select ‘Monitor Client Was Launched From’ if you want the target viewer to be launched using the same display as the application that is being used on the client (for example, a web browser or applet).
       b. Use ‘Select From Detected Monitors’ to select from a list of monitors that are currently detected by the application. If a previously selected monitor is no longer detected, ‘Currently Selected Monitor Not Detected’ is displayed.
     - To configure additional launch settings:
Chapter 5: KVM Clients

a. Select 'Enable Single Cursor Mode' to enable single mouse mode as the default mouse mode when the server is accessed.

b. Select 'Enable Scale Video' to automatically scale the display on the target server when it is accessed.

c. Select 'Pin Menu Toolbar' if you want the toolbar to remain visible on the target when it is in Full Screen mode. By default, while the target is in Full Screen mode, the menu is only visible when you hover your mouse along the top of the screen.

d. Always Show Tool Bar and Always Show Status Bar are per-user settings that are stored in the computer you are accessing the client from, so if you use a different computer, the setting may be different. Select to keep tool bar and status bar visible as default, deselect to keep tool bar and status bar hidden as default.

3. Click OK.
Configuring Port Scan Settings in VKC/VKCS and AKC

Configuring port scan options in VKC/VKCS and AKC applies to scanning from the Remote Console.

To configure port scan options for the Local Console, see Configure Local Console Scan Settings (on page 127)

Use the port scanning feature to search for selected targets, and display them in a slide show view, allowing you to monitor up to 32 targets at one time.

You can connect to targets or focus on a specific target as needed. Scans can include standard targets, blade servers, tiered devices, and KVM switch ports.

Configure scan settings from either the VKC/VKCS or AKC.

See Scanning Ports - Remote Console (on page 116)

Use the Scan Settings tab to customize the scan interval and default display options.

Configure Port Scan

To set scan settings:

1. Click Tools > Options. The Options dialog appears.
2. Select the Scan Settings tab.
3. In the "Display Interval (10-255 sec):" field, specify the number of seconds you want the target that is in focus to display in the center of the Port Scan window.
4. In the "Interval Between Ports (10 - 255 sec):" field, specify the interval at which the device should pause between ports.
5. In the Display section, change the default display options for the thumbnail size and split orientation of the Port Scan window.
6. Click OK.

![Options dialog box](image.png)

**Collecting a Diagnostic Snapshot of the Target**

Administrators are able to collect a “snapshot” of a target from either the VKC/VKCS or Active KVM Client (AKC).

The “snapshot” function generates log files and image files from the target.

It then bundles these files in a zip file that can be sent to Technical Support in order to help diagnose technical problems you may be encountering.

The following files are included in the zip file:

- **screenshot_image.png**
  This is a screenshot of the target that captures a picture of the issue you are experiencing. This feature operates in the same as the “Screenshot from Target” feature.

- **raw_video_image.png**
  A snapshot image created from raw video data. Please note that client’s postprocessing is applied, just as if it were a “regular” screen update.

- **raw_video_ycbcr420.bin**
  Binary file of the raw snapshot.

- **raw_video_ycbcr420.txt**
  Text file containing data used to help diagnose issues.
• Log.txt file:
  These are the client logs.
  Note that the logs are included even if you have not enabled
  information to be captured in them. VKC uses internal memory to
  capture the information in this case.

*Collect a Diagnostic Snapshot from VKC, VKCS, and AKC*
To capture a diagnostic snapshot:

**Steps**

1. Access a target, and then click Tools > Collect a Diagnostic Snapshot. Several messages are displayed as the information is collected.

2. You are prompted to save the zip file containing the diagnostic files.

3. The zip file containing the diagnostic files that were collecting opens.
View Options

View Toolbar
You can use the Virtual KVM client with or without the toolbar display.

► **To toggle the display of the toolbar (on and off):**
  • Choose View > View Toolbar.

View Status Bar
By default, the status bar is displayed at the bottom of the target window.

► **To hide the status bar:**
  • Click View > Status Bar to deselect it.

► **To restore the status bar:**
  • Click View > Status Bar to select it.

Scaling
Scaling your target window allows you to view the entire contents of the target server window.
This feature increases or reduces the size of the target video to fit the Virtual KVM Client window size, and maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

► **To toggle scaling (on and off):**
  • Choose View > Scaling.
Chapter 5: KVM Clients

**Full Screen Mode**

When you enter Full Screen mode, the target's full screen is displayed and acquires the same resolution as the target server.

The hot key used for exiting this mode is specified in the Options dialog, see *Tool Options* [on page 61].

While in Full Screen mode, moving your mouse to the top of the screen displays the Full Screen mode menu bar.

If you want the menu bar to remain visible while in Full Screen mode, enable the Pin Menu Toolbar option from the Tool Options dialog. See *Tool Options* [on page 61].

▶ **To enter full screen mode:**

- Choose View > Full Screen, or click the Full Screen button.

▶ **To exit full screen mode:**

- Press the hot key configured in the Tool's Options dialog. The default is Ctrl+Alt+M.

If you want to access the target in full screen mode at all times, you can make Full Screen mode the default.

▶ **To set Full Screen mode as the default mode:**

1. Click Tools > Options to open the Options dialog.
2. Select Enable Launch in Full Screen Mode and click OK.

---

**Connect to Virtual Media**

See *Virtual Media* [on page 26]
Smart Cards

Using the ThinkSystem Digital KVM Switch, you are able to mount a smart card reader onto a target server to support smart card authentication and related applications.

For a list of supported smart cards, smart card readers, and additional system requirements, see **Smart Card Minimum System Requirements, CIMs and Supported/Unsupported Smart Card Readers** [on page 72].

**Note:** The USB Smart Card token (eToken NG-OTP) is only supported from the remote client.

Smart card reader mounting is also supported from the Local Console. See **Local Console Smart Card Access** [on page 128].

Smart Card Minimum System Requirements, CIMs and Supported/Unsupported Smart Card Readers

Before you begin using a smart card reader, review the following:

- **Smart Card Minimum System Requirements** [on page 145]
- Supported Computer Interface Module (CIMs) Specifications
- Supported and Unsupported Smart Card Readers

Authentication When Accessing a Smart Card Reader

When accessing a server remotely, you can select an attached smart card reader and mount it onto the server.

Smart card authentication is used with the target server, it is not used to log into the device. Therefore, changes to smart card PIN and credentials do not require updates to device accounts.

PC Share Mode and Privacy Settings when Using Smart Cards

When PC-Share mode is enabled on the device, multiple users can share access to a target server.

However, when a smart card reader is connected to a target, the device will enforce privacy regardless of the PC-Share mode setting.

In addition, if you join a shared session on a target server, the smart card reader mounting will be disabled until exclusive access to the target server becomes available.
Smart Card Reader Detected

After a KVM session is established with a target server, a Smart Card menu and button are available in VKC and AKC.

Once the Smart Card button is selected or Smart Card is selected from the menu, the smart card readers that are detected as attached to the remote client are displayed in a dialog.

From this dialog, you can attach additional smart card readers, refresh the list of smart card readers attached to the target, and detach smart card readers.

You are also able to remove or reinsert a smart card. This function can be used to provide notification to a target server OS that requires a removal/reinsertion in order to display the appropriate login dialog. Using this function allows the notification to be sent to a single target without affecting other active KVM sessions.

Mount a Smart Card Reader

When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached.

Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS.

When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

To mount a smart card reader from VKC or AKC:
1. Click the Smart Card menu and then select Smart Card Reader. Alternatively, click the Smart Card button in the toolbar.
2. Select the smart card reader from the Select Smart Card Reader dialog.
3. Click Mount.
4. A progress dialog will open. Check the ‘Mount selected card reader automatically on connection to targets’ checkbox to mount the smart card reader automatically the next time you connect to a target. Click OK to begin the mounting process.
Update a Smart Card Reader

▶ To update the smart card in the Select Smart Card Reader dialog:
  • Click Refresh List if a new smart card reader has been attached to the client PC.

Send Smart Card Remove and Reinsert Notifications

▶ To send smart card remove and reinsert notifications to the target:
  • Select the smart card reader that is currently mounted and click the Remove/Reinsert button.

Unmount (Remove) a Smart Card Reader

▶ To unmount a smart card reader:
  • Select the smart card reader to be unmounted and click the Unmount button.

Digital Audio

The ThinkSystem Digital KVM Switch supports end-to-end, bidirectional, digital audio connections for digital audio playback and capture devices from a remote client to a target server.

The audio devices are accessed over a USB connection.

Current device firmware is required.

One of the following CIMs must be used:

- ThinkSystem S-USB cable for Digital KVM: SC17A30053
- ThinkSystem D-USB cable for Digital KVM: SC17A30049

Windows®, Linux®, and Mac® operating systems are supported. VKC, VKCS, and AKC support connections to audio devices.

*Note: Audio CDs are not supported by virtual media so they do not work with the audio feature.*

Before you begin using the audio feature, review the audio related information documented in the following sections:

- **Supported Audio Device Formats** [on page 75]
- Recommendations for Dual Port Video
- Dual Video Port Group Supported Mouse Modes
- CIMs Required for Dual Video Support
- Informational Notes, Audio
Supported Audio Device Formats

The ThinkSystem Digital KVM Switch supports one playback and capture device and one record device on a target at a time. The following audio device formats are supported:

- Stereo, 16 bit, 44.1K
- Mono, 16 bit, 44.1K
- Stereo, 16 bit, 22.05K
- Mono, 16 bit, 22.05K
- Stereo, 16 bit, 11.025K
- Mono, 16 bit, 11.025K

Digital Audio VKC and AKC Icons

<table>
<thead>
<tr>
<th>Audio icons</th>
<th>Icon name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Speaker Icon" /></td>
<td>Speaker</td>
<td>These icons are located in status bar at the bottom of the client window. Green, blinking waves indicate an audio playback session is currently streaming. A black speaker icon is displayed when the session is muted. The icon is grayed out when no audio is connected.</td>
</tr>
<tr>
<td><img src="image" alt="Microphone Icon" /></td>
<td>Microphone</td>
<td>These icons are located in the status bar at the bottom of the client window. Red, blinking waves indicate an audio capture session is currently underway. The Speaker icon, indicating a playback session is streaming, is also displayed when a session is underway. A black Microphone icon is displayed when the session is muted. When the Microphone icon is grayed out, no audio is connected.</td>
</tr>
</tbody>
</table>
Audio Playback and Capture Recommendations and Requirements

Audio Level
- Set the target audio level to a mid-range setting.
  
  For example, on a Windows® client, set the audio to 50 or lower.

This setting must be configured through the playback or capture audio device, not from the client audio device control.

Recommendations for Audio Connections when PC Share Mode is Enabled

If you are using the audio feature while running PC Share mode, audio playback and capture are interrupted if an additional audio device is connected to the target.

For example, User A connects a playback device to Target1 and runs an audio playback application then User B connects a capture device to the same target. User A’s playback session is interrupted and the audio application may need to be restarted.

The interruption occurs because the USB device needs to be re-enumerated with the new device configuration.

It may take some time for the target to install a driver for the new device.

Audio applications may stop playback completely, go to the next track, or just continue playing.

The exact behavior is dependent on how the audio application is designed to handle a disconnect/reconnect event.

Bandwidth Requirements

The table below details the audio playback and capture bandwidth requirements to transport audio under each of the selected formats.

<table>
<thead>
<tr>
<th>Audio format</th>
<th>Network bandwidth requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.1 KHz, 16bit stereo</td>
<td>176 KB/s</td>
</tr>
<tr>
<td>44.1 KHz, 16bit mono</td>
<td>88.2 KB/s</td>
</tr>
<tr>
<td>2.05 KHz, 16bit stereo</td>
<td>88.2 KB/s</td>
</tr>
<tr>
<td>22.05 KHz, 16bit mono</td>
<td>44.1 KB/s</td>
</tr>
<tr>
<td>11.025 KHz, 16bit stereo</td>
<td>44.1 KB/s</td>
</tr>
<tr>
<td>11.025 KHz, 16bit mono</td>
<td>Audio 22.05 KB/s</td>
</tr>
</tbody>
</table>
In practice, the bandwidth used when an audio device connects to a target is higher due to the keyboard and video data consumed when opening and using an audio application on the target.

A general recommendation is to have at least a 1.5MB connection before running playback and capture.

However, high video-content, full-color connections using high-target screen resolutions consume much more bandwidth and impact the quality of the audio considerably.

To help mitigate quality degeneration, there are a number of recommended client settings that reduce the impact of video on audio quality at lower bandwidths:

- Connect audio playback at the lower quality formats. The impact of video consuming bandwidth is much less notable at 11k connections than at 44k.
- Set the connection speed under Connection Properties to a value that best matches the client to server connection.
- Under Connection Properties, set the color depth to as low a value as possible. Reducing the color depth to 8 bit color considerably reduces the bandwidth consumed.
- Set Smoothing to High. This will improve the appearance of the target video by reducing displayed video noise.
- Under Video settings, set the Noise Filter to its highest setting of 7 (highest value) so less bandwidth is used for target screen changes.
**Saving Audio Settings**

Audio device settings are applied on a per ThinkSystem Digital KVM Switch device basis.

Once the audio devices settings are configured and saved on the ThinkSystem Digital KVM Switch, the same settings are applied to it.

For example, you can configure a Windows® audio device to use a stereo, 16 bit, 44.1K format.

When you connect to different targets and use that Windows audio device, the stereo, 16 bit, 44.1K format is applied to each target server.

For both playback and recording devices, the device type, device format, and the buffer settings applied to the device are saved.

See **Connecting and Disconnecting from a Digital Audio Device** [on page 79] for information on connecting to and configuring an audio device, and **Adjusting Capture and Playback Buffer Size (Audio Settings)** for information on audio device buffer settings.

If you are using the audio feature while running PC Share mode and VM Share mode so multiple users can access the same audio device on a target at once, the audio device settings of the user who initiates the session are applied to all users who join the session.

So, when a user joins an audio session, the target machine settings are used. See **Connecting to Multiple Targets from a Single Remote Client** [on page 78].

**Connecting to Multiple Targets from a Single Remote Client**

Connect to audio on up to four (4) target servers at the same time from a single, remote client.

See **Connecting and Disconnecting from a Digital Audio Device** [on page 79] for information on connecting to audio devices.

A Speaker icon is displayed in the status bar at the bottom of the client window. It is grayed out when no audio is being used. When the Speaker icon and Microphone icon are displayed in the status bar, the session is being captured as it is streamed.

*Note: When an audio session is underway, be sure to keep the session active or change the ThinkSystem Digital KVM Switch’s idle timeout time so the audio session does not time out.*
Operating System Audio Playback Support

Review the table shown here to see which client works with audio playback/capture for each operating system:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Audio playback and capture supported by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows®</td>
<td>• Active KVM Client (AKC)</td>
</tr>
<tr>
<td></td>
<td>• Virtual KVM Client (VKC)</td>
</tr>
<tr>
<td>Linux®</td>
<td>• Virtual KVM Client (VKC)</td>
</tr>
<tr>
<td>Mac®</td>
<td>• Virtual KVM Client (VKC)</td>
</tr>
</tbody>
</table>

Connecting and Disconnecting from a Digital Audio Device

Audio device settings are applied on a per ThinkSystem Digital KVM Switch device basis.

Once the audio devices settings are configured and saved on the ThinkSystem Digital KVM Switch, the same settings are applied to it.

See Saving Audio Settings (on page 78) for more information.

Note: If you are using the audio feature while running PC Share mode and VM Share mode, see Audio Playback and Capture Recommendations and Requirements (on page 76) for important information. See also Connecting to Multiple Targets from a Single Remote Client (on page 78).

Connect to a Digital Audio Device

1. Connect the audio device to the remote client PC prior to launching the browser connection to the ThinkSystem Digital KVM Switch.
2. Connect to the target from the Port Access page.
3. Once connected, click the Audio button in the toolbar.
   The Connect Audio Device dialog appears. A list of available audio devices connected to the remote client PC is displayed.
   Note: If there are no available audio devices connected to the remote client PC, the Audio icon is grayed out.
4. Check Connect Playback Device if you are connecting to a playback device.
5. Select the device that you wish to connect from the drop-down list.
6. Select the audio format for the playback device from the Format: drop-down.

   *Note: Select the format that you wish to use based on the available network bandwidth. Formats with lower sampling rates consume less bandwidth and may tolerate more network congestion.*

7. Select the “Mount selected playback device automatically on connection to target” checkbox to automatically connect an audio playback device when you connect to an audio supporting target.

8. Check Connect Recording Device if you are connecting a recording device.

   *Note: The device names listed in the Connect Recording Device drop-down are truncated to a maximum of 30 characters for Java clients.*

9. Select the device that you wish to connect from the drop-down list.

10. Select the audio format for the recording device from the Format: drop-down.

11. Click OK. If the audio connection is established, a confirmation message appears. Click OK.

    If the connection was not established, an error message appears.

    Once an audio connection is established, the Audio menu changes to Disconnect Audio. The settings for the audio device are saved and applied to subsequent connections to the audio device.

    A Speaker icon 🎧 is displayed in the status bar at the bottom of the client window. It is grayed out when no audio is being used. When the Speaker icon and Microphone icon 🎤 are displayed in the status bar, the session is being captured as it is streamed.

**Disconnect from an Audio Device**

- **To disconnect from the audio device:**
  - Click the Audio icon 🎧 in the toolbar and select OK when you are prompted to confirm the disconnect. A confirmation message appears. Click OK.
Adjusting Capture and Playback Buffer Size [Audio Settings]

Once an audio device is connected, the capture and playback buffer size can be adjusted as needed.

This feature is useful for controlling the quality of the audio, which may be impacted by bandwidth limitations or network spikes.

Increasing the buffer size improves the audio quality but may impact the delivery speed.

The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

The buffer size can be adjusted whenever needed, including during an audio session.

Audio settings are configured in VKC or AKC.

Adjust Audio Settings

► To adjust audio settings:
1. Select Audio Settings from the Audio menu. The Audio Settings dialog opens.
2. Adjust the capture and/or playback buffer size as needed. Click OK.

Active KVM Client (AKC) Help

Recommended Minimum Active KVM Client (AKC) Requirements

It is recommended that the Active KVM Client (AKC) machines meet the following minimum requirements.

- Client machine with either a -
  - ‘modern’ dual-core CPU for a single connections, or
  - ‘modern’ quad core CPU for two or more simultaneous connections
- 4GB of RAM
**AKC Supported Microsoft .NET Framework**
The Active KVM Client (AKC) requires Windows .NET® version 4.0 or 4.5.

**AKC Supported Operating Systems**
When launched from Internet Explorer®, the Active KVM Client (AKC) allows you to reach target servers via the ThinkSystem Digital KVM Switch.

AKC is compatible with the following platforms:
- Windows XP® operating system
- Windows Vista® operating system [up to 64 bit]
- Windows 7® operating system [up to 64 bit]
- Windows 8® operating system [up to 64 bit]
- Windows 10 ® operating system [up to 64 bit]

*Note: You must be using Windows 7 if WINDOWS PC FIPs is turned on and you are accessing a target using AKC and a smartcard.*

Since .NET is required to run AKC, if you do not have .NET installed or you have an unsupported version of .NET installed, you will receive a message instructing you to check the .NET version.

*Note: Windows XP® operating system users should verify a working version of .NET 4.0 or 4.5 already installed before you launch AKC. If you do not verify your .NET version is working, you may be prompted to download a file versus receiving the default message to check your .NET version.*

**AKC Supported Browsers**
- Internet Explorer® 10 (and later)
- Chrome on Windows platforms. You must have the Chrome ClickOnce plugin installed.

**Prerequisites for Using AKC**

**Allow Cookies**
Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.
Include ThinkSystem Digital KVM Switch IP Address in ‘Trusted Sites Zone’

Windows Vista®, Windows® 7 and Windows 2008 server users should ensure that the IP address of the device being accessed is included in their browser’s Trusted Sites Zone.

Disable ‘Protected Mode’

Windows Vista®, Windows® 7 and Windows 2008 server users should ensure that Protected Mode is not on when accessing this device.

Enable AKC Download Server Certificate Validation

If the administrator has enabled the Enable AKC Download Server Certificate Validation option:

- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.
- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

Proxy Server Configuration for Use with VKC, VKCS, and AKC

When the use of a Proxy Server is required, a SOCKS proxy must also be provided and configured on the remote client PC.

Note: If the installed proxy server is only capable of the HTTP proxy protocol, you cannot connect.

To configure the SOCKS proxy:
1. On the remote client PC, select Control Panel > Internet Options.
   b. Select ‘Use a proxy server for your LAN’.
   c. Click Advanced. The Proxy Settings dialog opens.
   d. Configure the proxy servers for all protocols.
   IMPORTANT: Do not select ‘Use the same proxy server for all protocols’.
   e. Click OK at each dialog to apply the settings.
2. Next, configure the proxy settings for the Java™ applets:
   a. Select Control Panel > Java.

c. Select “Use Proxy Server”.

d. Click Advanced. The Advanced Network Settings dialog opens.

e. Configure the proxy servers for all protocols.

**IMPORTANT:** Do not select ‘Use the same proxy server for all protocols’.

*Note:* The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

---

**Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC)**

Once you have logged on to the ThinkSystem Digital KVM Switch Remote Console, access target servers via the Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC).

- **To connect to an available server:**
  1. On the Port Access page, click on the port name of the target server you want to connect to. The Port Action menu opens.
  2. Click Connect.

See **Port Action Menu** (on page 20) for details on additional available menu options.
HTML KVM Client (HKC) Help

The HTML KVM client (HKC) provides KVM over IP access that runs in the browser without applets or browser plugins. HKC uses Javascript, NOT Java.

HKC runs on Linux and Mac clients, and on Windows clients without .NET in Internet Explorer 11 (not supported in IE 10 or lower), Edge, Firefox, Chrome and Safari browsers. See KVM Client Launching for a full matrix of clients.

Many KVM features are supported. Future releases will provide more advanced KVM features.

- **Supported Features:**
  - Connection Properties
  - USB Profiles
  - Video Settings
  - Input Settings
  - Audio Playback
  - Virtual Media
  - Dual Video Targets on IE, Edge, Firefox and Chrome
  - Keyboard Macros
  - Import and Export of Keyboard Macros
  - Send Text to Target
  - Keyboard and Mouse Settings
  - Single Mouse Mode - not available on IE browser
  - Port Scanning

- **Not supported:**
  - Smartcard
  - Tools Menu for setting Client launch settings
  - Limited keyboard support: US-English, UK-English, French, and German are supported
  - Hotkeys for keyboard macros
  - Pre-populated keyboard macros for Sun targets
  - Can only create Macros from keys that exist on the client PC (US-English, UK-English, French, or German), no special function keys
  - Single Mouse mode - not available on IE
  - Virtual Media r/w not supported
  - Local file transfer supported by Chrome and Firefox browsers only
  - USB drive connects
Chapter 5: KVM Clients

- Favorites
- Audio capture
- Dual video targets not supported on Safari. Use Chrome or Firefox to connect to dual video targets on Mac OS.

▶ Known Issues:
- When Single Mouse Mode in the Edge browser is selected for the first time, the user is prompted to turn off the local mouse pointer. Select the bottom part of the Yes button.
- Target connections from Chrome 61 running on Fedora requires HardWare Acceleration to be enabled.
- If erratic mouse response is seen in Single Mouse mode on Fedora clients using the default Gnome desktop, use the Gnome classic desktop.
- To enable scrollbars on Mac Browser target connections: On the OS menu bar, choose System Preferences > General > Show scroll bars: Always.
- Internet Explorer and Edge support only 6 sessions at a time. The error displayed when attempting to connect to a seventh target is “Error could not connect to target.” For IE11, you can increase the sessions allowed in the Group policy editor. See https://jwebsocket.org/documentation/reference-guide/internet-explorer-tips.
- For IE11 and Edge IPv6 device connections, either use device hostname or literal IPv6 as UNC. See https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names
- For Mac/Safari IPv6 device connections, use device hostname.
- Client Keyboard input selection should be set for each device individually.
- If encountering issues on browsers that have previously connected to an older version, it may be necessary to clear the Cache Web Content from the browser.
- To launch HKC automatically in Safari browser: Use http://<IP Address>/hkc, OR use http://<IP Address>/ if “Java content on browser” is disabled in Java Control Panel, and “Java Plugin” is disabled in the browser.
- From Chrome running on Linux, to get ‘`’ or ‘^’, the key needs to be hit three times, or twice followed by a space.
- For Mac Client browsers, ensure that the device certificate is installed and trusted. The certificate Common name should match the IP address/Hostname used to connect to the device. See SSL Certificates for information on creating and installing certificates.
• On a default build of Redhat 7/Firefox ESR 24.5, there is no target video displayed on HKC connections. Older versions of Firefox lack HTML5 functions needed to support HKC. Upgrade Firefox to the latest available version.

**Connection Properties**

Connection properties manage streaming video performance over remote connections to target servers.

The properties are applied only to your connection - they do not impact the connection of other users accessing the same target servers.

If you make changes to connection properties, they are retained by the client.

➤ **To view connection properties:**
  • Choose File > Connection Properties.

**Default Connection Properties**

The ThinkSystem Digital KVM Switch comes configured to provide optimal performance for the majority of video streaming conditions.

Default connection settings are:

• Optimized for: Text Readability - video modes are designed to maximize text readability.
  
  This setting is ideal for general IT and computer applications, such as performing server administration.

• Video Mode - defaults to Full Color 2.
  
  Video frames transmit in high-quality, 24-bit color. This setting is suitable where a high-speed LAN is used.

• Noise Filter - defaults to 2.
  
  The noise filter setting does not often need to be changed.
Click Reset to regain the default connection properties.

### Connection Properties

![Connection Properties Diagram](image)

**Text Readability**

Text Readability is designed to provide video modes with lower color depth but text remains readable. Greyscale modes are even available when applying lower bandwidth settings.

This setting is ideal when working with computer GUIs, such as server administration.

When working in full color video modes, a slight contrast boost is provided, and text is sharper.

In lower quality video modes, bandwidth is decreased at the expense of accuracy.

**Color Accuracy**

When Color Accuracy is selected, all video modes are rendered in full 24-bit color with more compression artifacts.

This setting applies to viewing video streams such as movies or other broadcast streams.

In lower quality video modes, sharpness of fine detail, such as text, is sacrificed.
Video Mode

The Video Mode slider controls each video frame’s encoding, affecting video quality, frame rate and bandwidth.

In general, moving the slider to the left results in higher quality at the cost of higher bandwidth and, in some cases, lower frame rate. Moving the slider to the right enables stronger compression, reducing the bandwidth per frame, but video quality is reduced.

In situations where system bandwidth is a limiting factor, moving the video mode slider to the right can result in higher frame rates.

When Text Readability is selected as the Optimized setting, the four rightmost modes provide reduced color resolution or no color at all. These modes are appropriate for administration work where text and GUI elements take priority, and bandwidth is at a premium.
Chapter 5: KVM Clients

**Noise Filter**

Unless there is a specific need to do so, do not change the noise filter setting. The default setting is designed to work well in most situations.

The Noise Filter controls how much interframe noise is absorbed by the ThinkSystem Digital KVM Switch.

**Connection Properties**

Moving the Noise Filter slider to the left lowers the filter threshold, resulting in higher dynamic video quality. However, more noise is likely to come through, resulting in higher bandwidth and lower frame rates.

Moving the slider to the right raises the threshold, allows less noise and less bandwidth is used. Video artifacts may be increased.

Moving the noise filter to the right may be useful when accessing a computer GUI over severely bandwidth-limited connections.
Chapter 5: KVM Clients

Connection Info
Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See Connection Properties (see “Default Connection Properties” on page 87) for help configuring the connection properties.

• Name of the ThinkSystem Digital KVM Switch
• IP address of the ThinkSystem Digital KVM Switch
• Port - The KVM communication TCP/IP port used to access ThinkSystem Digital KVM Switch.
• Data In/Second - Data rate received from the ThinkSystem Digital KVM Switch
• Data Out/Second - Data rate sent to the ThinkSystem Digital KVM Switch.
• FPS - Video frames per second from the ThinkSystem Digital KVM Switch.
• Average FPS - Average number of video frames per second.
• Connect Time - The duration of the current connection.
• Horizontal Resolution - The target server horizontal resolution.
• Vertical Resolution - The target server vertical resolution.
• Refresh Rate - Refresh rate of the target server.
• Protocol Version - communications protocol version.

➢ To view connection info:
Choose File > Connection Info.

Connection Info

Device Name: ThinkSystemKVM
IP Address: 192.168.59.106
Port: 443
Data In/Second: 5 kB/s
Data Out/Second: 70 B/s
FPS: 3
Avg. FPS: 1.48
Connect Time: 00:00:25
Horizontal Resolution: 1024
Vertical Resolution: 768
Refresh Rate: 60 Hz
Protocol Version: 1.31

OK
**USB Profile**

Select a USB profile that best applies to the KVM target server.

For example, if the server is running Windows® operating system, it would be best to use the Generic profile.

Or, to change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

- **To set a USB profile for a target server:**
  - Choose USB Profile, then choose Generic, or choose Other Profiles to select from a menu.

- **To view details on USB profiles:**
  Choose USB Profile > Help on USB Profiles.

**Input Menu**

**Keyboard Layout**

- **To set your keyboard type.**
  - Choose Input > Keyboard Layout, then select your keyboard type.
    - de
    - en-gb
    - en-us
    - fr

![Keyboard Layout Image](image-url)
Send Macro

Due to frequent use, several keyboard macros are preprogrammed.

To send a preprogrammed macro:
• Choose Input > Send Macro, then select the macro:
  ▪ Ctrl+Alt+Del: Sends the key sequence to the target without affecting the client.
  ▪ Alt+F4: Closes a window on a target server.
  ▪ Alt+Tab: Switch between open windows on a target server.
  ▪ Print Screen: Take a screenshot of the target server.
Macro Editor

Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by your client PC.

Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one ThinkSystem Digital KVM Switch, your macros will only be available on the browser and ThinkSystem Digital KVM Switch where they were created. To reuse your macros in another ThinkSystem Digital KVM Switch device, you can import and export the macro files. See Import and Export Macros (on page 96).

To access the Macro Editor:

- Choose Inputs > Macro Editor.
- Select a macro from the Macros list to view the key combination.

To add a new macro:

1. Choose Inputs > Macro Editor.
2. Click Add New Macro.
3. Enter a Name for the new macro. The name will appear in the Send Macro menu once the macro is saved.
4. Click Add Key, then press the key you want to add to the macro. The key press and key release appear in the Keys list.
   - To add more keys, click Add Key again, and press another key.
   - To remove a key, select it in the Keys list and click Delete Key.
5. To put the key in the correct sequence, click to select a key in the Keys list, then click the up and down arrows.
6. Click OK to save.

### Delete a Macro

- **To delete a macro:**
  1. Choose Inputs > Macro Editor.
  2. Select the macro, then click Delete Macro.
3. Click OK.

**Import and Export Macros**

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one ThinkSystem Digital KVM Switch, your macros will only be available on the browser and ThinkSystem Digital KVM Switch where they were created. To reuse your macros in another ThinkSystem Digital KVM Switch device, you can import and export the macro files. Imported and exported macro files created on HKC are only compatible with HKC, and cannot be used on AKC or VKC. Likewise, macro files created on AKC or VKC cannot be imported for use on HKC.

Macros are exported to an xml file named “usermacros.xml”. Files are saved in your browser’s default download location. Default macros are not exported.

**To export and import macros:**

1. Choose Input > Macro Editor. The list of macros created for your browser and ThinkSystem Digital KVM Switch displays in the Macro Editor dialog.
2. To export the list, click the Export button, then save the file.
3. Log in to the ThinkSystem Digital KVM Switch where you want to import the macros.
4. Choose Input > Macro Editor.
5. Click Import, then click Open to Import and select the usermacros.xml file, and click OK.

6. The macros found in the file display in the list. Select the macros you want to import, then click OK.
   - Macro names must be unique. If a macro with the same name already exists, an error message appears. Click the Edit icon to rename the macro, then click the checkmark to save the name.

### Send Text to Target

Use the Send Text to Target function to send text directly to the target. If a text editor or command prompt is open and selected on the target, the text is pasted there.

1. Choose Input > Send Text to Target. The Send Text to Target dialog appears.

2. Enter the text you want sent to the target. Supported keyboard characters only.

3. Click OK.
Mouse Modes

You can operate in either single mouse mode or dual mouse mode. When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

When controlling a target server, the Remote Console displays two mouse cursors - one belonging to your ThinkSystem Digital KVM Switch client workstation, and the other belonging to the target server.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

On fast LAN connections, you can use single mouse mode, and view only the target server’s pointer.

You can toggle between these two modes (single mouse and dual mouse).
**Absolute**

In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed.

This mode is supported on servers with USB ports and is the default mode for virtual media CIMs.

Absolute Mouse Synchronization requires the use of a virtual media CIM:

- ThinkSystem S-USB cable for Digital KVM: SC17A30053
- ThinkSystem D-USB cable for Digital KVM: SC17A30049

▶ **To enter Absolute Mouse Synchronization Mode:**
- Choose Input > Mouse Modes > Absolute.

**Intelligent**

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

▶ **To enter Intelligent mouse mode:**
- Choose Input > Mouse Mode > Intelligent. The mouse will synch. See *Intelligent Mouse Synchronization Conditions* (on page 59).
Standard

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target server.

In order for the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

To enter Standard mouse mode:
- Choose Input > Mouse Modes > Standard.

Single

Single Mouse mode uses only the target server mouse cursor; the client mouse cursor no longer appears onscreen.

Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine.

To enter Single mouse mode:
- Choose Inputs > Mouse Modes > Single.
- A message appears at the top of the client window: Press Esc to show your cursor.
To exit Single mouse mode:

- Press Esc.
- Mouse mode changes back to dual mode.

Mouse Sync

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse cursor with the client mouse cursor.

Note: This option is available only in Standard and Intelligent mouse modes.

To synchronize the mouse cursors:

- Choose Inputs > Mouse Sync.
Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as “Enhanced pointer precision” or “Snap mouse to default button in dialogs” should be disabled.
- Choose “Best Possible Video Mode” in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.
Video Menu

Refresh Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

- The Refresh Screen command forces a refresh of the video screen.
- The Auto-Sense command automatically detects the target server’s video settings.
- The Color Calibration command calibrates the video to enhance the colors being displayed.
- In addition, you can manually adjust the settings using the Video Settings command.

To force a refresh of the video screen:

- Choose Video > Refresh Video.

Screenshot

Take a screenshot of a target server using the Screenshot command.

To take a screenshot of the target server:

1. Choose Video > Screenshot.
2. The screenshot file appears as a download to view or save. Exact options depend on your client browser.

Auto Sense

The Auto Sense command forces a re-sensing of the video settings, such as resolution and refresh rate, and redraws the video screen.

► To automatically re-sense the video settings:
  • Choose Video > Auto Sense.
  
  A message stating that the auto adjustment is in progress appears.
Color Calibration

The Color Calibration command optimizes the color levels, such as hue, brightness, and saturation, of the transmitted video images.

The color settings are on a target server-basis.

Note: When color is successfully calibrated, the values are cached and reused each time you switch to the target. Changes to the brightness and contrast in Video Settings are not cached. Changing resolution resets the video to the cached values again. You can clear the cached values in Video > Clear Video Settings Cache. See Clear Video Settings Cache (on page 54).

► To calibrate color:
• Choose Video > Color Calibration.

A message stating that the color calibration is in progress appears.

Video Settings

Use the Video Settings command to manually adjust the video settings.

► To change the video settings:
1. Choose Video > Video Settings to open the Video Settings dialog.
2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:
   a. PLL Settings
      Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances, this setting should not be changed because the autodetect is usually quite accurate.
      Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.
   b. Brightness: Use this setting to adjust the brightness of the target server display.
Chapter 5: KVM Clients

c. Brightness Red - Controls the brightness of the target server display for the red signal.
d. Brightness Green - Controls the brightness of the green signal.
e. Brightness Blue - Controls the brightness of the blue signal.
f. Contrast Red - Controls the red signal contrast.
g. Contrast Green - Controls the green signal.
h. Contrast Blue - Controls the blue signal.

If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Technical Support before making any changes.

i. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.
j. **Vertical Offset** - Controls the vertical positioning of the target server display on your monitor.

### Video Settings

<table>
<thead>
<tr>
<th>PLL Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock</td>
<td>1344</td>
</tr>
<tr>
<td>Phase</td>
<td>20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Color Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brightness Red</td>
<td>0</td>
</tr>
<tr>
<td>Brightness Green</td>
<td>0</td>
</tr>
<tr>
<td>Brightness Blue</td>
<td>0</td>
</tr>
<tr>
<td>Contrast Red</td>
<td>65</td>
</tr>
<tr>
<td>Contrast Green</td>
<td>69</td>
</tr>
<tr>
<td>Contrast Blue</td>
<td>70</td>
</tr>
<tr>
<td>Horizontal Offset</td>
<td>288</td>
</tr>
<tr>
<td>Vertical Offset</td>
<td>-36</td>
</tr>
</tbody>
</table>

- Automatic Color Calibration

### Video Sensing

- Best possible video mode
- Quick sense video mode

[OK] [Cancel]
Clear Video Settings Cache

You can clear the video settings cache to delete old settings that do not apply anymore, such as when a target server is replaced. When you clear the video settings cache, the server automatically does a video auto-sense and color calibration. The new values are cached and reused when the target is accessed again.

➢ To clear the video settings cache:
  ● Choose Video > Clear Video Settings Cache in the toolbar.

View Menu

The View Menu contains options to customize your HKC display.

➢ Toolbar and Statusbar:
The toolbar contains icons for some commands. The Statusbar displays screen resolution at the bottom of the client window.

➢ Scale Video:
Scale Video scales your video to view the entire contents of the target server window in your HKC window. The scaling maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

➢ Fullscreen:
Fullscreen sets the target window to the size of your full screen, removing your client from the view.
  ● Press Esc to exit fullscreen.
Virtual Media Menu

Due to browser resources, virtual media file transfer is slower on HKC than the other KVM clients.

Connect Files and Folders

The Connect Files and Folders command provides an area to drag and drop files or folders that you want to connect to on virtual media.

Supported browsers: Chrome and Firefox

File size limit: 4GB per file

To connect files and folders:

1. Choose Virtual Media > Connect Files and Folders. Or, click the matching icon in toolbar.
2. Drag files or folders onto the Map Virtual Media Files and Folders dialog. Click OK.
3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.

To disconnect files and folders:
- Choose Virtual Media > Disconnect Files and Folders. Or, click the matching icon in the toolbar.

Connect ISO
The Connect ISO command maps a virtual media ISO image to the target. You can connect to ISO images on your client or on remote servers.
File size limit: 4GB per file

To map virtual media ISO images:
1. Choose Virtual Media > Connect ISO. Or, click the matching icon in the toolbar.
2. Select the option for your file’s location:

- Select **ISO Image** if the ISO file is directly accessible on your client. Click Browse, select the ISO file, and click OK. The filename appears next to the Browse button.

- Select **Remote Server ISO Image** if your ISO file is on a remote server. Remote ISO files must be pre-configured by an administrator for the mapping to appear here. See [Virtual Media File Server Setup (File Server ISO Images Only)](on page 36). Select the Hostname, then select the ISO file from the Image list. Enter the file server’s username and password.

3. Click OK to map the selected file to the target. A message appears to show virtual media is connected.

- **To disconnect ISO:**
  - Choose Virtual Media > Disconnect ISO. Or, click the matching icon in the toolbar.
Audio Menu
The Audio menu contains audio connection and settings.

Note: IE does not support audio. The menu will appear grayed out.

Connect Audio
The Connect Audio command connects your playback device, selects audio format and gives an option to mount the selected playback device automatically when you connect to the target.

HKC connects the client PC’s default audio playback device. To use a different device, it must be set as default in the client OS.

Note: For best quality, limit the number of audio sessions to a maximum of four KVM sessions.

To connect audio:
1. Choose Audio > Connect Audio, or click the matching icon in the toolbar.
2. In the Connect Audio Device dialog, select the Connect Playback Device checkbox.

Connect Audio Device

- Connect Playback Device
- Format:
  stereo, 16bit, 44.100 Hz
- Mount selected playback device automatically on connection to target

OK  Cancel
3. Select the Format:

- stereo, 16bit, 44.100 Hz
- mono, 16bit, 44.100 Hz
- stereo, 16bit, 22.050 Hz
- mono, 16bit, 22.050 Hz
- stereo, 16bit, 11.025 Hz
- mono, 16bit, 11.025 Hz

4. Select the “Mount selected playback device automatically on connection to target” checkbox to enable the option. This setting will connect audio automatically the next time you connect to targets.

5. Click OK. A success message appears.

▶ To disconnect audio:
1. Choose Audio > Disconnect Audio, or click the matching icon in the toolbar.

**Audio Settings**

The Audio Settings command is enabled when audio is connected. Use the Audio Settings to set the buffer and volume.

Increasing the buffer size improves the audio quality but may impact the delivery speed.

The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

▶ To configure audio settings:
1. Choose Audio > Audio Settings while Audio is connected.
Chapter 5: KVM Clients

2. Set the Buffer and Volume using the arrows or sliders.

3. Click OK.
Overview

When you log in via a network connection, you access the Remote Console. The first page accessed is the Port Access page.

Use the Remote Console to access and scan target servers and change your password.

For more in the Remote Console interface elements, see ThinkSystem Digital KVM Switch Remote Console Interface.
Scanning Ports - Remote Console

Use the port scanning feature to search for selected targets and display them in individual thumbnails as part of a slide show.

This feature allows you to monitor up to 32 targets at one time since you can view each target server individually as it is displayed during the slide show.

Connect to targets or focus on a specific target as needed.

Scans can include standard targets, blade servers, tiered devices, and KVM switch ports.

For dual video port groups, the primary port is included in a port scan, but the secondary port is not included when connecting from a remote client. Both ports can be included in the scan from the Local Port.

**Note:** The scan port feature is available from the Remote Console and Local Console, but the feature varies slightly.

Scanning Ports Slide Show - Remote Console

When you start a scan, the Port Scan window opens.

As each target is found, it is displayed as a thumbnail in a slide show.

The slide show scrolls through the target thumbnails based on the default interval of 10 seconds or according to the interval you specify.

As the scan scrolls through the targets, the target that is the focus of the slide show displays in the center of the page.

The name of the target is displayed below its thumbnail and in the task bar at the bottom of the window.

If a target is busy, a blank screen is displayed instead of the target server access page.

Configure scan settings for the Remote Console from VKC, VKCS, or AKC.

See Configuring Port Scan Settings in VKC/VKCS and AKC (on page 66)

**Note:** Scan port settings for the Local Console are configured on the Local Port Settings page. See Scanning Ports - Local Console (on page 125)
Target Status Indicators During Port Scanning - Remote Console

The status of each target is indicated by green, yellow and red lights that are displayed below the target thumbnail.

As the target is the focus of the rotation, the indicator is in the task bar also shows the status.

Lights for each target are gray until they are the focus of the slide show. The status lights indicate the following:

- Green - the target is up/idle or up/connected
- Yellow - the target is down but connected
- Red - the target is down/idle, busy, or otherwise not accessible
Using Scan Port Options

Following are options available to you while scanning targets. The exception of the Expand/Collapse icon, all of these options are selected from the Options menu in the upper left of the Port Scan viewer. The options will return to their defaults when you close the window.

Note: Configure scan settings such as the display interval from either the Virtual KVM Client (VKC) or Active KVM Client (AKC). See Configuring Port Scan Settings in VKC/VKCS and AKC [on page 66]  

- Hide or View Thumbnails
  - Use the Expand/Collapse icon at the upper left of the window to hide or view thumbnails. Expanded is the default view.

- Pause the Thumbnail Slide Show
  - Pause thumbnails from rotating between one target and the next by selecting Options > Pause. Rotating thumbnails is the default setting.

- Resume the Thumbnail Slide Show
  - Resume the thumbnail rotation by selecting Options > Resume.

- Size the Thumbnails in the Port Scan Viewer
  - Enlarge the size of the thumbnails by selecting Options > Size > 360x240.
  - Minimize the size of the thumbnails by selecting Options > Size > 160x120. This is the default thumbnail size.

- Change the Orientation of the Port Scan Viewer
  - View thumbnails along the bottom of the Port Scan viewer by selecting Options > Split Orientation > Horizontal.
  - View thumbnails along the right of the Port Scan viewer by selecting Options > Split Orientation > Vertical. This is the default view.

Scan for Targets

- To scan for targets:
  1. Click the Set Scan tab on the Port Access page.
  2. Select the targets you want to include in the scan by selecting the checkbox to the left of each target, or select the checkbox at the top of the target column to select all targets.
3. Leave the Up Only checkbox selected if you only want targets that are up to be included in the scan. Deselect this checkbox if you want to include all targets, whether up or down.

4. Click Scan to begin the scan.
As each target is scanned, it is displayed in slide show view on the page.

5. Click Options > Pause to pause the slide show and stop it from moving between targets, click Options > Resume to resume the slide show.

6. Click on a target thumbnail to scan it next.

7. Connect to a target by double clicking on its thumbnail.

---

**Changing a Password**

**To change your ThinkSystem Digital KVM Switch password:**


2. Type your current password in the Old Password field.

3. Type a new password in the New Password field. Retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and special characters.

4. Click OK.

5. You will receive confirmation that the password was successfully changed. Click OK.
Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, see Strong Passwords.

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

OK Cancel
Chapter 7  ThinkSystem Digital KVM Switch
Local Console

In This Chapter
Overview .................................................................................................. 121
Accessing a Target Server ...................................................................... 121
Local Console Video Resolution Behavior .............................................. 122
Simultaneous Users ................................................................................ 122
Local Port Hot Keys and Connect Keys.................................................. 123
Scanning Ports - Local Console.............................................................. 125
Local Console Smart Card Access.......................................................... 128
Local Console USB Profile Options ......................................................... 130
ThinkSystem Digital KVM Switch Local Console Factory Reset............. 130
Resetting the ThinkSystem Digital KVM Switch Using the Reset Button on
the Device .................................................................................................. 131

Overview

The Local Console interface provides access to the ThinkSystem Digital
KVM Switch while at the rack.

This section contains help on tasks performed by end users at the Local
Console.

Accessing a Target Server

To access a target server:

1. Click the Port Name of the target you want to access. The Port Action
   Menu is displayed.
2. Choose Connect from the Port Action menu. The video display
   switches to the target server interface.
Local Console Video Resolution Behavior

By default, monitors are typically set to the highest resolution they support.

Once a monitor is connected to the ThinkSystem Digital KVM Switch Local Console, ThinkSystem Digital KVM Switch detects the monitor’s native resolution. As long as the native resolution is supported by the Local Console, ThinkSystem Digital KVM Switch uses that resolution.

If the native resolution is not supported by the Local Console, and no other resolution is supported by the monitor and Local Console, ThinkSystem Digital KVM Switch uses the resolution of the last monitor that was connected to the Local Console.

For example, you connect a monitor set to a resolution of 1600x1200@60Hz to the ThinkSystem Digital KVM Switch Local Console. ThinkSystem Digital KVM Switch uses that resolution since it is supported by the Local Console.

If the next monitor you connect to the Local Console is not set to a supported resolution, ThinkSystem Digital KVM Switch uses the resolution of 1024x768@60.

For a list of supported Local Console video resolutions, see Supported ThinkSystem Digital KVM Switch Local Port DVI Resolutions (see “ThinkSystem Digital KVM Switch Supported Local Port DVI Resolutions” on page 141).

Consider reviewing Video Mode and Resolution Notes for additional information.

Simultaneous Users

The ThinkSystem Digital KVM Switch Local Console provides an independent access path to the connected KVM target servers.

Using the Local Console does not prevent other users from simultaneously connecting over the network. And even when remote users are connected to the ThinkSystem Digital KVM Switch, you can still simultaneously access your servers from the rack via the Local Console.
Local Port Hot Keys and Connect Keys

Because the ThinkSystem Digital KVM Switch Local Console interface is completely replaced by the interface for the target device you are accessing, a hot key is used to disconnect from a target and return to the local port GUI.

A connect key is used to connect to a target or switch between targets. The Local Port hot key allows you to rapidly access the ThinkSystem Digital KVM Switch Local Console user interface when a target device is currently being viewed.

See Select the Local Port Hotkey and Select the Local Port Connect Key for more information.

Return to the Local Console from a Target Device - Default Hot Key

- Press the Scroll Lock hot key twice rapidly
  The video display switches from the target device interface to the ThinkSystem Digital KVM Switch Local Console interface.

Local Port Auto-Sense (Video Refresh) - Default Hot Key

To perform an auto-sense (video refresh) on the ThinkSystem Digital KVM Switch local port via hot key:

- Press and hold the Shift key, and quickly press the Scroll Lock key twice, and then release.

Connect Key Examples

<table>
<thead>
<tr>
<th>Standard servers</th>
<th>Key sequence example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect key action</td>
<td>Key sequence example</td>
</tr>
<tr>
<td>Access a port from the local port</td>
<td>Press Left ALT &gt; Press and Release 5 &gt; Release Left ALT</td>
</tr>
<tr>
<td>Switch between ports</td>
<td>Press Left ALT &gt; Press and Release 1 &gt; Press and Release 1 &gt; Release Left ALT</td>
</tr>
<tr>
<td>Disconnect from a target and return to the local port</td>
<td>Double-click Scroll Lock</td>
</tr>
</tbody>
</table>
## Blade chassis

<table>
<thead>
<tr>
<th>Connect key action</th>
<th>Key sequence example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access a port from the local port GUI</td>
<td>Access port 5, slot 2:</td>
</tr>
<tr>
<td></td>
<td>• Press Left ALT &gt; Press and Release 5 &gt; Press and Release 2 &gt; Release Left ALT</td>
</tr>
<tr>
<td>Switch between ports</td>
<td>Switch from target port 5, slot 2 to port 5, slot 11:</td>
</tr>
<tr>
<td></td>
<td>• Press Left ALT &gt; Press and Release 5 &gt; Press and Release 2 &gt; Press and Release 1 &gt; Release Left ALT</td>
</tr>
<tr>
<td>Disconnect from a target and return to the local port GUI</td>
<td>Disconnect from target port 5, slot 11 and return to the local port GUI (the page from which you connected to target):</td>
</tr>
<tr>
<td></td>
<td>• Double Click Scroll Lock</td>
</tr>
</tbody>
</table>

## Special Sun Key Combinations

The following key combinations for Sun™ Microsystems server’s special keys operate on the Local Console port. These special keys are available from the Keyboard menu when you connect to a Sun target device:

<table>
<thead>
<tr>
<th>Sun key</th>
<th>Local port key combination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Again</td>
<td>Ctrl + Alt + F2</td>
</tr>
<tr>
<td>Props</td>
<td>Ctrl + Alt + F3</td>
</tr>
<tr>
<td>Undo</td>
<td>Ctrl + Alt + F4</td>
</tr>
<tr>
<td>Stop A</td>
<td>Break a</td>
</tr>
<tr>
<td>Front</td>
<td>Ctrl + Alt + F5</td>
</tr>
<tr>
<td>Copy</td>
<td>Ctrl + Alt + F6</td>
</tr>
<tr>
<td>Open</td>
<td>Ctrl + Alt + F7</td>
</tr>
<tr>
<td>Find</td>
<td>Ctrl + Alt + F9</td>
</tr>
<tr>
<td>Cut</td>
<td>Ctrl + Alt + F10</td>
</tr>
<tr>
<td>Paste</td>
<td>Ctrl + Alt + F8</td>
</tr>
<tr>
<td>Mute</td>
<td>Ctrl + Alt + F12</td>
</tr>
</tbody>
</table>
### Scanning Ports - Local Console

Use the port scanning feature to search for selected targets and display them in individual thumbnails as part of a slide show.

This feature allows you to monitor up to 32 targets at one time since you can view each target server individually as it is displayed during the slide show.

Connect to targets or focus on a specific target as needed.

Scans can include standard targets, blade servers, tiered devices, and KVM switch ports.

For dual video port groups, the primary port is included in a port scan, but the secondary port is not included when connecting from a remote client. Both ports can be included in the scan from the Local Port.

Click on the thumbnail of any target server to exit scan mode and connect to the target, or use the Local Port ConnectKey sequence.

To exit scan mode, click the Stop Scan button in the thumbnail view, or use the DisconnectKey sequence hot key.

*Note: The scan port feature is available from the Remote Console and Local Console, but the feature varies slightly. See Scanning Ports - Remote Console [on page 116]*

<table>
<thead>
<tr>
<th>Sun key</th>
<th>Local port key combination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compose</td>
<td>Ctrl + Alt + KPAD *</td>
</tr>
<tr>
<td>Vol +</td>
<td>Ctrl + Alt + KPAD +</td>
</tr>
<tr>
<td>Vol -</td>
<td>Ctrl + Alt + KPAD -</td>
</tr>
<tr>
<td>Stop</td>
<td>No key combination</td>
</tr>
<tr>
<td>Power</td>
<td>No key combination</td>
</tr>
</tbody>
</table>
Scanning Port Slide Show - Local Console

When you start a scan, the Port Scan window opens.

As each target is found, it is displayed as a thumbnail in a slide show.

The slide show scrolls through the target thumbnails based on the default interval of 10 seconds or according to the interval you specify.

As the scan scrolls through the targets, the target that is the focus of the slide show displays in the center of the page.

The name of the target is displayed below its thumbnail and in the task bar at the bottom of the window.

If a target is busy, a blank screen is displayed instead of the target server access page.

Configure the time between the slide show thumbnail rotation and the thumbnail focus interval on the Local Port Settings page.

See Configure Local Console Scan Settings [on page 127]

Note: Configure scan settings for the Remote Console from VKC, VKCS, or AKC. See Configuring Port Scan Settings in VKC/VKCS and AKC
**Target Status Indicators During Port Scanning - Local Console**

In thumbnail view on the Local Console, the status of each target is indicated below the thumbnail on the page until it is the focus of the slide show view.

The scanning status of each target is displayed as:

- not scanned
- connecting
- scanned
- skipped

---

**Configure Local Console Scan Settings**

Do the following to configure Local Console scan port options.

*Note: Configure scan settings for the Remote Console from VKC, VKCS, or AKC. See Configuring Port Scan Settings in VKC/VKCS and AKC (on page 66)*

**To configure the Local Console scan port settings:**

1. On the Local Console, select Device Settings.
2. In the Local Port Settings section, select Local Port Scan Mode.
3. Change the display interval as needed:
   - Display Interval - changes the scan display interval.
   - Interval Between Ports - change interval between switching different port during scan.
Scan for Targets - Local Console

To scan for targets:
1. Click the Set Scan tab on the Port Access page.
2. Select the targets you want to include in the scan by selecting the checkbox to the left of each target, or select the checkbox at the top of the target column to select all targets.
3. Leave the Up Only checkbox selected if you only want targets that are up to be included in the scan. Deselect this checkbox if you want to include all targets, whether up or down.
4. Click Scan to begin the scan.

As each target is scanned, it is displayed in slide show view on the page.

Local Console Smart Card Access

To use a smart card to access a server at the Local Console, plug a USB smart card reader into the ThinkSystem Digital KVM Switch using one of the USB ports located on the ThinkSystem Digital KVM Switch.

Once a smart card reader is plugged in or unplugged from the ThinkSystem Digital KVM Switch, the ThinkSystem Digital KVM Switch autodetects it.

For a list of supported smart cards and additional system requirements, see Supported Smart Card Readers (on page 147), Unsupported Smart Card Readers (on page 148) and Smart Card Minimum System Requirements (on page 145).

When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached.

Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS.

When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

To mount a smart card reader onto a target via the ThinkSystem Digital KVM Switch Local console:
1. Plug a USB smart card reader into the ThinkSystem Digital KVM Switch using one of the USB ports located on the device. Once attached, the smart card reader will be detected by the ThinkSystem Digital KVM Switch.
2. From the Local Console, click Tools.
3. Select the smart card reader from the Card Readers Detected list. Select None from the list if you do not want a smart card reader mounted.
4. Click OK. Once the smart card reader is added, a message will appear on the page indicating you have completed the operation successfully. A status of either Selected or Not Selected will appear in the left panel of the page under Card Reader.

▶ To update the Card Readers Detected list:
• Click Refresh if a new smart card has been mounted. The Card Readers Detected list will be refreshed to reflect the newly added smart card reader.
Local Console USB Profile Options

From the USB Profile Options section of the Tools page, you can choose from the available USB profiles.

The ports that can be assigned profiles are displayed in the Port Name field and the profiles that are available for a port appear in the Select Profile To Use field after the port is selected. The profiles selected for use with a port appear in the Profile In Use field.

To apply a USB profile to a local console port:
1. In the Port Name field, select the port you want to apply the USB profile to.
2. In the Select Profile To Use field, select the profile to use from among those available for the port.
3. Click OK. The USB profile will be applied to the local port and will appear in the Profile In Use field.

ThinkSystem Digital KVM Switch Local Console Factory Reset

Note: It is recommended that you save the audit log prior to performing a factory reset.

The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, see Audit Log.

To perform a factory reset:
2. Choose the appropriate reset option from the following options:
   - Full Factory Reset
     Removes the entire configuration and resets the appliance completely to the factory defaults.
     Because of the complete nature of this reset, you will be prompted to confirm the factory reset.
   - Network Parameter Reset
     Resets the network parameters of the appliance back to the default values (click Device Settings > Network Settings to access this information).

3. Click Reset to continue. You will be prompted to confirm the factory reset because all network settings will be permanently lost.

4. Click OK proceed. Upon completion of full factory reset, the ThinkSystem Digital KVM Switch device is automatically restarted.

---

Resetting the ThinkSystem Digital KVM Switch Using the Reset Button on the Device

On the back panel of the device, there is a Reset button. It is recessed to prevent accidental resets (you need a pointed object to press this button).

The actions that are performed when the Reset button is pressed are defined on the Encryption & Share page. See Encryption & Share.

*Note: It is recommended that you save the audit log prior to performing a factory reset.*

The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, see Audit Log.

**To reset the device:**
1. Power off the ThinkSystem Digital KVM Switch.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the ThinkSystem Digital KVM Switch device back on.
4. Continue holding the Reset button for 10 seconds.
Appendix B  Updating the LDAP Schema

In This Chapter
Returning User Group Information ......................................................... 132
Setting the Registry to Permit Write Operations to the Schema ........... 133
Creating a New Attribute ......................................................................... 133
Adding Attributes to the Class ............................................................... 134
Updating the Schema Cache ................................................................. 136
Editing rciusergroup Attributes for User Members ......................... 136

Returning User Group Information
Use the information in this section to return User Group information (and
assist with authorization) once authentication is successful.

From LDAP/LDAPS
When an LDAP/LDAPS authentication is successful, the ThinkSystem
Digital KVM Switch determines the permissions for a given user based
on the permissions of the user’s group. Your remote LDAP server can
provide these user group names by returning an attribute named as
follows:
rciusergroup   attribute type: string

This may require a schema extension on your LDAP/LDAPS server.
Consult your authentication server administrator to enable this attribute.
In addition, for Microsoft® Active Directory®, the standard LDAP
memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory®
administrator.

Returning user group information from Microsoft’s® Active Directory for
Windows 2000® operating system server requires updating the
LDAP/LDAPS schema. See your Microsoft documentation for details.
1. Install the schema plug-in for Active Directory. See Microsoft Active
   Directory documentation for instructions.
Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

To permit write operations to the schema:
1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.

   ![Change Schema Master](image)

   The schema master manages modifications to the schema. Only one server in the enterprise performs this role.

   **Current schema master (online):**
   rcj-gcf42nzmz.mypc.mydomain.com

   To transfer the schema master role to the targeted domain controller below, click **Change**.
   rcj-gcf42nzmz.mypc.mydomain.com

2. Select the “Schema can be modified on this Domain Controller” checkbox. **Optional**
3. Click OK.

Creating a New Attribute

To create new attributes for the rciusergroup class:
1. Click the + symbol before Active Directory® Schema in the left pane of the window.
2. Right-click Attributes in the left pane.
3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

![Create New Attribute dialog]

4. Type \textit{rciusergroup} in the Common Name field.
5. Type \textit{rciusergroup} in the LDAP Display Name field.
6. Type 1.3.6.1.4.1.13742.50 in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type 1 in the Minimum field.
10. Type 24 in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

- To add attributes to the class:
  1. Click Classes in the left pane of the window.
2. Scroll to the user class in the right pane and right-click it.

3. Choose Properties from the menu. The user Properties dialog appears.

4. Click the Attributes tab to open it.

5. Click Add.
6. Choose rciusergroup from the Select Schema Object list.

7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

To update the schema cache:
1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

To edit the individual user attributes within the group rciusergroup:
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.
3. Go to the directory where the support tools were installed. Run `adsiedit.msc`. The ADSI Edit window opens.

4. Open the Domain.

5. In the left pane of the window, select the CN=Users folder.
6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.

8. Click Edit. The String Attribute Editor dialog appears.

9. Type the user group [created in the ThinkSystem Digital KVM Switch] in the Edit Attribute field. Click OK.
Appendix C Specifications

In This Chapter

Hardware ................................................................................................. 139
Software................................................................................................. 153

Hardware

<table>
<thead>
<tr>
<th>Dimensions and Physical Specifications</th>
</tr>
</thead>
</table>
| **SM27A17644** | 16 server ports  
2 remote users  
1 local port for use at the rack | Dual Power  
110V/240V,  
50-60Hz  
1.8A 60W 52 KCAL | 17.3” x 13.15” x  
1.73” | 9.08lbs | 0º - 45º C | 0-85 % RH | 439x334x44mm | 4.12kg | 32º - 113º F |
Supported Target Server Video Resolutions

Following is a complete list of supported video resolutions when accessing a target from the Remote Console.

- 640x350@70Hz
- 640x350@85Hz
- 640x400@56Hz
- 640x400@84Hz
- 640x400@85Hz
- 640x480@60Hz
- 640x480@66.6Hz
- 640x480@72Hz
- 640x480@75Hz
- 640x480@85Hz
- 720x400@70Hz
- 720x400@84Hz
- 720x400@85Hz
- 800x600@56Hz
- 800x600@60Hz
- 800x600@70Hz
- 800x600@72Hz
- 800x600@75Hz
- 800x600@85Hz
- 800x600@90Hz
- 800x600@100Hz
- 832x624@75.1Hz
- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768@72Hz
- 1024x768@85Hz
- 1024x768@75Hz
- 1024x768@90Hz
- 1024x768@100Hz
- 1152x864@60Hz
- 1152x864@70Hz
- 1152x864@75Hz
- 1152x864@85Hz
- 1152x870@75.1Hz
- 1280x720@60Hz
- 1280x960@60Hz
• 1280x960@85Hz
• 1280x1024@60Hz
• 1280x1024@75Hz
• 1280x1024@85Hz
• 1360x768@60Hz
• 1366x768@60Hz
• 1368x768@60Hz
• 1400x1050@60Hz
• 1440x900@60Hz
• 1600x1200@60Hz
• 1680x1050@60Hz
• 1920x1080@60Hz

**ThinkSystem Digital KVM Switch Supported Local Port DVI Resolutions**

Following are the resolutions supported when connecting to a DVI monitor from the Local port.

• 1920x1080@60Hz
• 1280x720@60Hz
• 1024x768@60Hz (default)
• 1024x768@75Hz
• 1280x1024@60Hz
• 1280x1024@75Hz
• 1600x1200@60Hz
• 800x600@60Hz
• 1280x768@60Hz
• 1366x768@60Hz
• 1360x768@60Hz
• 1680x1050@60Hz
• 1440x900@60Hz
Target Server Video Resolution - Supported Connection Distances and Refresh Rates

The maximum supported distance is a function of many factors including the type/quality of the Cat5 cable, server type and manufacturer, video driver and monitor, environmental conditions, and user expectations.

The following table summarizes the maximum target server distance for various video resolutions and refresh rates:

<table>
<thead>
<tr>
<th>Target server video resolution</th>
<th>Maximum distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024x768@60Hz (and below)</td>
<td>150’ (45 m)</td>
</tr>
<tr>
<td>1280x1024@60Hz</td>
<td>100’ (30 m)</td>
</tr>
<tr>
<td>1280x720@60Hz</td>
<td>75’ (22 m)</td>
</tr>
<tr>
<td>1600x1200@60Hz</td>
<td>50’ (15 m)</td>
</tr>
<tr>
<td>1920x1080@60Hz</td>
<td>50’ (15 m)</td>
</tr>
</tbody>
</table>

See Supported Target Server Video Resolutions (on page 140) for the video resolutions supported by the ThinkSystem Digital KVM Switch.

*Note: Due to the multiplicity of server manufacturers and types, OS versions, video drivers, and so on, as well as the subjective nature of video quality, performance cannot be guaranteed across all distances in all environments.*

Supported Computer Interface Modules (CIMs) Specifications

<table>
<thead>
<tr>
<th>CIM model</th>
<th>Description</th>
<th>Dimensions (WxDxH)</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThinkSystem D-USB cable for Digital KVM SC17A30049</td>
<td>Dual USB CIM for:</td>
<td>1.7” x 3.5” x 0.8”</td>
<td>0.25lb</td>
</tr>
<tr>
<td></td>
<td>▪ OS virtual media</td>
<td>43 x 90 x 19mm</td>
<td>0.11kg</td>
</tr>
<tr>
<td></td>
<td>▪ Smartcard/CAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Audio</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Absolute Mouse Synchronization</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Specifications

<table>
<thead>
<tr>
<th>CIM model</th>
<th>Description</th>
<th>Dimensions (WxDxH)</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThinkSystem S-USB cable for Digital KVM SC17A30053</td>
<td>USB CIM for:</td>
<td>1.3” x 3.0” x 0.6”</td>
<td>0.20lb</td>
</tr>
<tr>
<td></td>
<td>- OS virtual media</td>
<td>33 x 76 x 15mm</td>
<td>0.09kg</td>
</tr>
<tr>
<td></td>
<td>- Absolute Mouse Synchronization</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Supported Remote Connections

<table>
<thead>
<tr>
<th>Remote connection</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet</td>
</tr>
<tr>
<td>Protocols</td>
<td>TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS</td>
</tr>
</tbody>
</table>

### Network Speed Settings

<table>
<thead>
<tr>
<th>Network switch port setting</th>
<th>Auto</th>
<th>1000/Full</th>
<th>100/Full</th>
<th>100/Half</th>
<th>10/Full</th>
<th>10/Half</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>Highest Available Speed</td>
<td>1000/Full</td>
<td>100/Half</td>
<td>100/Full</td>
<td>ThinkSystem Digital KVM Switch: 10/Full Switch: 10/Half</td>
<td>10/Half</td>
</tr>
</tbody>
</table>
Appendix C: Specifications

<table>
<thead>
<tr>
<th>ThinkSystem Digital KVM Switch network speed setting</th>
<th>100/Full</th>
<th>100/Half</th>
<th>10/Full</th>
<th>10/Half</th>
</tr>
</thead>
<tbody>
<tr>
<td>100/Full</td>
<td>ThinkSystem Digital KVM Switch: 100/Full</td>
<td>ThinkSystem Digital KVM Switch: 100/Half</td>
<td>ThinkSystem Digital KVM Switch: 100/Full</td>
<td>No Communication</td>
</tr>
<tr>
<td>100/Half</td>
<td>100/Half</td>
<td>ThinkSystem Digital KVM Switch: 100/Full</td>
<td>ThinkSystem Digital KVM Switch: 100/Half</td>
<td>No Communication</td>
</tr>
<tr>
<td>10/Full</td>
<td>ThinkSystem Digital KVM Switch: 10/Full</td>
<td>No Communication</td>
<td>No Communication</td>
<td>10/Full</td>
</tr>
<tr>
<td>10/Half</td>
<td>10/Half</td>
<td>No Communication</td>
<td>No Communication</td>
<td>No Communication</td>
</tr>
</tbody>
</table>

Legend:
- Does not function as expected
- Supported
- Functions; not recommended
- NOT supported by Ethernet specification; product will communicate, but collisions will occur
Per Ethernet specification, these should be “no communication,” however, note that the ThinkSystem Digital KVM Switch behavior deviates from expected behavior.

**Note:** For reliable network communication, configure the ThinkSystem Digital KVM Switch and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure the ThinkSystem Digital KVM Switch and LAN Switch to Autodetect (recommended), or set both to a fixed speed.duplex such as 100MB/s/Full.

**Dell Chassis Cable Lengths and Video Resolutions**

In order to maintain video quality, it is recommended to use the following cable lengths and video resolutions when you are connecting to Dell® blade chassis from the ThinkSystem Digital KVM Switch:

<table>
<thead>
<tr>
<th>Video resolution</th>
<th>Cable length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024x768@60Hz</td>
<td>50’ (15.24 m)</td>
</tr>
<tr>
<td>1280x1024@60Hz</td>
<td>50’ (15.24 m)</td>
</tr>
<tr>
<td>1600x1200@60Hz</td>
<td>30’ (9.14 m)</td>
</tr>
</tbody>
</table>

**Smart Card Minimum System Requirements**

**Local Port Requirements**

The basic interoperability requirement for local port attachment to the ThinkSystem Digital KVM Switch is:

- All devices [smart card reader or token] that are locally attached must be USB CCID-compliant.
Target Server Requirements

When using smart card readers, the basic requirements for interoperability at the target server are:

- The IFD (smart card reader) Handler must be a standard USB CCID device driver (comparable to the generic Microsoft® USB CCID driver).
- ThinkSystem D-USB cable for Digital KVM - SC17A30049 CIM is required and must be using firmware version 3A6E or later.
- Blade chassis server connections, where a CIM per blade is used, are supported.
- Blade chassis server connections, where a CIM per chassis is used, is only supported for IBM® BladeCenter® models H and E with auto-discovery enabled.

Windows XP Targets

Windows XP® operating system targets must be running Windows XP SP3 in order to use smart cards with the ThinkSystem Digital KVM Switch.

Linux Targets

If you are using a Linux® target, the following requirements must be met to use smart card readers.

- CCID Requirements
  If the CIM/CCID is not recognized as a smart card reader by your Linux target, you may need to update the CCID driver version to 1.3.8 or above and update the driver configuration file (Info.plist).

<table>
<thead>
<tr>
<th>Operating system</th>
<th>CCID requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 5</td>
<td>ccid-1.3.8-1.el5</td>
</tr>
<tr>
<td>SuSE 11</td>
<td>pcsccid-1.3.8-3.12</td>
</tr>
<tr>
<td>Fedora® Core 10</td>
<td>ccid-1.3.8-1.fc10.i386</td>
</tr>
</tbody>
</table>
Remote Client Requirements

The basic requirements for interoperability at the remote client are:

- The IFD (smart card reader) Handler must be a PC/SC compliant device driver.
- The ICC (smart card) Resource Manager must be available and be PC/SC compliant.
- The JRE® Java™ 1.8 with smart card API must be available for use by the client application.

Remote Linux Client Requirements

If you are using a Linux® client, the following requirements must be met to use smart card readers with the ThinkSystem Digital KVM Switch device.

*Note: User login to client, on smart card insertion, may take longer when 1 or more KVM sessions are actively in place to targets. As the login process to these targets is also under way.*

- **PC/SC Requirements**

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Required PC/SC</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 5</td>
<td>pcsclite-1.4.4-0.1.el5</td>
</tr>
<tr>
<td>SuSE 11</td>
<td>pcsclite-1.4.102-1.24</td>
</tr>
<tr>
<td>Fedora® Core 10</td>
<td>pcsclite-1.4.102.3.fc10.i386</td>
</tr>
</tbody>
</table>

- **Create a Java® Library Link**

  A soft link must be created to the libpcsclite.so after upgrading RHEL 4, RHEL 5 and FC 10. For example, ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so, assuming installing the package places the libraries in /usr/lib or /user/local/lib

- **PC/SC Daemon**

  When the pcscl daemon (resource manager in framework) is restarted, restart the browser

**Supported Smart Card Readers**

<table>
<thead>
<tr>
<th>Type</th>
<th>Vendor</th>
<th>Model</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB</td>
<td>SCM Microsystems</td>
<td>SCR331</td>
<td>Verified on local and remote</td>
</tr>
</tbody>
</table>
## Appendix C: Specifications

<table>
<thead>
<tr>
<th>Type</th>
<th>Vendor</th>
<th>Model</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB</td>
<td>SCM Microsystems</td>
<td>SCR331</td>
<td>Verified on local and remote</td>
</tr>
<tr>
<td>USB</td>
<td>ActivIdentity®</td>
<td>ActivIdentity USB Reader v2.0</td>
<td>Verified on local and remote</td>
</tr>
<tr>
<td>USB</td>
<td>ActivIdentity</td>
<td>ActivIdentity USB Reader v3.0</td>
<td>Verified on local and remote</td>
</tr>
<tr>
<td>USB</td>
<td>Gemalto®</td>
<td>GemPC USB-SW</td>
<td>Verified on local and remote</td>
</tr>
<tr>
<td>USB Keyboard/Card combo</td>
<td>Dell®</td>
<td>USB Smart Card Reader Keyboard</td>
<td>Verified on local and remote</td>
</tr>
<tr>
<td>USB Keyboard/Card combo</td>
<td>Cherry GmbH</td>
<td>G83-6744 SmartBoard</td>
<td>Verified on local and remote</td>
</tr>
<tr>
<td>USB reader for SIM-sized cards</td>
<td>Omnikey</td>
<td>6121</td>
<td>Verified on local and remote</td>
</tr>
<tr>
<td>Integrated (Dell Latitude D620)</td>
<td>O2Micro</td>
<td>O2776</td>
<td>Remote only</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>ActivIdentity</td>
<td>ActivIdentity PCMCIA Reader</td>
<td>Remote only</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>SCM Microsystems</td>
<td>SCR243</td>
<td>Remote only</td>
</tr>
</tbody>
</table>

*Note: SCM Microsystems SCR331 smart card readers must be using SCM Microsystems firmware v5.25.*

## Unsupported Smart Card Readers

The following card readers are not supported.

If a smart card reader does not appear in the supported smart card readers table or in the unsupported smart card readers table, its function cannot be guaranteed.

<table>
<thead>
<tr>
<th>Type</th>
<th>Vendor</th>
<th>Model</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Keyboard/Card combo</td>
<td>HP®</td>
<td>ED707A</td>
<td>No interrupt endpoint =&gt; not compatible with Microsoft® driver</td>
</tr>
<tr>
<td>USB Keyboard/Card combo</td>
<td>SCM Microsystems</td>
<td>SCR338</td>
<td>Proprietary card reader implementation (not CCID-compliant)</td>
</tr>
</tbody>
</table>
## Audio Playback and Capture Recommendations and Requirements

### Audio Level

- Set the target audio level to a mid-range setting.
  
  For example, on a Windows® client, set the audio to 50 or lower.

This setting must be configured through the playback or capture audio device, not from the client audio device control.

### Recommendations for Audio Connections when PC Share Mode is Enabled

If you are using the audio feature while running PC Share mode, audio playback and capture are interrupted if an additional audio device is connected to the target.

For example, User A connects a playback device to Target1 and runs an audio playback application then User B connects a capture device to the same target. User A’s playback session is interrupted and the audio application may need to be restarted.

The interruption occurs because the USB device needs to be re-enumerated with the new device configuration.

It may take some time for the target to install a driver for the new device.

Audio applications may stop playback completely, go to the next track, or just continue playing.

The exact behavior is dependent on how the audio application is designed to handle a disconnect/reconnect event.

### Bandwidth Requirements

The table below details the audio playback and capture bandwidth requirements to transport audio under each of the selected formats.

<table>
<thead>
<tr>
<th>Audio format</th>
<th>Network bandwidth requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.1 KHz, 16bit stereo</td>
<td>176 KB/s</td>
</tr>
<tr>
<td>44.1 KHz, 16bit mono</td>
<td>88.2 KB/s</td>
</tr>
<tr>
<td>2.05 KHz, 16bit stereo</td>
<td>88.2 KB/s</td>
</tr>
</tbody>
</table>
### Audio format | Network bandwidth requirement
---|---
22.05 KHz, 16bit mono | 44.1 KB/s
11.025 KHz, 16bit stereo | 44.1 KB/s
11.025 KHz, 16bit mono | Audio 22.05 KB/s

In practice, the bandwidth used when an audio device connects to a target is higher due to the keyboard and video data consumed when opening and using an audio application on the target.

A general recommendation is to have at least a 1.5MB connection before running playback and capture.

However, high video-content, full-color connections using high-target screen resolutions consume much more bandwidth and impact the quality of the audio considerably.

To help mitigate quality degeneration, there are a number of recommended client settings that reduce the impact of video on audio quality at lower bandwidths:

- Connect audio playback at the lower quality formats. The impact of video consuming bandwidth is much less notable at 11k connections than at 44k
- Set the connection speed under Connection Properties to a value that best matches the client to server connection
- Under Connection Properties, set the color depth to as low a value as possible. Reducing the color depth to 8 bit color considerably reduces the bandwidth consumed
- Set Smoothing, to High. This will improve the appearance of the target video by reducing displayed video noise
- Under Video settings, set the Noise Filter to its highest setting of 7 (highest value) so less bandwidth is used for target screen changes

### Audio in a Mac Environment

Following are known issues in a Mac® environment.

- On Mac clients, only one playback device is listed on the Connect Audio panel. The device listed is the default and is displayed on the Connect Audio panel as Java Sound Audio Engine.
- Using audio on a Mac target through Skype® may cause the audio to be corrupted.
Number of Supported Audio/Virtual Media and Smartcard Connections

Following are the number of simultaneous Audio/Virtual Media and Smartcard connections that can be made from a client to a target:

- 1 smartcard
- 1 virtual media
- 1 Smartcard and 1 virtual media
- 2 virtual media

Certified Modems

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

ThinkSystem Digital KVM Switch Supported Keyboard Languages

The ThinkSystem Digital KVM Switch provides keyboard support for the languages listed in the following table.

*Note: You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for the ThinkSystem Digital KVM Switch Local Console functions. For more information about non-US keyboards, see Informational Notes. Note: It is strongly recommended that you use system-config-keyboard to change languages if you are working in a Linux environment.*

<table>
<thead>
<tr>
<th>Language</th>
<th>Regions</th>
<th>Keyboard layout</th>
</tr>
</thead>
<tbody>
<tr>
<td>US English</td>
<td>United States of America and most of English-speaking countries: for example, Canada, Australia, and New Zealand.</td>
<td>US Keyboard layout</td>
</tr>
<tr>
<td>US English</td>
<td>United States of America and most of English-speaking countries: for example, Netherlands</td>
<td>US Keyboard layout</td>
</tr>
<tr>
<td>International</td>
<td>United States of America and most of English-speaking countries: for example, Netherlands</td>
<td>US Keyboard layout</td>
</tr>
<tr>
<td>UK English</td>
<td>United Kingdom</td>
<td>UK layout keyboard</td>
</tr>
<tr>
<td>Chinese Traditional</td>
<td>Hong Kong S. A. R., Republic of China [Taiwan]</td>
<td>Chinese Traditional</td>
</tr>
</tbody>
</table>
### Appendix C: Specifications

<table>
<thead>
<tr>
<th>Language</th>
<th>Regions</th>
<th>Keyboard layout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chinese Simplified</td>
<td>Mainland of the People’s Republic of China</td>
<td>Chinese Simplified</td>
</tr>
<tr>
<td>Korean</td>
<td>South Korea</td>
<td>Dubeolsik Hangul</td>
</tr>
<tr>
<td>Japanese</td>
<td>Japan</td>
<td>JIS Keyboard</td>
</tr>
<tr>
<td>French</td>
<td>France</td>
<td>French (AZERTY) layout keyboard.</td>
</tr>
<tr>
<td>German</td>
<td>Germany and Austria</td>
<td>German keyboard [QWERTZ layout]</td>
</tr>
<tr>
<td>French</td>
<td>Belgium</td>
<td>Belgian</td>
</tr>
<tr>
<td>Norwegian</td>
<td>Norway</td>
<td>Norwegian</td>
</tr>
<tr>
<td>Danish</td>
<td>Denmark</td>
<td>Danish</td>
</tr>
<tr>
<td>Swedish</td>
<td>Sweden</td>
<td>Swedish</td>
</tr>
<tr>
<td>Hungarian</td>
<td>Hungary</td>
<td>Hungarian</td>
</tr>
<tr>
<td>Slovenian</td>
<td>Slovenia</td>
<td>Slovenian</td>
</tr>
<tr>
<td>Italian</td>
<td>Italy</td>
<td>Italian</td>
</tr>
<tr>
<td>Spanish</td>
<td>Spain and most Spanish speaking countries</td>
<td>Spanish</td>
</tr>
<tr>
<td>Portuguese</td>
<td>Portugal</td>
<td>Portuguese</td>
</tr>
</tbody>
</table>

---

### Using a Windows Keyboard to Access Mac Targets

A Windows® keyboard can be used to access a Mac® connected to a ThinkSystem Digital KVM Switch. Windows keys are then used to emulate the special Mac keys. This is the same as connecting a Windows keyboard directly to the Mac.
TCP and UDP Ports Used

► Listening TCP Ports:
* 80: http access (configurable)
* 443: https access (configurable)
* 22: SSH access (if enabled, configurable)

► Listening UDP Ports:
* 162: SNMP access (if SNMP Agent is enabled)

► TCP Ports Outgoing:
* 389: LDAP authentication (if LDAP is enabled, configurable)
* 636: LDAPS/StartTLS (if LDAPS/StartTLS is enabled, configurable)
* 25: SMTP (email) (if enabled)
* 445: SMB (Windows File System) access (Remote ISO image access).

► UDP Ports Outgoing:
* 514: Syslog (if enabled, configurable)
* 1812: RADIUS authentication (if enabled, configurable)
* 1813: RADIUS authentication (if enabled, configurable)

Software

Supported Operating Systems, Browsers and Java Versions

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Browsers</th>
<th>Java</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10</td>
<td>Windows Edge</td>
<td>Java 1.7 or later</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer® 11</td>
<td>for VKC</td>
</tr>
<tr>
<td></td>
<td>Chrome 46</td>
<td>Java 1.8.0_40 or</td>
</tr>
<tr>
<td></td>
<td>Firefox® 41</td>
<td>later for VKCs</td>
</tr>
<tr>
<td>Windows 7® Home Premium SP1 64-bit</td>
<td>Internet Explorer® 10, 11</td>
<td></td>
</tr>
<tr>
<td>Windows 7 Ultimate SP1 64-bit</td>
<td>Firefox® 29.0.1, 30, 40</td>
<td></td>
</tr>
<tr>
<td>Windows 7 Ultimate 32-bit</td>
<td>Chrome® 35, 45</td>
<td></td>
</tr>
<tr>
<td>Windows 8® 64-bit</td>
<td>Safari® 7.0.3, 7.0.5</td>
<td></td>
</tr>
<tr>
<td>Windows XP® Home Edition with SP 3</td>
<td>Edge</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012® Standard 64-bit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Operating Systems

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Browsers</th>
<th>Java</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008®</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003®</td>
<td></td>
<td></td>
</tr>
<tr>
<td>openSUSE® 11.4 Celadon (x86_64)</td>
<td>Firefox 16.0.2</td>
<td></td>
</tr>
<tr>
<td>openSUSE® 13.2</td>
<td>Firefox 33</td>
<td></td>
</tr>
<tr>
<td>Fedora® 18 (Spherical Cow)</td>
<td>Firefox 24</td>
<td></td>
</tr>
<tr>
<td>Fedora® 22</td>
<td>Firefox 38</td>
<td></td>
</tr>
<tr>
<td>RHEL® 6.4</td>
<td>Firefox 21</td>
<td></td>
</tr>
<tr>
<td>Mac® OS X Mountain Lion® 10.7.5</td>
<td>Firefox 25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Safari 6.0.5</td>
<td></td>
</tr>
<tr>
<td>Mac OS X Mountain Lion 10.8.5 *</td>
<td>Firefox 25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Safari 6.1.1</td>
<td></td>
</tr>
<tr>
<td>Mac 10.10.4</td>
<td>Safari 9.0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chrome 45</td>
<td></td>
</tr>
<tr>
<td>Mac 10.10.5</td>
<td>Safari 9.0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chrome 46</td>
<td></td>
</tr>
<tr>
<td>Solaris® 10 64-bit</td>
<td>Firefox 3.6.23</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Upon upgrading from OS X 10.8.2 to OS X 10.8.3, Safari® may block Java™.*
JRE Requirements and Browser Considerations for Mac

Java Runtime Environment Requirements for Mac
Install Java Runtime Environment 8 (JRE)® on PCs and Macs® when using the Virtual KVM Client (VKC) to access target devices via ThinkSystem Digital KVM Switch.

This ensures in order to provide high performance, KVM-over-IP video processing when remotely accessing target devices/PCs/Macs.

The latest version of JRE for Mac can be downloaded from the Oracle Support website.

Browser Considerations for Mac
Java may be disabled by default in certain browsers. Enable Java and accept all security warnings in order to use ThinkSystem Digital KVM Switch.

Certain versions of Safari® block Java for security reasons. Since Java is required to use ThinkSystem Digital KVM Switch, use Firefox® instead. Additionally, you may be required to navigate through a number of messages. Select ‘Do Not Block’ if these messages are displayed.

Virtual KVM Client (VKC), VKCS, and Active KVM Client (AKC) Requirements
Microsoft .NET® 4.0 (or later) is required to use ThinkSystem Digital KVM Switch with the Microsoft Windows®-based Active KVM Client (AKC).

Java™ 1.8 is required to use the Java-based . Java 1.8.0_40 or higher is required to use the VKCS.

Java 1.8.0_40 or later is required for VKCS, the standalone VKC client used on Chrome.

ThinkSystem Digital KVM Switch checks your current Java version and prompts you to update it if it is not compatible.

VKC can only be launched from a 32-bit browser, or 64-bit browser.

Following are the Java 32-bit and 64-bit Windows operating system requirements.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Operating system</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows x64 32-bit mode</td>
<td>Windows XP®</td>
<td>• Internet Explorer® 7.0, 9.0, 10.0 or 11.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Firefox® 1.06 - 4 or later</td>
</tr>
</tbody>
</table>
### Appendix C: Specifications

<table>
<thead>
<tr>
<th>Mode</th>
<th>Operating system</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2003</td>
<td>Windows Vista®</td>
<td>• Internet Explorer 9.0, 10.0 or 11.0</td>
</tr>
<tr>
<td></td>
<td>Windows 7®</td>
<td>• Internet Explorer 9.0, 10.0 or 11.0</td>
</tr>
<tr>
<td></td>
<td>Windows x64</td>
<td>• Firefox 1.06 - 4 or later</td>
</tr>
<tr>
<td>64-bit mode</td>
<td>Windows XP</td>
<td>64bit OS, 32bit browsers:</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional®</td>
<td>• Internet Explorer 6.0 SP1++, 7.0 or 8.0</td>
</tr>
<tr>
<td></td>
<td>Windows XP Tablet®</td>
<td>• Firefox 1.06 - 4 or later</td>
</tr>
<tr>
<td></td>
<td>Windows Vista</td>
<td>64bit mode, 64bit browsers:</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003</td>
<td>• Internet Explorer 7.0, 8.0, 9.0, 10.0 or 11.0</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 7</td>
<td></td>
</tr>
</tbody>
</table>

Note that a JRE™ plug-in is available for the Windows® 32-bit and 64-bit operating systems.
See Java Runtime Environment (JRE) Notes for additional information.

**Multi-Language Keyboard JRE Requirement**

In order for multi-language keyboards to work in the ThinkSystem Digital KVM Switch and Virtual KVM Client (VKC), install the multi-language version of JRE™.
Events Captured in the Audit Log and Syslog

Following is a list and description of the events that are captured by the ThinkSystem Digital KVM Switch audit log and syslog:

- Access Login - A user has logged in to the ThinkSystem Digital KVM Switch
- Access Logout - A user has logged out of the ThinkSystem Digital KVM Switch
- Active USB Profile - The USB profile is active
- CIM Connected - A CIM was connected
- CIM Disconnected - A CIM was disconnected
- Connection Lost - The connection to the target was lost
- Disconnected User - A user was disconnected from a port
- Duplicate CIM Serial - A CIM has same serial number with other CIM.
- Login Failed - User login failed
- Password Changed - Password change occurred
- Port Connect - Port was connected
- Port Disconnect - Port was disconnected
- Port Status Change - Change in the port status
- Scan Started - A target scan was started
- Scan Stopped - A target scan was stopped
- Session Timeout - A session timeout occurred
- USB Profile Set Modify Failed - Failed to change USB Profile Set.
- USB Profile Set Modified - USB Profile Set was modified.
- USB Net Present - A broadband modem is plugged in.
- USB Net Absent - A broadband modem is unplugged.
- VM Image Connected - A VM image was connected
- VM Image Disconnected - A VM image was disconnected
## Appendix D  FAQ

### Overview

**What is the ThinkSystem Digital 2x1x16 KVM Switch?**

ThinkSystem Digital 2x1x16 KVM Switch is a high performance digital KVM (keyboard, video, mouse) switch that provides two IT administrators with Java-free access and control of 16 servers over the network with BIOS-level functionality. ThinkSystem Digital 2x1x16 KVM Switch is completely hardware and OS-independent; users can troubleshoot and reconfigure servers even when servers are down.

At the rack, ThinkSystem Digital 2x1x16 KVM Switch provides the same functionality, convenience, and space and cost savings as traditional analog KVM switches. However, ThinkSystem Digital 2x1x16 KVM Switch also integrates the industry’s highest performing KVM-over-IP technology, allowing multiple administrators to access servers from PC and laptop.

**Can the ThinkSystem Digital 2x1x16 KVM Switch be rack mounted?**

Yes. The ThinkSystem Digital 2x1x16 KVM Switch ships standard with 19” rack mount brackets.

**How large is the ThinkSystem Digital 2x1x16 KVM Switch?**

The ThinkSystem Digital 2x1x16 KVM Switch models fit in a standard 19” rack. It is 1U high and 13.15” deep.

### Remote Access

**How many users can remotely access servers on the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH?**

ThinkSystem Digital 2x1x16 KVM Switch allows remote connections to 1 or 2 of the 16 servers connected to it.

**Can two people look at the same server at the same time?**

Yes. Actually, up to eight people can access and control any single server at the same time.

**Can two people access the same server, one remotely and one from the local port?**

Yes. The local port is completely independent of the remote “ports.” The local port can access the same server using the PC-Share feature.

**In order to access ThinkSystem Digital 2x1x16 KVM Switch from a laptop or PC, what hardware, software or network configuration is required?**

Because ThinkSystem Digital 2x1x16 KVM Switch is completely Web-accessible, it doesn’t require customers to install proprietary software on laptops and PC’s used for access. ThinkSystem Digital 2x1x16 KVM Switch can be accessed through major Web browsers, including: Internet Explorer®, Firefox®, Safari and Chrome. ThinkSystem Digital 2x1x16 KVM Switch can be accessed on Windows, Linux and Mac® desktops, via Active KVM Windows Client, the new Java-free HTML KVM Client and the Java™-based Virtual KVM Client™.
ThinkSystem Digital 2x1x16 KVM Switch administrators can also perform remote management [set passwords and security, rename servers, change IP address, etc.] using a convenient browser-based interface.

Is Java required?
The THINKSYSTEM DIGITAL 2X1X16 KVM Switch’s KVM Client Software does sophisticated video processing which was originally built on the powerful Java platform. Non-Java KVM Clients are now available for Windows (AKC) and Linux/Mac (HKC). The HTML-based HKC provides basic KVM-over-IP access, runs in the browser and does not require a separate applet or browser plugin.

What is the file size of the applet that’s used to access ThinkSystem Digital 2x1x16 KVM Switch? How long does it take to retrieve?
The Virtual KVM Client (VKC) applet used to access ThinkSystem Digital 2x1x16 KVM Switch is approximately 500KB in size. The following chart describes the time required to retrieve ThinkSystem Digital 2x1x16 KVM Switch’s applet at different network speeds:

<table>
<thead>
<tr>
<th>Network Speed</th>
<th>Time Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>100Mbps</td>
<td>0.05 seconds</td>
</tr>
<tr>
<td>60Mbps</td>
<td>0.08 seconds</td>
</tr>
<tr>
<td>10Mbps</td>
<td>0.4 seconds</td>
</tr>
<tr>
<td>5Mbps</td>
<td>0.8 seconds</td>
</tr>
<tr>
<td>512Kbps</td>
<td>8 seconds</td>
</tr>
</tbody>
</table>

How do I access servers connected to ThinkSystem Digital 2x1x16 KVM Switch if the network ever becomes unavailable?
You can access servers at the rack or via a telephone or wireless modem. ThinkSystem Digital 2x1x16 KVM Switch offers a dedicated modem port for attaching to an external telephone modem. The THINKSYSTEM DIGITAL 2X1X16 KVM Switch can also connect to Sierra Wireless Cellular modems via USB. We recommend the Sierra Wireless ES450 modem.

Do you have a Windows KVM Client?
Yes. We have a native .NET Windows Client called the Active KVM Client (AKC) for use on Windows systems. This KVM Client does not utilize Java.

Do you have a Non-Windows KVM Client?
Yes, there are two non-windows clients: the Java-based VKC and the Java-free HKC.

Do you have a HTML5 KVM Client?
Yes, the new HTML KVM Client runs in the browser and does not use a downloaded applet or a browser plugin.

Do your KVM Clients have multi-language support?
Yes. The ThinkSystem Digital 2x1x16 KVM Switch’s remote HTML User Interface and the AKC and VKC Clients support the Japanese, Simplified Chinese and Traditional Chinese languages.

How can I minimize my use of the Active KVM Client (AKC), which runs on Windows platforms does not use Java. AKC is a full-featured KVM Client with the same features.
Java? | as the Java-based VKC KVM Client. Launch AKC via <IP Address>/akc. A new HTML KVM Client is now available for Linux and Mac platforms. For customers looking to minimize their use of Java, this KVM Client runs in the browser and does not utilize Java or .NET. The HTML KVM Client supports virtual media and audio output. For Java-free administration of the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH (no server access), launch via <IP Address>/admin

Do your KVM Clients support dual monitors? | Yes, both AKC and VKC support it. For customers wishing to enhance their productivity by using multiple monitors on their desktops, the ThinkSystem Digital 2x1x16 KVM Switch can launch KVM sessions to multiple monitors, either in full screen or standard modes.

Do you support servers with dual video cards? | Yes, servers with dual video cards are supported via AKC and VKC with an extended desktop configuration available to the remote user.

**Universal Virtual Media**

| Which ThinkSystem Digital 2x1x16 KVM Switch supports virtual media? | All ThinkSystem Digital 2x1x16 KVM Switch supports virtual media.

| Which types of virtual media does the ThinkSystem Digital 2x1x16 KVM Switch support? | ThinkSystem Digital 2x1x16 KVM Switch supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives and ISO images.

| What is required for virtual media? | A ThinkSystem Digital 2x1x16 KVM Switch virtual media dongle is required. There are two VGA-based dongles: the THINKSYSTEM S-USB CABLE FOR DIGITAL KVM and the THINKSYSTEM D-USB CABLE FOR DIGITAL KVM.

The THINKSYSTEM S-USB CABLE FOR DIGITAL KVM has a single USB connector and is for customers who will use virtual media at the operating system level.

The THINKSYSTEM D-USB CABLE FOR DIGITAL KVM has dual USB connectors and should be purchased by customers who wish to utilize virtual media at the operating system and BIOS level. The THINKSYSTEM D-USB CABLE FOR DIGITAL KVM is also required for smart card authentication and digital audio.

Both support virtual media sessions to target servers supporting the USB 2.0 interface. These dongles support Absolute Mouse Synchronization™ as well as remote firmware updates.

| Is virtual media secure? | Yes. Virtual media sessions are secured using 256-bit AES or 128-bit AES encryption.

| Which KVM Clients support Virtual Media? | The existing VKC and AKC KVM Clients support the full range of virtual media options. The new HKC supports remote and local ISO images.
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does virtual media really support audio?</td>
<td>Yes. Audio playback and recording to a server connected to the ThinkSystem Digital 2x1x16 KVM Switch is supported. You can listen to sounds and audio playing on a remote server in the data center using the speakers connected to your desktop PC or laptop. You can also record on the remote server using a microphone connected to your PC or laptop. THINKSYSTEM D-USB CABLE FOR DIGITAL KVM is required.</td>
</tr>
<tr>
<td>What is a USB profile?</td>
<td>Certain servers require a specifically configured USB interface for USB-based services such as virtual media. The USB profile tailors the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH’s USB interface to the server to accommodate these server-specific characteristics.</td>
</tr>
<tr>
<td>Why would I use a USB profile?</td>
<td>USB profiles are most often required at the BIOS level where there may not be full support for the USB specification when accessing virtual media drives. However, profiles are sometimes used at the OS level, for example, for mouse synchronization for Macintosh and Linux servers.</td>
</tr>
<tr>
<td>How is a USB profile used?</td>
<td>Individual ports or groups of ports can be configured by the administrator to use a specific USB profile in the THINKSYSTEM DIGITAL 2X1X16 KVM Switch’s port configuration page. A USB profile can also be selected in the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH Client when required. See the user guide for more information.</td>
</tr>
<tr>
<td>Do I always need to set a USB profile when I use virtual media?</td>
<td>No. In many cases, the default USB profile is sufficient when using virtual media at the OS level or operating at the BIOS level without accessing virtual media.</td>
</tr>
<tr>
<td>What profiles are available? Where can I find more information?</td>
<td>Consult the user guide for the available profiles and for more information.</td>
</tr>
</tbody>
</table>

### Bandwidth and KVM-over-IP Performance

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How is bandwidth used in KVM-over-IP systems?</td>
<td>ThinkSystem Digital 2x1x16 KVM Switch offers high performance KVM-over-IP technology — totally new video processing that provides flexible, high performance video, efficient use of bandwidth and anytime/anywhere access via LAN, WAN or Internet. The ThinkSystem Digital 2x1x16 KVM Switch digitizes compresses and encrypts the keyboard, video and mouse signals from the target server and transmits IP packets over the IP network to the remote KVM client to create the remote session to the user. The THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH provides an at-the-rack experience based on its industry-leading video processing algorithms. Screen changes, i.e., video accounts for the majority of the bandwidth used — and keyboard and mouse activity are significantly less. It is important to note that bandwidth is only used when the user is active. The amount of bandwidth used is based on the amount of change</td>
</tr>
</tbody>
</table>
### Appendix D: FAQ

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>to the server’s video display screen.</td>
<td>If there are no changes to the video — the user is not interacting with the server—there is generally little or no bandwidth used. If the user moves the mouse or types a character, then there is a small amount of bandwidth used. If the display is running a complex screen saver or playing a video, then there can be a larger amount of bandwidth used.</td>
</tr>
<tr>
<td>How does bandwidth affect KVM-over-IP performance?</td>
<td>In general, there is a trade-off between bandwidth and performance. The more bandwidth available, the better performance can be. In limited bandwidth environments, performance can degrade. The ThinkSystem Digital 2x1x16 KVM Switch has been optimized to provide strong performance in a wide variety of environments.</td>
</tr>
<tr>
<td>What factors affect bandwidth?</td>
<td>There are many factors that determine how much bandwidth will be used. The primary factor, noted above, is the amount of change in the target server’s video display. This is dependent on the user’s task and actions. Other factors include the server’s video resolution, networking speed and characteristics, client PC resources and video card noise.</td>
</tr>
</tbody>
</table>
| How much bandwidth does THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH use for common tasks? | Bandwidth primarily depends on the user’s tasks and actions. The more the server’s video screen changes, the more bandwidth are utilized. Here are some example bandwidth measurements:  
  - Idle Desktop: 1-2 KBps  
  - Move Mouse: 7-13 KBps  
  - Typing: 5-11 KBps  
  - Drag Shortcut: 33-50 KBps  
  - Scroll Settings: 450-1200 KBps  
  - Screensaver: 1000-1500 KBps  
  - Drag Image: 740-1200 KBps  
  - Watch Video: 2200-2500 KBps  
  Bandwidth does vary according to the application, screen resolution and the video settings of the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH. |
| How do I optimize performance and bandwidth?                            | THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH provides a variety of settings in our remote clients for the user to optimize bandwidth and performance. The default settings will provide an at-the-rack level of performance in standard LAN/WAN environments with economical use of bandwidth. The Connection Properties dialog box can be used to manage the tradeoff between video quality and low bandwidth. With three simple settings you can operate in a wide variety of environments.  
  - Optimize For. Use this setting to configure the video engine for standard IT/computer applications or for video/broadcast  

<table>
<thead>
<tr>
<th><strong>Appendix D: FAQ</strong></th>
</tr>
</thead>
</table>

- Video Mode. Move the slider to the left for the highest possible video quality and to the right for the least amount of bandwidth.
- Noise Filter. In most cases, the default setting will work best, however you can move to the left for more responsive video and to the right for lower bandwidth.

For slow Internet connections, the use of 8-bit color or lower bit depths can reduce bandwidth and improve performance.

Other tips to decrease bandwidth include:
- Use a solid desktop background instead of a complex image
- Disable screensavers
- Use a lower video resolution on the target server
- Uncheck the “Show window contents while dragging” option in Windows
- Use simple images, themes and desktops (e.g., Windows Classic)

<table>
<thead>
<tr>
<th><strong>I want to connect over the Internet. What type of performance should I expect?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>It depends on the bandwidth and latency of the Internet connection between your remote client and the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH. With a cable modem or high speed DSL connection, your performance can be very similar to a LAN/WAN connection. For lower speed links, use the suggestions above to improve performance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>I have a high bandwidth environment. How can I optimize performance?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The default settings will work well. You can move the Connection Properties settings to the left for increased video performance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>What is the maximum remote (over IP) video resolution supported?</strong></th>
</tr>
</thead>
</table>
| The ThinkSystem Digital 2x1x16 KVM Switch is the first and only KVM-over-IP switch to support full high definition (HD) remote video resolution — 1920x1200 at frame rates up to 30 frames per second with digital audio.  
In addition, popular widescreen formats are supported, including 1920x1080, 1920x1200, 1600x1200, 1680x1050 and 1440x900, so remote users can work with today’s higher resolution monitors. |

<table>
<thead>
<tr>
<th><strong>How much bandwidth is used for audio?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>It depends on the type of audio format used, but to listen to CD quality audio, approximately 1.5 Mbps is used.</td>
</tr>
</tbody>
</table>

**Ethernet and IP Networking**

<table>
<thead>
<tr>
<th><strong>What is the speed of ThinkSystem Digital 2x1x16 KVM Switch’s Ethernet interfaces?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ThinkSystem Digital 2x1x16 KVM Switch supports gigabit as well as 10/100 Ethernet. THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto detected or manually set) and optionally with independent IP addresses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Can I access ThinkSystem Digital 2x1x16 KVM Switch over Ethernet?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes. ThinkSystem Digital 2x1x16 KVM Switch not only uses standard Ethernet, but also very conservative bandwidth with very high quality</td>
</tr>
<tr>
<td>Question</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>a wireless connection?</td>
</tr>
<tr>
<td>Does the ThinkSystem Digital 2x1x16 KVM Switch offer dual gigabit Ethernet ports to provide redundant failover or load balancing?</td>
</tr>
<tr>
<td>Can I use ThinkSystem Digital 2x1x16 KVM Switch with a VPN?</td>
</tr>
<tr>
<td>Can I use THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH with a proxy server?</td>
</tr>
<tr>
<td>How many TCP ports must be open on my firewall in order to enable network access to ThinkSystem Digital 2x1x16 KVM Switch?</td>
</tr>
<tr>
<td>Are these ports configurable?</td>
</tr>
<tr>
<td>Can ThinkSystem Digital 2x1x16 KVM Switch be used with Citrix®?</td>
</tr>
<tr>
<td>Can the ThinkSystem Digital 2x1x16 KVM Switch use DHCP?</td>
</tr>
<tr>
<td>I'm having problems connecting to the ThinkSystem Digital 2x1x16 KVM Switch over my IP network. What could be the problem?</td>
</tr>
</tbody>
</table>
the appropriate choice for its network.

- Duplicate IP address. If the IP address of the ThinkSystem Digital 2x1x16 KVM Switch is the same as another device, network connectivity may be inconsistent.
- Port 5000 conflicts. If another device is using port 5000, the ThinkSystem Digital 2x1x16 KVM Switch default port must be changed (or the other device must be changed).
- When changing the IP address of a ThinkSystem Digital 2x1x16 KVM Switch, or swapping in a new ThinkSystem Digital 2x1x16 KVM Switch, sufficient time must be allowed for its IP and Mac® addresses to be known throughout the Layer 2 and Layer 3 networks.

### IPv6 Networking

<table>
<thead>
<tr>
<th>What is IPv6?</th>
<th>IPv6 is the acronym for Internet Protocol Version 6. IPv6 is the “next generation” IP protocol which will replace the current IP Version 4 (IPv4) protocol. IPv6 addresses a number of problems in IPv4, such as the limited number of IPv4 addresses. It also improves IPv4 in areas such as routing and network auto-configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years. IPv6 treats one of the largest headaches of an IP network from the administrator’s point of view – configuring and maintaining an IP network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why does ThinkSystem Digital 2x1x16 KVM Switch support IPv6 networking?</td>
<td>Many customers require IPv6-compatible products.</td>
</tr>
<tr>
<td>What is “dual stack” and why is it required?</td>
<td>Dual stack is the ability to simultaneously support both IPv4 and IPv6 protocols. Given the gradual transition from IPv4 to IPv6, dual stack is a fundamental requirement for IPv6 support.</td>
</tr>
<tr>
<td>How do I enable IPv6 on the ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>Use the “Network Settings” page, available from the “Device Settings” tab. Enable IPv6 addressing and choose manual or auto-configuration. Consult the user guide for more information.</td>
</tr>
<tr>
<td>What if I have an external server with an IPv6 address that I want to use with my ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>The ThinkSystem Digital 2x1x16 KVM Switch can access external servers via their IPv6 addresses, for example, an SNMP manager, syslog server or LDAP server. Using the ThinkSystem Digital 2x1x16 KVM Switch’s dual-stack architecture, these external servers can be accessed via: (1) an IPv4 address, (2) IPv6 address or (3) hostname. So, the ThinkSystem Digital 2x1x16 KVM Switch supports the mixed IPv4/IPv6 environment many customers will have.</td>
</tr>
</tbody>
</table>
## Appendix D: FAQ

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What if my network doesn’t support IPv6?</td>
<td>The ThinkSystem Digital 2x1x16 KVM Switch’s default networking is set at the factory for IPv4 only. When you are ready to use IPv6, then follow the above instructions to enable IPv4/IPv6 dual-stack operation.</td>
</tr>
<tr>
<td>Where can I get more information on IPv6?</td>
<td>See <a href="http://www.ipv6.org">www.ipv6.org</a> for general information on IPv6. The ThinkSystem Digital 2x1x16 KVM Switch user guide describes the ThinkSystem Digital 2x1x16 KVM Switch’s support for IPv6.</td>
</tr>
</tbody>
</table>

### Servers

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does ThinkSystem Digital 2x1x16 KVM Switch depend on a Windows server to operate?</td>
<td>Absolutely not. Because users depend on the KVM infrastructure to always be available in any scenario whatsoever (as they will likely need to use the KVM infrastructure to fix problems), ThinkSystem Digital 2x1x16 KVM Switch is designed to be completely independent from any external server.</td>
</tr>
<tr>
<td>What should I do to prepare a server for connection to ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>Set the mouse parameter options to provide users with the best mouse synchronization and turn off screensavers and any power management features that affect screen display.</td>
</tr>
<tr>
<td>What about mouse synchronization?</td>
<td>In the past, KVM-over-IP mouse synchronization was a frustrating experience. The ThinkSystem Digital 2x1x16 KVM Switch’s Absolute Mouse Synchronization provides for a tightly synchronized mouse without requiring server mouse setting changes on Windows and Apple® Mac servers. For other servers, the Intelligent Mouse mode or the speedy, single mouse mode can be used to avoid changing the server mouse settings.</td>
</tr>
</tbody>
</table>

### Blade Servers

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can I connect blade servers to the ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>Yes. ThinkSystem Digital 2x1x16 KVM Switch supports popular blade server models from many of the leading blade server manufacturers.</td>
</tr>
<tr>
<td>Which blade servers are supported?</td>
<td>The following models are supported: HP BladeSystem c3000 and c7000; IBM BladeCenter® H and E; and Cisco UCS B- Series.</td>
</tr>
<tr>
<td>Which types of access and control are available?</td>
<td>The ThinkSystem Digital 2x1x16 KVM Switch provides automated and secure KVM access: (1) at the rack, (2) remotely over IP, (3) by modem.</td>
</tr>
<tr>
<td>Do I have to use hotkeys to switch between blades?</td>
<td>Some blade servers require you to use hotkeys to switch between blades. With the ThinkSystem Digital 2x1x16 KVM Switch, you don’t have to use these hotkeys. Just click on the name of the blade server, and the ThinkSystem Digital 2x1x16 KVM Switch will automatically switch to that blade without the explicit use of the hotkey.</td>
</tr>
<tr>
<td>Can I access the blade server’s management module?</td>
<td>Yes. You can define the URL of the management module and access it from the ThinkSystem Digital 2x1x16 KVM Switch. If configured, one-click access is available.</td>
</tr>
</tbody>
</table>
### How many blade servers can I connect to a ThinkSystem Digital 2x1x16 KVM Switch?

For performance and reliability reasons, you can connect up to eight blade chassis to a ThinkSystem Digital 2x1x16 KVM Switch, regardless of model. We recommend only connecting up to two times the number of remote connections supported by the device. For example, with a ThinkSystem Digital 2x1x16 KVM Switch with two remote channels, we recommend connecting up to four blade server chassis. You can, of course, connect individual servers to the remaining server ports.

### Is virtual media supported?

This depends on the blade server. HP blades can support virtual media. The IBM BladeCenter (except for BladeCenter T) supports virtual media if configured appropriately. A virtual media THINKSYSTEM USB CABLE – THINKSYSTEM S-USB CABLE FOR DIGITAL KVM or THINKSYSTEM D-USB CABLE FOR DIGITAL KVM – must be used.

### Is Absolute Mouse Synchronization supported?

Servers with internal KVM switches inside the blade chassis typically do not support absolute mouse technology. For HP blade, a THINKSYSTEM USB CABLE can be connected to each blade, so Absolute Mouse Synchronization is supported.

### Is blade access secure?

Yes. Blade access uses all of the standard ThinkSystem Digital 2x1x16 KVM Switch security features such as 128-bit or 256-bit encryption. In addition, there are blade-specific security features such as per blade access permissions and hotkey-blocking that eliminates unauthorized access.

### Installation

<table>
<thead>
<tr>
<th>Besides the unit itself, what do I need to order from to install ThinkSystem Digital 2x1x16 KVM Switch?</th>
<th>Each server that connects to ThinkSystem Digital 2x1x16 KVM Switch requires a THINKSYSTEM USB CABLE that connects directly to the keyboard, video and mouse ports of the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which kind of Cat5 cabling should be used in my installation?</td>
<td>ThinkSystem Digital 2x1x16 KVM Switch can use any standard UTP (unshielded twisted pair) cabling, whether Cat5, Cat5e or Cat6. Often in our manuals and marketing literature, will simply say “Cat5” cabling for short. In actuality, any brand UTP cable will suffice for the ThinkSystem Digital 2x1x16 KVM Switch.</td>
</tr>
<tr>
<td>Which types of servers and PCs can be connected to ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>The ThinkSystem Digital 2x1x16 KVM Switch is completely vendor independent. Any server with standards-compliant keyboard, video and mouse ports can be connected. In addition, servers with serial ports can be controlled using the THINKSYSTEM USB CABLEs.</td>
</tr>
<tr>
<td>How do I connect servers to ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>Servers that connect to the ThinkSystem Digital 2x1x16 KVM Switch require a THINKSYSTEM USB CABLE, which connects directly to the keyboard, video and mouse ports of the server. Connect each THINKSYSTEM USB CABLE to ThinkSystem Digital 2x1x16 KVM Switch using standard UTP (unshielded twisted pair) cable such as Cat5, Cat5e or Cat6.</td>
</tr>
</tbody>
</table>
### Appendix D: FAQ

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How far can my servers be from ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>In general, servers can be up to 150 feet (45 m) away from the ThinkSystem Digital 2x1x16 KVM Switch, depending on the type of server. (See user manual.) For the THINKSYSTEM S-USB CABLE FOR DIGITAL KVM THINKSYSTEM USB CABLEs that supports virtual media and Absolute Mouse Synchronization, a 100-foot (30 m) or less range is recommended.</td>
</tr>
<tr>
<td>Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to ThinkSystem Digital 2x1x16 KVM Switch from locking up when I switch away from them?</td>
<td>Each THINKSYSTEM USB CABLE acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation).</td>
</tr>
<tr>
<td>Are there any agents that must be installed on servers connected to ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>Servers connected to ThinkSystem Digital 2x1x16 KVM Switch do not require any software agents to be installed because ThinkSystem Digital 2x1x16 KVM Switch connects directly to the servers' physical keyboard, video and mouse ports.</td>
</tr>
<tr>
<td>What happens if I disconnect a server from ThinkSystem Digital 2x1x16 KVM Switch and reconnect it to another ThinkSystem Digital 2x1x16 KVM Switch unit, or connect it to a different port on the same ThinkSystem Digital 2x1x16 KVM Switch unit?</td>
<td>ThinkSystem Digital 2x1x16 KVM Switch will automatically update the server port names when servers are moved from port to port. Furthermore, this automatic update does not just affect the local access port, but propagates to all remote clients.</td>
</tr>
</tbody>
</table>

### Local Port

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can I access my servers directly from the rack?</td>
<td>Yes. At the rack, ThinkSystem Digital 2x1x16 KVM Switch functions just like a traditional KVM switch — allowing control of up to 16 servers using a single keyboard, monitor and mouse. You can switch between servers by the browser-based user interface or via a hotkey.</td>
</tr>
<tr>
<td>Can I consolidate the local ports of multiple THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH s?</td>
<td>Yes. You can connect the tiering ports of multiple THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH switches to another THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH using the “tiering” feature of the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH. You can then access the servers connected to your THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH devices from a single point in the data center via a consolidated port list.</td>
</tr>
<tr>
<td>When I am using the local port,</td>
<td>No. The ThinkSystem Digital 2x1x16 KVM Switch local port has a</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>do I prevent other users from accessing servers remotely?</td>
<td>completely independent access path to the servers. This means a user can access servers locally at the rack – without compromising the number of users that access the rack remotely at the same time.</td>
</tr>
<tr>
<td>Can I use a USB keyboard or mouse at the local port?</td>
<td>Yes. The ThinkSystem Digital 2x1x16 KVM Switch has USB keyboard and mouse ports on the local port. ThinkSystem Digital 2x1x16 KVM Switch switches do not have PS/2 local ports. Customers with PS/2 keyboards and mice should utilize a PS/2 to USB adapter.</td>
</tr>
<tr>
<td>Is there an onscreen display (OSD) for local, at-the-rack access?</td>
<td>Yes, but ThinkSystem Digital 2x1x16 KVM Switch’s at-the-rack access goes way beyond conventional OSDs. Featuring the industry’s first browser-based DVI interface for at-the-rack access, ThinkSystem Digital 2x1x16 KVM Switch’s local port uses the same interface for local and remote access. Moreover, most administrative functions are available at the rack.</td>
</tr>
<tr>
<td>How do I select between servers while using the local port?</td>
<td>The local port displays the connected servers using the same user interface as the remote client. Users connect to a server with a simple click of the mouse or via a hotkey.</td>
</tr>
<tr>
<td>How do I ensure that only authorized users can access servers from the local port?</td>
<td>Users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that: If the ThinkSystem Digital 2x1x16 KVM Switch is configured to interact with an external RADIUS, LDAP or Active Directory® server, users attempting to access the local port will authenticate against the same server. If the external authentication servers are unavailable, ThinkSystem Digital 2x1x16 KVM Switch ails over to its own internal authentication database.</td>
</tr>
</tbody>
</table>

**Dual Power Supplies**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does ThinkSystem Digital 2x1x16 KVM Switch have a dual power option?</td>
<td>Yes. All ThinkSystem Digital 2x1x16 KVM Switch models come equipped with dual AC inputs and power supplies with automatic failover. Should one of the power inputs or power supplies fail, then the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH will automatically switch to the other.</td>
</tr>
<tr>
<td>Does the power supply used by ThinkSystem Digital 2x1x16 KVM Switch automatically detect voltage settings?</td>
<td>Yes. ThinkSystem Digital 2x1x16 KVM Switch’s power supply can be used in AC voltage ranges from 100–240 volts, at 50–60 Hz.</td>
</tr>
<tr>
<td>If a power supply or input fails, will I be notified?</td>
<td>The ThinkSystem Digital 2x1x16 KVM Switch front panel LED will notify the user of a power failure. An entry will also be sent to the audit log and displayed on the remote client user interface. If configured by the administrator, then SNMP or syslog events will be generated.</td>
</tr>
</tbody>
</table>
### Local Port Consolidation, Tiering and Cascading

**How do I physically connect multiple ThinkSystem Digital 2x1x16 KVM Switch devices together into one solution?**

To physically connect multiple THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH devices together for consolidated local access, you can connect the tiering ports of multiple “tiered” (or “cascaded”) THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH switches to a “base” switch using the tiering ports of the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH. You can then access the servers connected to your switch devices from a single point in the data center via a consolidated port list.

The tiering port must be used to connect the tiered THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH switch to the base switch.

Access via the consolidated port list is available in the data center or even from a remote PC. All servers connected to the tiered THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH’s can be accessed via a hierarchical port list or via search (with wildcards).

Virtual media, smart card, audio and blade server access via tiered access is not supported with Tiering.

### Security

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Is the ThinkSystem Digital 2x1x16 KVM Switch FIPS 140-2 Certified?</strong></td>
<td>The ThinkSystem Digital 2x1x16 KVM Switch uses an embedded FIPS 140-2 validated cryptographic module running on a Linux platform per FIPS 140-2 implementation guidelines. This cryptographic module is used for encryption of KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.</td>
</tr>
<tr>
<td><strong>What kind of encryption does ThinkSystem Digital 2x1x16 KVM Switch use?</strong></td>
<td>ThinkSystem Digital 2x1x16 KVM Switch uses industry-standard (and extremely secure) 256-bit AES, 128-bit AES or 128-bit encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and ThinkSystem Digital 2x1x16 KVM Switch that is not completely secured by encryption.</td>
</tr>
<tr>
<td><strong>Does ThinkSystem Digital 2x1x16 KVM Switch support AES encryption as recommended by the U.S. government’s NIST and FIPS standards?</strong></td>
<td>Yes. The ThinkSystem Digital 2x1x16 KVM Switch utilizes the Advanced Encryption Standard (AES) for added security. 256-bit and 128-bit AES is available. The weaker RC4 encryption is no longer supported. AES is a U.S. government-approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.</td>
</tr>
<tr>
<td><strong>Does ThinkSystem Digital 2x1x16 KVM Switch allow encryption of video data? Or does it only encrypt keyboard and mouse data?</strong></td>
<td>Unlike competing solutions, which only encrypt keyboard and mouse data, ThinkSystem Digital 2x1x16 KVM Switch does not compromise security – it allows encryption of keyboard, mouse, video and virtual media data.</td>
</tr>
<tr>
<td>**How does ThinkSystem Digital 2x1x16 KVM **</td>
<td>Through a very simple configuration, ThinkSystem Digital 2x1x16 KVM **</td>
</tr>
<tr>
<td><strong>2x1x16 KVM Switch integrate with external authentication servers such as Active Directory, RADIUS or LDAP?</strong></td>
<td>Switch can be set to forward all authentication requests to an external server such as LDAP, Active Directory or RADIUS. For each authenticated user, ThinkSystem Digital 2x1x16 KVM Switch receives from the authentication server the user group to which that user belongs. ThinkSystem Digital 2x1x16 KVM Switch then determines the user’s access permissions depending on the user group to which he or she belongs.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>How are usernames and passwords stored?</strong></td>
<td>Should ThinkSystem Digital 2x1x16 KVM Switch’s internal authentication capabilities be used, all sensitive information, such as usernames and passwords, is stored in an encrypted format. Literally no one, including technical support or product engineering departments, can retrieve those usernames and passwords.</td>
</tr>
<tr>
<td><strong>Does ThinkSystem Digital 2x1x16 KVM Switch support strong passwords?</strong></td>
<td>Yes. The ThinkSystem Digital 2x1x16 KVM Switch has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.</td>
</tr>
<tr>
<td><strong>Can I upload my own digital certificate to the ThinkSystem Digital 2x1x16 KVM Switch?</strong></td>
<td>Yes. Customers can upload self-signed or certificate authority-provided digital certificates to the ThinkSystem Digital 2x1x16 KVM Switch for enhanced authentication and secure communication. We recommend this for fewer browser messages and higher security.</td>
</tr>
<tr>
<td><strong>Does the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH support a configurable security banner?</strong></td>
<td>Yes. For government, military and other security-conscious customers requiring a security message before user login, the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH can display a user-configurable banner message and optionally require acceptance.</td>
</tr>
<tr>
<td><strong>My security policy does not allow the use of standard TCP port numbers. Can I change them?</strong></td>
<td>Yes. For customers wishing to avoid the standard TCP/IP port numbers to increase security, the ThinkSystem Digital 2x1x16 KVM Switch allows the administrator to configure alternate port numbers.</td>
</tr>
<tr>
<td><strong>Is the SSL protocol supported?</strong></td>
<td>SSLv1, SSLv2 and SSLv3 are disabled for security reasons. The more secure TLS protocol is used. Furthermore, the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH administrator has control over which TLS versions can be used.</td>
</tr>
<tr>
<td><strong>Is two factor authentications supported to log into the THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH?</strong></td>
<td>Yes, RSA SecureID is supported via RADIUS for two factor authentication to log into the ThinkSystem Digital 2x1x16 KVM Switch.</td>
</tr>
</tbody>
</table>

**Smart Cards and CAC Authentication**

| **Does ThinkSystem Digital 2x1x16 KVM Switch support smart card and CAC** | Yes. Smart cards and DoD common access cards [CAC] authentication to target servers is supported. |
## Authentication

**What is CAC?**

Mandated by Homeland Security Presidential Directive 12 (HSPD-12), CAC is a type of smart card created by the U.S. government and used by U.S. military and government staff. The CAC card is a multi-technology, multipurpose card; the goal is to have a single identification card. For more information, see the FIPS 201 standards.

<table>
<thead>
<tr>
<th>Which THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH models support smart cards/CAC?</th>
<th>All ThinkSystem Digital 2x1x16 KVM Switch is supported.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do enterprise and SMB customers use smart cards, too?</td>
<td>Yes. However, the most aggressive deployment of smart cards is in the U.S. federal government.</td>
</tr>
<tr>
<td>Which THINKSYSTEM USB CABLEs support smart card/CAC?</td>
<td>THINKSYSTEM D-USB CABLE FOR DIGITAL KVM. The THINKSYSTEM S-USB CABLE FOR DIGITAL KVM does not.</td>
</tr>
<tr>
<td>Which smart card readers are supported?</td>
<td>The required reader standards are USB CCID and PC/SC. Consult the user documentation for a list of certified readers and more information.</td>
</tr>
</tbody>
</table>

## Manageability

**Can ThinkSystem Digital 2x1x16 KVM Switch be remotely managed and configured via Web browser?**

Yes. ThinkSystem Digital 2x1x16 KVM Switch can be completely configured remotely via Web browser. Besides the initial setting of ThinkSystem Digital 2x1x16 KVM Switch’s IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and ThinkSystem Digital 2x1x16 KVM Switch’s default IP address, you can even configure the initial settings via Web browser.)

Java is not required for THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH administration if launched using <IP Address>/admin.

**Can I back up and restore ThinkSystem Digital 2x1x16 KVM Switch’s configuration?**

Yes. ThinkSystem Digital 2x1x16 KVM Switch’s device and user configurations can be completely backed up for later restoration in the event of a catastrophe.

**What auditing or logging does ThinkSystem Digital 2x1x16 KVM Switch offer?**

For complete accountability, ThinkSystem Digital 2x1x16 KVM Switch logs all major user events with a date and time stamp. For instance, reported events include: user login, user logout, user access of a particular server, unsuccessful login, configuration changes, etc.

**Can ThinkSystem Digital 2x1x16 KVM Switch integrate with syslog?**

Yes. In addition to ThinkSystem Digital 2x1x16 KVM Switch’s own internal logging, ThinkSystem Digital 2x1x16 KVM Switch can send all logged events to a centralized syslog server.

**Can ThinkSystem Digital 2x1x16 KVM Switch integrate**
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>with SNMP?</td>
<td>SNMP traps to SNMP management systems. SNMP v2 and v3 are supported.</td>
</tr>
<tr>
<td>Can THINKSYSTEM DIGITAL 2X1X16 KVM SWITCH send events via Email?</td>
<td>Yes, the THINKSYSTEM DIGITAL 2X1X16 KVM Switch can send events via email to an administrator. The administrator can configure the specific events to be sent by email.</td>
</tr>
<tr>
<td>Can an administrator log-off a user?</td>
<td>Yes, administrators can view which users are logged into which ports and can log-off a user from a specific port or from the device if required.</td>
</tr>
<tr>
<td>Can ThinkSystem Digital 2x1x16 KVM Switch’s internal clock be synchronized with a timeserver?</td>
<td>Yes. ThinkSystem Digital 2x1x16 KVM Switch supports the industry-standard NTP protocol for synchronization with either a corporate timeserver, or with any public timeserver (assuming that outbound NTP requests are allowed through the corporate firewall).</td>
</tr>
</tbody>
</table>

### Documentation and Support

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where do I find documentation on the ThinkSystem Digital 2x1x16 KVM Switch?</td>
<td>Check the Lenovo Support page for documentation.</td>
</tr>
<tr>
<td>What is ThinkSystem Digital 2x1x16 KVM Switch’s default IP address?</td>
<td>192.168.0.192</td>
</tr>
<tr>
<td>What is ThinkSystem Digital 2x1x16 KVM Switch’s default username and default password?</td>
<td>The ThinkSystem Digital 2x1x16 KVM Switch’s default username is “admin” and the default password is “lenovo “ [all lower case]. However, for the highest level of security, the ThinkSystem Digital 2x1x16 KVM Switch forces the administrator to change the default password when the unit is first booted up.</td>
</tr>
<tr>
<td>I changed and subsequently forgot ThinkSystem Digital 2x1x16 KVM Switch’s administrative password; can you retrieve it for me?</td>
<td>ThinkSystem Digital 2x1x16 KVM Switch contains a hardware reset button that can be used to factory reset the device, which will reset the administrative password on the device to the default password.</td>
</tr>
</tbody>
</table>
Index

A

Absolute • 99
Absolute Mouse Synchronization • 58
Access a Virtual Media Drive on a Client Computer • 30
Access and Copy Connection Information • 44, 47
Access Connection Properties • 43
Accessing a Target Server • 121
Active KVM Client (AKC) Help • 4, 81
Active System Partition • 35
Active System Partitions • 33
Add New Macro • 94
Adding Attributes to the Class • 135
Additional Security Warnings • 6, 8
Adjust Audio Settings • 81
Adjusting Capture and Playback Buffer Size (Audio Settings) • 81
Adjusting Video Settings • 54
AKC Supported Browsers • 82
AKC Supported Microsoft .NET Framework • 82
AKC Supported Operating Systems • 82
Allow Cookies • 82
Allow Pop-Ups • 5
Audio in a Mac Environment • 151
Audio Level • 76, 150
Audio Menu • 112
Audio Playback and Capture
  Recommendations and Requirements • 76, 79, 150
Audio Settings • 113
Authentication When Accessing a Smart Card Reader • 72
Auto Sense • 104
Auto-Sense Video Settings • 53

B

Bandwidth Requirements • 76, 150
Blade Chassis - Port Access Page • 18
Build a New Macro • 50

C

Calibrating Color • 54
Certified Modems • 152
Changing a Password • 119
CIMs Required for Virtual Media • 27
Clear Video Settings Cache • 54, 105, 108
Client Launch Settings • 64
Collect a Diagnostic Snapshot from VKC, VKCS, and AKC • 68
Collecting a Diagnostic Snapshot of the Target • 67
Color Accuracy • 44, 88
Color Calibration • 105
Conditions when Read/Write is Not Available • 29, 31
Configure Local Console Scan Settings • 66, 126, 127
Configure Port Scan • 66
Configuring Connection Properties • 43, 47
Configuring Port Scan Settings in VKC/VKCS and AKC • 66, 116, 118, 127
Connect • 20
Connect Audio • 112
Connect Drive Permissions (Linux) • 34
Connect Drive Permissions (Mac) • 36
Connect Files and Folders • 109
Connect ISO • 110
Connect Key Examples • 123
Connect to a Digital Audio Device • 79
Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC) • 42, 84
Connect to Virtual Media • 71
Connecting and Disconnecting from a Digital Audio Device • 78, 79
Connecting and Disconnecting from Virtual Media • 30
Connecting to Multiple Targets from a Single Remote Client • 78, 79
Connection Info • 91
Connection Information • 47
Connection Properties • 87
Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional) • 12
Creating a New Attribute • 134

D
Default Connection Properties • 87, 91
Default Connection Property Settings - Optimized for Best Performance • 43
Delete a Macro • 95
Dell Chassis Cable Lengths and Video Resolutions • 146
Digital Audio • 74
Digital Audio VKC and AKC Icons • 75
Dimensions and Physical Specifications • 140
Disable ‘Protected Mode’ • 83
Disconnect • 21
Disconnect from an Audio Device • 80
Disconnect from Virtual Media Drives • 32
Drive Partitions • 33, 35
Dual Mouse Modes • 58
Dual Port Video Groups - Port Access Page • 18

E
Editing rciusergroup Attributes for User Members • 137
Enable AKC Download Server Certificate Validation • 83
Enter Intelligent Mouse Mode • 58
Events Captured in the Audit Log and Syslog • 158
Example 1
Import the Certificate into the Browser • 9, 11
Example 2
Add the ThinkSystem Digital KVM Switch to Trusted Sites and Import the Certificate • 10
Export Macros • 52

F
FAQ • 159
From LDAP/LDAPS • 133
From Microsoft Active Directory • 133
Full Screen Mode • 71

G
General Settings • 61
Get Started Using ThinkSystem Digital KVM Switch • 5

H
Hardware • 1, 140
HTML KVM Client (HKC) Help • 85

I
Import and Export Macros • 94, 96
Import Macros • 51
Importing and Exporting Macros • 51
Include ThinkSystem Digital KVM Switch IP Address in ‘Trusted Sites Zone’ • 83
Input Menu • 92
Installing a Certificate • 6, 8
Intelligent • 99
Intelligent Mouse Mode • 58
Intelligent Mouse Synchronization Conditions • 59, 99, 102
Introduction • 1

J
Java Validation and Access Warning • 6, 7
JRE Requirements and Browser Considerations for Mac • 156

K
Keyboard • 49
Keyboard Layout • 92
Keyboard Limitations • 63
Keyboard Macros • 49
KVM Client Applications • 4
KVM Client Launching • 38
KVM Clients • 14, 38

L
Left Panel • 23
Local Console Smart Card Access • 72, 128
Local Console USB Profile Options • 130
Local Console Video Resolution Behavior • 122
Local Port Auto-Sense (Video Refresh) - Default Hot Key • 123
Local Port Hot Keys and Connect Keys • 123
Local Port Requirements • 146
Logging In • 14

M
Macro Editor • 94
Mapped Drives • 33
Mount a Smart Card Reader • 73
Mounting CD-ROM/DVD-ROM/ISO Images • 31, 36
Mounting Local Drives • 28
Mouse Modes • 98
Mouse Options • 57
Mouse Sync • 101
Mouse Synchronization Tips • 60
Multi-Language Keyboard JRE Requirement • 157

N
Network Speed Settings • 144
Noise Filter • 46, 90
Notes on Mounting Local Drives • 28
Number of Supported Audio/Virtual Media and Smartcard Connections • 152
Number of Supported Virtual Media Drives • 30

O
Operating System Audio Playback Support • 79
Optimize for
  Selections • 44
Overview • 15, 26, 39, 115, 121

P
Package Contents • 1
PC Share Mode and Privacy Settings when Using Smart Cards • 72
Port Access Page (Remote Console Display) • 17
Port Action Menu • 17, 20, 42, 84
Prerequisites for Using AKC • 82
Prerequisites for Using Virtual Media • 27
Proxy Server Configuration for Use with VKC, VKCS, and AKC • 41, 83

R
Recommendations for Audio Connections when PC Share Mode is Enabled • 76, 150
Recommended Minimum Active KVM Client [AKC] Requirements • 81
Recommended Minimum Virtual KVM Client [VKC] Requirements • 39
Refresh Screen • 103
Refreshing the Screen • 53
Remote and Local Console Interfaces • 3
Remote Client Requirements • 148
Remote Linux Client Requirements • 148
Remote PC VM Prerequisites • 27
Resetting the ThinkSystem Digital KVM Switch Using the Reset Button on the Device • 132
Return to the Local Console from a Target Device - Default Hot Key • 123
Returning User Group Information • 133
Root User Permission Requirement • 33

S
Saving Audio Settings • 78, 79
Scaling • 70
Scan for Targets • 118
Scan for Targets - Local Console • 128
Scanning Port Slide Show - Local Console • 126
Scanning Ports - Local Console • 116, 125
Scanning Ports - Remote Console • 17, 19, 66, 116, 125
Scanning Ports Slide Show - Remote Console • 116
Screenshot • 103
Screenshot from Target Command (Target Screenshot) • 56
Security Warnings and Validation Messages • 6, 8, 14
Send Ctrl+Alt+Del Macro • 49
Send LeftAlt+Tab [Switch Between Open Windows on a Target Server] • 49
Send Macro • 93
Send Smart Card Remove and Reinsert Notifications • 74
Send Text to Target • 49, 97
Set Scan Tab • 19
Setting the Registry to Permit Write Operations to the Schema • 134
Simultaneous Users • 122
Single • 100
Single Mouse Mode • 61
Smart Card Minimum System Requirements • 72, 128, 146
Smart Card Minimum System Requirements, CIMs and Supported/Unsupported Smart Card Readers • 72
Smart Card Reader Detected • 73
Smart Cards • 72
Software • 2, 154
Special Sun Key Combinations • 124
Specifications • 140
Standard • 100
Standard Mouse Mode • 60
Supported Audio Device Formats • 74, 75
Supported Computer Interface Modules (CIMs) Specifications • 143
Supported Operating Systems, Browsers and Java Versions • 154
Supported Remote Connections • 144
Supported Smart Card Readers • 128, 148
Supported Target Server Video Resolutions • 141, 143
Supported Tasks Via Virtual Media • 28
Supported Virtual Media Operating Systems • 29
Supported Virtual Media Types • 29
Switch From • 21
Synchronize Your Mouse • 60

T

Target Server Requirements • 147
Target Server Video Resolution - Supported Connection Distances and Refresh Rates • 143
Target Server VM Prerequisites • 27
Target Status Indicators During Port Scanning - Local Console • 127

Target Status Indicators During Port Scanning - Remote Console • 117
TCP and UDP Ports Used • 154
Text Readability • 44, 88
ThinkSystem Digital KVM Switch Interface and Navigation • 15
ThinkSystem Digital KVM Switch Local Console • 3, 25, 121
ThinkSystem Digital KVM Switch Local Console Factory Reset • 131
ThinkSystem Digital KVM Switch Local Console Interface • 25
ThinkSystem Digital KVM Switch Photos and Features • 3
ThinkSystem Digital KVM Switch Remote Console • 3, 115
ThinkSystem Digital KVM Switch Remote Console Interface • 16
ThinkSystem Digital KVM Switch Supported Keyboard Languages • 152
ThinkSystem Digital KVM Switch Supported Local Port DVI Resolutions • 122, 142
ThinkSystem Digital KVM Switch Virtual Media Prerequisites • 27
Tiered Devices - Port Access Page • 18
Tool Options • 61, 71

U

Unmount (Remove) a Smart Card Reader • 74
Unsupported Smart Card Readers • 128, 149
Update a Smart Card Reader • 74
Updating the LDAP Schema • 133
Updating the Schema Cache • 137
USB Profile • 92
USB Profiles • 48
Using a Windows Keyboard to Access Mac Targets • 153
Using Scan Port Options • 118

V

Video Menu • 103
Video Mode • 45, 89
Video Properties • 53
Video Settings • 105
View by Group Tab • 19
Index

View by Search Tab • 19
View Menu • 108
View Options • 70
View Status Bar • 70
View Toolbar • 70
Virtual KVM Client (VKC and VKCs) Help • 4, 39
Virtual KVM Client (VKC), VKCS, and Active
    KVM Client (AKC) Requirements • 156
Virtual KVM Client Java Requirements • 40
Virtual Media • 26, 71
Virtual Media File Server Setup (File Server
    ISO Images Only) • 36, 111
Virtual Media in a Linux Environment • 33
Virtual Media in a Mac Environment • 35
Virtual Media in a Windows XP Environment • 32
Virtual Media Menu • 109
Notices and Trademark

Notices  Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice. The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

LENOVO is a trademark of Lenovo. All other trademarks are the property of their respective owners.

© 2018 Lenovo.