Dominion KX III User Guide

Copyright © 2026 ACME Teleportation Devices
DKX3-v3.10.0-0R-E
September 2026
Release 3.10.0

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without the express prior written consent of Raritan, Inc.

© Copyright 2026 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.

CE c UL us LISTED 1F61 I.T.E.

Contents

What's new in the KX III User Guide **11**

Introduction **12**

Package Contents. . . . 12
KX III Device Photos and Features. . . . 12
Hardware. . . . 12
Software. . . . 13
Photos. . . . 14
Supported Number of Ports and Remote Users per Model. . . . 14
Remote/Local Console Interfaces and User Station. . . . 14
KVM Client Applications. . . . 15
Online Help. . . . 15

Get Started Using KX III **16**

Install and Configure KX III. . . . 16
Default Login - Change the Password. . . . 16
Allow Pop-Ups. . . . 16
Security Warnings and Validation Messages. . . . 16
Java Validation and Access Warning. . . . 17
Additional Security Warnings. . . . 18
Installing a Certificate. . . . 19
Example 1: Import the Certificate into the Browser. . . . 19
Example 2: Add the KX III to Trusted Sites and Import the Certificate. . . . 20
Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional). . . . 21
Logging In to KX III. . . . 23

KX III Interface and Navigation **24**

KX III Remote Console Interface. . . . 24
Port Access Page (Remote Console Display). . . . 24
Port Action Menu. . . . 27
DKX3-808 Fast Switching 29
Left Panel. . . . 29
KX III Local Console Interface. . . . 31

Virtual Media **32**

Overview. . . . 32
Prerequisites for Using Virtual Media. . . . 32

KX III Virtual Media Prerequisites. 32
Remote PC VM Prerequisites. 33
Target Server VM Prerequisites. 33
CIMs Required for Virtual Media. 33
Supported Tasks Via Virtual Media. 33
Supported Virtual Media Types. 34
Conditions when Read/Write is Not Available. 34
Supported Virtual Media Operating Systems. 34
Number of Supported Virtual Media Drives. 34
Virtual Media. 35
Access a Virtual Media Drive on a Client Computer. 35
Access a Virtual Media Image File. 36
Mounting CD-ROM/DVD-ROM/ISO Images. 36
Disconnect from Virtual Media Drives. 37
Virtual Media in a Linux Environment. 37
Active System Partitions. 37
Mapped Drives. 37
Drive Partitions. 38
Root User Permission Requirement. 38
Connect Drive Permissions (Linux). 38
Virtual Media in a Mac Environment. 38
Active System Partition. 38
Drive Partitions. 38
Connect Drive Permissions (Mac). 38
Virtual Media File Server Setup (File Server ISO Images Only). 39

KVM Clients **40**

KVM Client Launching. 40
Virtual KVM Client (VKC and VKCs) Help. 41
Recommended Minimum Virtual KVM Client (VKC) Requirements. 41
Optimize for: Selections. 41
Virtual KVM Client Java Requirements. 41
Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC) 42
Configuring Connection Properties. 42
Connection Information. 45
USB Profiles. 46
Keyboard. 47
Video Properties 51
Mouse Options 54
Tool Options. 58
View Options. 64

Connect to Virtual Media. . . . 67
Smart Cards. . . . 67
Digital Audio. . . . 69
Power Control Using VKC, VKCS, and AKC. . . . 74
Version Information. . . . 74
Overview. . . . 75
Active KVM Client (AKC). . . . 75
Recommended Minimum Active KVM Client (AKC) Requirements. . . . 75
AKC Supported Microsoft .NET Framework. . . . 75
AKC Supported Operating Systems. . . . 75
AKC Supported Browsers. . . . 76
Prerequisites for Using AKC. . . . 76
Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC) . . . 76
HTML KVM Client (HKC). . . . 77
Connection Properties. . . . 79
Connection Info. . . . 81
USB Profile. . . . 82
Keyboard and Mouse Menu. . . . 83
Video Menu. . . . 95
View Menu. . . . 100
Virtual Media Menu. . . . 101
Audio Menu. . . . 105
Power Control Menu. . . . 107
Using HKC on Apple iOS Devices. . . . 107

Serial Access With Dominion Serial Access Module 115

Connect DSAM. . . . 116
DSAM LED Operation. . . . 116
Supported USB Device Combinations. . . . 117
View DSAM Serial Ports. . . . 117
Configure DSAM Serial Ports. . . . 118
Serial Port Keyword List. . . . 121
Upgrade DSAM Firmware. . . . 121
Supported CLI Commands. . . . 121
Command Line Interface Shortcuts. . . . 125
Command Line Interface High-Level Commands. . . . 125
Supported Escape Key Characters. . . . 125
Browser Tips for HSC. . . . 125
Connect to DSAM Serial Targets in Port Access Page. . . . 127

Connect to DSAM Serial Target with URL Direct Port Access. . . . 128
Connect to DSAM Serial Target via SSH. . . . 128
HTML Serial Console (HSC) Help. . . . 128
HSC Functions. . . . 128

Dominion User Station **138**
Overview. . . . 138
User Station Photo and Features. . . . 138
Operating the User Station. . . . 139

KX III Remote Console **141**
Overview. . . . 141
Scanning Ports - Remote Console. . . . 141
Scanning Ports Slide Show - Remote Console. . . . 141
Target Status Indicators During Port Scanning - Remote Console. . . . 142
Using Scan Port Options. . . . 143
Scan for Targets. . . . 144
Changing a Password. . . . 145
Managing Favorites. . . . 145
Enable Favorites. . . . 146
Access and Display Favorites. . . . 146
Discovering Devices on the Local Subnet. . . . 146
Discovering Devices on the KX III Subnet. . . . 147

KX III Local Console **149**
Accessing a Target Server. . . . 149
Local Console Video Resolution Behavior. . . . 149
Simultaneous Users. . . . 150
Local Port Hot Keys and Connect Keys. . . . 150
Return to the Local Console from a Target Device - Default Hot Key. . . . 150
Local Port Auto-Sense (Video Refresh) - Default Hot Key. . . . 150
Connect Key Examples. . . . 150
Special Sun Key Combinations. . . . 151
Scanning Ports - Local Console. . . . 152
Scanning Port Slide Show - Local Console. . . . 152
Target Status Indicators During Port Scanning - Local Console. . . . 154
Configure Local Console Scan Settings. . . . 154
Scan for Targets - Local Console. . . . 154
Local Console Smart Card Access. . . . 154
Using a Smart Card at the Local Port. . . . 156
Local Console USB Profile Options. . . . 157
KX III Local Console Factory Reset. . . . 157
Resetting the KX III Using the Reset Button. . . . 157

Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality 159
About the Cat5 Reach DVI. . . . 159
Connect Cat5 Reach DVI and Cat5 Reach DVI. . . . 159

Updating the LDAP Schema 161
Returning User Group Information. . . . 161
From LDAP/LDAPS. . . . 162
From Microsoft Active Directory. . . . 162
Setting the Registry to Permit Write Operations to the Schema. . . . 162
Creating a New Attribute. . . . 164
Adding Attributes to the Class. . . . 165
Updating the Schema Cache. . . . 166
Editing rciusergroup Attributes for User Members. . . . 166

Cisco ISE for RADIUS Users 168
Settings to Configure on Raritan Product. . . . 169
Settings to Configure on Cisco ISE. . . . 170
Step 1: Add Raritan Network Devices. . . . 170
Step 2: Create/Edit User. . . . 171
Step 3: Configure Allowed Authentication Protocol Service (PAP/CHAP/MS-CHAP). . . . 172
Step 4: Create Authorization Profile. . . . 173
Step 5: Configure/Create Authorization Policy. . . . 175
Troubleshooting Tips. . . . 176

Specifications 176
Hardware. . . . 176
Dimensions and Physical Specifications. . . . 176
Supported Target Server Video Resolutions. . . . 178
KX III Supported Local Port DVI Resolutions. . . . 179
Target Server Video Resolution - Supported Connection Distances and Refresh Rates. . . . 180
Supported Computer Interface Module (CIMs) Specifications. . . . 181
Supported Digital Video CIMs for Mac. . . . 184
Digital CIM Timing Modes. . . . 184
Digital CIM Established and Standard Modes. . . . 185
DVI Compatibility Mode. . . . 186
Supported Remote Connections 186
Network Speed Settings. . . . 186
Dell Chassis Cable Lengths and Video Resolutions 187
Smart Card Minimum System Requirements. . . . 187
Supported Smart Card Readers. . . . 188
Unsupported Smart Card Readers. . . . 189
Audio Playback and Capture Recommendations and Requirements. . . . 189
Number of Supported Audio/Virtual Media and Smartcard Connections. . . . 190

Certified Modems. . . . 191
KX III Supported Keyboard Languages. . . . 191
Mac Mini BIOS Keystroke Commands. . . . 192
Using a Windows Keyboard to Access Mac Targets. . . . 193
TCP and UDP Ports Used. . . . 193
Software. . . . 194
Supported Operating Systems, Browsers and Java Versions. . . . 194
Multi-Language Keyboard JRE Requirement. . . . 196
Events Captured in the Audit Log and Syslog. . . . 196
BSMI Certification. . . . 197

Informational Notes 197

Overview. . . . 197
Java Runtime Environment (JRE) Notes. . . . 197
Java Not Loading Properly on Mac. . . . 197
AKC Download Server Certification Validation IPv6 Support Notes. . . . 198
Dual Stack Login Performance Issues. . . . 198
CIM Notes. . . . 198
Windows 3-Button Mouse on Linux Targets. . . . 198
Target Video Picture Not Centered (Mouse Out of Synch). . . . 198
Powerstrip is not detected. . . . 198
Virtual Media Notes. . . . 199
Cannot Connect to Drives from Linux Clients. . . . 199
Virtual Media via VKC and AKC in a Windows Environment 199
Virtual Media Not Refreshed After Files Added. . . . 199
Virtual Media Linux Drive Listed Twice. . . . 199
Disconnecting Mac and Linux Virtual Media USB Drives 199
Target BIOS Boot Time with Virtual Media. . . . 200
Virtual Media Connection Failures Using High Speed for Virtual Media Connections. . . . 200
USB Port and Profile Notes. . . . 200
VM-CIMs and DL360 USB Ports. . . . 200
Help Choosing USB Profiles. . . . 200
Changing a USB Profile when Using a Smart Card Reader. . . . 201
Video Mode and Resolution Notes. . . . 201
Video Image Appears Dark when Using a Mac. . . . 201
Video Shrinks after Adjusting Target Clock. . . . 202
Black Stripe/Bar(s) Displayed on the Local Port. . . . 202
Sun Composite Synch Video. . . . 202
SUSE/VESA Video Modes. . . . 202
Keyboard Notes. . . . 203

French Keyboard. . . . 203
Keyboard Language Preference (Fedora Linux Clients). . . . 204
Macros Not Saving on Linux Targets. . . . 205
Mac Keyboard Keys Not Supported for Remote Access. . . . 205
Mouse Notes. . . . 206
Mouse Pointer Synchronization (Fedora) . . . 206
Single Mouse Mode when Connecting to a Target Under CC-SG Control. . . . 206
Mouse Sync Issues in Mac OS. . . . 206
Audio . . . 206
Audio Playback and Capture Issues. . . . 206
Audio in a Linux Environment. . . . 207
Audio in a Windows Environment. . . . 207
Smart Card Notes. . . . 207
Smart Card Connections to Fedora Servers. . . . 207
CC-SG Notes. . . . 207
Virtual KVM Client Version Not Known from CC-SG Proxy Mode. . . . 207
Moving Between Ports on a Device. . . . 207
Browser Notes. . . . 208
Resolving Issues with Firefox Freezing when Using Fedora. . . . 208

Frequently Asked Questions **208**

General FAQs. . . . 208
Remote Access. . . . 209
Universal Virtual Media. . . . 212
Bandwidth and KVM-over-IP Performance. . . . 214
IPv6 Networking. . . . 216
Servers. . . . 216
Installation. . . . 217
Local Port - KX III. . . . 218
Blade Servers. . . . 219
Extended Local Port. . . . 220
Dual Power Supplies. . . . 220
Intelligent Power Distribution Unit (PDU) Control. . . . 221
Ethernet and IP Networking. . . . 222
Local Port Consolidation, Tiering and Cascading. . . . 223
Computer Interface Modules (CIMs). . . . 224
Security. . . . 225
Smart Cards and CAC Authentication. . . . 226
Manageability. . . . 227
Documentation and Support. . . . 227
Miscellaneous. . . . 228

Third Party Licenses **229**

Licenses - Ccid. 229
Licenses - Clish. 229
Licenses - Dropbear. 233
Licenses - Iperf. 234
Licenses - LIBXML2. 237
Licenses - Net-SNMP. 237
Licenses - Open LDAP. 242
Licenses - OpenSSL. 243
Licenses - WPA Supplicant and Hostapd. 244

Index **245**

What's new in the KX III User Guide

What's New in KX III Release 3.10.0

- FIPS 140-3 support.
- Supports Static Routes.

Introduction

The Dominion KX III is an enterprise-class, secure, KVM-over-IP switch that provides multiple users with remote BIOS-level control of 8 to 64 servers.

KX III comes with standard features such as DVI/HDMI/DisplayPort digital and analog video, audio, virtual media, smart card/CAC, blade server support, and mobile access.

Deploy KX III individually, or with Raritan's CommandCenter Secure Gateway (CC-SG).

In This Chapter

Package Contents. 12
KX III Device Photos and Features. 12
Remote/Local Console Interfaces and User Station. 14
KVM Client Applications. 15
Online Help. 15

Package Contents

Each KX III ships as a fully-configured stand-alone product in a standard 1U or 2U form with 19" rackmount chassis.

- 1 - KX III device
- 1 - Quick Setup Guide
- 1 - Rackmount kit
- 2 - AC power cords
- 1 - Set of 4 rubber feet (for desktop use)
- 1 - Application note

KX III Device Photos and Features

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:
  - For virtual media and Absolute Mouse Synchronization, use one of the following CIMs:
  - D2CIM-VUSB
  - D2CIM-DVUSB
  - D2CIM-DVUSB-DVI
  - D2CIM-DVUSB-HDMI

    - D2CIM-DVUSB-DP
    - D2CIM-VUSB-USBC
    - D2CIM-DVUSB-MDP
  - Required for PS2 connection:
    - DCIM-PS2
- 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 and power management from an iPhone® or iPad®
- Support for tiering in which a base KX III 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
- Integrated power control
- 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*

**Note: Virtual media and Absolute Mouse Synchronization require use of a D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP CIM or D2CIM-VUSB-USBC*

- Support for digital audio over USB
- Port scanning and thumbnail view of up to 32 targets 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
- Power control associated directly with servers to prevent mistakes
- Integration with Raritan's CommandCenter Secure Gateway (CC-SG) management unit
- CC Unmanage feature to remove device from CC-SG control
- Support of Raritan PDUs
- Support for remote IP access from the new Dominion KX III User Station
- Support for access to serial targets using the Dominion Serial Access Module (DSAM)

Photos

Front View



Supported Number of Ports and Remote Users per Model

Model	Ports	Remote users
<kx>-864	64	8
<kx>-832	32	8
<kx>-816	16	8
<kx>-808	8	8
<kx>-464	64	4
<kx>-432	32	4
<kx>-416	16	4
<kx>-232	32	2
<kx>-216	16	2
<kx>-132	32	1
<kx>-116	16	1
<kx>-108	8	1

Remote/Local Console Interfaces and User Station

Use the Remote Console interface to configure and manage the KX III over a network connection.

Use the Local Console interface to access the KX III while at the rack.

See: KX III Remote Console Interface, KX III Local Console Interface respectively.

The Dominion User Station provides an alternative interface for IP access to the KX III's target servers. See: Dominion User Station (on page 138).

KVM Client Applications

KX III works with -

- Active KVM Client (AKC) - Default client, Windows only. Microsoft .NET® 4.5 or above, Microsoft Edge WebView2 required to use KX III with the Microsoft Windows®-based Active KVM Client (AKC). See Active KVM Client (AKC) (on page 75)
- Virtual KVM Client (VKC) -Azul OpenJDK or OpenJRE Java-8 can be used for the Java-based . See Virtual KVM Client (VKC and VKCs) Help (on page 41)
- HTML KVM Client (HKC) - Runs on Linux, Mac, and Windows without .Net. Supports Edge, Firefox, Chrome and Safari browsers. See HTML KVM Client (HKC) (on page 77).

Online Help

KX III online help is considered your primary help resource.

KVM Client help is provided as part of KX III online help.

Online help is accompanied by the KX III Quick Setup Guide, which is included with your KX III and can be found on the Support page of Raritan's website.

The Support page also contains a PDF version of the end user help sections of online help, and a PDF containing the KX III administrator help sections.

See the KX III Release Notes for important information on the current release before you begin using the KX III.

To use online help, JavaScript must be enabled in your browser.

Get Started Using KX III

This section walks you through high-level tasks to start using KX III.

In This Chapter

Install and Configure KX III. 16
Default Login - Change the Password. 16
Allow Pop-Ups. 16
Security Warnings and Validation Messages. 16
Installing a Certificate. 19
Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional). 21
Logging In to KX III. 23

Install and Configure KX III

If you have not already done so, install and configure KX III.

See the KX III Quick Setup Guide that came with the KX III device or download it from the Raritan Support website.

Default Login - Change the Password

The KX III device is shipped with the following default settings. You are forced to change the password at first login to a strong password.

- Username = `admin`
- Password = `raritan`
- IP address = `192.168.0.192`

Important: For backup and business continuity purposes, it is strongly recommended you create a backup administrator username and password, and keep that information in a secure location.

Allow Pop-Ups

Regardless of the browser you are using, you must allow pop-ups in order to launch the KX III Remote Console.

Security Warnings and Validation Messages

When logging in to KX III, security warnings and application validation messages may appear.

These include -

- Additional security warnings based on your browser and security settings

See Additional Security Warnings (on page 18)

- If you choose to use the Virtual KVM Client (VKC/VKCS), you may see Java™ security warnings and requests to validate KX III.
  See Java Validation and Access Warning (on page 17) and Installing a Certificate (on page 19).

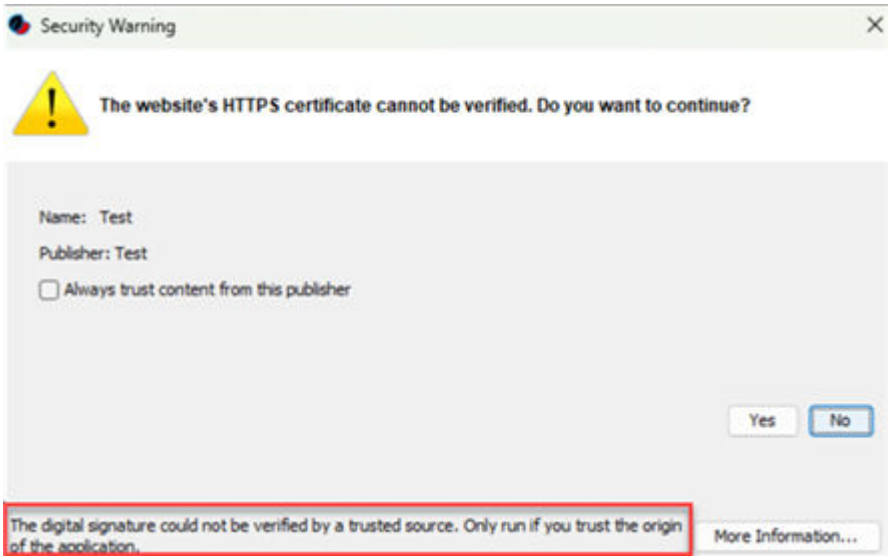
Note! Use the HTML KVM Client (HKC) instead to avoid Java. The HKC is Java-Free. See KVM Client Launching (on page 40).

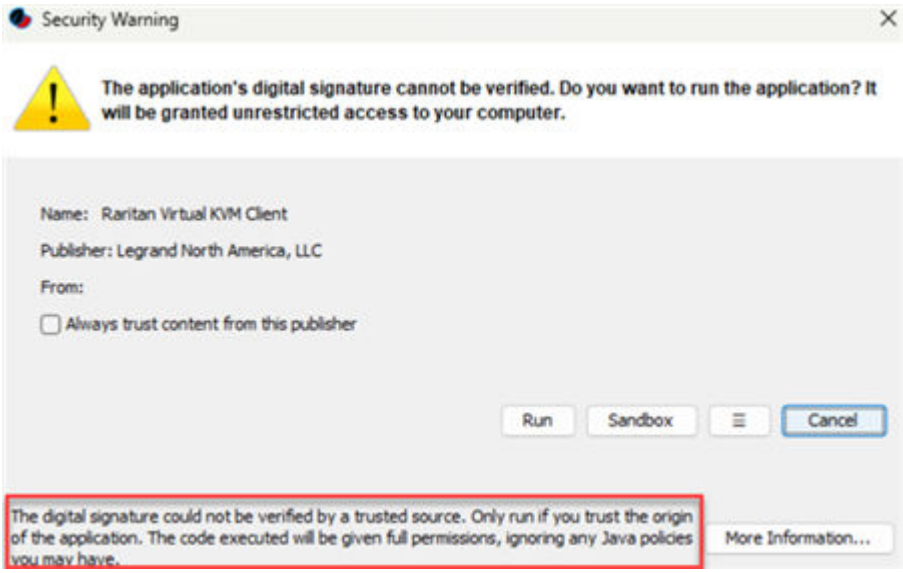
Java Validation and Access Warning

When logging in to KX III using the Java-based client, Java prompts you to validate KX III, and to allow access to the application.

Installing an SSL certificate in each KX III device is recommended to reduce Java warnings, and enhance security.

See SSL and TLS Certificates





Additional Security Warnings

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

It is necessary to accept these warnings to launch the KX III 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 KX III's SSL certificate.

Depending on your browser and security settings, additional security warnings may be displayed when you log in to KX III.

It is necessary to accept these warnings to launch the KX III Remote Console. For more information, see Security Warnings and Validation Messages (on page 16).

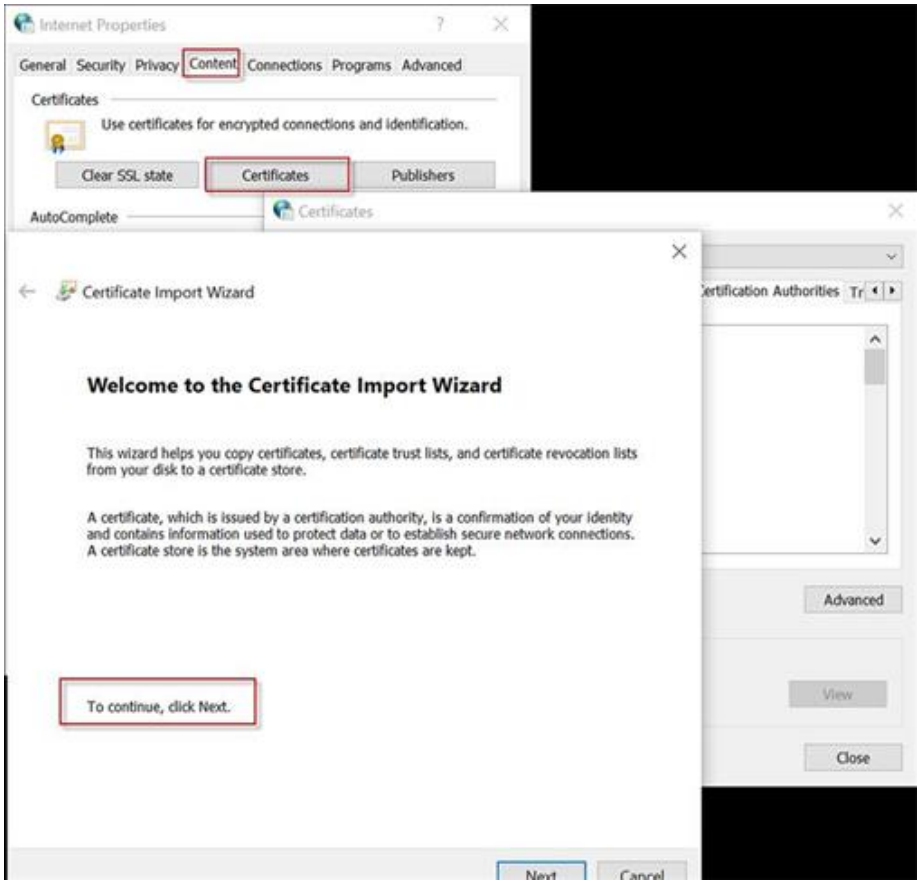
Two sample methods on how to install an SSL Certificate in the browser are provided here. Specific methods and steps depend on your browser and operating system. See your browser and operating system help for details.

Example 1: Import the Certificate into the Browser

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

1. Open a browser, then log in to KX III.
2. Click More Information on the first 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 the Settings or more tools for your browser, and import the certificate. The following example shows the Edge > more Tools > Internet Options method.



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 KX III to Trusted Sites and Import the Certificate

In this example, the KX III's URL is added as a Trusted Site, and the Self Signed Certificate is added as part of the process.

1. Open an Edge browser, then select Settings >Launch the Internet Options settings by entering "Internet Options" in the search bar for Windows.
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 KX III 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 Edge browser, then log in to KX III.
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.

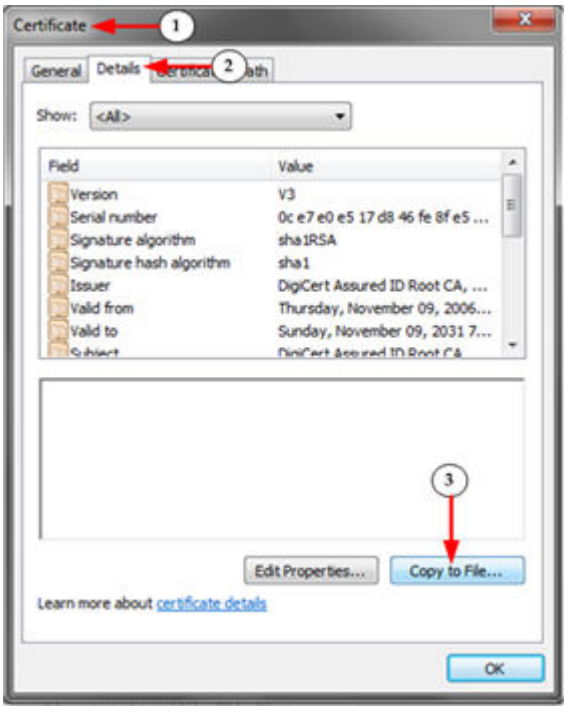
For details see, Example 1: Import the Certificate into the Browser (on page 19).

Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)

KX III 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.



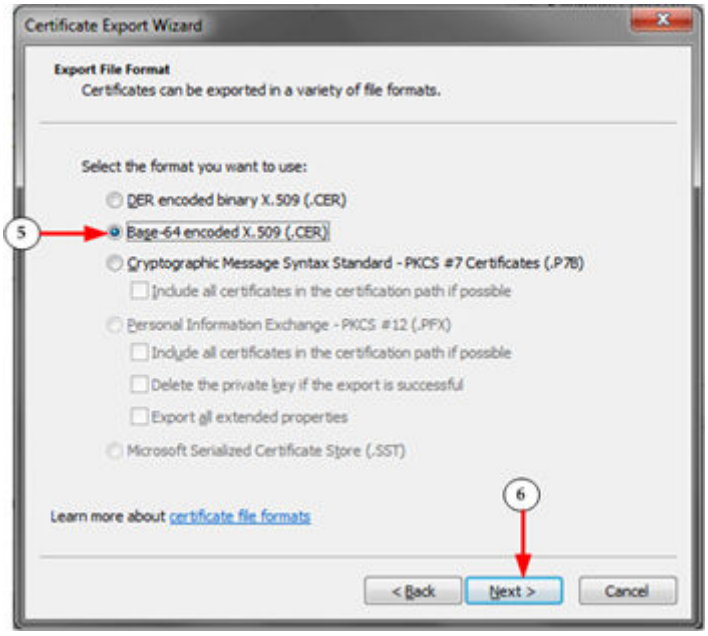
1. Locate the DEGHKVM0001.cer binary file on your Windows machine.

Double-click on the DEGHKVM0001.cer file to open its Certificate dialog.

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 KX III.

Logging In to KX III

Log in to your KX III Remote Console from any workstation with network connectivity. See the Release Notes for supported browser versions.

Logging in and using KX III 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 16).

► *To log in via Remote Console:*

1. Launch a supported web browser, and enter the IP address assigned to the KX III.
2. A default client is launched based on your PC and browser settings. See KVM Clients (on page 40). You can also choose a client by entering the URL directly. See KVM Client Launching (on page 40).
3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable). If security warnings appear, click to accept.

KX III Interface and Navigation

The KX III Remote Console and the KX III Local Console are web-based graphical user interfaces.

Use the Remote Console interface to configure and manage the KX III over a network connection.

Use the Local Console interface to access the KX III while at the rack.

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

If you have the Dominion User Station, you can also use it to access targets. See Dominion User Station (on page 138).

In This Chapter

KX III Remote Console Interface. 24
KX III Local Console Interface. 31

KX III Remote Console Interface

The KX III Remote Console is a browser-based graphical user interface that allows you to log in to targets connected to the KX III and to remotely administer the KX III.

The KX III Remote Console provides a network connection to your connected KVM target servers. When you log into a KVM target server using the KX III Remote Console, a KVM Client window opens.

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

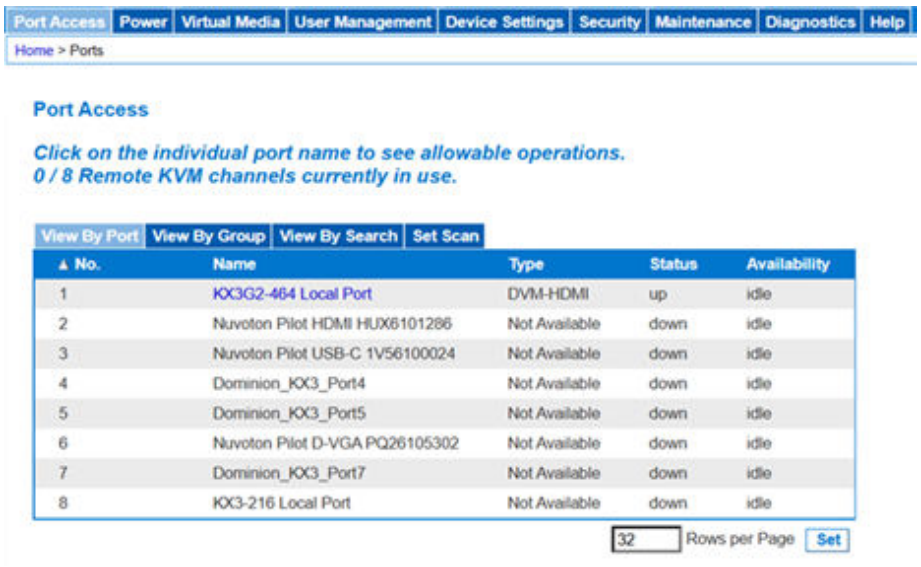
- Virtual Media
- Favorites
- Backup/Restore
- Firmware Upgrade
- SSL Certificates
- Audio

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 27).

If a KX III port has no CIM connected or is connected to a CIM with no name, a default port name of Dominion_Model Name_PortNumber is assigned to the port. PortNumber is the number of the KX III physical port.



Four tabs are provided on the page allowing you to view by port, view by group, view by search and scan ports. A fifth tab, View by Serial, is available when an optional DSAM is connected.

You can 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 up to 32 targets that are connected to the KX III. See Scanning Ports - Remote Console (on page 141)

Tiered Devices - Port Access Page

If you are using a tiered configuration in which a base KX III 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 port 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 its primary port.

Note: Two KVM channels are required and if 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

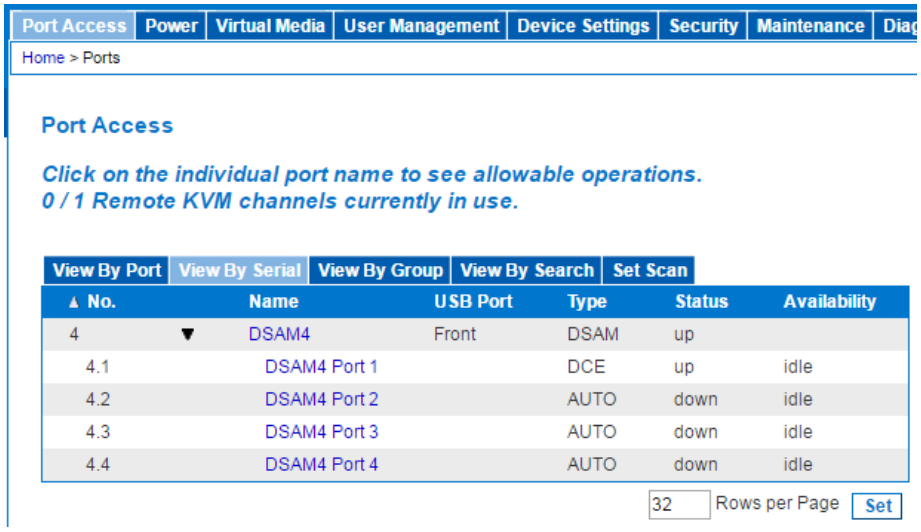
The View by Group tab displays blade chassis, 'standard' port groups, and dual video port groups. Click the Expand Arrow icon ▶ next to a group to view the ports assigned to the port group.

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.

View by Serial Tab

The View By Serial tab is visible when a Dominion Serial Access Module (DSAM) is connected by USB. Up to 4 serial targets can be connected to the DSAM by USB.



Set Scan Tab

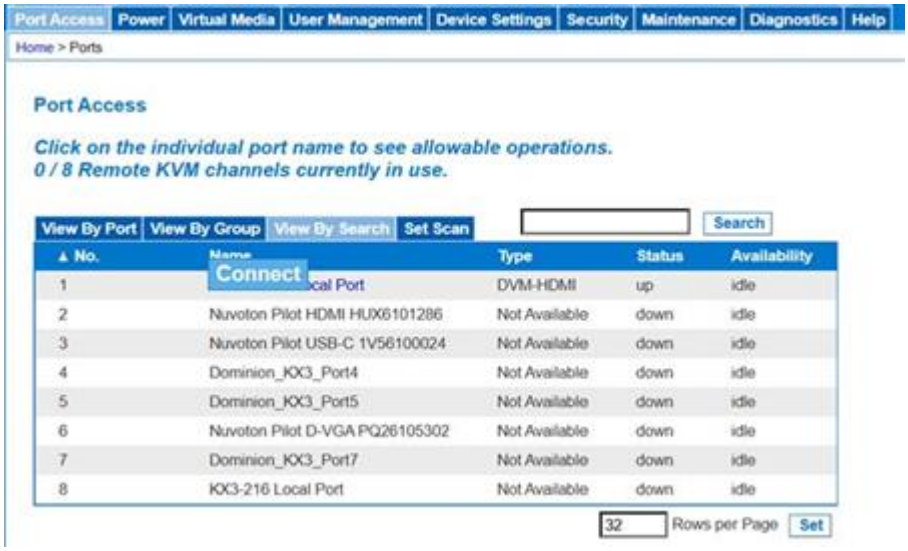
The port scanning feature is accessed from the Set Scan tab on the Port Access page. The feature allows you to define a set of KVM targets to be scanned. Thumbnail views of the scanned targets are also available. Select a thumbnail to open that target in its Virtual KVM Client window.

See Scanning Ports - Remote Console (on page 141) 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.



Connect

- Connect - Creates a new connection to the target server

  For the KX III Remote Console, a new KVM Client page appears.

  For the KX III Local Console, the display switches to the target server, and switches away from the local user interface.

  On the local port, the KX III Local Console interface must be visible in order to perform the switch.

  Hot key switching is also available from the local port.

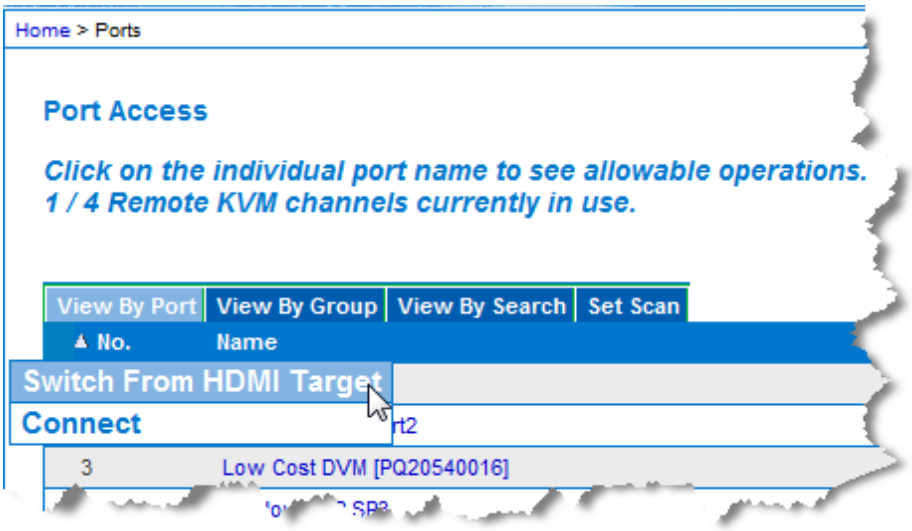
Note: This option is not available from the KX III Remote Console for an available port if all connections are busy.

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 KVM Client is opened.

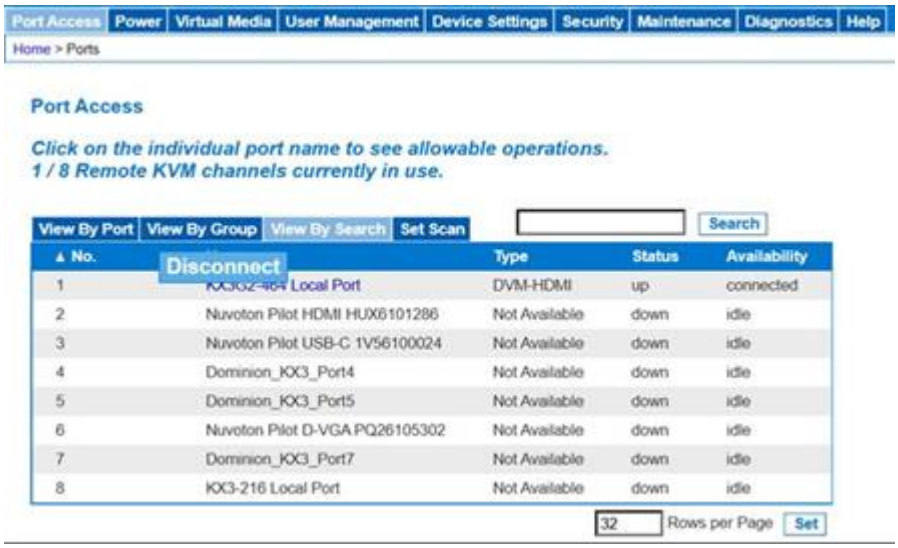
Note: This menu item is not available on the KX III Local Console.



Disconnect

- Disconnect - Disconnects this port and closes the 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 KX III Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.



Power On

- Power On - Powers on the target server through the associated outlet

This option is visible only when there are one or more power associations to the target, and when the user has permission to operate this service.

Provided you have privileges to do so, you can manage power from the Virtual KVM Client (VKC) and Active KVM Client (AKC) as well. See: Power Control

Power Off

- Power Off - Powers off the target server through the associated outlets

  This option is visible only when there are one or more power associations to the target, when the target power is on (port status is up), and when user has permission to operate this service.

  Provided you have privileges to do so, you can manage power from the Virtual KVM Client (VKC) and Active KVM Client (AKC) as well. See: Power Control

Power Cycle

- Power Cycle - Power cycles the target server through the associated outlets

  This option is visible only when there are one or more power associations to the target, and when the user has permission to operate this service.

  Provided you have privileges to do so, you can manage power from the Virtual KVM Client (VKC) and Active KVM Client (AKC) as well. See: Power Control

DKX3-808 Fast Switching

DKX3-808 maintains the video connections to the servers, enabling faster connections to servers and faster switching between channels.

Some Video Settings do not apply to DKX3-808 targets:

- Automatic Color Calibration
- Video Sensing: Best possible video mode/Quick sense video mode

Left Panel

The left panel of the KX III 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.

Information	Description	When displayed?
Time & Session	The date and time the current session started	Always
User	Username	Always
State	The current state of the application, either idle or active. If idle, the application tracks and displays the time the session has been idle.	Always

Information	Description	When displayed?
Your IP	The IP address used to access the KX III	Always
Last Login	The last login date and time	Always
Under CC-SG Management	The IP address of the CC-SG device managing the KX III	When the KX III is being managed by CC-SG
Device Information	Information specific to the KX III you are using	Always
Device Name	Name assigned to the device	Always
IP Address	The IP address of the KX III	Always
Firmware	Current version of firmware	Always
Device Model	Model of the KX III	Always
Network	The name assigned to the current network	Always
PowerIn1	Status of the power 1 outlet connection. Either on or off, or Auto-detect off	Always
PowerIn2	Status of the power 2 outlet connection. Either on or off, or Auto-detect off	Always
Configured As Base or Configured As Tiered	If you are using a tiering configuration, this indicates if the KX III you are accessing is the base device or a tiered device.	When the KX III is part of a tiered configuration
Port States	The statuses of the ports being used by the KX III	Always

Information	Description	When displayed?
Serial Port States	The statuses of the DSAM serial ports connected to the KX III	When a DSAM is connected to the KX III
Connected Users	The users, identified by their username and IP address, who are currently connected to the KX III	Always
Online Help	Links to online help	Always
Favorite Devices	See Managing Favorites (on page 145)	When enabled
FIPS Mode	FIPS Mode: EnabledSSL Certificate: FIPS Mode Compliant	When FIPS is enabled

KX III Local Console Interface

There are many similarities among the KX III Local Console and the KX III Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

For details on using the Local Console see KX III Local Console (on page 149).

Virtual Media

In This Chapter

Overview. 32
Prerequisites for Using Virtual Media. 32
Supported Tasks Via Virtual Media. 33
Supported Virtual Media Types. 34
Supported Virtual Media Operating Systems. 34
Number of Supported Virtual Media Drives. 34
Virtual Media. 35
Virtual Media in a Linux Environment. 37
Virtual Media in a Mac Environment. 38
Virtual Media File Server Setup (File Server ISO Images Only). 39

Overview

All KX III 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 KX III comes equipped with virtual media to enable remote management tasks using the widest variety of media/images.

Virtual media sessions are secured using the strongest encryption offered by the browser, typically 256 bit AES. Older browsers may only support 128 bit AES.

HKC does not support all virtual media features. See HTML KVM Client (HKC) for details

Prerequisites for Using Virtual Media

KX III Virtual Media Prerequisites

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

Remote PC VM Prerequisites

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

Note: If you are using Windows, disable User Account Control or select Run as Administrator when starting Edge. To do this, click the Start Menu, locate Edge, right-click and select Run as Administrator.

Target Server VM Prerequisites

- KVM target servers must support USB connected drives.

CIMs Required for Virtual Media

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

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP
- D2CIM-VUSB-USBC
- D2CIM-DVUSB-MDP

The black USB connector on the DVUSB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media.

For CIMs with two USB plugs, keep both connected to the device.

The device may not operate properly if both plugs are not connected 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

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 when using AKC and VKCS.

- External hard drives
- Internal and USB-mounted CD and DVD drives
- USB mass storage devices
- ISO images (disk images)
- IMG files
- DMG files
- ISO 9660 is the standard supported. However, other ISO standards can be used.

Note: Due to browser limitations, HKC supports a different set of virtual media types.

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 ® 11
- openSUSE
- Fedora®
- RHEL®
- macOS

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 connection settings 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 settings support 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.

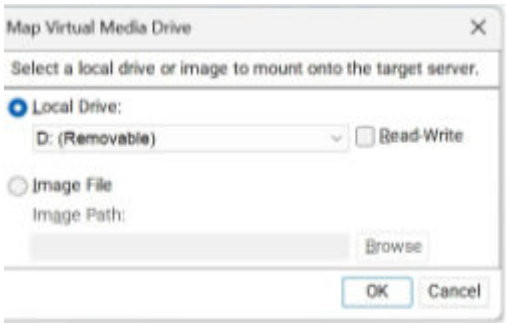
Virtual Media

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.
3. If you want Read and Write capabilities, select the Read-Write checkbox. This option is disabled for nonremovable drives. See: Conditions when Read/Write is Not Available (on page 34) 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.

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

Access a Virtual Media Image File

Use the "Image File" option to access a disk image of a removable disk.

► *Image file guidelines:*

- Image files created using dd on Linux (dd if=/dev/sdb of=disk.img) or similar tools such as Win32DiskImager on Windows, or Mac Disk Utility are supported.
- Apple DMG files:
  - DMG image files of a FAT32 USB drive are recognized on all OSs.
  - DMG images files of a folder on a Mac Drive are recognized only on Mac OS targets.
  - Image should be created via Mac Disk Utility using the following settings: Encryption: None; Image format: read/write.
  - Not supported: Encrypted or compressed dmg images, MacOS install images, DMG files downloaded from the Apple support site.

► *To access a virtual media image file:*

1. From the KVM client, choose Virtual Media > Connect Drive, or click the Connect Drive... button . The Map Virtual Media Drive dialog appears.
2. Select the Image File option, then click Browse to find and select the .img or .dmg file.
3. Click OK. The media will be mounted on the target server virtually.

Mounting CD-ROM/DVD-ROM/ISO Images

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

Note: ISO 9660 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 OK.
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 OK.

4. For remote ISO images on a file server:
   a. Choose the Remote Server ISO Image option.
   b. Choose Hostname and Image from the drop-down list. The file servers and image paths available are those that you configured using the Virtual Media Shared Images page. Only items you configured using the Virtual Media Shared Images 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 OK.

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.

Disconnect from Virtual Media Drives

► *To disconnect the virtual media drives:*

- For local drives, choose Virtual Media > Disconnect Drive.
- For CD-ROM, DVD-ROM, and ISO images, choose Virtual Media > Disconnect CD-ROM/ISO Image.

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 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.

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)

Linux users must have read-only permissions for the removable device they wish to connect to the target. For /dev/sdb1 run the following as root user:

```
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)

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, and also unmount the drive after doing so.

For /dev/sdb1, run the following commands as root user:

```
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

root@admistrator-desktop:~# diskutil umount /dev/sdb1
```

Note: To connect VM drives from the latest Mac OS, JavaLauncher requires full disk access.

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. ISO 9660 format is the standard supported. However, other CD-ROM extensions may also work.

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

Use the Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using virtual media. File server ISO images specified here are available for selection in the Remote Server ISO Image Hostname and Image drop-down lists in the Map Virtual Media CD/ISO Image dialog. See Mounting CD-ROM/DVD-ROM/ISO Images (on page 36).

► *To designate file server ISO images for virtual media access:*

1. Choose Virtual Media from the Remote Console. The File Server Setup page opens.
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.

KVM Clients

There are a variety of KVM clients to support your individual configuration.

- HKC is best for Linux and Mac users without Java.
- AKC is best for Windows Platforms, using Chrome or Edge browsers.
- VKC is best for Linux and Mac users with Java.

KVM Client	Name	Platforms	Features
HTML KVM Client	HKC	• Linux • Mac • Windows • HTML and Javascript	• Java-Free • Supports most features • See HTML KVM Client (HKC) (on page 77) for supported features
Active KVM Client	AKC	• Windows	• Full-featured KVM Client • Java-Free • Requires .Net
Virtual KVM Client	VKC	• Linux • Mac • Windows	• Full-featured KVM Client • Requires Java

In This Chapter

KVM Client Launching. 40
Virtual KVM Client (VKC and VKCs) Help. 41
Overview. 75
Active KVM Client (AKC). 75
HTML KVM Client (HKC). 77

KVM Client Launching

KVM Client	Name	URL to Force Launch
HTML KVM Client - Java-Free	HKC	<KX III IP Address>/hkc OR <KX III IP Address>/
Active KVM Client - Requires .NET	AKC	<KX III IP Address>/akc
Virtual KVM Client - Requires Java	VKCs	<KX III IP Address>/vkcs

Virtual KVM Client (VKC and VKCs) Help

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

Optimize for: Selections

Virtual KVM Client Java Requirements

A supported Java version is required. Check the release notes for latest supported version.

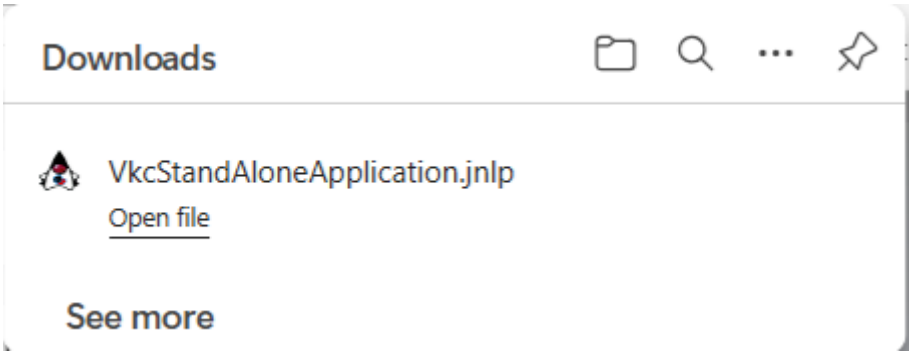
If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

Note: VKC cannot be launched from Safari, 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: You can allow and open the file from the browser downloads in the top right corner.
- Edge: You can allow and open the file from the browser downloads in the top right corner.



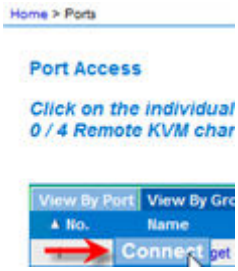
- On browsers launched from an Apple Mac: Save the jnlp file locally. File will be shown as blocked under System Settings/Privacy and Security - select option Open Anyway.
- Firefox: The current default setting in Firefox on Windows saves the file and runs from the download. You can launch from the browser with this setting: Tools>Options>Applications, then select "Jnlp File" in the Content Type column, and change the Action from "Always ask" to "Use Java Web Launcher".

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

Once you have logged on to the KX III 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 27) for details on additional available menu options.

Configuring Connection Properties

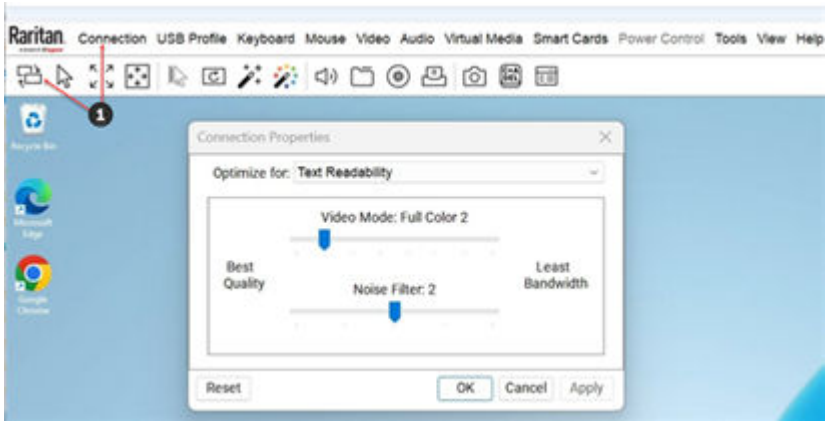
Connection properties manage streaming video performance over remote connections to target servers.

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



Default Connection Property Settings - Optimized for Best Performance

The KX III comes configured to provide optimal performance for the majority of video streaming conditions.

► *KX3 default connection settings:*

- Optimized for: Text Readability - video modes are designed to maximize text readability.

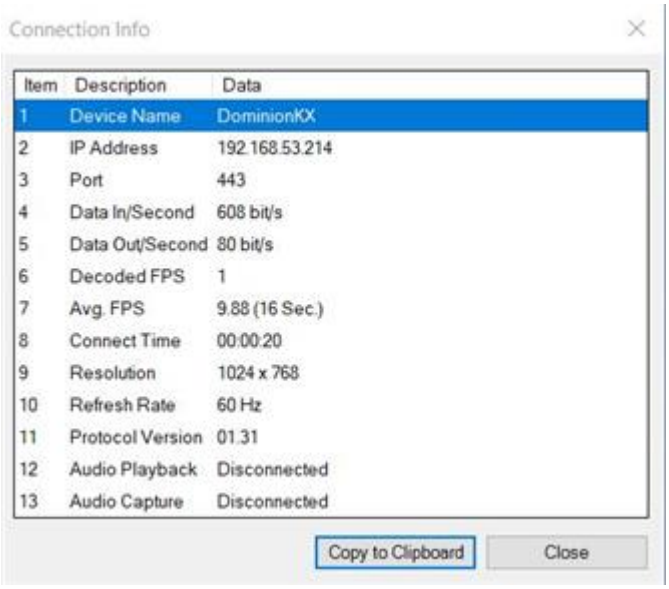
  This setting is ideal for general IT and computer applications, such as performing server administration.
- Video Mode - defaults to Full Color 2.

  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.

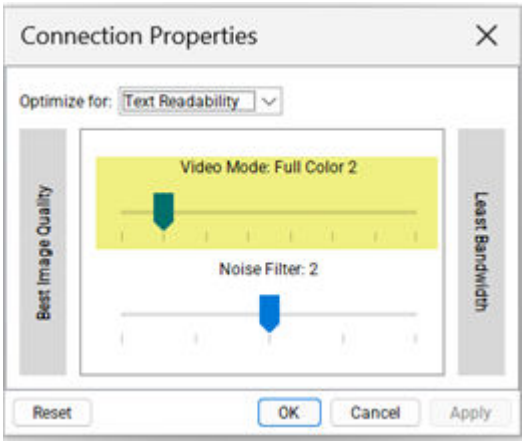
Click Reset on the Connection Properties dialog at any time to return to the default settings.

Tip: Use the Connection Information dialog to monitor the connection in real-time. See Access and Copy Connection Information



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.

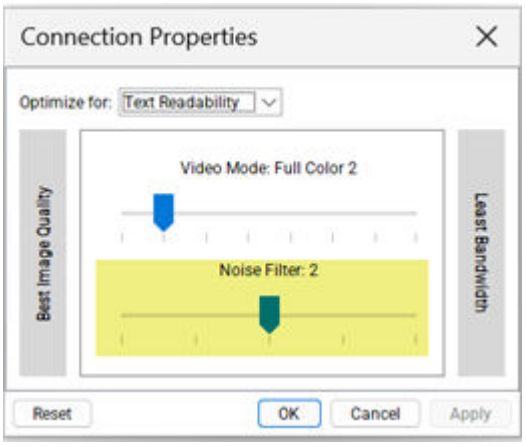
These modes are appropriate for administration work where text and GUI elements take priority, and bandwidth is at a premium.

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

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 KX III.



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

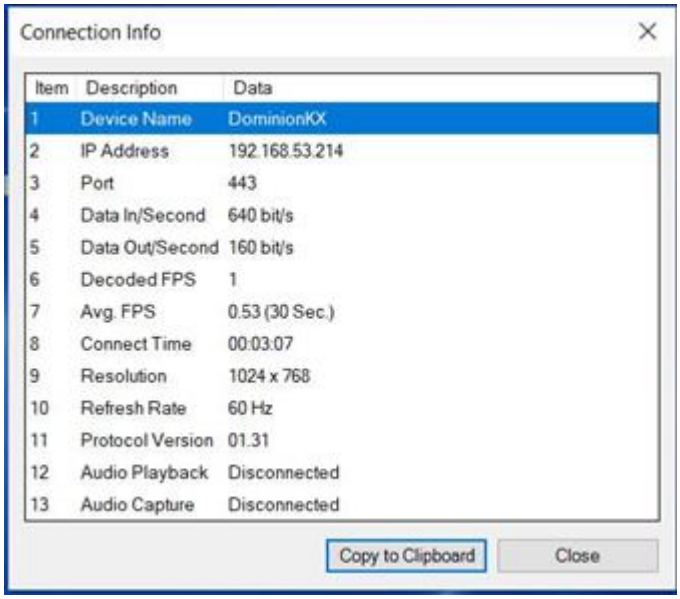
Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See Configuring Connection Properties (on page 42)

► *To open connection info:*

1. Click Connection > Info.

Note: Clicking Copy to Clipboard copies the information for pasting.



► *Current connection information:*

- Name of the KX III
- IP address of the KX III
- Port - The KVM communication TCP/IP port used to access KX III.
- Data In/Second - Data rate received from the KX III
- Data Out/Second - Data rate sent to the KX III.
- Connect Time - The duration of the current connection.
- FPS - Video frames per second transmitted received from the KX III.
- Average FPS - Average video frames per second.
- Resolution - The target server horizontal and vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - The version of the protocol.
- Audio Playback - The status of audio playback.
- Audio Capture - The status of audio recording.

USB Profiles

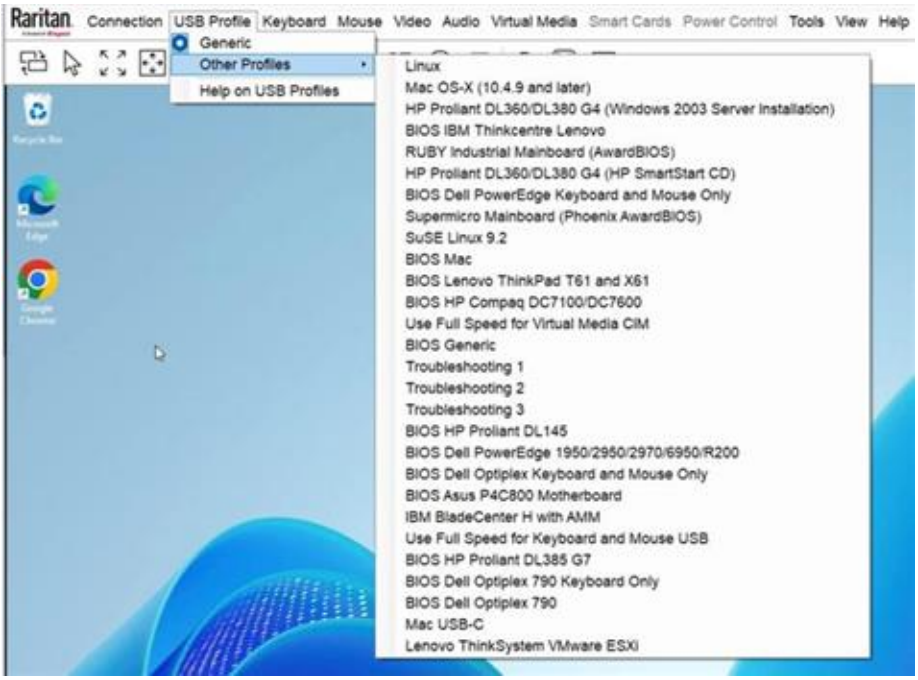
Select a USB profile that best applies to the KVM target server.

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.

Setting CIM Keyboard/Mouse Options

► *To access the DCIM-USBG2 setup menu:*

1. Put the mouse focus on a window such as Note Pad (Windows® operating system) or an equivalent.
2. Select Set CIM Keyboard/Mouse options. This is the equivalent of sending the Left-Control and Num Lock to the target. The CIM setup menu options are then displayed.
3. Set the language and mouse settings.
4. Exit the menu to return to normal CIM functionality.

Send Text to Target

► *To use the Send Text to Target function for the macro:*

1. Click the Keyboard > Send Text to Target or click  in the toolbar.
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.

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 Alt + F4. This appears in the Macro Sequence box as follows:

Press Left Alt

Press F4

Release F4

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 fields 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.

Construct Macro From Text

Construct Macro From Text will enable you to work more efficiently by producing frequently used phrases and paragraphs with a single command. Create a new macro and then assign text to it.

► *To add text to a macro:*

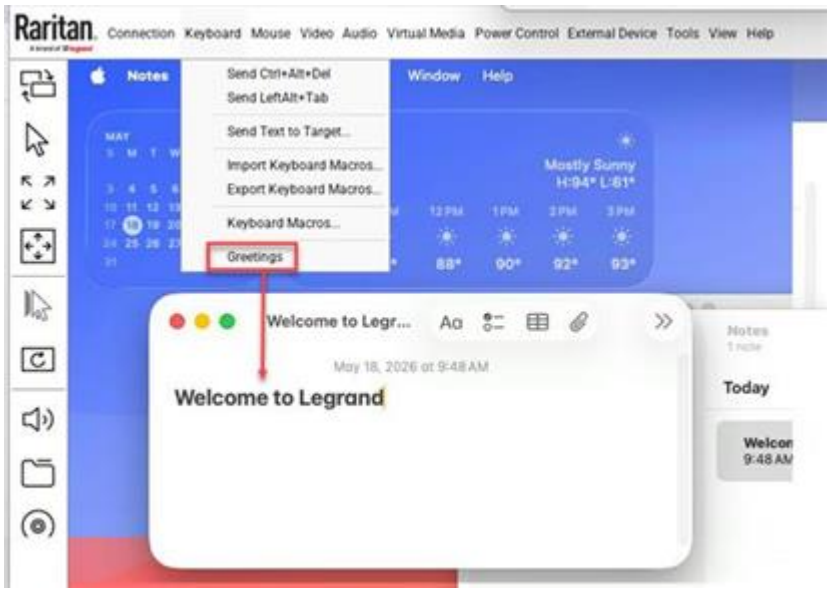
1. Choose Keboard > Keyboard Macros.



2. Click Add > Construct Macro From Text.
3. Enter text in the text box and then click OK to save.
4. Click OK again in the Add Keyboard Macro to save the macro and click Close.

► *To use macros with text:*

1. Connect to target you want to send macro to.
2. Choose Keyboard > select the macro you created.
3. Macro will be sent to the target.



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:

- 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 hotkey that already exists, the hotkey for the imported macro is discarded.

Export Macros

1. Choose Keyboard > 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 52).

► *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.

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

      Brightness Green - Controls the brightness of the green signal.

      Brightness Blue - Controls the brightness of the blue signal.
   c. Contrast Red - Controls the red signal contrast.

      Contrast Green - Controls the green signal.

      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.

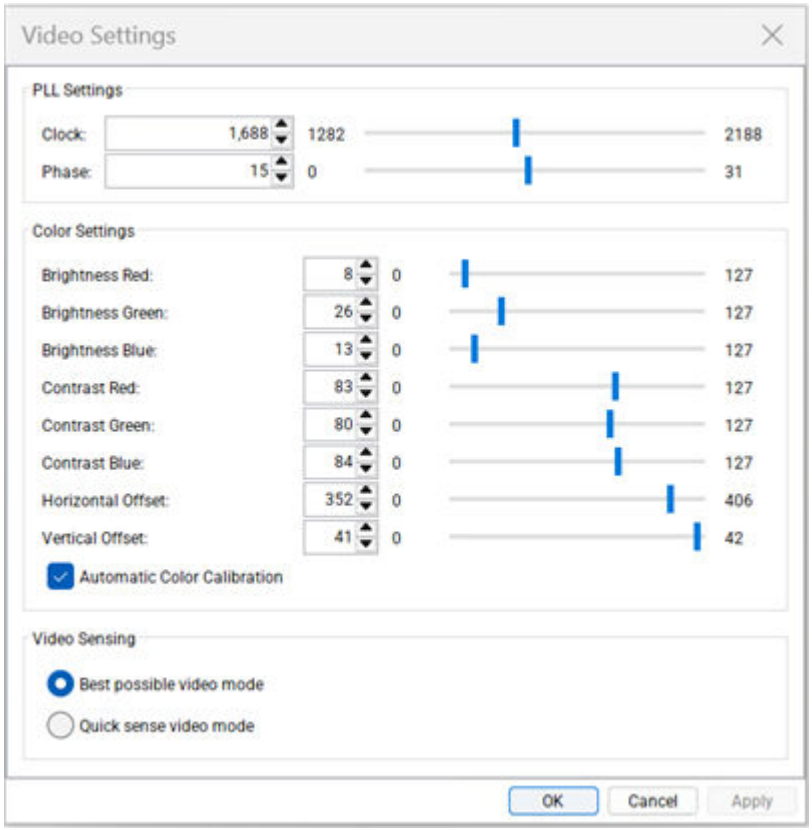
      ---

   d. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.
   e. 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 KX III 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.

Intelligent mode requires that "Enhanced Pointer Precision" is unticked on the target (Control Panel/ Mouse/Pointer Options) and mouse speed is 50%.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when Intelligent and Standard Modes don't work. You can toggle between these two modes (single mouse and dual mouse).

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.

- Absolute Mouse Synchronization requires the use of a virtual media CIM - D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP, D2CIM-VUSB-USBC

► *To enter Absolute Mouse Synchronization:*

- Choose Mouse > Absolute from the KVM client.

The black USB connector on the DVUSB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media.

For CIMs with two USB plugs, keep both 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.
- For optimal mouse performance, set the target mouse speed to 50%. Avoid using extremely low or high mouse speed settings.
- The target advanced mouse properties such as “Enhanced pointer precision" or “Snap mouse to default button in dialogs” should be disabled.
- 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.

Cursor Shape

In dual mouse modes, you can select a custom cursor shape for your session. To make the cursor selection permanent, see Client Launch Settings (on page 61).

► *To change the cursor shape:*

- Choose Mouse > Cursor Shape, then select from the list.

- Default which is an arrow
- Dot
- Crosshair
- Transparent



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

1. Click Tools > Options. The Options dialog appears.
   - Select the Enable Logging checkbox only if directed to by Technical Support.
     This option creates a log file in your home directory.
   - Keyboard Type--not visible in AKC, because the keyboard type defaults to the local client:

- English (UK)
- English (US/Int'l)
- French (France)
- German (Germany)
- Japanese
- United Kingdom
- 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

- Select Adjust Full Screen Window Size to Target Resolution Instead of Client Resolution if you prefer. Option not available for Linux clients. See Adjust Full Screen Window Size to Target Resolution (on page 61) for examples.
- Disable Menu in Full Screen: This option prevents the menu from popping back up when cursor approaches while in Full Screen mode.
- Configure hotkeys:
  - Toggle 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 hotkey used for toggling in and out of this mode.
  - Toggle Single Cursor Mode - Hotkey.

    When you enter single cursor mode, only the target server mouse cursor is visible.

    This is the hotkey used to toggle in and out of single cursor mode, removing and bringing back the client mouse cursor.
  - Toggle Scaling Mode - Hotkey.

    When you enter scaling mode, the target server scales to fit your display.

    This is the hotkey used to toggle in and out of scaling mode.
  - 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 Toggle 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.

1. 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

On Linux, Azul's OpenJDK/JRE may encounter issues generating correct key events for foreign-language keyboards configured via System Preferences. Use the methods outlined in the following table to configure foreign keyboards.

Language	Configuration method
US Intl	Default
French	Keyboard Indicator
German	System Settings (Control Center)
Japanese	System Settings (Control Center)
UK	System Settings (Control Center)
Korean	System Settings (Control Center)
Belgian	Keyboard Indicator
Norwegian	Keyboard Indicator
Danish	Keyboard Indicator
Swedish	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Italian	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

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

Adjust Full Screen Window Size to Target Resolution

When Adjust Full Screen Window Size to Target Resolution instead of Client Resolution is enabled, the client starts in full-screen in a window equal to the target's resolution, not the resolution of the client monitor. If you have a multi-monitor client, a full-screen window may cover more than one monitor. See General Settings for instructions on enabling the setting.

► *Example:*

The client has a multi-head environment with 8 monitors, 1920 x 1080 each with the following arrangement:

1	2	3	4
5	6	7	8

A KVM session is launched on monitor 6 with a the target resolution of 3840 x 1080. The client window opens on monitor 6 and 7 in native resolution and covers both monitors by 100%.

Client Launch Settings

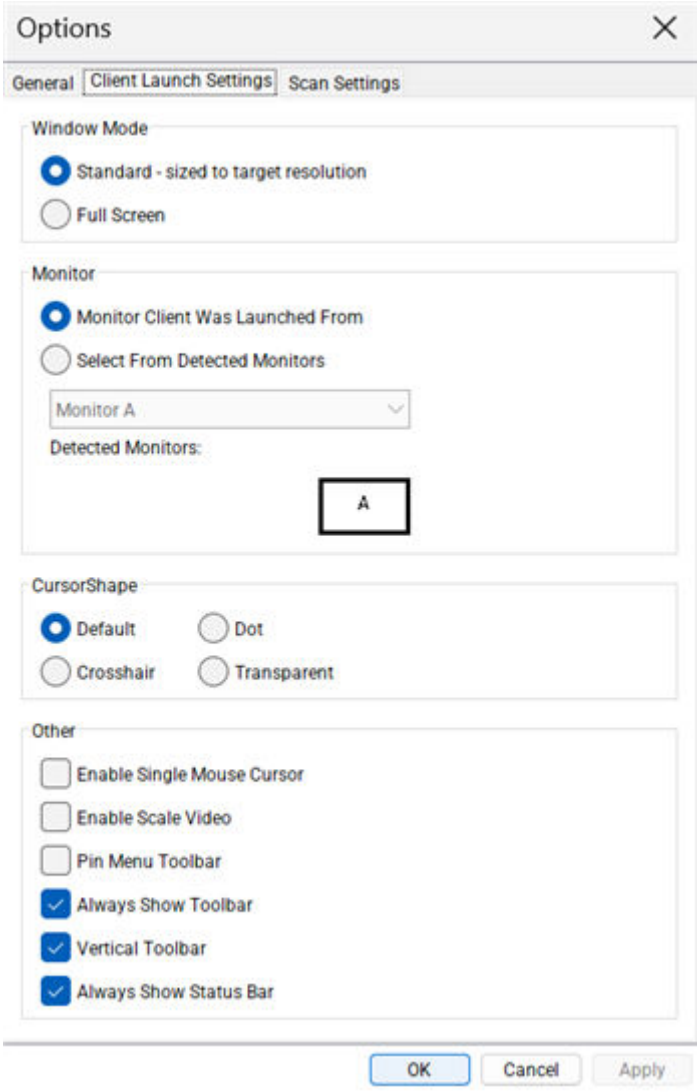
Configuring client launch settings allows you to define the screen settings for a KVM session.

► *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:
     - 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).
     - Select 'Full Screen' to open the target window in full screen mode.
   - To configure the monitor on which the target viewer is launched:
     - 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).
     - 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 cursor shape:
     - Select Default arrow, Dot, Crosshair, or Transparent to set the cursor shape for all sessions. Use the Mouse menu to change the cursor shape during a session.
   - To configure additional launch settings:

- Select 'Enable Single Cursor Mode' to enable single mouse mode as the default mouse mode when the server is accessed.
- Select 'Enable Scale Video' to automatically scale the display on the target server when it is accessed.
- 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.
- Always Show Tool Bar, Vertical Toolbar 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 154)

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 141)

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" 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" 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.

Collecting a Diagnostic Snapshot of the Target

Administrators are able to collect a "snapshot" of a target.

The "snapshot" function generate log files and image files from the target.

It then bundles these files in a zip file that can be sent to Technical Support 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 like 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.

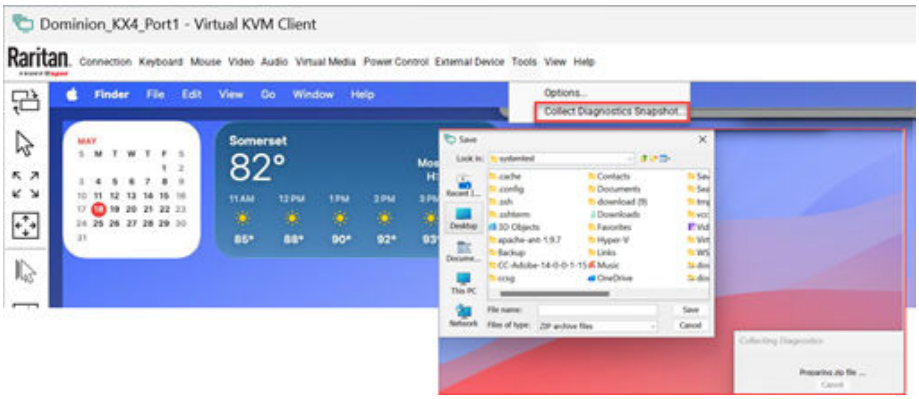
- Log.txt file:

  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

To capture a diagnostic snapshot:



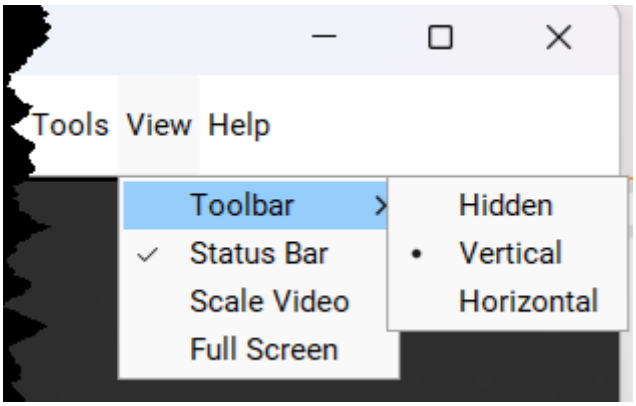
Steps	
1	Access a target, and then click Tools > Collect a Diagnostic Snapshot. Several messages are displayed as the information is collected.
2	You are prompted to save the zip file containing the diagnostic files.
3	The zip file containing the diagnostic files is saved.

View Options

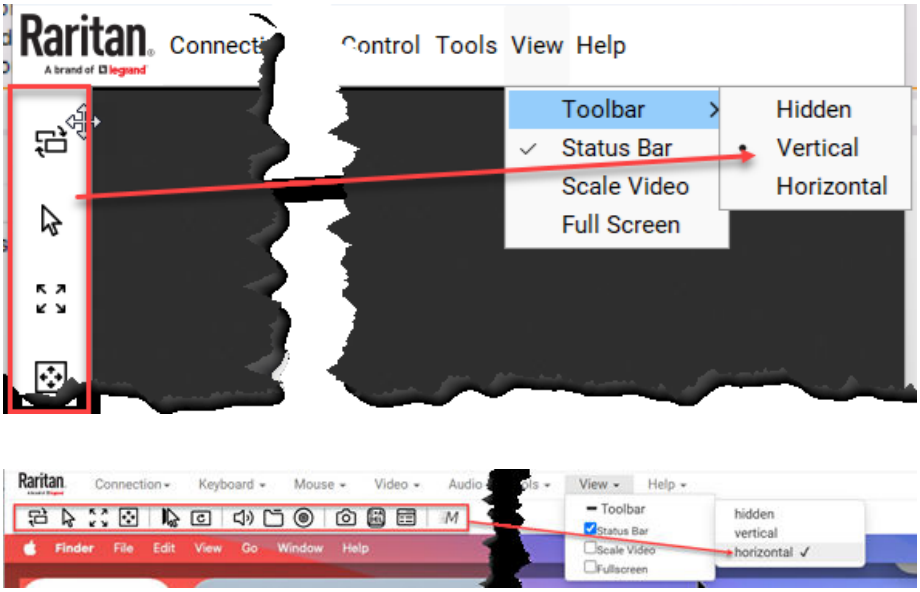
View Toolbar

You can change the Virtual KVM client's toolbar position (Vertical or Horizontal) or hide it from being displayed.

- Choose View > Toolbar.



- Select Hidden from the list, so the toolbar is no longer displayed.
- You can also select Vertical/Horizontal to display the toolbar vertically or horizontally.



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.

Scale Video

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):

► *To turn off scaling:*

- Click View > Scale Video to deselect it.

► *To turn on scaling:*

- Click View > Scale Video to select it.

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 hotkey used for exiting this mode is specified in the Options dialog, see Tool Options (on page 58).

While in Full Screen mode, moving your mouse to the top of the screen displays the Full Screen mode menu bar. The behavior of the menu in full screen mode is affected by some options on the Tool Options menu. See Tool Options > General Settings > Full Screen options

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 58).

► *To enter full screen mode:*

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

► *To exit full screen mode:*

- Press the hotkey 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 32)

Smart Cards

Using the KX III, 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 67).

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 154).

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 187)
- Supported Computer Interface Module (CIMs) Specifications (on page 181)
- Supported Smart Card Readers (on page 188)

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 KX III 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.

The audio devices are accessed over a USB connection.

- Current device firmware is required.
- One of the following CIMs must be used:
  - D2CIM-DVUSB
  - D2CIM-DVUSB-DVI
  - D2CIM-DVUSB-HDMI
  - D2CIM-DVUSB-DP
  - D2CIM-DVUSB-MDP

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 next sections.

Note: Audio formats are no longer selectable from all clients (HKC, AKC, VKCs). It is now set to Stereo 16 bit 44100Hz and cannot be changed.

Digital Audio VKC and AKC Icons

These icons are located in status bar at the bottom of the client window.

Icon Name	Audio Icons	Description
Speakers		Blinking waves indicate an audio playback session is currently streaming
		A black speaker icon is displayed when the audio playback session is connected, but not streaming audio.
		A cross in front of the speaker icon means the audio is disconnected.
Microphone		Blinking waves indicate an audio capture session is currently underway.
		A black Microphone icon is displayed without waves when connected, but not is use.
		A slash on the microphone icon indicates the microphone is disconnected.

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.

Audio format	Network bandwidth requirement
44.1 KHz, 16bit stereo	176 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 audio/video.

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

Once the audio devices settings are configured and saved on the KX III, the same settings are applied to it.

See: Connecting and Disconnecting from a Digital Audio Device (on page 72) for information on connecting to and configuring an audio device, and Adjusting Capture and Playback Buffer Size (Audio Settings) (on page 73) 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.

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 72) 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 audio is connected, the idle user timeout setting is ignored.

Operating System Audio Playback Support

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

Operating system	Audio playback and capture supported by:
Windows®	• Active KVM Client (AKC) • Virtual KVM Client (VKC)
Linux®	• Virtual KVM Client (VKC)
Mac®	• Virtual KVM Client (VKC)

Connecting and Disconnecting from a Digital Audio Device

Audio device settings are applied on a per KX III device basis.

Once the audio devices settings are configured and saved on the KX III, the same settings are applied to it.

See: Saving Audio Settings (on page 71) 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 70), Audio Playback and Capture Recommendations and Requirements (on page 189) for important information.

Connect to a Digital Audio Device

► *To connect to an audio device:*

1. Connect the audio device to the remote client PC prior to launching the browser connection to the KX III.
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 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.

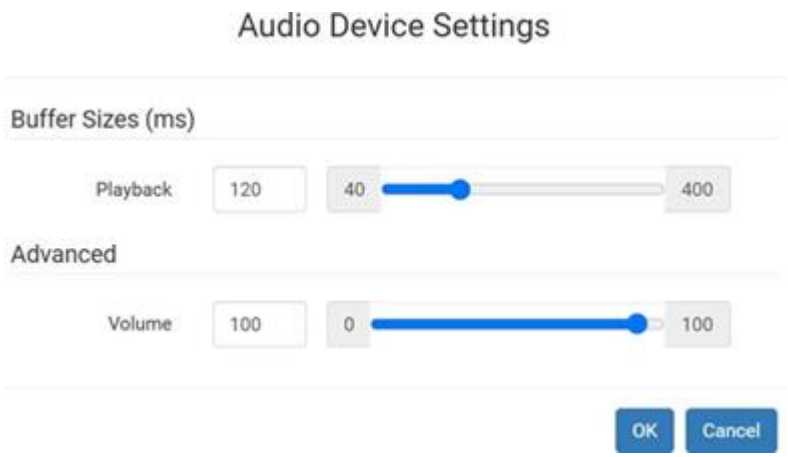
The buffer size can be adjusted whenever needed, including during an audio session.

Audio settings are configured in VKC or AKC.

Adjust Audio Settings

► *To adjust audio settings:*

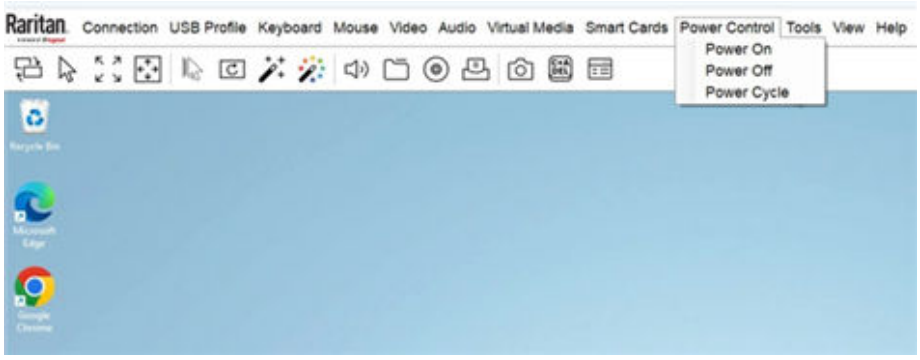
1. Select Audio Settings from the Audio menu. The Audio Settings dialog opens.
2. Adjust the capture and/or playback buffer size as needed. Click OK.



Power Control Using VKC, VKCS, and AKC

You can power on, power off, and power cycle a target through the outlet it is connected to.

Access the target, and then select a power control option from the Power Control menu.



The menu option is disabled if you do not have permission for power control, and when outlets are not associated with the port.

Note: The KVM client's Power Control can manage the outlets of the PDU connected to the KVM device.

Version Information

For version information about the client, in case you require assistance from Raritan Technical Support.

► *Virtual KVM Client:*

- Choose Help > About Raritan Virtual KVM Client.

► *Active KVM Client:*

- Choose Help > About Raritan Active KVM Client.

► *HTML KVM Client:*

- Choose Help > About Raritan HTML KVM Client.

Overview

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.

Active KVM Client (AKC)

To launch AKC, enter https://<IP address>/akc in a browser.

The Active KVM Client (AKC) is based on Microsoft Windows .NET® technology.

This allows you to run the client in a Windows environments without Java..

For details on using the features, see Virtual KVM Client (VKC and VKCs) Help (on page 41).

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®. See the Release Notes for supported versions.

AKC Supported Operating Systems

When launched from Edge®, the Active KVM Client (AKC) allows you to reach target servers via the KX III.

AKC is compatible with the following platforms:

- Windows 11 ® operating system (up to 64 bit)
  See the Release Notes for the latest supported versions.

AKC Supported Browsers

See the Release Notes for supported browser versions.

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 KX III IP Address in 'Trusted Sites Zone'

Add the IP address of the device being accessed to the browser's Trusted Sites Zone.

Disable 'Protected Mode'

Make sure that Protected Mode is not on when accessing this device.

Device certificate requirement for AKC

To validate the AKC server certificate following steps must be performed

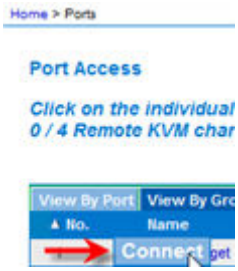
- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.
- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

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

Once you have logged on to the KX III 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 27) for details on additional available menu options.

HTML KVM Client (HKC)

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

HKC runs on Linux and Mac clients, and on Windows clients in, Edge, Firefox, Chrome and Safari browsers.

A mobile version of HKC also runs on iOS v10 and higher. See KVM Client Launching (on page 40) 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
- Audio Playback
- Virtual Media
- Dual Video Targets
- Keyboard Macros
- Import and Export of Keyboard Macros

- Send Text to Target
- Keyboard and Mouse Settings
- Single Mouse Mode
- Power Control

► *Not supported:*

- Port Scanning
- Smartcard
- Limited Tools Menu options.
- Limited keyboard support: US-English, UK-English, French, German, Swiss-German, Swedish and Japanese 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, no special function keys except for delay key.
- Virtual Media write not supported.
- USB drive connects.
- Audio capture.

► *Tips and Known Issues:*

- 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 and TLS Certificates for information on creating and installing certificates
- 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.
- 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.

- From Chrome running on Linux, to get ´ ` or ^, the key needs to be hit three times, or twice followed by a space.
- If HKC does not load, but rather displays a white screen, your browser memory may be full. Close all browser windows and try again.
- In Chrome, disable the background throttling to prevent background tabs from disconnecting after a certain amount of time. Go to chrome://flags, then search for "throttle". Set "Throttle Javascript timers in backgound" and "Calculate window occlusion on Windows" to "Disabled". Restart chrome to apply settings.

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 KX III comes configured to provide optimal performance for the majority of video streaming conditions.

► *KX3 default connection settings:*

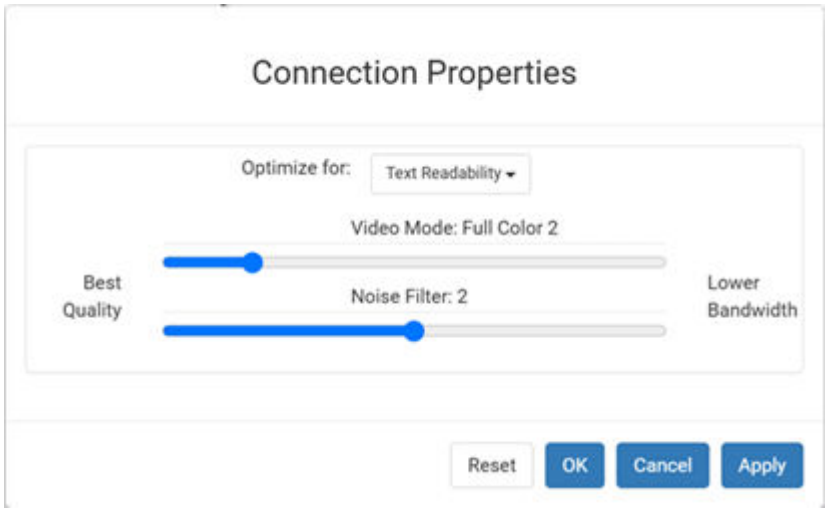
- Optimized for: Text Readability - video modes are designed to maximize text readability.

  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.

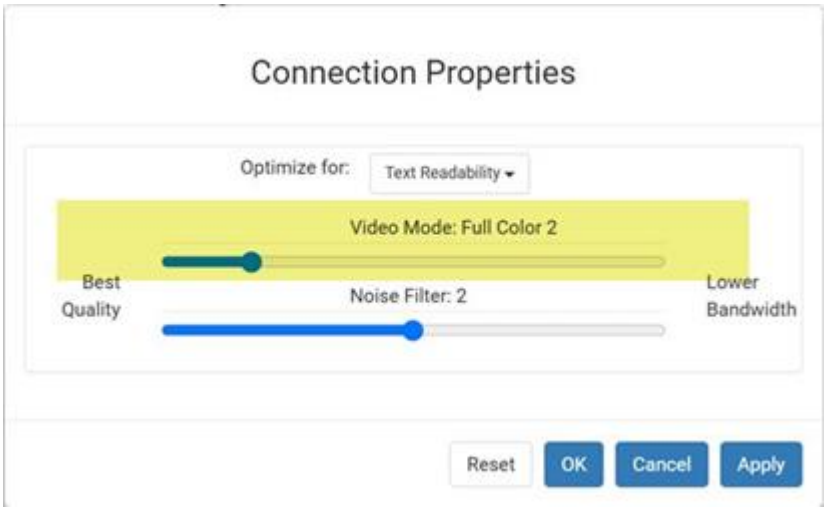
  The noise filter setting does not often need to be changed.

Click Reset to regain the default connection properties.



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.

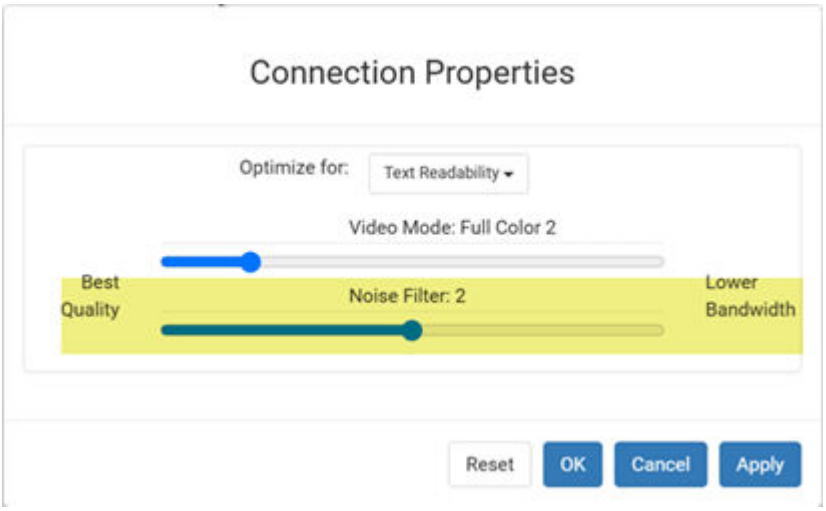
When Text Readability is selected as the Optimized setting, the four rightmost modes provide reduced color resolution or no color at all.

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

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 KX III.



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.

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.

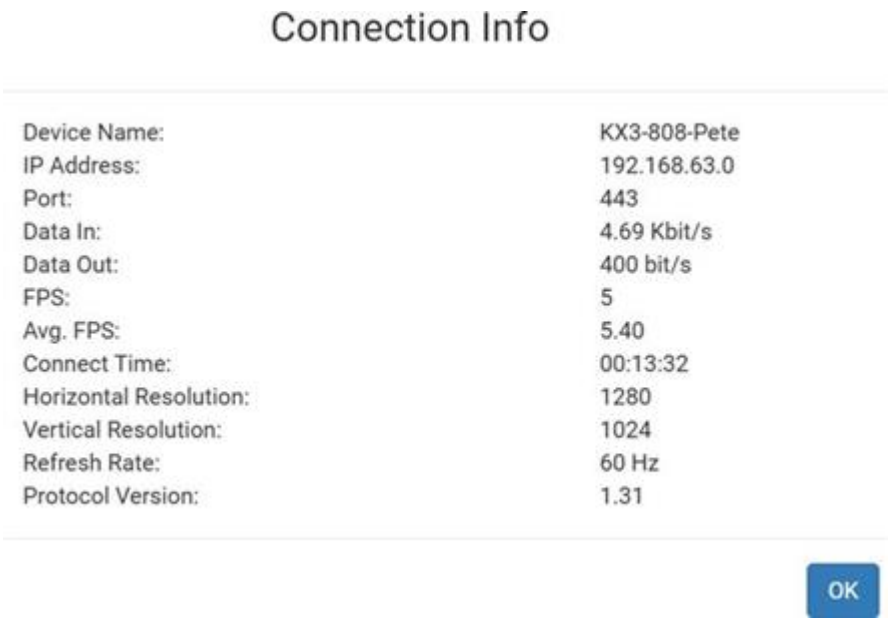
See Default Connection Properties (on page 79) for help configuring the connection properties.

- Name of the device
- IP address of the device
- Port - The KVM communication TCP/IP port used to access the device

- Data In/Second - Data rate received from the device
- Data Out/Second - Data rate sent to the device
- FPS - Video frames per second from the device.
- Average FPS - Average number of video frames per second.
- Connect Time - The duration of the current connection.
- Resolution - The target server's horizontal and vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - communications protocol version.
- Subsampling - Adaptive color subsampling
- Audio Playback Sample Rate - Audio playback sample rate seen if audio is connected.

► *To view connection info:*

- Choose File > Connection Info.



USB Profile

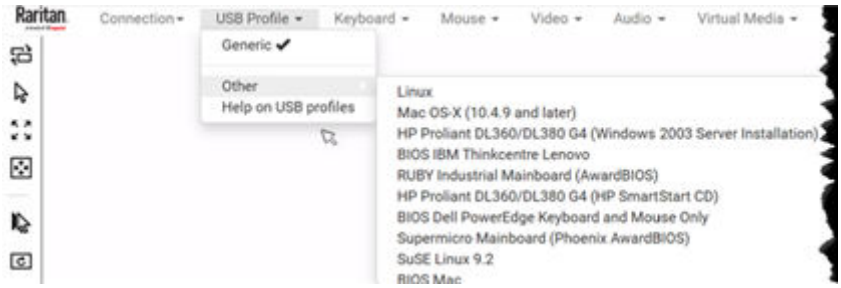
Select a USB profile that best applies to the KVM target server.

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.



Note: When using the D2CIM-VUSB-USBC on Mac targets, you must select the "Mac USB-C" profile.

► *To view details on USB profiles:*

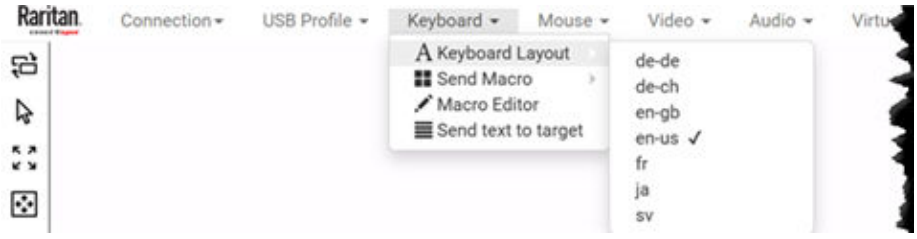
Choose USB Profile > Help on USB Profiles.

Keyboard and Mouse Menu

Keyboard Layout

► *To set your keyboard type.*

- Choose Input > Keyboard Layout, then select your keyboard type.
  - de-de
  - de-ch
  - en-gb
  - en-us
  - fr
  - ja
  - sv

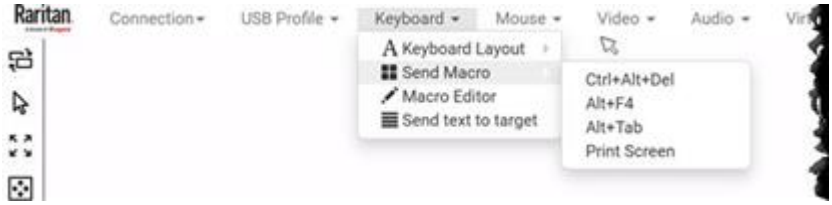


Send Macro

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.

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 KX III, your macros will only be available on the browser and KX III where they were created. To reuse your macros in another KX III device, you can import and export the macro files. See Import and Export Macros (on page 89).

► *To Access the Macro Editor:*

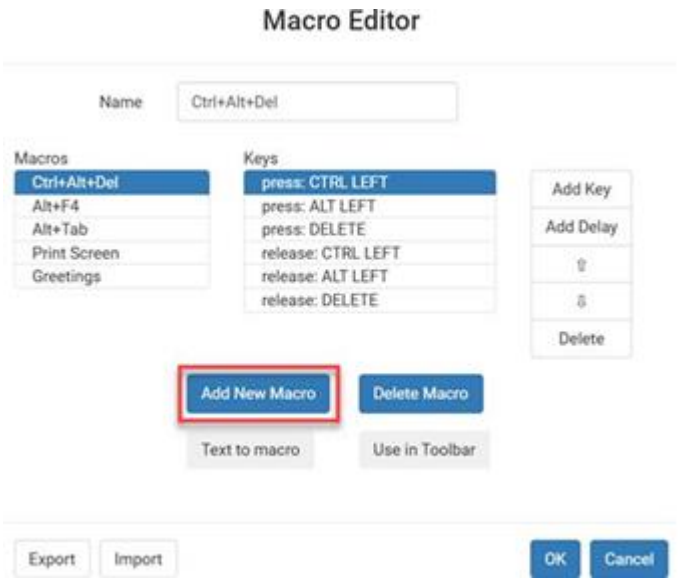
- Choose Keyboard > Macro Editor.
- Select a macro from the Macros list to view the key combination.



Add New Macro

► *To add a new macro:*

1. Choose Keyboard > Macro Editor.
2. Click Add New Macro.



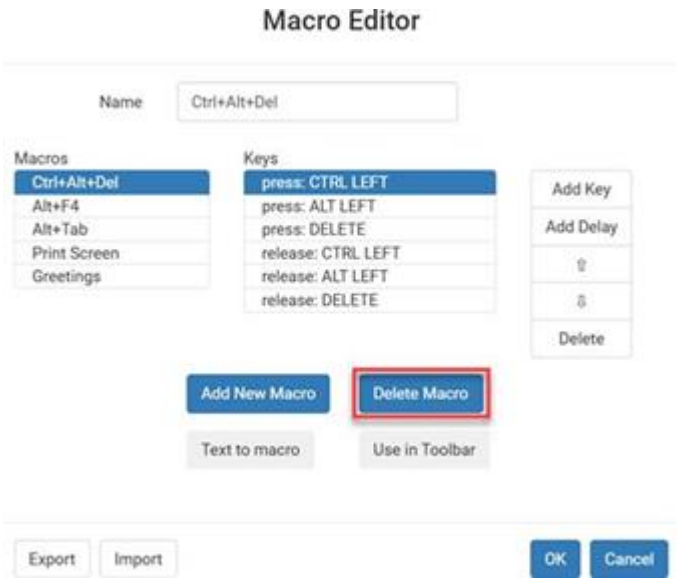
3. Enter a Name for the new macro. The name will appear in the Send Macro menu once the macro is saved.
4. Click Add Key, then press the key you want to add to the macro. The key press and key release appear in the Keys list.
   - To add more keys, click Add Key again, and press another key.
   - To remove a key, select it in the Keys list and click Delete.
5. To put the keys in the correct sequence, click to select a key in the Keys list, then click the up and down arrows.
6. To add a 500 ms delay to a key sequence, click Add Delay. A delay in the middle of a press-and-release key sequence indicates holding down a key. Add multiple delays to indicate a longer press-and-hold of a key. Click the up and down arrows to move the delays into the correct sequence.
7. Click OK to save. To use this macro from your toolbar, click Use in Toolbar. See Add a Macro to the Toolbar (on page 87) for more details.

This example shows a macro for a Mac bootup sequence that requires a 2-second delay.

Delete a Macro

► *To delete a macro:*

1. Choose Keyboard > Macro Editor.
2. Select the macro, then click Delete Macro.
3. Click OK.



Add a Macro to the Toolbar

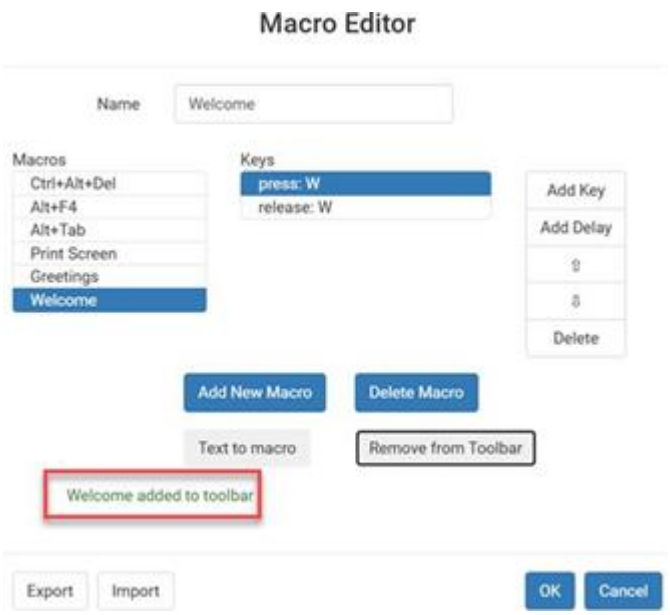
You can add a single macro to your HKC toolbar, so that you can use the macro by clicking an icon.

► *To add a macro to the toolbar:*

1. Choose Keyboard > Macro Editor.
2. Select a macro from the Macros list.
3. Click Use in Toolbar.



4. A message appears to confirm the macro is added to the toolbar.



5. To remove the macro from the toolbar, click Remove from Toolbar, or select a different macro and click Use in Toolbar.
6. Click OK and exit the Macro Editor. The macro icon is added to the toolbar when one has been set.



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 KX III, your macros will only be available on the browser and KX III where they were created. To reuse your macros in another KX III 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.

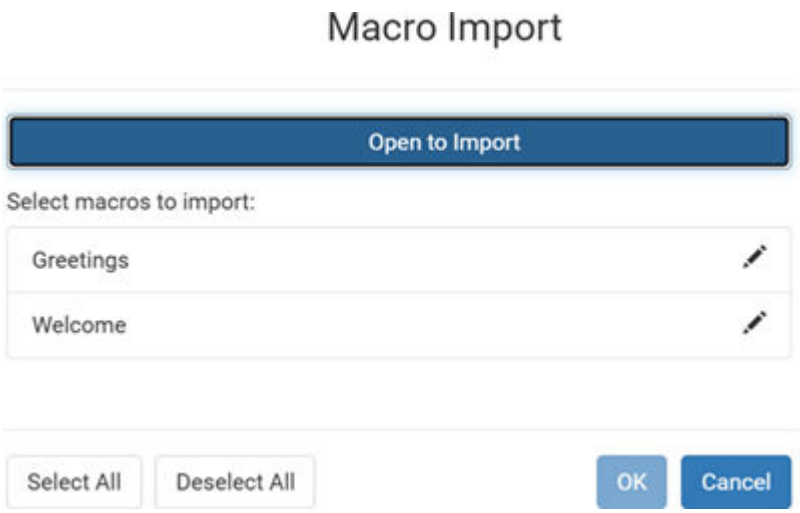
Macros are exported to an xml file named "usermacros.xml". Files are saved in your browser's default download location. Default macros are not exported.

Note: When exporting macros from Edge browser, a Down arrow is briefly displayed at the bottom of the KVM window and a file named "unconfirmed.crdownload" is saved to the default download directory. To use this file as a macro input file, rename it with a .xml extension.

► *To export and import macros:*

1. Choose Keyboard > Macro Editor. The list of macros created for your browser and KX III displays in the Macro Editor dialog.
2. To export the list, click the Export button, then save the file.
3. Log in to the KX III 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.



Known Issues for Macros

- You cannot add the Command (Windows) key to a macro from Fedora browsers. The key is consumed by the OS.

Text to macro

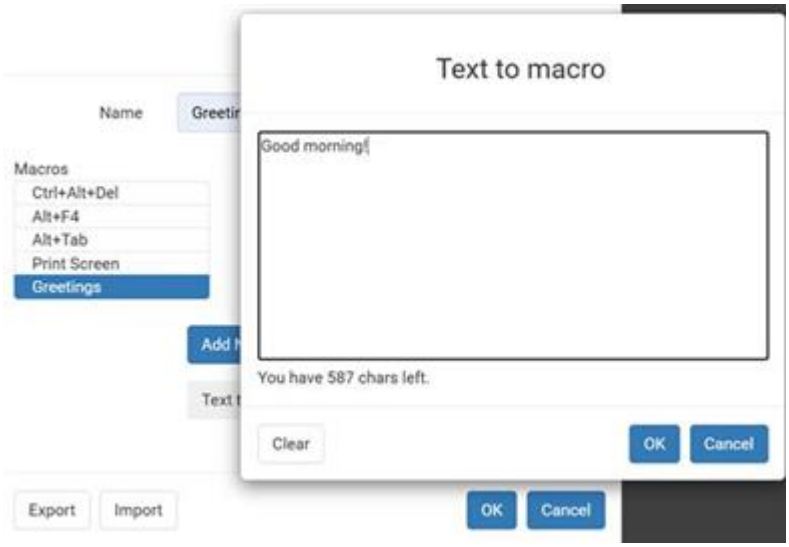
Text to macros will enable you to work more efficiently by producing frequently used phrases and paragraphs with a single command. Create a new macro and then assign text to it.

► *To add text to a macro:*

1. Choose Keyboard > Macro Editor.



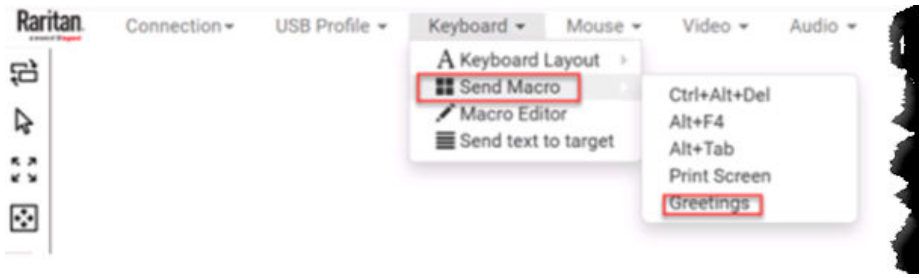
2. Select to add new macro and enter a macro name.
3. Click Text to macro.



4. Enter text in the text box and then click OK to save.
5. Click OK again in the Macro Editor to save the macro.

► *To use macros with text:*

1. Connect to target you want to send macro to
2. Choose Input > Send Macro and then select the macro you created.
3. Macro will be sent to the target.



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.

► *To send text to target:*

1. Choose Keyboard > Send text to target or click  in the toolbar.
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 KX III 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.

Intelligent mode requires that "Enhanced Pointer Precision" is unticked on the target (Control Panel/ Mouse/Pointer Options) and mouse speed is 50%.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when Intelligent and Standard Modes don't work. You can toggle between these two modes (single mouse and dual mouse).

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.

- Absolute Mouse Synchronization requires the use of a virtual media CIM - D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP, D2CIM-VUSB-USBC

► *To enter Absolute Mouse Synchronization Mode:*

- Choose Input > Mouse Modes > Absolute.

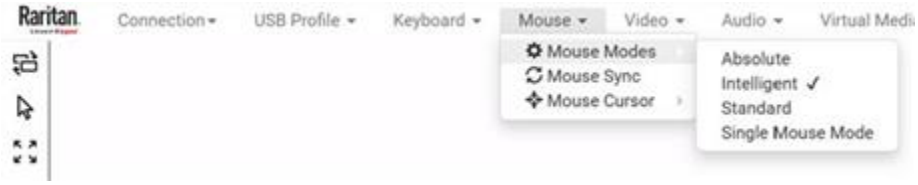


Intelligent

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target.

► *To enter Intelligent mouse mode:*

- Choose Mouse > Mouse Mode > Intelligent. The mouse will sync. See Intelligent Mouse Synchronization Conditions (on page 56), Intelligent Mouse Synchronization Conditions (on page 95).



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 Mouse > Mouse Modes > Standard.



Single

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

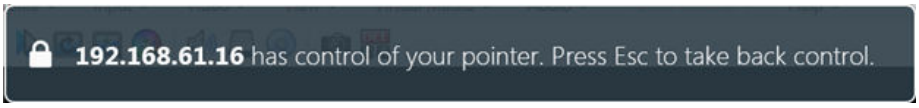
Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine. Single mouse mode is not available on Edge.

► *To enter Single mouse mode:*

- Choose Mouse > 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.
- For optimal mouse performance, set the target mouse speed to 50%. Avoid using extremely low or high mouse speed settings.
- The target advanced mouse properties such as “Enhanced pointer precision" or “Snap mouse to default button in dialogs” should be disabled.
- 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 52).

► *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.

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

   Brightness Green - Controls the brightness of the green signal.

   Brightness Blue - Controls the brightness of the blue signal.

c. Contrast Red - Controls the red signal contrast.

   Contrast Green - Controls the green signal.

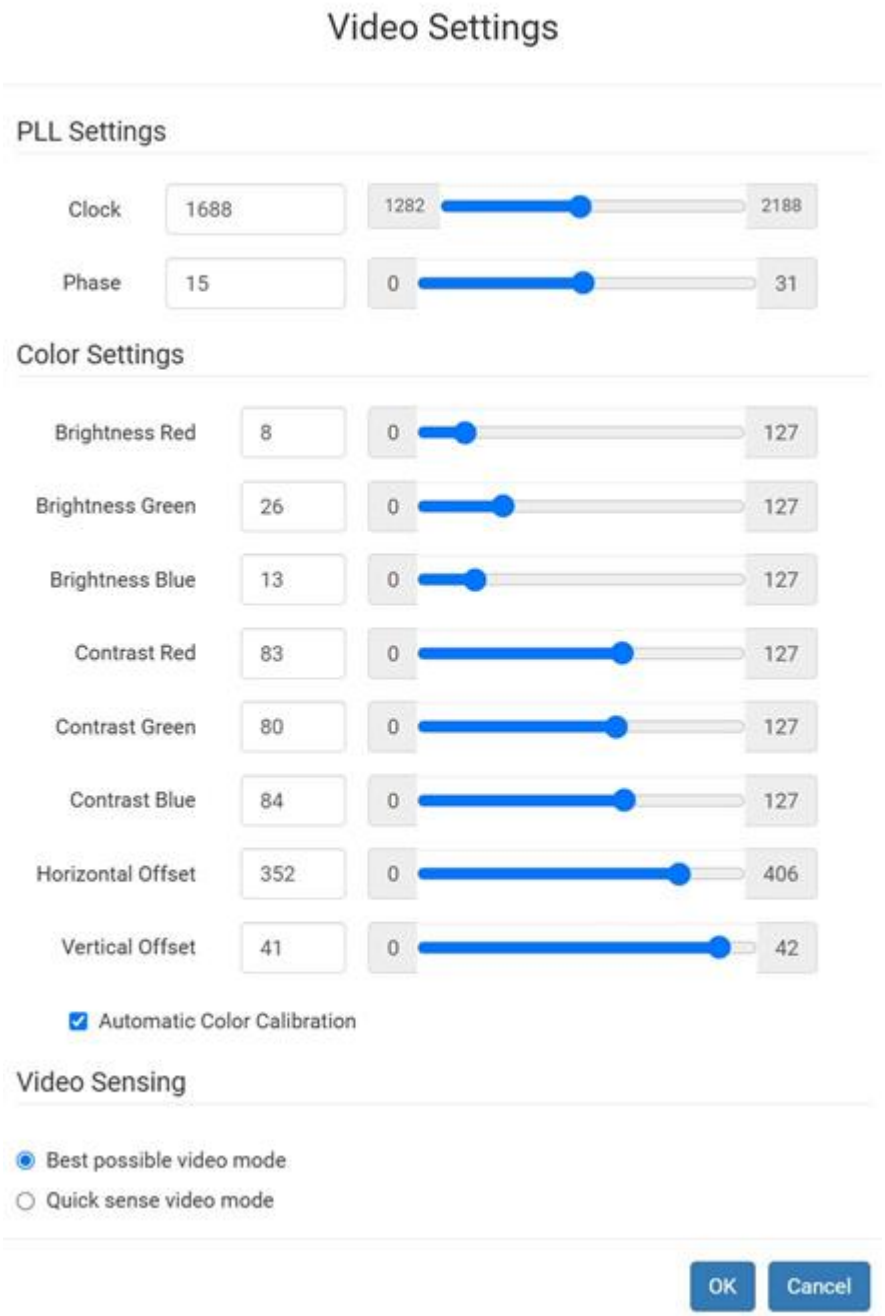
   Contrast Blue - Controls the blue signal.

   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.

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

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



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.

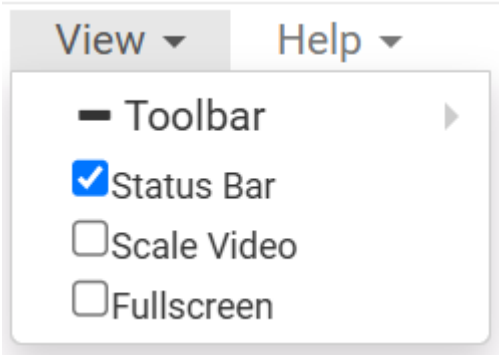
► *To clear the video settings cache:*

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



View Menu

The View Menu contains options to customize your HKC display.



► *Toolbar:*

The Toolbar selection allows a user to set it to Hidden, Vertical or Horizontal view. By default, the toolbar is displayed vertically, but you can reposition it horizontally or hide it entirely.

► *Status Bar:*

The Status Bar 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 limitations, HKC supports a different set of virtual media functions than the other KVM Clients.

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 by means of virtual media.

Supported browsers: Chrome, Firefox, Safari, Edge.

File size limit: 4GB per file

► *To connect files and folders:*

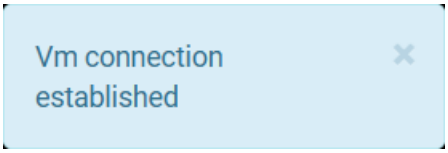
1. Choose Virtual Media > Connect Files and Folders. Or, click the matching icon in toolbar.



2. Drag files or folders onto the Map Virtual Media Files and Folders dialog. Click OK.

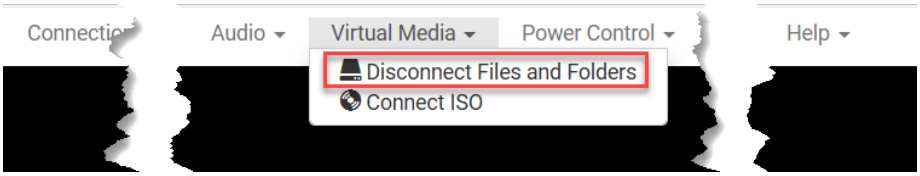


3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.



► *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 image file to the target. You can connect ISO, DMG or IMG files from your client PC or ISO files from a remote server.

Note: If connection to your SAMBA server is lost while transferring files from your image file to the target, keyboard and mouse control will be lost for several minutes, but will recover.

► *To map virtual media image files:*

1. Choose Virtual Media > Connect ISO. Or, click the matching icon in the toolbar.

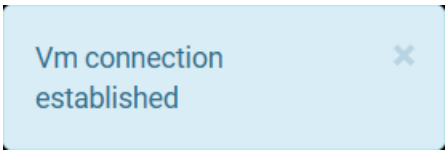


2. Select the option for your file's location:



- Select ISO Image if the image file is directly accessible on your client. Click Browse, select the ISO, DMG or IMG file, and click OK. The filename appears next to the Choose File button.
- Select Remote Server ISO Image for ISO files 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 39). Select the Hostname, then select the image 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.

Audio quality deteriorates if multiple target connections are open. To preserve quality, limit to four target connections open on HKC when an audio session is running.

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.

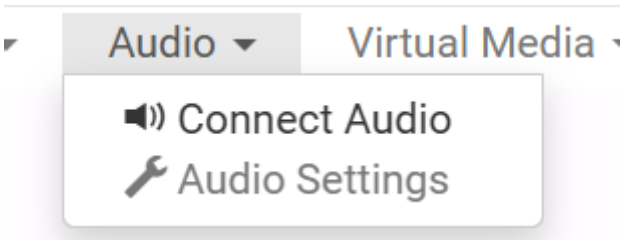
HKC connects the client PC's default audio playback device. To use a different device, it must be set as default in the client OS.

Only 44.1 kHz is available on Microsoft Edge for Windows, Google Chrome for Mac, Windows, and Linux, Firefox for Mac, Windows, and Linux, Safari for Mac, and iOS devices.

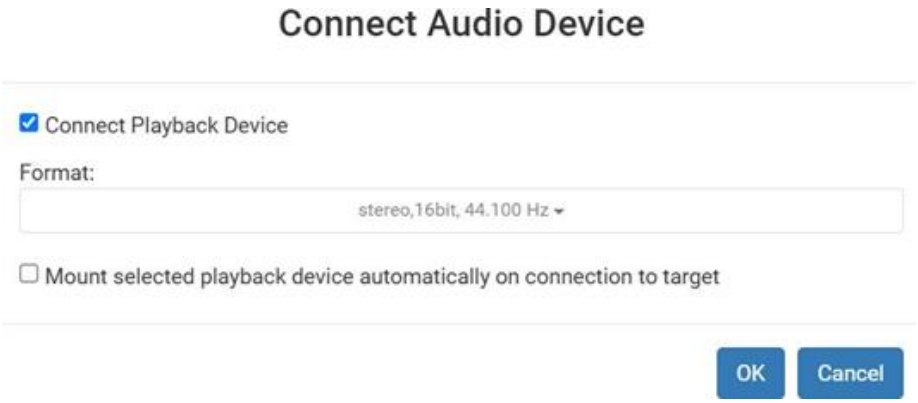
Note: For best quality, limit the number of audio sessions to a maximum of four KVM sessions.

► *To connect audio:*

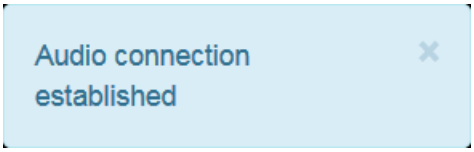
1. Choose Audio > Connect Audio, or click the matching icon in the toolbar.



2. In the Connect Audio Device dialog, select the Connect Playback Device checkbox.



3. 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 the target.
4. Click OK. A success message appears.



► *To disconnect audio:*

1. Choose Audio > Disconnect Audio, or click the matching icon in the toolbar.

Audio Settings

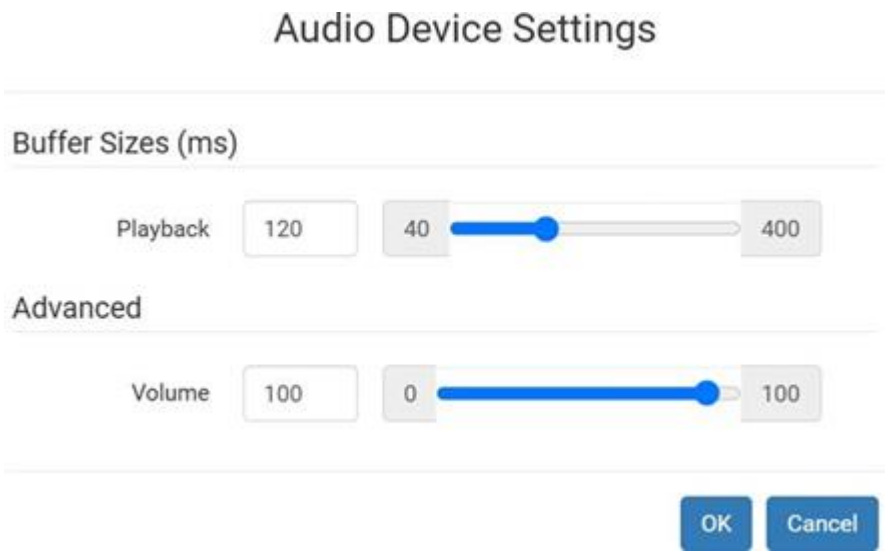
The Audio Settings option is enabled when audio is connected. Use the Audio Settings to set the buffer and volume.

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



3. Click OK.

Power Control Menu

See: Power Control

Using HKC on Apple iOS Devices

KX III supports remote access to targets from Apple mobile devices with iOS 10.0 or higher, using a mobile version of HKC. Due to Apple iOS limitations, you may notice some differences in operation. See: Limitations on Apple iOS Devices (on page 113).

Install Certificate on Apple iOS Device

You must install a CA-signed certificate on your Apple iOS device before you can connect to KX III. Access is prevented if only the default certificate is present. Depending on your browser, you may see an error such as "This Connection is Not Private".

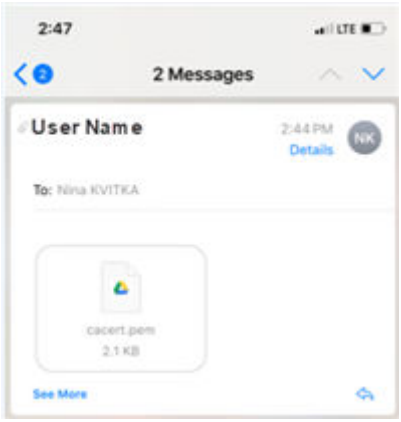
When creating certificates, the certificate Common name should match the IP address/Hostname used to connect to the device.

Install both the KX III certificate and the CA certificate used to sign the KX III certificate.

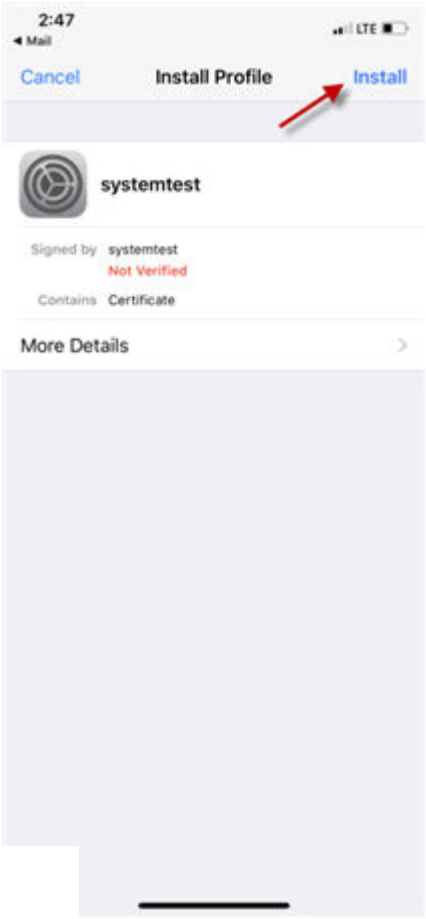
Note: If you have issues launching connections from IOS devices, check that the certificate meets Apple requirements: https://support.apple.com/en-us/HT210176

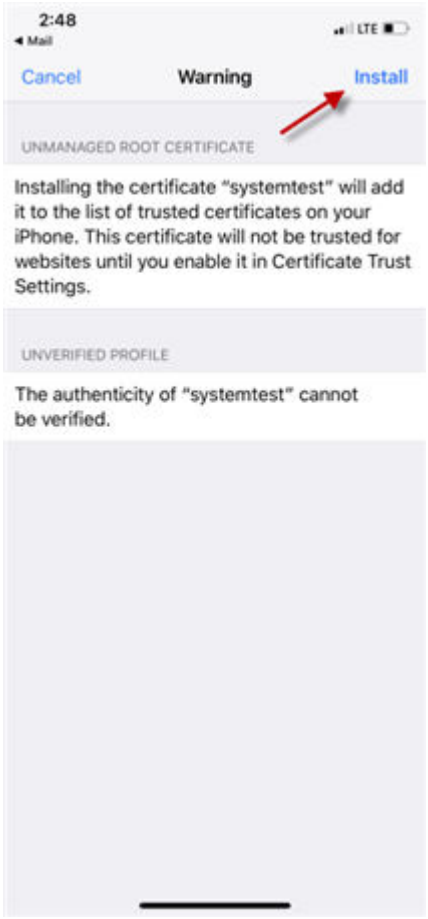
► *To install the certificate on an IOS device:*

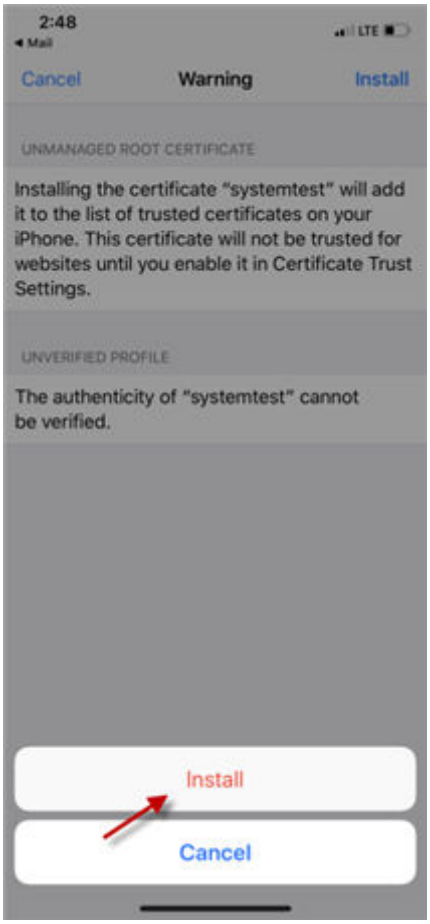
1. Email the certificate file to an email account that can be opened on the iOS device. Open the email and tap the attachment.



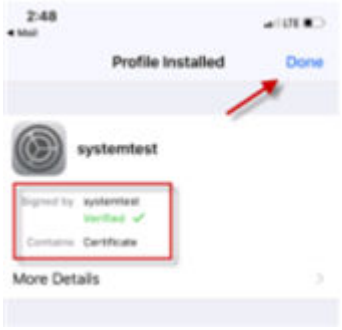
2. The certificate downloads as a "profile" that you have to install. You can have only one profile ready to install at a time. For example, if you download a profile and don't install it, and then download a second profile, only the second profile is available to be installed. If a profile is not installed within 8 minutes of downloading it, it is automatically deleted.
3. To install the profile, go to Settings, then tap Profile Downloaded.
4. Tap install, then follow prompts as presented to verify and Install.







5. When complete the certificate is marked Verified. Tap Done.



Touch Mouse Functions

Use the touchscreen equivalent for each mouse function. Some touch settings are configurable. See: Tools Menu (on page 111).

Single Finger Touch	Mouse Equivalent
touch down - move - release	move mouse pointer

short tap	left click
double short tap	left double-click
short tap - touch down - hold for 250ms	mouse equivalent of Right Click"
short tap - touch down - move - release	hold down left mouse button and move, as in drag and drop or select
Two Finger Touch	**Mouse Equivalent**
touch down - move - release	move screen

Keyboard Access on Mobile

Keyboard access to the target is through a virtual keyboard, available on the toolbar. For all other actions requiring keyboard input, the IOS popup keyboard displays automatically.

Manage HKC iOS Client Keyboard Macros

The HKC iOS client includes a list of default macros. You can create additional macros using the HKC Macro Editor or import macros from a file. See Macro Editor (on page 84) and Import and Export Macros (on page 89).

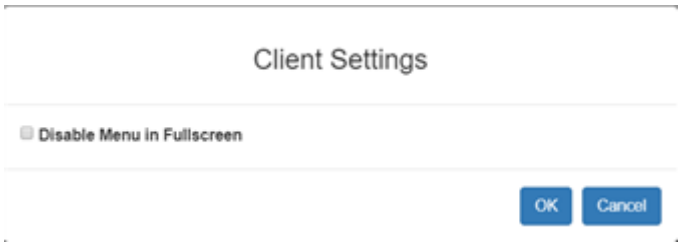
Note: To import macros when using an Apple iOS device, first export the file from HKC using a PC client. Add the file to a Cloud location to access from the IOS device for import.

Tools Menu

The Tools menu contains options for HKC target connection settings.

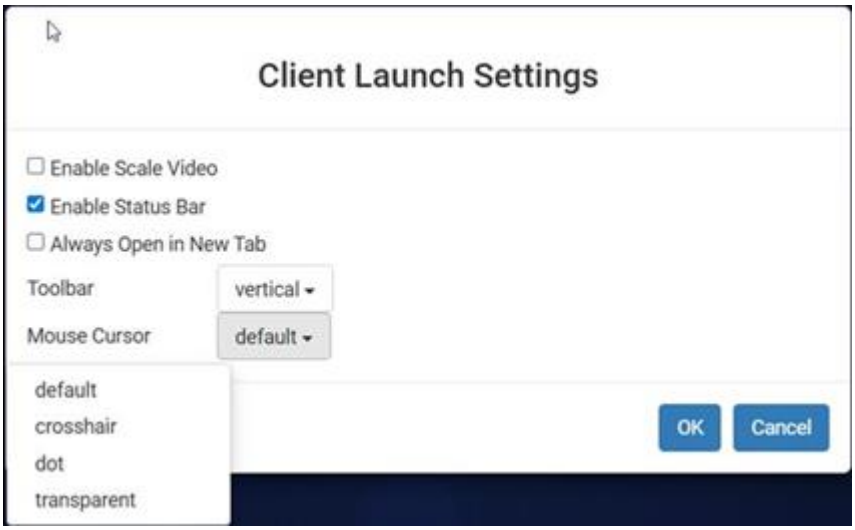
► *Client Settings:*

- Choose Tools > Client Settings to access the Disable Menu in Fullscreen option.
- When selected, the menu bar will not be available in fullscreen mode. This setting is specific to the client, so it must be set for each client device and each browser used for access.



► *Launch Settings:*

- Choose Tools > Launch settings to access Client Launch Settings options.
- This menus allows selection of Enable Scale Video, Toolbar options Vertical, Horizontal or Hidden, Enable Status Bar, Always Open in New Tab, and Mouse Cursor at target launch.



Note: "Always Open in New Tab" only applies to KVM target connections, serial connections are still opened in a new browser window and does not apply to HKC targets launched from CC-SG browser.

► *Touch Settings - enabled for iOS clients:*

- Tap Tools > Touch Settings to access the Client Touch Settings. Customize the Touch Input and Gesture Scrolling settings for your mobile device.

- Double Click Time: Time between two touch taps for the equivalent of a mouse double click.
- Mouse Click Hold Time: Time to hold after touch down for the equivalent of a mouse right click.
- Use Left Hand Mouse: Enable if the target OS's primary mouse button is set to Right.
- Enable Inverted Scroll x-Axis: If selected, two-finger movement to the right moves the screen to the left instead of the default right.
- Enable Inverted Scroll y-Axis: If selected, two-finger movement up moves the screen down instead of the default up.

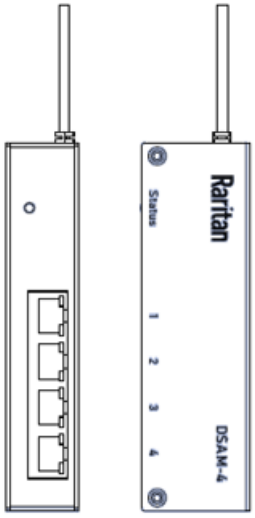
Limitations on Apple iOS Devices

Mobile access with iOS devices is supported for several Raritan products. Not all limitations apply to all products. Differences are noted.

- Target connections are closed after about one minute if the browser is in background, or if your iOS device enters Auto Lock mode
- Unable to create Macros for some special characters: F1-F24, ESC, Control, Alt, OS Meta keys and others. A selection of commonly used keys are available in the default Macro list. These keys can be edited. Additional keys such as F1-24 and arrows can be added using a Macro Import.
- In Safari on iOS, must refresh the connection to device after a KVM or Serial target launch in order to access menu options or serial targets. Not needed in Chrome on iOS.
- iOS does not support auto connect audio device to targets.
- On Ubuntu 14.04 target, no response to mouse click and hold on target items to simulate right clicking.
- Dual Target connection issues: Both target windows have to be closed separately. Only 1 port of a Dual target opened from Safari on iOS 11.x devices.
- Options "FullScreen" and "Resize window to fit screen" are not enabled/available on iOS.
- KB locale from the Client Virtual Keyboard must match input locale of device and OS locale of the target.
- iOS client target window does not have scrollbars. Unscaled video can be scrolled horizontally/vertically by sliding two fingers left/right or up/down. See: Touch Mouse Functions (on page 110).
- On Safari, users are prompted to save passwords when switching from a target with a server VM connection to another target. These prompts can be turned off by unchecking the box "Usernames and passwords" in Safari > Preferences > AutoFill.
- On Safari, the onscreen keyboard includes word forecast. Selecting a forecast word adds a space at the end. For example, at login screen, selecting "admin" enters "admin ". Similar behavior occurs for VM File server Username and other areas.
- Cannot move menu option panels such as Connection Info.
- iOS On-Screen keyboard is displayed from all mouse clicks on the HTML admin page if keyboard "Go" is tapped to save setting changes instead of tapping the Save button.
- For DSAM targets opened from iOS clients, every time a menu item is selected and closed the on-screen keyboard is displayed.
- The VM Files and Folders Option from the Virtual Media menu is disabled as not possible to drag and drop files to panel.
- Not all Accented letters are processed from iOS client.
- Macro files exported from iOS devices using Safari are automatically given the name "unknown" and need to be renamed with an xml extension to be imported to another client.

- Macro file export from Chrome on iOS devices is not possible due to issues with downloading data.
- Only characters supported by target will be processed. There is no response from iOS characters such as ¥, § and … that are found on iPad keyboards.
- With the onscreen keyboard, selecting ' character or "Return" key, brings keyboard display back to first in list.
- On default IOS client settings, characters ' and " are not processed from macro or send text to target options. The work around is to turn smart punctuation off

Serial Access With Dominion Serial Access Module



Connecting a KX III and a Dominion Serial Access Module (DSAM) provides access to devices such as LAN switches and routers that have a RS-232 serial port.

The DSAM is a 2- or 4 port serial module that derives power from the KX III.

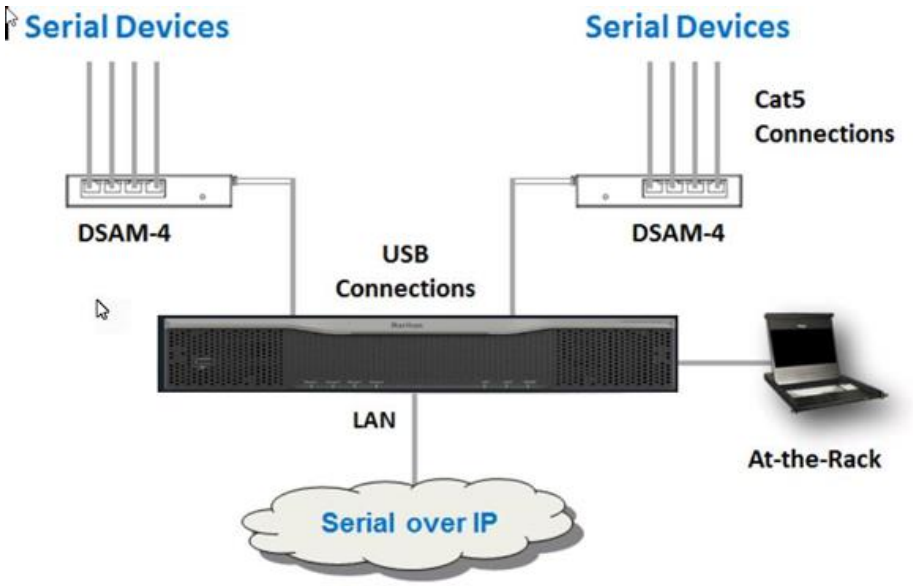
Connect a maximum of 2 DSAM modules to the KX III using USB cables. DSAM can be mounted in a 0U configuration.

In This Chapter

Connect DSAM. 116
View DSAM Serial Ports. 117
Configure DSAM Serial Ports. 118
Serial Port Keyword List. 121
Upgrade DSAM Firmware. 121
Supported CLI Commands. 121
Browser Tips for HSC. 125
Connect to DSAM Serial Targets in Port Access Page. 127
Connect to DSAM Serial Target with URL Direct Port Access. 128
Connect to DSAM Serial Target via SSH. 128
HTML Serial Console (HSC) Help. 128

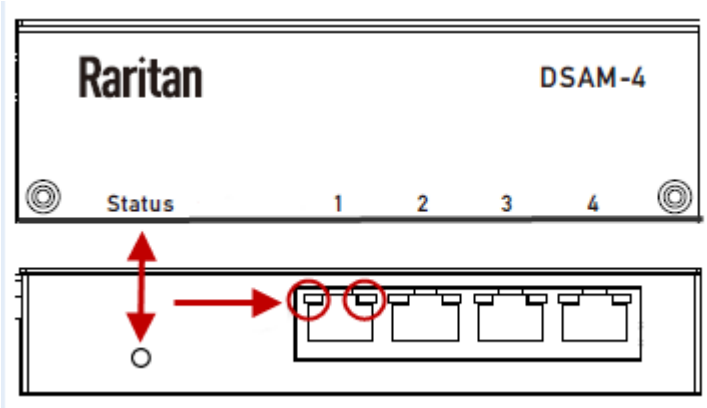
Connect DSAM

1. Connect the DSAM unit's USB cable to the TOP USB port on the rear of KX III device. Additional DSAM units can be added at any other USB port.
2. Connect the serial devices to the serial ports on the DSAM unit.



DSAM LED Operation

The DSAM unit has one LED for status, and 2 LEDs on each port.



► *Status LED:*

The Status LED is labeled on the unit front. Light is on back. The Status LED gives information at bootup and upgrade.

- Green LED - Slow blink: DSAM booting up but not controlled by KX III.
- Blue LED - Slow blink: DSAM controlled by KX III.
- Blue LED - Fast blink: Firmware upgrade in progress.

► *Port LEDs:*

Each port has a left Green LED and a right Yellow LED.

- Green LED: Port is set as DCE
- Yellow LED: Port is set as DTE
- LEDs off: Port is set as AUTO and no target is connected

Supported USB Device Combinations

Each USB device draws from a fixed pool of USB resources. There are limits on the number of USB devices that can be connected to the KX III at the same time.

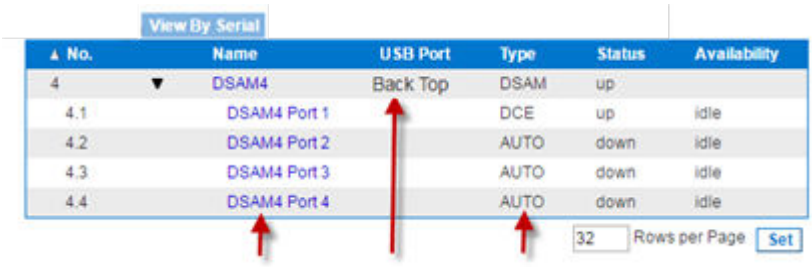
The following device combinations are supported for all KX III hardware versions.

If you have the latest 2020-released KX III hardware, which have a hardware revision number beginning with A or higher, the USB-combination in the last column is supported. Older hardware revision numbers begin with 0-9. To check your hardware version: Go to Maintenance > Device Information > Hardware Revision number.

Device	Combo 1	Combo 2	Combo 3	Combo 4	Combo 5	New KX3 Hardware
4-Port DSAM	X			X		X
4-Port DSAM	X	X	X			X
2-Port DSAM		X	X		X	
2-Port DSAM						
Keyboard and Mouse		X		X	X	X
SmartCard				X	X	X
Wireless Modem			X	X	X	X
DSAM Ports	8	6	6	4	2	8

View DSAM Serial Ports

When a DSAM unit is connected to the KX III, a new tab is available in the Ports page. The View by Serial tab shows all connected serial ports.



► *To view DSAM serial ports:*

In the Port Access page, click the View By Serial tab.

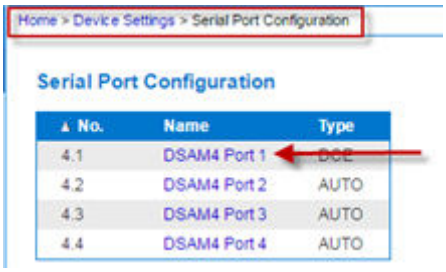
- Ports are listed by physical USB position on the DSAM unit.
- USB Port column indicates which KX III USB port DSAM is plugged into.
- Type column indicates port's DTE/DCE setting.

Configure DSAM Serial Ports

The serial port configuration options are available when a DSAM unit is connected.

► *To configure DSAM serial ports:*

1. Choose Device Settings > Serial Port Configuration.
2. Click the Port Name for the port you want to configure.



3. The Port Type is set to Serial only.
4. Enter a meaningful name for the serial target or leave the default name.



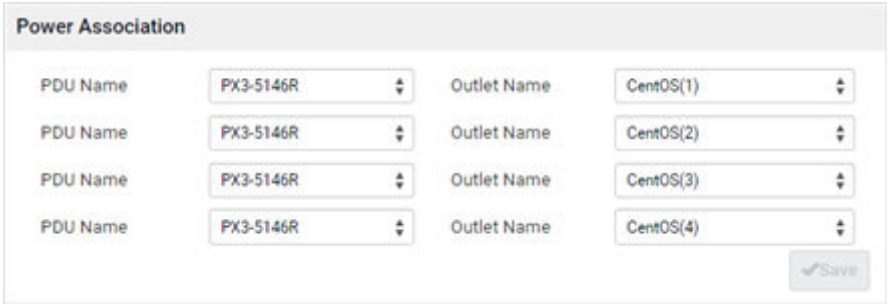
Power Association

If an outlet is connected to the same server that the port is connected to, a power association can be made with the target device.

A port can have up to four associated outlets, and you can associate a different rack PDU (power strip) with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

To use this feature, you need Raritan remote rack PDU(s).

1. Select the Power Strip Name and associate a name with each of the power strip's outlets by selecting from the Outlet Name drop-down.
2. Click OK. A confirmation message is displayed.



Serial Port Settings

Configure the remaining port settings.

1. Select the terminal emulation type from the drop-down menu in the Emulation field. This is the terminal emulation mode used to match the serial targets connected to the ports.
   - VT100
   - VT220
   - VT320
   - ANSI
2. Set Encoding if you want to always use a specific character encoding for this port. Encoding overrides the global setting for the port to whatever value you set.
   - DEFAULT
   - US-ASCII
   - 8BIT-ASCII
   - ISO-8859-1
   - ISO-8859-15
   - UTF-8
   - Shift-JIS
   - EUC-JP
   - EUC-CN
   - EUC-KR
3. In the Equipment Type field, indicate whether you want the KX III to automatically detect a physical connection to the target. The default is Auto Detection.

Force DTE causes KX III to act as a piece of data terminal detection equipment to detect targets connected to it.

Force DCE causes KX III to act as a piece of data communications equipment to detect equipment connected to it.

Note: If the target has the ability to autodetect either DTE or DCE, you must select either Force DTE or Force DCE for the port. KX III does not support autodetection of both DCE and DTE on the same port.

---

4. Select the value of Bits Per Second (BPS) from the BPS drop-down menu.
   - BPS options: 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
5. Select the Parity/Bits from the Parity Bits drop-down menu.
6. Select the Flow Control from the Flow Control drop-down menu.
7. Select the Stop Bits from the Stop Bits drop-down menu.
8. If you need to configure the delay between when individual characters are sent via the port, enter the time in milliseconds in the Char Delay field.
9. To configure the delay between when lines of text are sent via the port, enter it in the Line Delay field.
10. Configure the sendbreak duration by entering the send break time in the Send Break Duration field. The send break is configurable from 0ms - 1000ms.
11. Select an option to allow single or multiple writers on a port at one time in the Multiple Writers field.
12. Select Always Active if you want to log activities coming into a port even if no user is connected.

The default option is to not maintain port access without a connected user, which means ignore data coming into a port when no user is connected.

This option is for port data logs.

Note: When no users are logged into a port session, port traffic, by default, is discarded .

---

13. If you do not want messages displayed to users connecting to KX III via Direct Port Access, select the Suppress Message checkbox.
14. Select the Escape Mode.

The escape sequence affects only the CLI. When entering the escape mode, the user is given a menu of commands that can be performed (for example, gethistory, power commands, and so on), a command to return to the port session, and a command to exit the port connection.

The default is None.

Change as follows:

- Select control from the drop-down menu in the Escape Mode field.

15. Type the character in the Escape Character field. The default for the KX III is] (closed bracket).

Raritan recommends that you do not use [or Ctrl-[. Either of these may cause unintended commands, such as invoking the Escape Command unintentionally. This key sequence is also triggered by the arrow keys on the keyboard.

16. Type a command in the Exit Command field, such as `logout`.

This is the command that is sent to your system when a user with write permission disconnects from the port.

The main function of this command is to ensure that the user's session on the target machine is closed; however, it is not imperative to have an Exit command configured on a port.

17. Click OK.

Apply Settings to Other Ports

Once finished, you can apply the same port settings to other ports.

1. Select the ports from the Apply Serial Port Settings To Other Ports section of the page.
2. Click OK to apply the port configuration settings.

Serial Port Keyword List

Port keywords work as a filter. If a keyword is detected, a notification is sent to the following:

- Audit Log
- Syslog Server (if configured)
- SNMP (if configured)
- SMTP (if configured)

This feature is useful for notifying administrators if a particular event occurs on a port.

For keywords to trigger when no users are connected to a port, "Always Active" must be selected on the port's Port Configuration page.

A list of existing port keywords is displayed on the Port Configuration page as well.

► *To configure serial port keywords:*

1. Choose Device Settings > Serial Port Keyword List. The Serial Port Keyword List page opens.
2. Click New at the bottom of list on the page. The Keyword page opens.
3. Type a keyword in the Keyword field.
4. Select the Port(s) you want to associate with that keyword.
5. Click Add to add them to the Selected box.
6. Click OK.

Upgrade DSAM Firmware

DSAM firmware is upgraded automatically during KX III device firmware upgrades if a new DSAM version is detected in the device firmware. You can also upgrade your DSAM firmware manually.

► *To upgrade the DSAM firmware manually:*

1. Choose Maintenance > DSAM Firmware Upgrade.
2. Select the checkboxes for the DSAM units you want to upgrade to the Upgrade DSAM Version listed.
3. Click Upgrade, then click OK to confirm. A progress message appears.
4. When firmware upgrade completes, a success message appears.

Supported CLI Commands

Port Connect Commands

Connect to a serial port using port number or port name. Use double quotes around port names that contain space symbols. For example: "DSAM Port 1".

```
admin > connect <port number>
```

admin > connect <port name>

- *Port number example:*

```
admin > connect 1.1
```

- *Port name example:*

```
admin > connect "DSAM Port 1"
```

Port Sub-Menu Commands

The port sub-menu can be reached using the escape key sequence.

Clear history buffer for this port.

```
admin > [portname] > clearhistory
```

Close this target connection. When a target is disconnected, the appropriate disconnect message appears.

```
admin > [portname] > close, quit, q
```

Display the history buffer for this port.

```
admin > [portname] > gethistory
```

Get write access for the port.

```
admin > [portname] > getwrite
```

Return to the target session.

```
admin > [portname] > return
```

Send a break to the connected target.

```
admin > [portname] > sendbreak
```

Lock write access to this port.

```
admin > [portname] > writelock
```

Unlock write access to this port.

```
admin > [portname] > writeunlock
```

Query Power status of this port.

```
admin > [portname] > powerstatus
```

Toggle Power On/Off of this port.

```
admin > [portname] > powertoggle
```

Power on the target.

```
admin > [portname] > poweron
```

Power off the target.

```
admin > [portname] > poweroff
```

Power cycle the target.

```
admin > [portname] > powercycle
```

Configure Ports Commands

Enter `admin >` to access the menu.

Command	Description	Parameters
`listports`	List accessible ports	NA

Enter `admin > config > port` to access the menu.

Command	Description	Parameters
`config port`		• port <number | range | *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) • name <port name> - Port name • bps <1200 | 1800 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 | 230400> - Port speed in bits-per-second • parity <none|even|odd> - Port parity type • flowcontrol <none|hw|sw> - Port flowcontrol type hw = hardware flow control sw =X on/X off) • eqtype <auto|dte|dce> - Equipment type (auto=>AUTO Detection, dte=>Force DTE, dce=>Force DCE) • Note: If the target has the ability to autodetect either DTE or DCE, you must select either Force DTE or Force DCE for the port. KX III does not support autodetection of both DCE and DTE on the same port. • escapemode <none|control> - Use Ctrl-key (escapemode=control) or single key (escapemode=none) as escape sequence; for example, Ctrl- => escapemode=control, escapechar= escapechar char-Escape character • Raritan recommends that you do not use or Ctrl- as the Escape command. Either of these may cause unintended commands, such as opening a menu, instead of invoking the Escape Command. • emulation <vt100 | vt220 | vt320 | ansi> - Target Emulation type • sendbreak <duration> - Duration of the sendbreak signal in milliseconds. • exitstring <cmd #delay; > - Execute exit string when port session closes, for example, config port 1 exitstring logout (execute logout on exit) config port 1 exitstring #0 (disable exit string for the port). The delay is the amount of time to wait after writing the command to the target. Number in seconds up to 60. • alwaysactive <true | false> - Determine whether data coming into a port is logged, for example, config port 1 alwaysactive true (always log activities coming into a port even if no user is connected) config port 1 alwaysactive false (ignore data coming into a port when no user is connected) • suppress - Determine whether none or all messages should be displayed during a DPA connection, such as "Authentication successful" • encoding - Target Encoding type (DEFAULT|US-ASCII|ISO-8859-1|ISO-8859-15|UTF-8|Shift-JIS|EUC-JP|EUC-CN|EUC-KR|8BIT-ASCII) • multiwrite - Port set in Multiple Writer Mode. • chardelay delay - Delay inserted between writing characters (0-9999ms) • linedelay delay - Delay inserted between writing lines (0-9999ms) • stopbits - Number of bits used to signal the end of a character (usually 1) (1/2) • stopbits <1/2> -Number of bits used to signal the end of a character • chardelay - Delay inserted between characters (0-9999) in ms • linedelay - Delay inserted between lines (0-9999) in ms • escapechar - Escape character • encoding - <DEFAULT/US-ASCII/ISO-8859-1/ISO-8859-15/UTF-8/Shift-JIS/EUC-JP/EUC-CN/EUC-KR/8BIT-ASCII> - Target encoding type • multiwrite <true/false> - Port set in multiple writer mode • suppress <true/false> - Suppress SX messages when connecting to this target(true/false) • sendbreak - Duration of sendbreak signal in ms

Command Line Interface Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter on your keyboard to execute the command.
- Press Tab on your keyboard to complete a command. Tab also completes parameters and values (if the value is part of an enumerated set).

Command Line Interface High-Level Commands

The CLI is menu based. Some commands move to a menu with a different command set.

The following common commands can be used at all levels of the command line interface (CLI):

- `top` – Return to the top level of the CLI hierarchy, or the `username` prompt.
- `history` – Displays the last 200 commands the user entered into the KX III CLI.
- `logout` – Logs the user out of the current session.
- `quit` – Moves the user back one level in the CLI hierarchy.
- `help` - Displays an overview of the CLI syntax.

Supported Escape Key Characters

The default escape key is CTRL]

The following characters are supported for customized escape keys.

- A-Z
- a-z
- [ ]
- { }
- ^
- _
- \
- |

Browser Tips for HSC

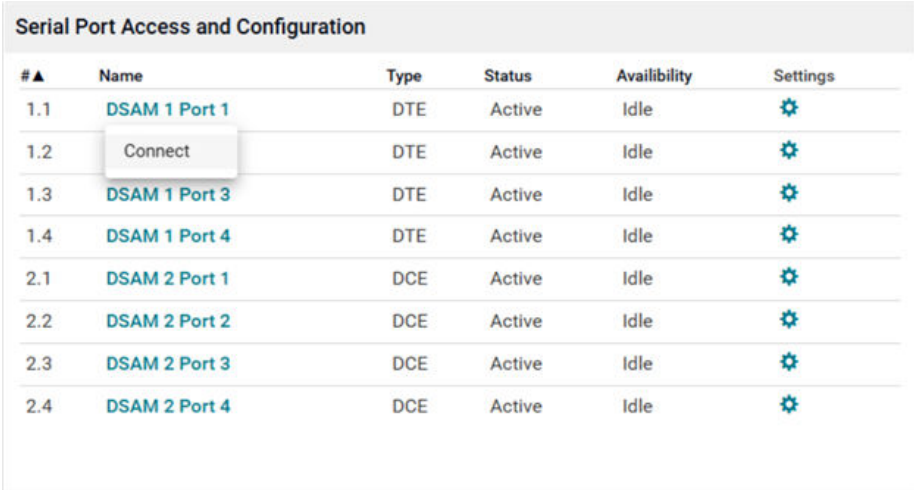
Some browsers have limitations that affect HSC.

- Edge & Chrome, disabling the background throttling to prevent background tabs from disconnecting after a certain amount of time. Go to chrome://flags, then search for "throttle". Set "Throttle Javascript timers in backgound" and "Calculate window occlusion on Windows" to "Disabled". Restart chrome to apply settings.
- Browser option to select certificate for authentication displayed on Edge and Chrome after session is idle for about 5 minutes, due to internal browser SSL caching and timeouts. If certificate is selected promptly, reconnection is successful. With longer idle times, authentication is not successful, and the browser should be restarted to reconnect. Issue is not observed in Firefox.
- Edge has an internal limitation on the number of websockets that are allowed to be created to a single server (6). This can be changed by modifying a registry variable as shown here : https://msdn.microsoft.com/en-us/library/ee330736(v=vs.85).aspx#websocket_maxconn.
- Edge,and Safari have a limitation when connecting to IPv6 devices. Using the numerical URL will not work when it attempts to establish a websocket connection. In these browsers, use the device hostname or literal IPv6 as UNC to connect to the SX II. See https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names
- When using HSC in IOS Safari, the keyboard may not appear in some pages if the "request desktop website" setting is enabled. To change the setting, go to Settings > Safari >Request Desktop Website, then make sure All Websites is not selected, and the device address is not selected. You can also set this per address by clicking the "aA" in Safari's URL pane when connected to the HSC port, then select "Website Settings" and make sure that "Request Desktop Website" is not selected.

Connect to DSAM Serial Targets in Port Access Page

► *To connect to DSAM serial targets:*

1. In the Port Access page, click the View By Serial tab to view the serial targets.
2. Click the port name you want to connect to. Click Connect.



3. The HTML Serial Console (HSC) window opens. See HTML Serial Console (HSC) Help (on page 128)



4. To exit the serial port, hit the hot-key. Default hot key is Scrolllock-Scrollock.

Connect to DSAM Serial Target with URL Direct Port Access

1. Choose Security > KVM Security, then select the Enable Direct Port Access via URL checkbox.
2. To connect with direct port access, type the URL:

"https://<IP Address>/dpa.asp?port=<serial port number>&username=<user name>&password=<password>"

Example: https://192.168.51.101/dpa.asp?port=1.4&username=admin&password=raritan0

---

3. HTML Serial Client (HSC) launches and connects to the serial target.

Connect to DSAM Serial Target via SSH

1. Choose Device Settings > Device Services, then select the Enable SSH checkbox.
2. Launch SSH client in client PC to connect to KX III.
3. After login, user will enter CLI interface.
4. Type command "connect <serial port number>", or type command "connect <name of serial port>".

Example-1: connect 4.1

Example-2: connect "DSAM4 Port1"

---

5. If successful, serial target is accessed.
6. To exit serial target, type escape-key-sequence, default is Ctrl-], then enter port sub-menu CLI interface.
7. Type "quit", then enter main CLI interface.

HTML Serial Console (HSC) Help

When you click Help it displays copyright and privacy statement information.

HSC Functions

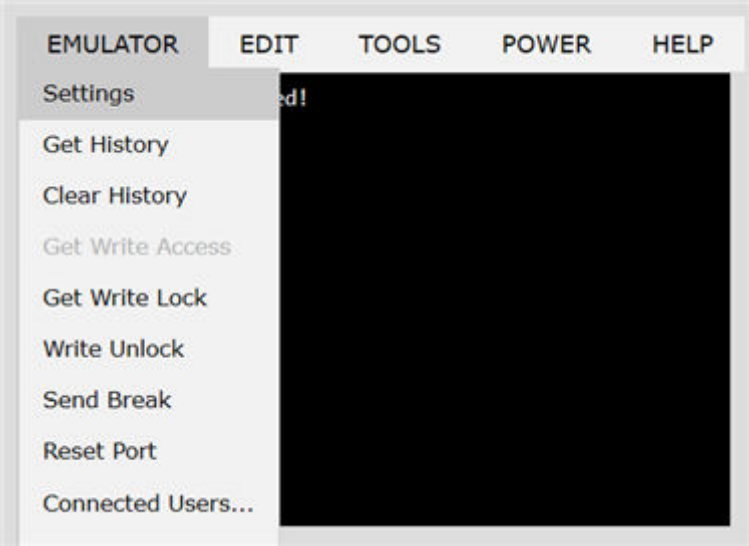
Emulator

IMPORTANT:

- HSC sessions are affected by the KX III Idle Timeout.
- If you have not changed the KX III Idle Timeout setting from the default, your session could be closed automatically if it exceeds the Idle Timeout period.
- Change the default Idle Timeout setting and then launch the HSC. See Login Limitations for details on changing the Idle Timeout setting.

Access Emulator Options

1. Select the Emulator drop-down menu to display a list of options.



Settings

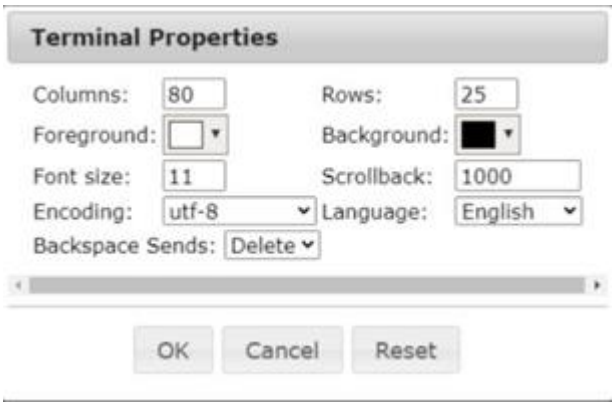
Note:

KX3 administrators can set Terminal emulation settings in Setup > Serial Port Configuration.

KX4-101 and KX3G2 administrators can set terminal emulation settings in DSAM Serial Ports > Settings.

SX2 administrators can set terminal emulation settings in Device Settings > Port Configuration.

1. Choose Emulator > Settings. The Terminal Properties dialog displays the default settings.



2. Set the terminal size by selecting the number of Columns and Rows. Default is 80 by 25.
3. Set the Foreground and Background colors. Default is white on black.
4. Set the Font size. Default is 11.
5. Set the Scrollback number to indicate the number of lines available for scrolling.
6. Choose one of the following from the Encoding drop-down menu:
   - UTF-8
   - 8BIT-ASCII
   - ISO-8859-1
   - ISO-8859-15
   - Shift-JIS
   - EUC-JP
   - EUC-KR
7. Choose one of the following from the Language drop-down menu:
   - English
   - Japanese
   - Korean
   - Chinese
   - Bulgarian
8. The Backspace Sends default is ASCII DEL, or you can choose Control-H from the Backspace Sends drop-down menu.
9. Click OK to save. If you changed the Language setting, the HSC changes to that language when the Display Settings window is closed.

The emulator settings are saved on a per port basis in the browser used for HSC, so make sure your browser is not set to delete history on exit.

Get History

History information can be useful when debugging, troubleshooting, or administering a target device. The Get History feature:

- Allows you to view the recent history of console sessions by displaying the console messages to and from the target device.
- Displays up to 512KB of recent console message history. This allows a user to see target device events over time.

When the size limit is reached, the text wraps, overwriting the oldest data with the newest.

Notes: History data is displayed only to the user who requested the history.

To view the Session History, choose Emulator > Get History.

Clear History

- To clear the history, choose Emulator > Clear History.

Get Write Access

Only users with permissions to the port get Write Access. The user with Write Access can send commands to the target device. Write Access can be transferred among users working in the HSC via the Get Write Access command.

To enable Write Access, choose Emulator > Click Get Write Access.

- You now have Write Access to the target device.
- When another user assumes Write Access from you:
  - The HSC displays a red block icon before Write Access in the status bar.
  - A message appears to the user who currently has Write Access, alerting that user that another user has taken over access to the console.

Get Write Lock

Write lock prevents other users from taking the write access while you are using it.

1. To get write lock, choose Emulator > Get Write Lock.
2. If Get Write Lock is not available, a request rejected message appears.

Write Unlock

To get Write Unlock, choose Emulator > Write Unlock.

Send Break

Some target systems such as Sun Solaris servers require the transmission of a null character (Break) to generate the OK prompt. This is equivalent to issuing a STOP-A from the Sun keyboard.

Only users with Write Access privileges can send a break.

To send an intentional “break” to a Sun Solaris server:

1. Verify that you have Write Access. If not, follow the instructions in the previous section to obtain write access.
2. Choose Emulator > Send Break. A Send Break Ack (Acknowledgement) message appears.
3. Click OK.

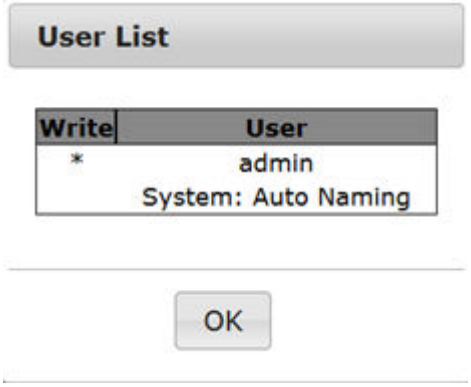
Reset Port

Reset Port resets the physical serial port on the SX2 and re-initializes it to the configured values regarding bps/bits, and so on.

Connected Users

The Connected Users command allows you to view a list of other users who are currently connected on the same port.

1. Choose Emulator > Connected Users.



2. A star appears in the Write column for the User who has Write Access to the console.

Exit

1. Choose Emulator > Exit to close the HSC.

Copy and Paste and Copy All

Data on the current visible page can be selected for copying. Copy and Paste are accessible in the HSC by right click in the terminal window. Select Copy or Paste in the context menu that appears.

To copy all text, use the Copy All option in the Edit menu.

If you need to paste a large amount of data, it is better to save the data in a file and use the Send a Text File function. Pasting a large amount of data in a browser windows can cause the browser to hang as it processes the data. See Send Text File (on page 133).

When pasting data to a port, the end of a line is sent as a carriage return.

The Cut option on the right-click menu is disabled.

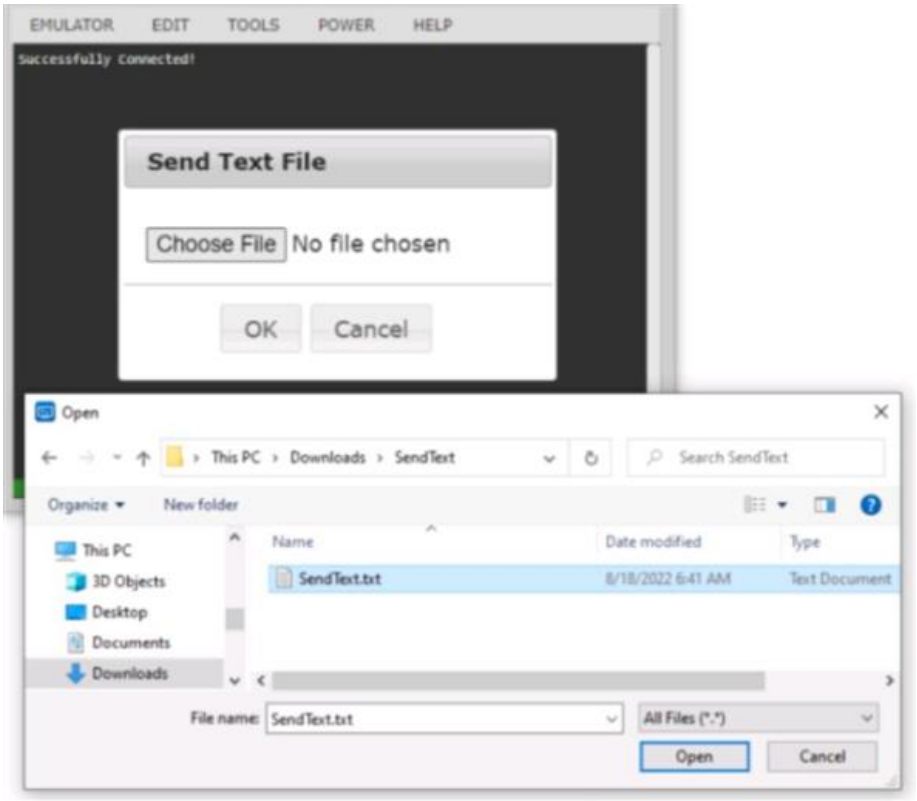
Do not use the Delete option that appears in the right-click menu of IE and some versions of Firefox. This Delete option will remove display lines entirely from the emulator window.

► *Browser-specific behaviors*

When copying from IE or Edge browsers, there are no end of line characters in the copied data. The pasted data appears to be all in one line and contains many spaces. When pasting back into a HSC window, the data may appear to be misaligned, but the data is complete.

Send Text File

1. Select Edit> Send Text File.
2. In the Send Text File dialog, click Browse to find the text file.
3. Click OK.
   - When you click OK, the selected file sends directly to the port.
   - If there is currently no target connected, nothing is visible on the screen.



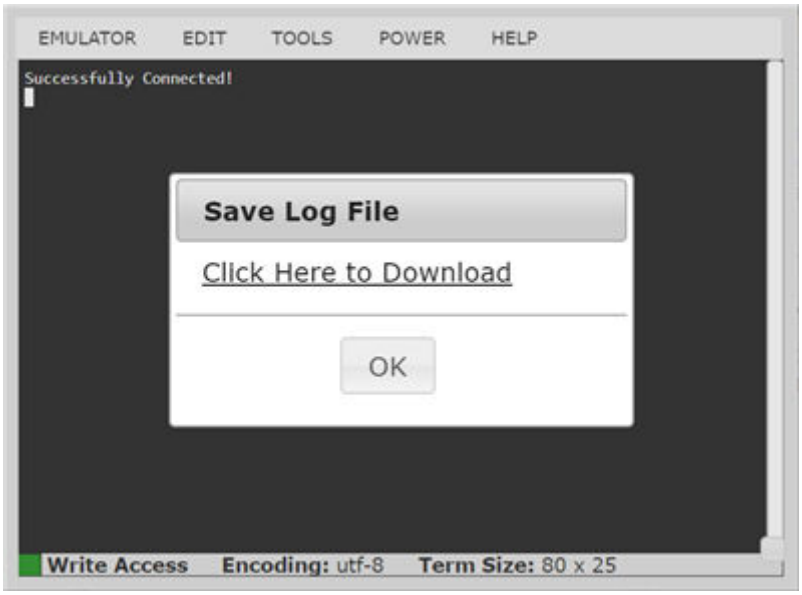
► *Note, if you are using a Mac® and/or Safari®, do the following in order to use this feature:*

1. In Safari, select Preferences.
2. Under the Security tab, select "Manage Website Settings"
3. Click on the KX III website.
4. Select "Run in unsafe mode" from the drop-down box.
5. Restart Safari.

Tools: Start and Stop Logging

The Tools menu contains options for creating a data history file and downloading it.

1. Choose Tools > Start Logging to start the storage of serial port data in memory.
2. Click Stop Logging to save the log file. A pop up message appears with a download link. Click to download the memory buffer into a text file.

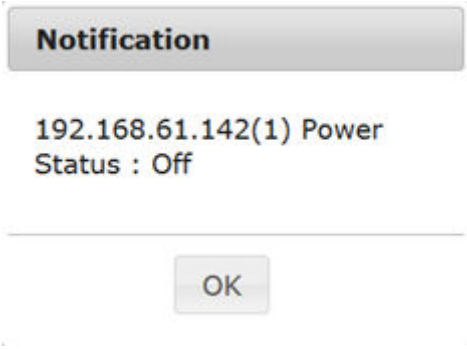


Power Status

Power Status in HSC shows the status of the outlet the target is plugged into.

1. Choose Power > Power Status.
2. The Notification dialog shows the status of the outlet as ON or OFF.

Status may also show no associated outlet, or no power permission to the port.



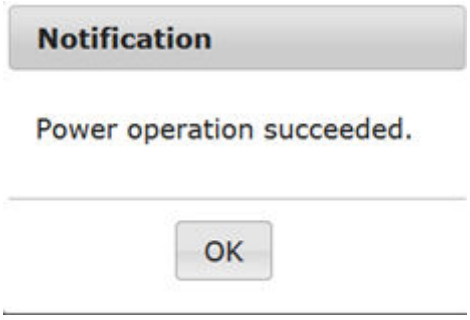


Power on a Target

Use this option to power on a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power On.
2. Click OK in the success message.

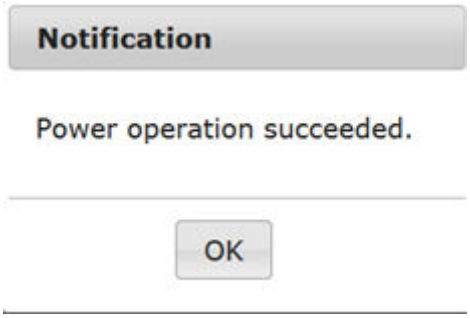


Power Off a Target

Use this option to power off a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power Off.
2. Click OK in the success message.



Power Cycle a Target

Power cycling allows you to turn a target off and then back on through the outlet it is plugged into.

This option is visible only when -

- there are one or more power associations to the target
- the target is already powered on (the port status us Up)
- you have permission to manage the target's power

1. Choose Power> Power Cycle.
2. Click OK in the success message.

Browser Tips for HSC

Some browsers have limitations that affect HSC.

- Edge & Chrome, disabling the background throttling to prevent background tabs from disconnecting after a certain amount of time. Go to chrome://flags, then search for "throttle". Set "Throttle Javascript timers in backgound" and "Calculate window occlusion on Windows" to "Disabled". Restart chrome to apply settings.
- Browser option to select certificate for authentication displayed on Edge and Chrome after session is idle for about 5 minutes, due to internal browser SSL caching and timeouts. If certificate is selected promptly, reconnection is successful. With longer idle times, authentication is not successful, and the browser should be restarted to reconnect. Issue is not observed in Firefox.
- Edge has an internal limitation on the number of websockets that are allowed to be created to a single server (6). This can be changed by modifying a registry variable as shown here : https://msdn.microsoft.com/en-us/library/ee330736(v=vs.85).aspx#websocket_maxconn.
- Edge,and Safari have a limitation when connecting to IPv6 devices. Using the numerical URL will not work when it attempts to establish a websocket connection. In these browsers, use the device hostname or literal IPv6 as UNC to connect to the SX II. See https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names
- When using HSC in IOS Safari, the keyboard may not appear in some pages if the "request desktop website" setting is enabled. To change the setting, go to Settings > Safari >Request Desktop Website, then make sure All Websites is not selected, and the device address is not selected. You can also set this per address by clicking the "aA" in Safari's URL pane when connected to the HSC port, then select "Website Settings" and make sure that "Request Desktop Website" is not selected.

Dominion User Station

To use a standalone appliance for remote access to KX III target servers instead of using the VKC or AKC clients on a PC or laptop, purchase Dominion User Stations from Raritan. The User Station is perfect for environments like labs, studios and control rooms where a PC or laptop is not wanted.

This chapter provides a brief introduction to the User Station. For detailed information, refer to the user documentation from the User Station's section on the Raritan website's Support page.

In This Chapter

Overview. 138
User Station Photo and Features. 138
Operating the User Station. 139

Overview

The Dominion User Station is designed to access servers and computer devices connected to KX III's from your LAN/WAN networks. ALL KX III models are supported. KX III Release 3.10.0 and above is required.

User Station Photo and Features

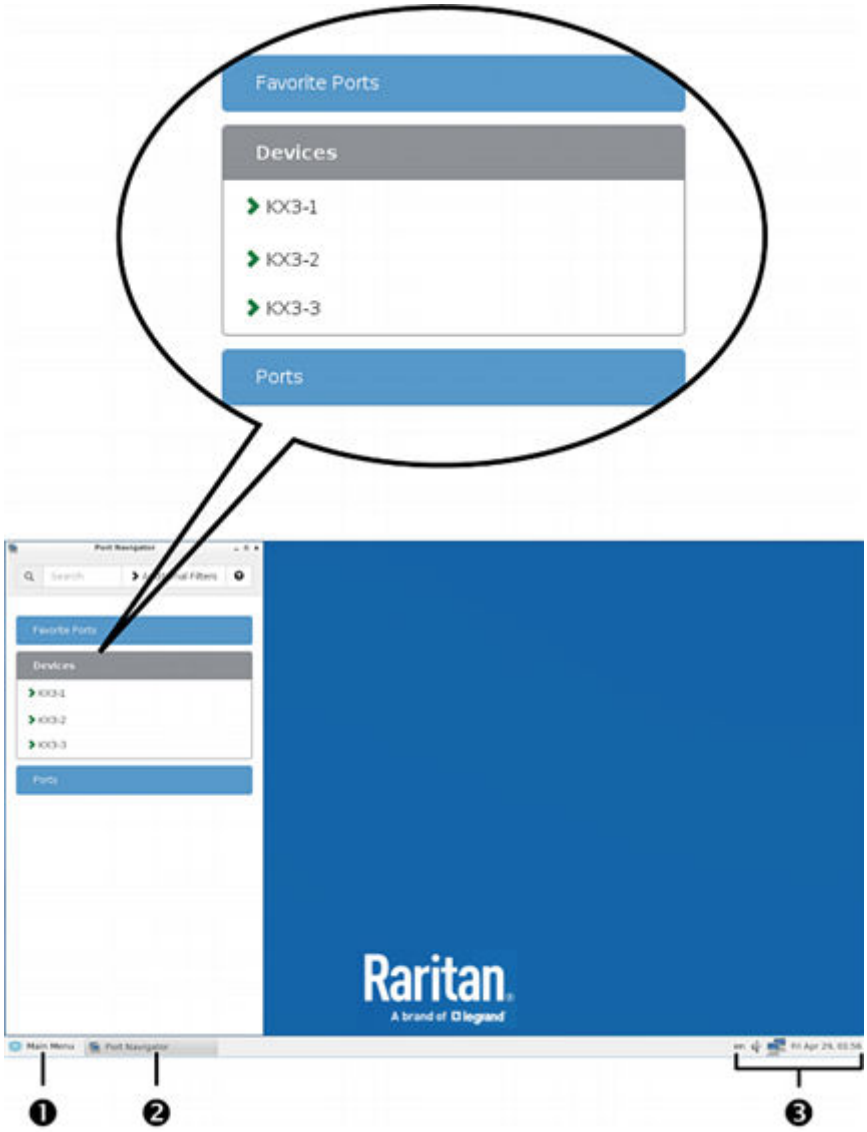


- Supports up to 4 monitors
- Three 1080p streaming video sessions at 30 FPS
- Supports USB-C, VGA, DVI, HDMI and DisplayPort video
- Favorites and hot-key switching
- Access hundreds of servers
- 1 Gigabit and 2.5 Gigabit ethernet ports
- Self-contained, low maintenance appliance
- Desktop, rack and VESA mountable

Operating the User Station

1. Have the required equipment properly connected to the User Station.
   a. Power OFF all devices.
   b. Connect a USB keyboard, mouse and monitors to the User Station.
   c. Connect the User Station to the LAN/WAN network.
2. Power on and log in to the User Station.
   - For initial login, use Raritan's default username and password: `admin` and `raritan`.
3. Add KX III's data. See: Logging In to KX III (on page 23).

4. The added KX III's are displayed in the Port Navigator window.



5. Click a KX III to show a list of its servers.
6. Click a target server, and a KVM Client opens, showing the target video. Now you can control the target with the attached keyboard and mouse.

For detailed information, refer to the user documentation from the User Station's section on the Raritan website's Support page.

KX III Remote Console

In This Chapter

Overview. 141
Scanning Ports - Remote Console. 141
Changing a Password. 145
Managing Favorites. 145

Overview

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

See: Logging In to KX III and KVM Ports

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

For more in the Remote Console interface elements, see: KX III 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.

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.

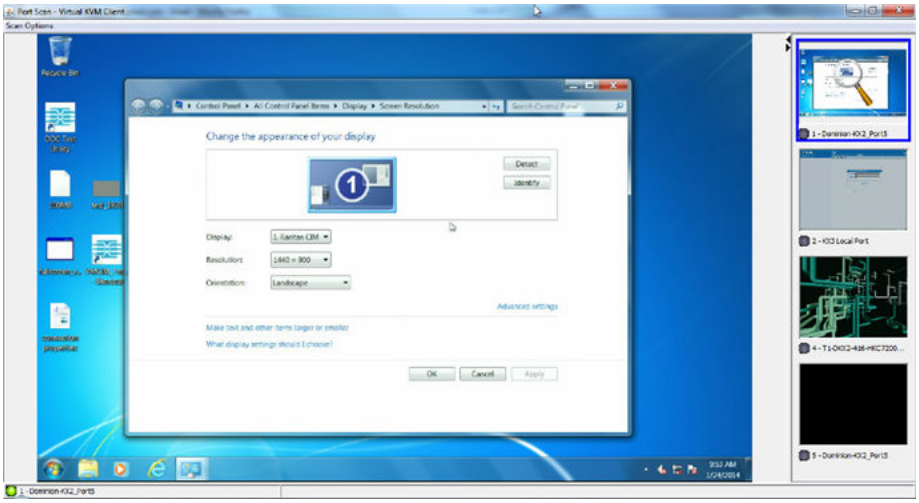
As each target is found, it is displayed as a thumbnail in a slide show.

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 above its thumbnail.

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



Configure scan settings for the Remote Console in the KVM client.

Note: Scan port settings for the Local Console are configured on the Local Port Settings page. See Scanning Ports - Local Console (on page 152)

Target Status Indicators During Port Scanning - Remote Console

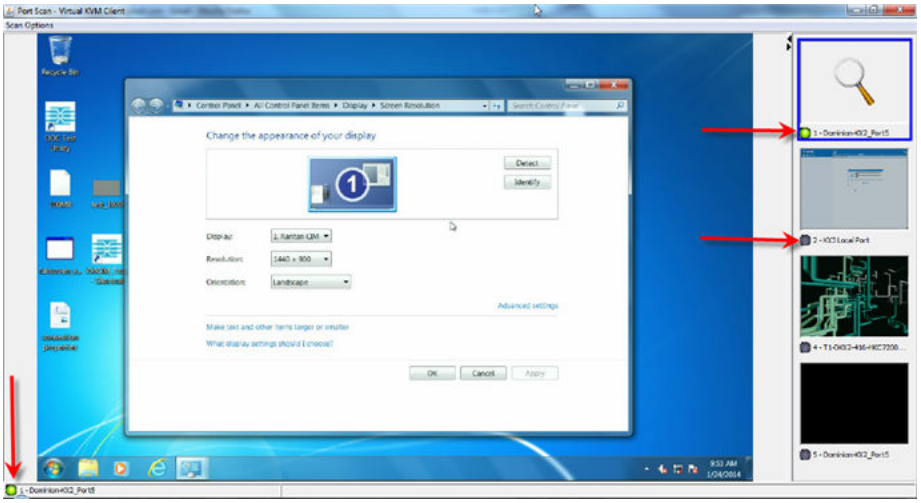
The status of each target is indicated by green, yellow and red lights that are displayed below the target thumbnail.

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.

With 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 the KVM Client.

► *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*

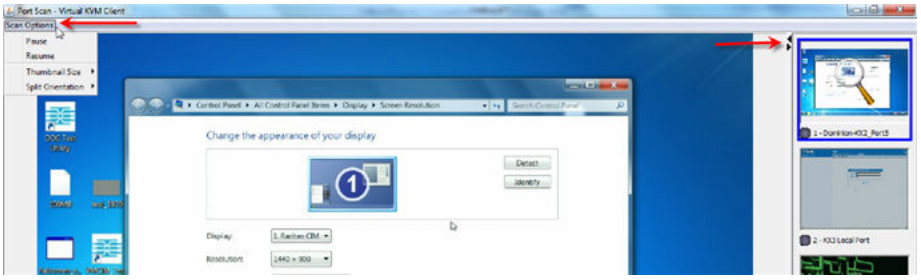
- Resume the thumbnail rotation by selecting Options > Resume.

► *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 selection 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.

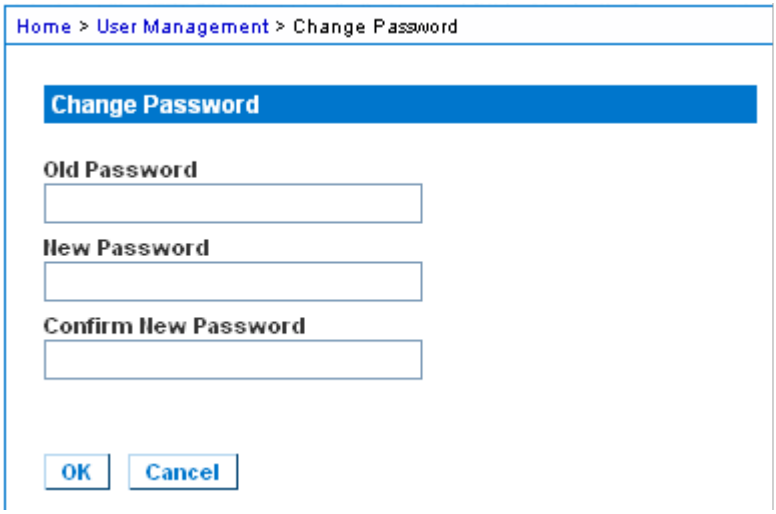
1. Click Options > Pause to pause the slide show and stop it from moving between targets, click Options > Resume to resume the slide show.
2. Click on a target thumbnail to scan it next.
3. Connect to a target by double clicking on its thumbnail.

Changing a Password

► *To change your KX III password:*

1. Choose User Management > Change Password. The Change Password page opens.
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.



Managing Favorites

A Favorites feature is provided so you can organize and quickly access the devices you use frequently.

The Favorite Devices section is located in the lower left sidebar of the Port Access page and provides the ability to:

- Create and manage a list of favorite devices
- Quickly access frequently-used devices
- List your favorites either by Device Name, IP Address, or DNS hostname
- Discover KX III devices on its subnet
- Retrieve discovered KX III devices from the connected Dominion device

---

Note: Due to browser limitations, HKC does not support Favorites.

Enable Favorites

- Click Enable in the Favorite Devices section of the left panel of the KX III interface, below Online Help.

Access and Display Favorites

► *To access a favorite KX III devices:*

- Click on a KX III listed beneath Favorite Devices in the left of the Remote Console.

► *To display favorites by Name, IP Address or Host Name:*

- Click Display by Name, Display by IP, or Display by Host Name.



Discovering Devices on the Local Subnet

This option discovers KX III devices on your local subnet. This is the subnet where the KX III Remote Console is running.

These devices can be accessed directly from this page or you can add them to your list of favorites.

► *To discover devices on the local subnet:*

1. Choose Manage > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page appears.
2. Choose the appropriate discovery port:
   - To use the default discovery port, select the Use Default Port 5000 checkbox.
   - To use a different discovery port:
     a. Deselect the Use Default Port 5000 checkbox.
     b. Type the port number in the Discover on Port field.
     c. Click Save.
3. Click Refresh. The list of devices on the local subnet is refreshed.

► *To add devices to your Favorites List:*

1. Select the checkbox next to the device name/IP address.
2. Click Add.

► *To access a discovered device:*

- Click the device name or IP address for that device. A new browser opens to that device.

Discovering Devices on the KX III Subnet

This feature is only available in the Java client , RSC.

This option discovers KX III devices on the device subnet. This is the subnet of the KX III device's IP address.

You can access these devices directly from the Subnet page or add them to your list of favorites.

This feature allows multiple KX III devices to interoperate and scale automatically.

The KX III Remote Console automatically discovers the KX III devices, and any other Raritan device, in the subnet of the KX III.

► *To discover devices on the device subnet:*

1. Choose Manage > Discover Devices - KX III Subnet.



The Discover Devices - KX III Subnet page appears.

2. Click Refresh. The list of devices on the local subnet is refreshed.

► *To add devices to your Favorites List:*

1. Select the checkbox next to the device name/IP address.
2. Click Add.

► *To access a discovered device:*

- Click the device name or IP address for that device. A new browser opens to that device.

KX III Local Console

The Local Console interface provides access to the KX III while at the rack.

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

In This Chapter

Accessing a Target Server. 149
Local Console Video Resolution Behavior. 149
Simultaneous Users. 150
Local Port Hot Keys and Connect Keys. 150
Scanning Ports - Local Console. 152
Local Console Smart Card Access. 154
Local Console USB Profile Options. 157
KX III Local Console Factory Reset. 157
Resetting the KX III Using the Reset Button. 157

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 KX III Local Console, KX III detects the monitor's native resolution. As long as the native resolution is supported by the Local Console, KX III 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, KX III 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 KX III Local Console. KX III 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, KX III uses the resolution of 1024x768@60.

For a list of supported Local Console video resolutions, see KX III Supported Local Port DVI Resolutions (on page 179).

Simultaneous Users

The KX III 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 KX III, you can still simultaneously access your servers from the rack via the Local Console.

Local Port Hot Keys and Connect Keys

Because the KX III 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 KX III 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 KX III Local Console interface.

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

► *To perform an auto-sense (video refresh) on the KX III 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

Standard servers	
Connect key action	**Key sequence example**
Access a port from the local port	• Press Left ALT > Press and Release 5 > Release Left ALT
Switch between ports	• Press Left ALT > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port	• Double-click Scroll Lock
Blade chassis	
Connect key action	**Key sequence example**
Access a port from the local port GUI	Access port 5, slot 2: • Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 2 > Release Left ALT

Standard servers	
Connect key action	**Key sequence example**
Switch between ports	Switch from target port 5, slot 2 to port 5, slot 11: • Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port GUI	Disconnect from target port 5, slot 11 and return to the local port GUI (the page from which you connected to target): • Double Click Scroll Lock

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:

Sun key	Local port key combination
Again	Ctrl+ Alt +F2
Props	Ctrl + Alt +F3
Undo	Ctrl + Alt +F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Mute	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	No key combination
Power	No key combination

Scanning Ports - Local Console

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 141)

Click 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 Local Port Hotkey sequence hot key.

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.

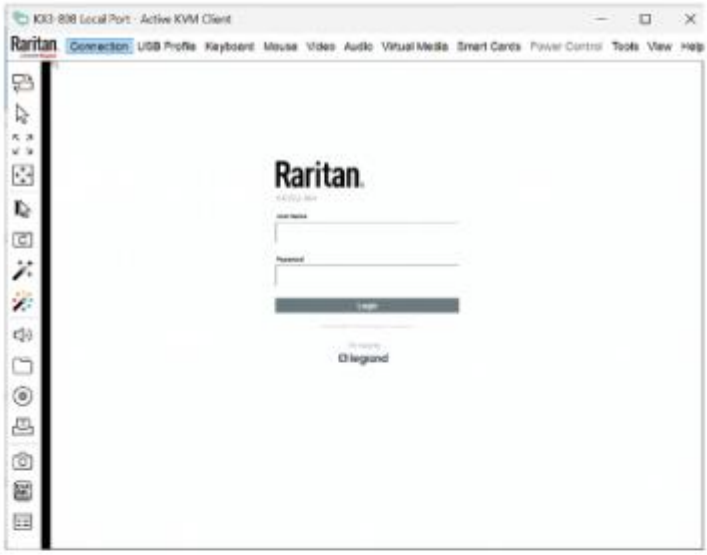
The name of the target is displayed above its thumbnail.

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 154)

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 63)







Target Status Indicators During Port Scanning - Local Console

When scanning on the Local Console, the status of each target is indicated below the thumbnail.

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.

► *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 KX III using one of the USB ports located on the KX III.

Once a smart card reader is plugged in or unplugged from the KX III, the KX III autodetects it.

For a list of supported smart cards and additional system requirements, see Supported Smart Card Readers (on page 188), Unsupported Smart Card Readers (on page 189) and Smart Card Minimum System Requirements (on page 187).

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.

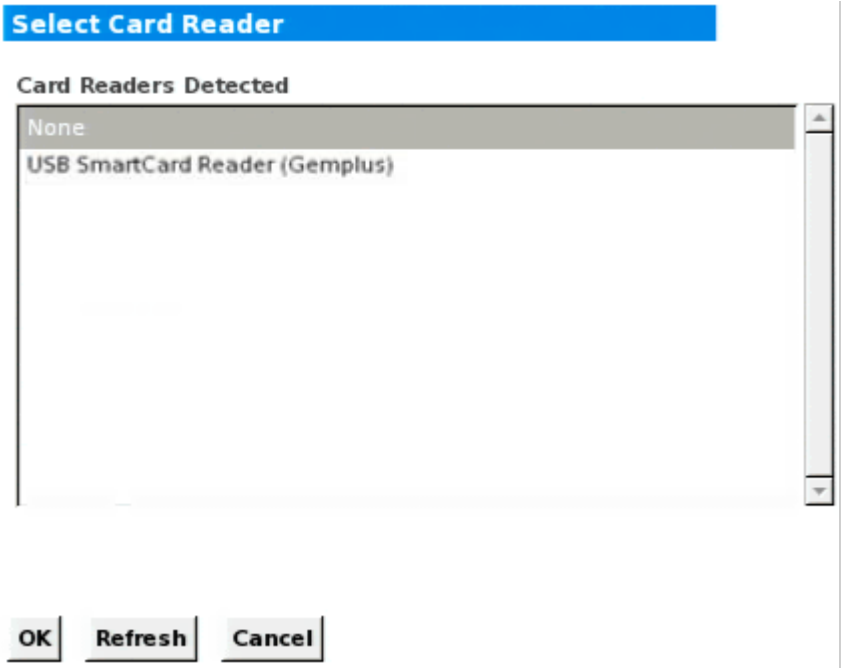
When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

► *To mount a smart card reader onto a target via the KX III Local console:*

1. Plug a USB smart card reader into the KX III using one of the USB ports located on the device. Once attached, the smart card reader will be detected by the KX III.
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.



Note: If a smart card reader is selected for local port login in Security>Local Smart Card Authentication, then that card reader cannot be selected for target connections; it will be listed, but cannot be chosen.

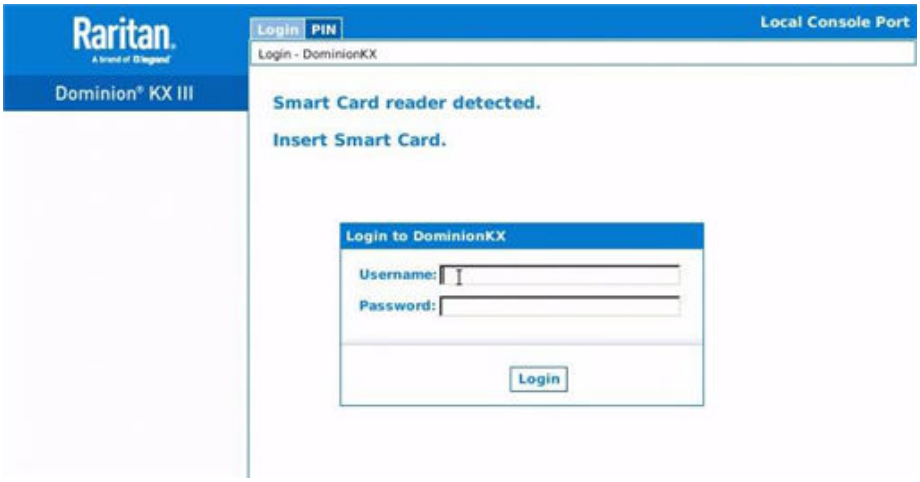
Using a Smart Card at the Local Port

When Local Smart Card Authentication is enabled, you can be authenticated by using your smart card at the card reader connected to a KX III USB port.

If Local Smart Card Authentication is enabled but not required, the Login tab remains accessible to allow for username/password login.

► *To use a smart card at the local port.*

1. When the card reader is detected, the Login page shows a PIN tab.



2. Insert a card. The PIN tab opens automatically.
3. Enter the PIN and click Login.



4. After successful entry of the card's PIN, access is granted if the card contains an authentication certificate approved by Client Certificate Authentication. See Client Certificate Authentication Settings.

If login fails, check the Audit log for failure information.

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.

KX III 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:*

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.
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).

1. Click Reset to continue. You will be prompted to confirm the factory reset because all network settings will be permanently lost.
2. Click OK proceed. Upon completion of full factory reset, the KX III device is automatically restarted.

Resetting the KX III Using the Reset Button

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).

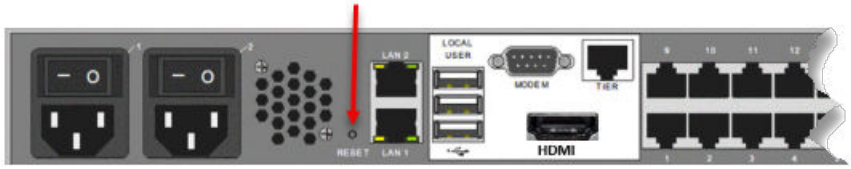
The actions that are performed when the Reset button is pressed are defined on the Encryption & Share page. See Encryption & Share.

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 KX III.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the KX III device back on.
4. Continue holding the Reset button for 10 seconds.



Appendix A Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality

An extended local port extends the reach of the local port beyond the rack the KX III is located, for example to another KVM switch.

This can be achieved by configuring a KX III to work with a Raritan Cat5 Reach DVI transmitter and receiver, which are then connected to a remote console or other device.

Once connected to the Cat5 Reach DVI, the KX III can be accessed up 500 feet (152 m) away.

Connecting the KX III to the Cat5 Reach DVI by daisy chaining Ethernet switches extends can extend the KX III's reach up to 3000 feet (914 m).

In This Chapter

About the Cat5 Reach DVI. 159
Connect Cat5 Reach DVI and Cat5 Reach DVI. 159

About the Cat5 Reach DVI

For details on the Cat5 Reach DVI, see the Cat5 Reach DVI online help available on the Raritan Support page.

Contact Raritan for additional information on the Cat5 Reach DVI, or for information on purchasing.

Connect Cat5 Reach DVI and Cat5 Reach DVI

Note: The images used in the diagrams are not specific to Cat5 Reach DVI but the connections are accurate.

This section introduces three scenarios involving KVM switches.

- Connect the Cat5 Reach DVI between any KVM switch and its local console.
- Connect the Cat5 Reach DVI between two KVM switches.
- Connect the Cat5 Reach DVI between a computer/server and a KVM switch.

Turn off all devices before making the connections.

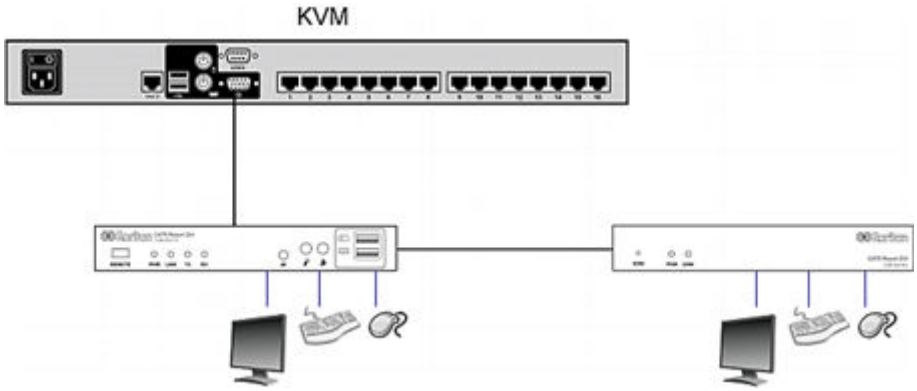
For detailed information on setting up the local and remote consoles, see Connecting a Keyboard/ Mouse/Video Source in Cat5 Reach DVI Help for more information.

► *To connect Cat5 Reach DVI and Cat5 Reach DVI:*

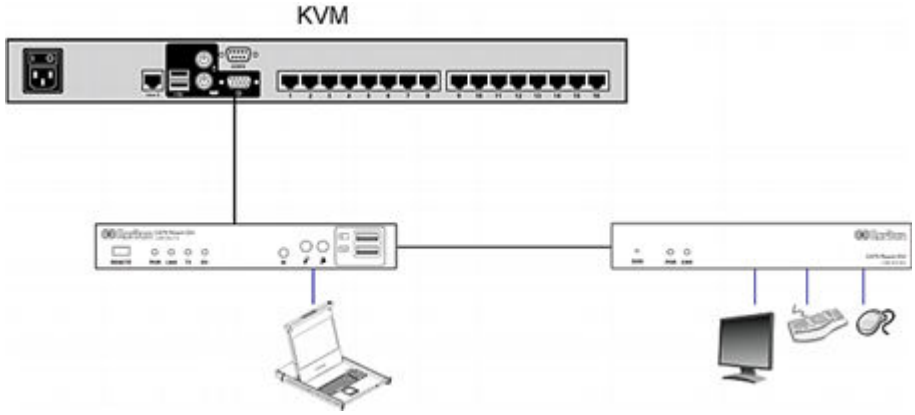
1. If you have not already done so, set up the local and remote consoles with the Cat5 Reach DVI transmitter and receiver, respectively.

See Basic Installation in Cat5 Reach DVI Help for more information.

2. Use a Cat5e/6 cable to connect the transmitter and receiver.
3. Connect the transmitter and receiver to an appropriate power source respectively.
4. Connect the local console ports of the KVM switch to the transmitter.
   a. Plug one end of the Raritan-provided DVI cable into the DVI-I IN port on the transmitter, and the other end into the KVM switch's video port.
   b. Plug the USB-B connector of the Raritan-provided USB cable into the USB-B port on the transmitter, and the other end into the KVM switch's local USB-A port.
5. Turn on the KVM switch.

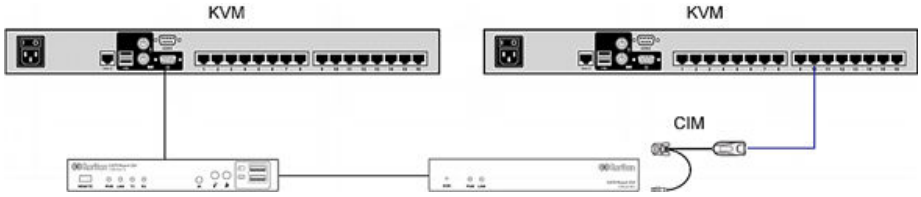


Tip: The local or remote console can be equipped with a KVM drawer instead of a set of keyboard, mouse and monitor. See the illustration below.



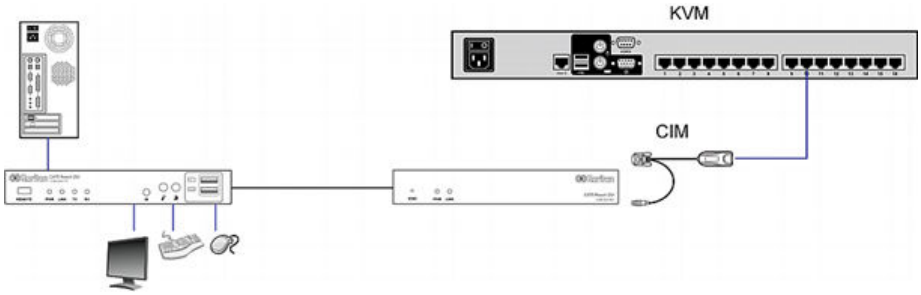
► *To increase the distance between two tiered KVM switches:*

1. Set up a remote console by connecting the receiver to a KVM switch.
   a. Connect a USB CIM to the receiver.
   b. Connect this USB CIM to any channel port on the KVM switch via a Cat5 cable.
2. Use a Cat5e/6 cable to connect the transmitter and receiver.
3. Connect the transmitter and receiver to an appropriate power source respectively.
4. Connect the KVM switch to the transmitter.
5. Turn on both KVM switches.



► *To increase the distance between any computer and a KVM switch:*

1. Set up an optional local console with the transmitter.
2. Set up a remote console by connecting the receiver to a KVM switch.
3. Use a Cat5e/6 cable to connect the transmitter and receiver.
4. Connect the transmitter and receiver to an appropriate power source respectively.
5. Connect the computer to the transmitter.
6. Turn on the computer.



Updating the LDAP Schema

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 KX III 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.

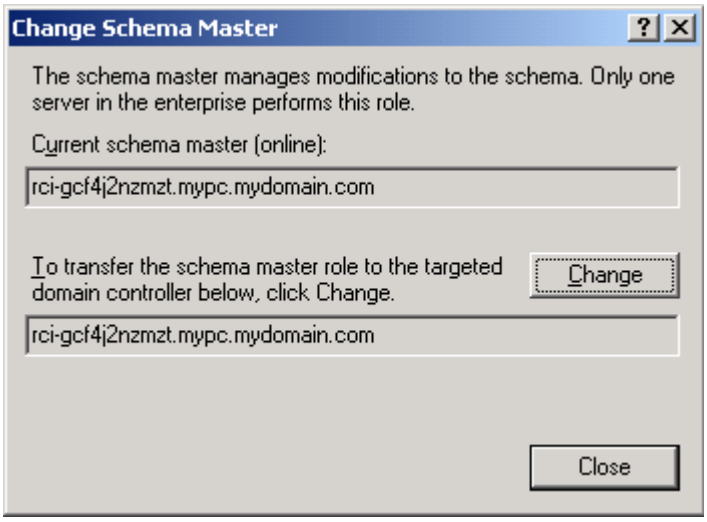
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

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.

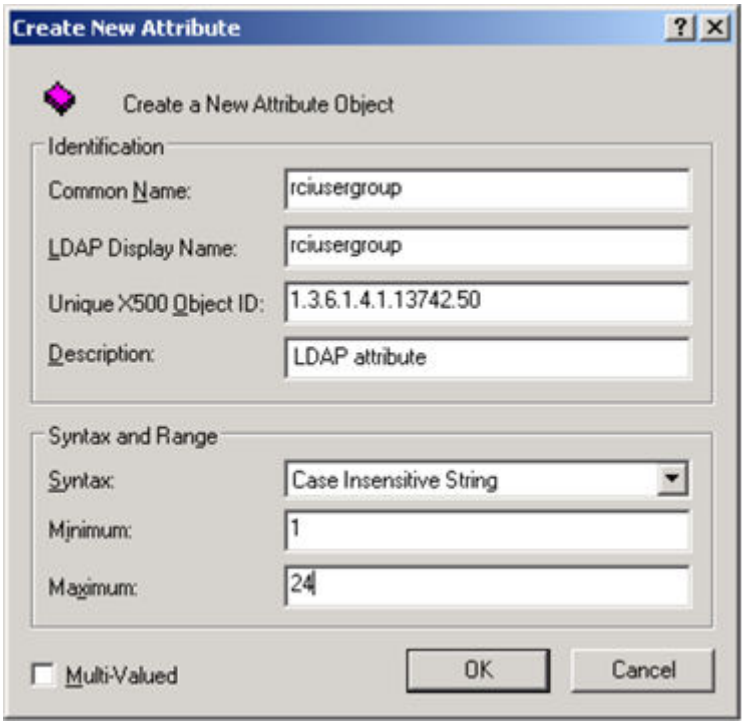


2. Select the "Schema can be modified on this Domain Controller" checkbox. Optional
3. Click OK.

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.

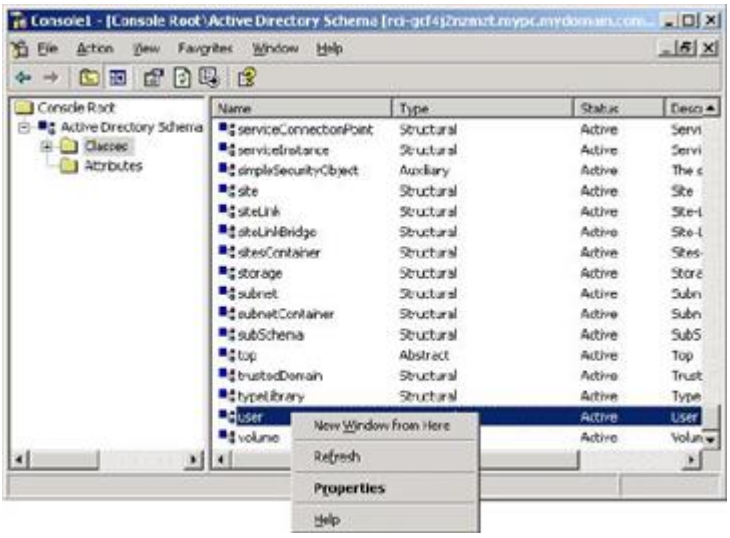


4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String 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:*

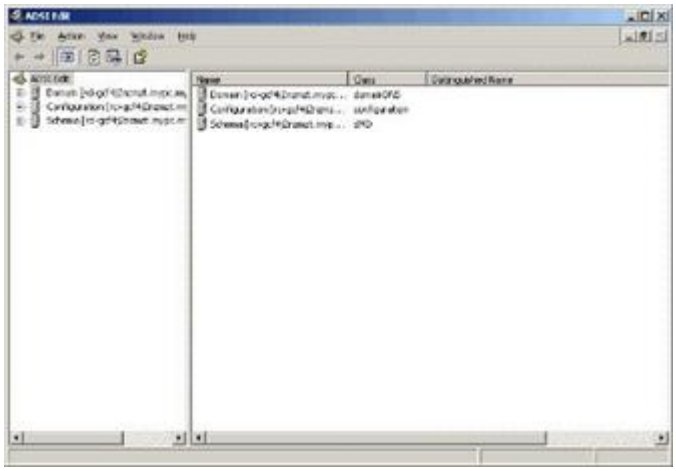
1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

Editing rciusergroup Attributes for User Members

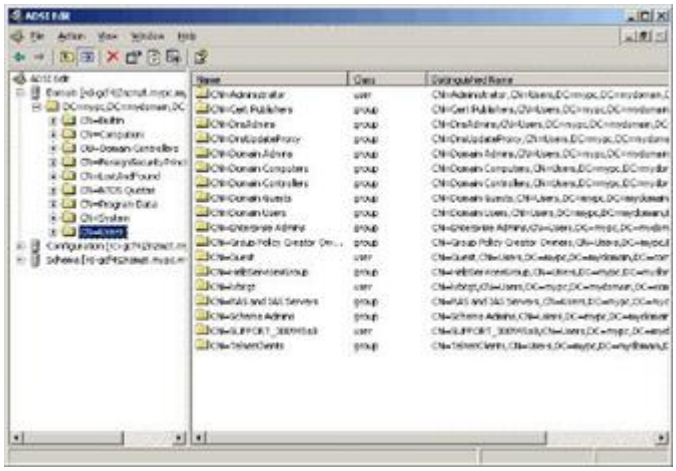
To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level 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.

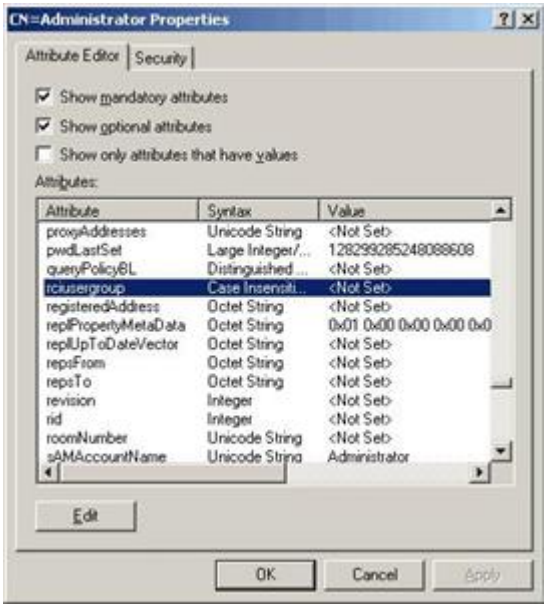


4. Open the Domain.
5. In the left pane of the window, select the CN=Users folder.



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 KX III) in the Edit Attribute field. Click OK.

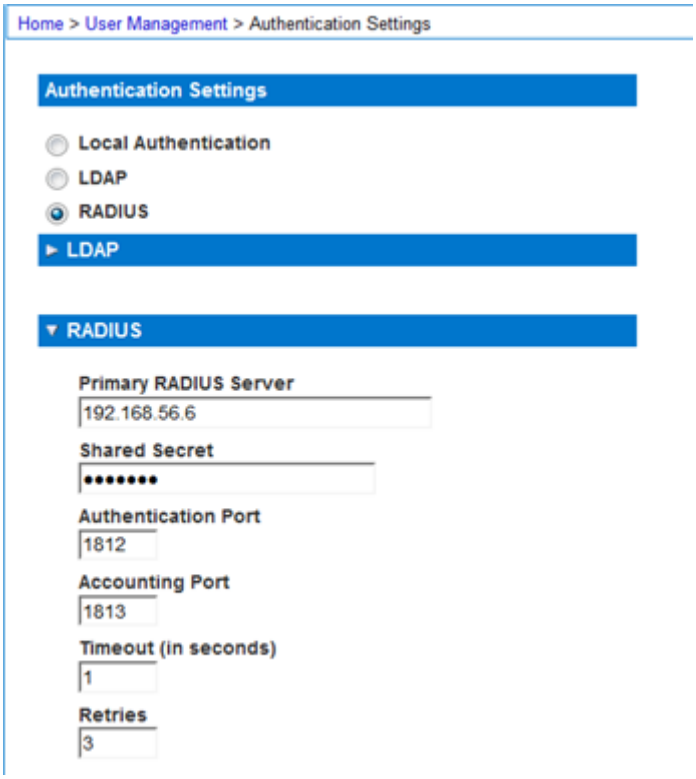


Cisco ISE for RADIUS Users

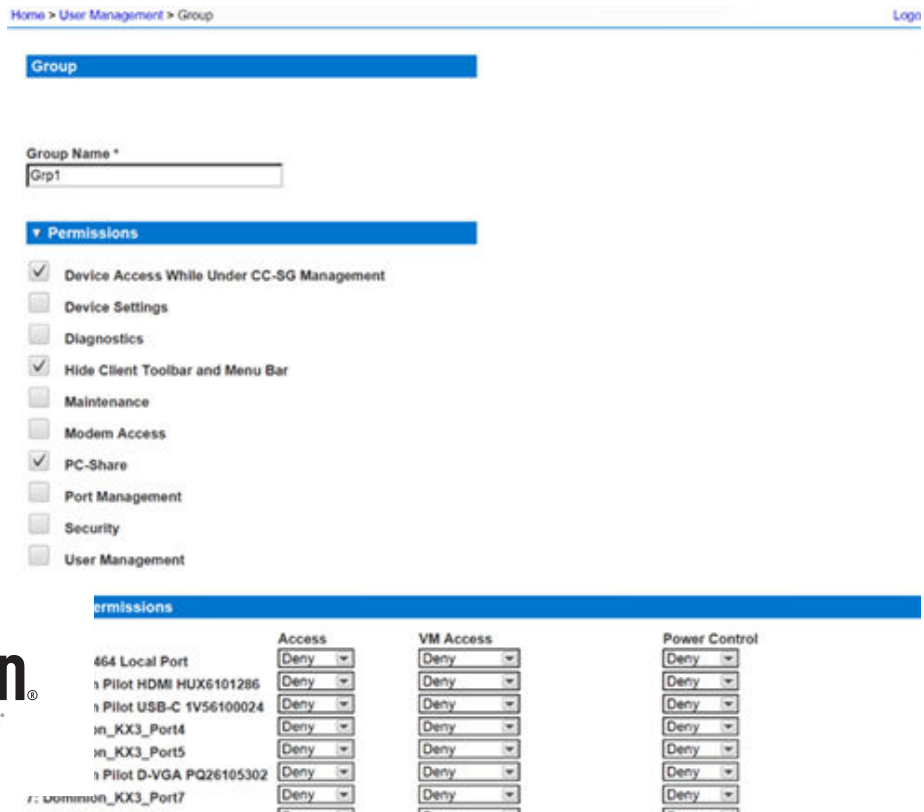
Authorization is performed by means of user's membership to local User Groups. When using remote authentication, since there is no user account locally, there needs to be way of returning user group information from remote authentication server that the product will then match and perform appropriate authorization. To achieve this objective, appropriate local group on the product must be created and remote authentication server configured to return appropriate matching group (case sensitive).

Settings to Configure on Raritan Product

1. Login to Raritan product with administrative account.
2. Access User Management>Authentication>RADIUS
3. Add the Cisco ISE 2.1.x Radius server.



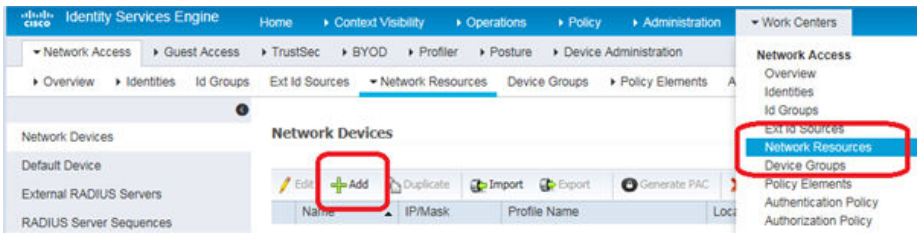
4. Create user group with appropriate permission and port permission by accessing User Management>User Group List.



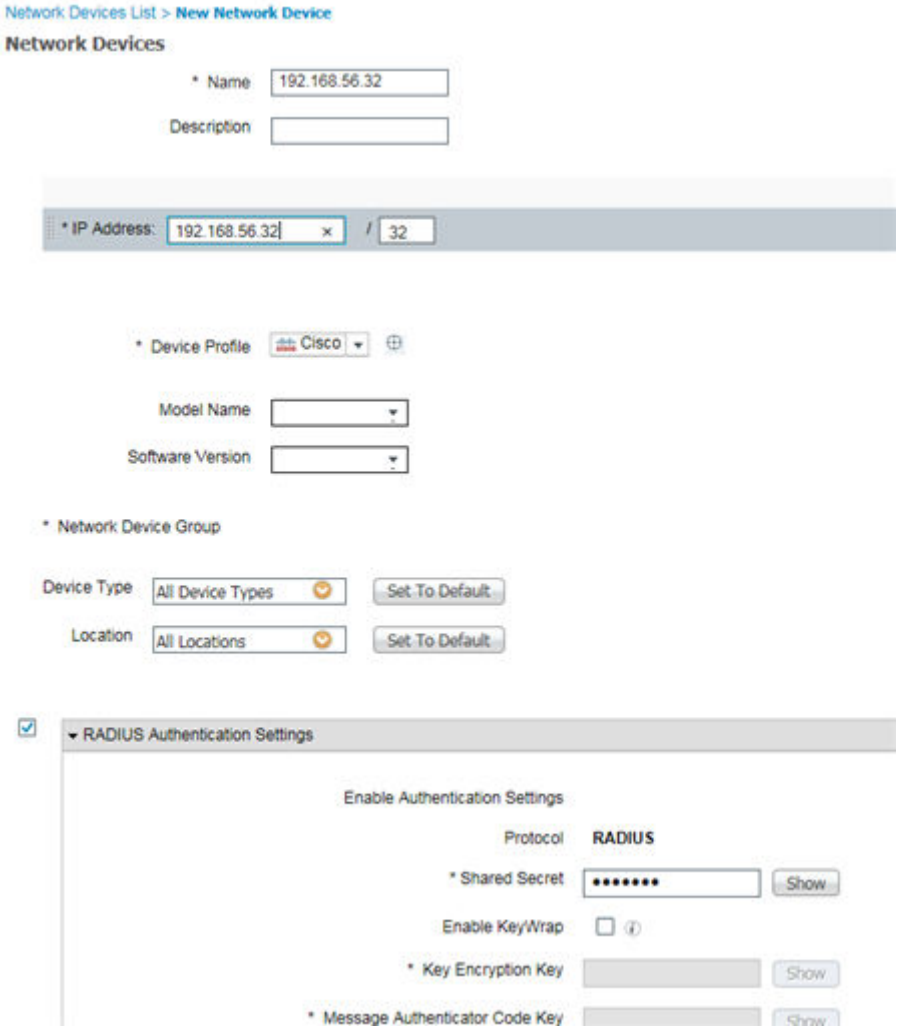
Settings to Configure on Cisco ISE

Step 1: Add Raritan Network Devices

1. Access Cisco ISE Web URL https://x.x.x.x/admin and login with administrative credentials.
2. Access Work Centers>Network Resources under Network Access section to load Network Device menu and click 



3. Configure Name, Description and IP Address/Range, and enable Radius Authentication Settings option. Set Shared secret then click Submit to save changes. If appropriate and applicable, assign Device Type and Location.

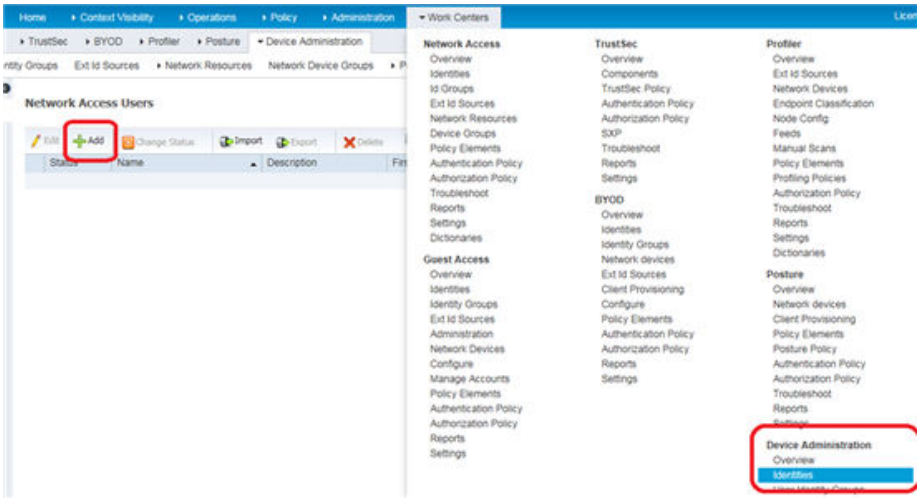


Step 2: Create/Edit User

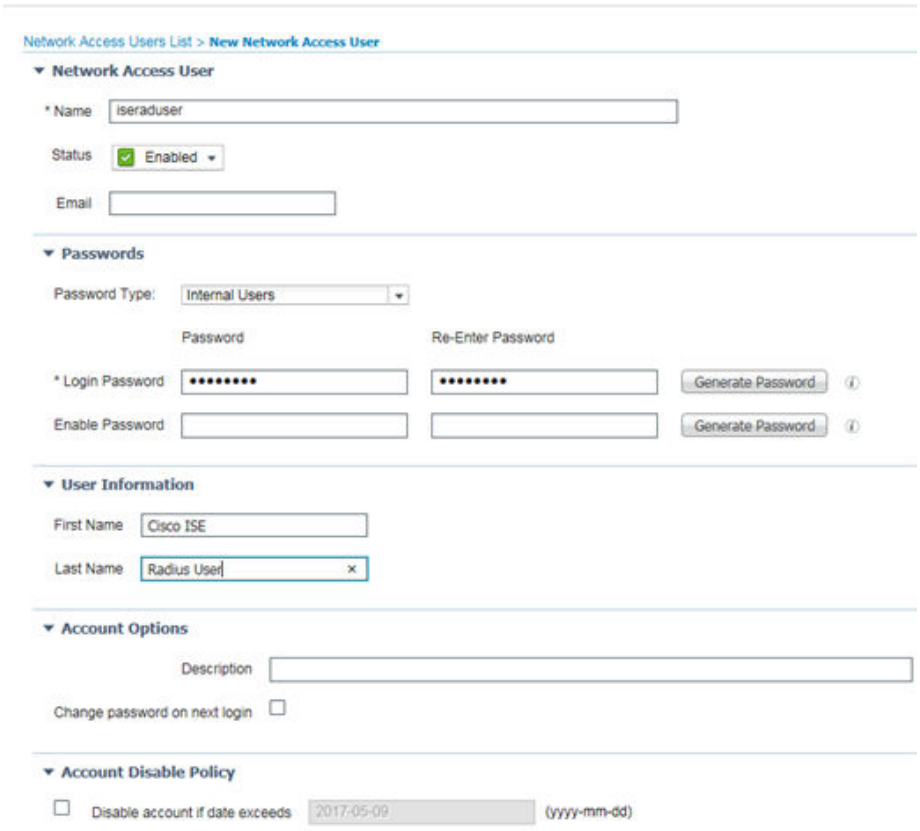
In production environments with user accounts or configured external identity source (AD/LDAP), kip this step.

1. Access Work Centers>Device Administration>Identities> and click 

to add a user

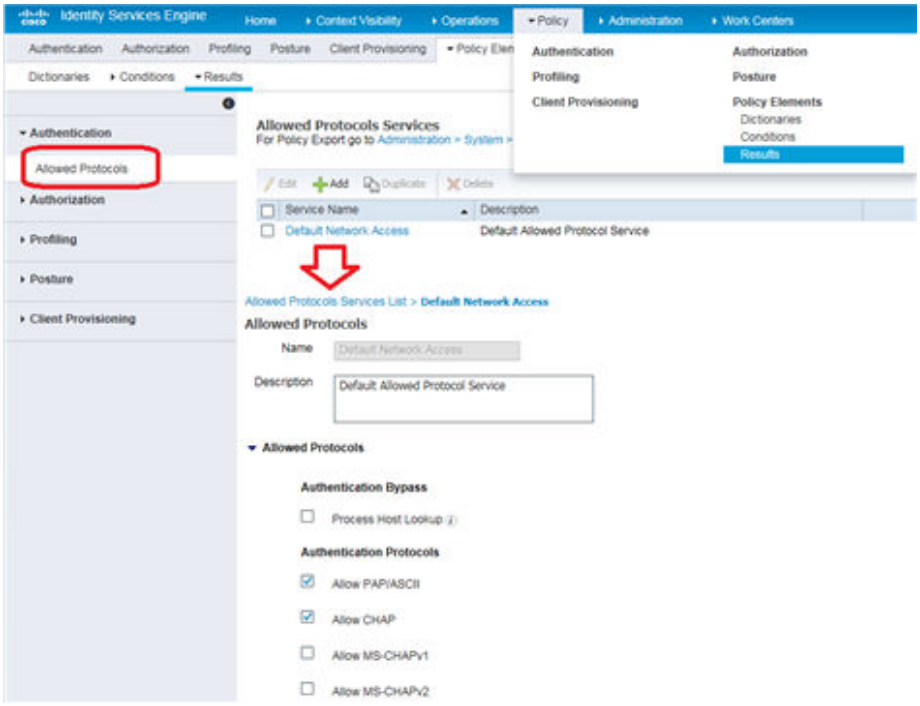


2. Configure required fields and click Submit to add user



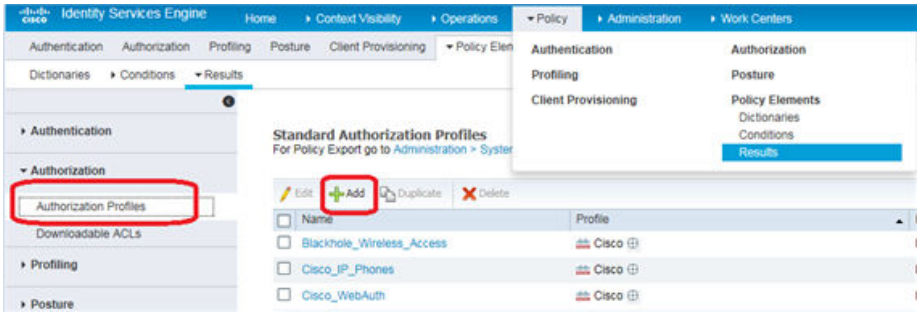
Step 3: Configure Allowed Authentication Protocol Service (PAP/CHAP/MS-CHAP)

1. Access Policy>Results under Policy Elements section. Select Allowed Protocols under Authentication Dropdown from left pane. Click to Edit Default Network Access and select CHAP. Xerus supports both PAP and CHAP authentication types. In case CHAP authentication type is desired, verify Global Authentication Type setting on Xerus RADIUS configuration is set to CHAP as well as this step is completed on Cisco ISE 2.1.x server.

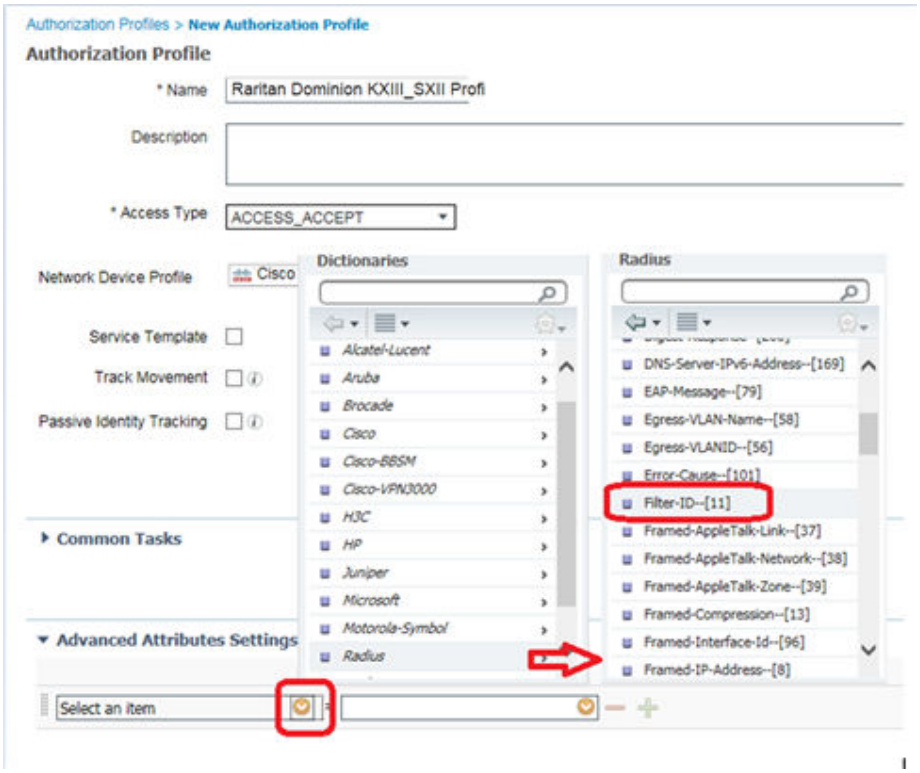


Step 4: Create Authorization Profile

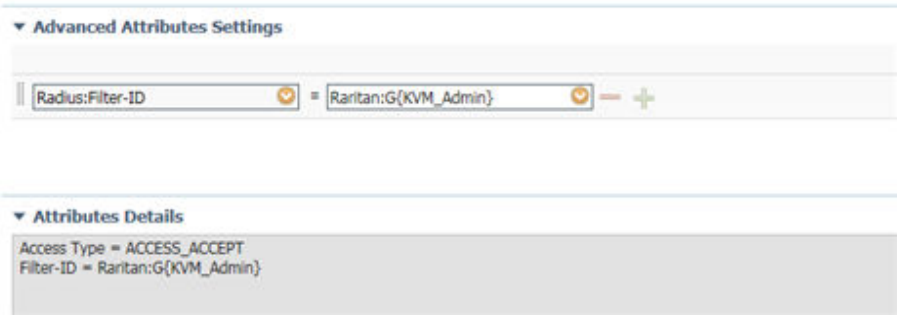
1. Access Policy>Results under Policy Elements, and from Authorization on left pane, choose Authorization Profiles and click Add
2. Under General Tab configure Policy Friendly Name.



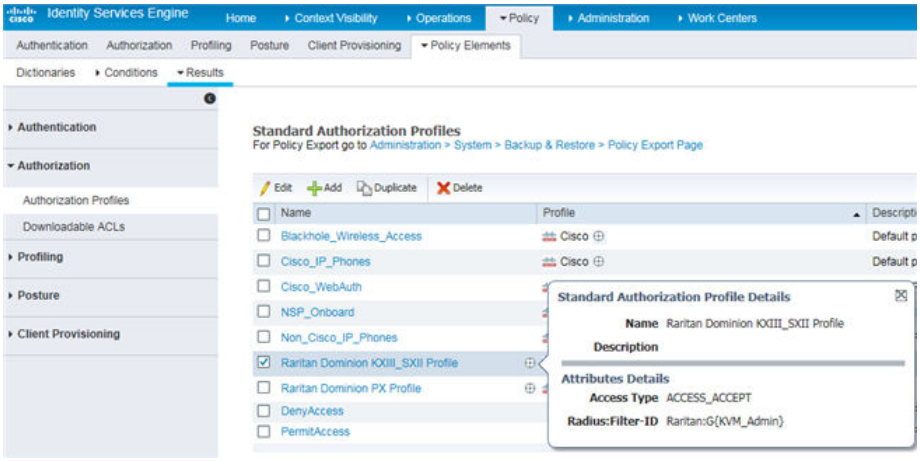
3. Specify appropriate Profile name. Scroll down to Advanced Attributes Settings section and click on drop down next to Select and Item text field. Select Radius and from Submenu select Filter-ID--[11] option.



4. Verify in the text box that it correctly displays attribute name Radius:Filter-ID. In the next test field, type attribute value Raritan:G{KVM_Admin} and click anywhere on the page to set it. Confirm Attribute Details display as shown below.

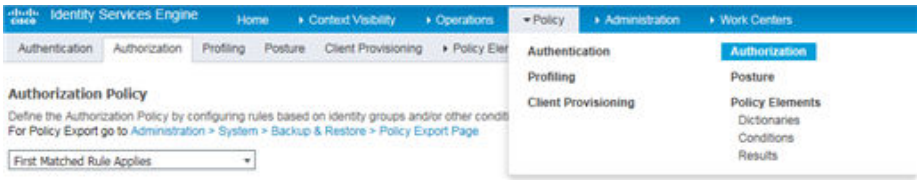


5. Click Submit to create new Authorization profile and return to profile list summary page. Verify profile name and mouse over  icon for preview of summary.

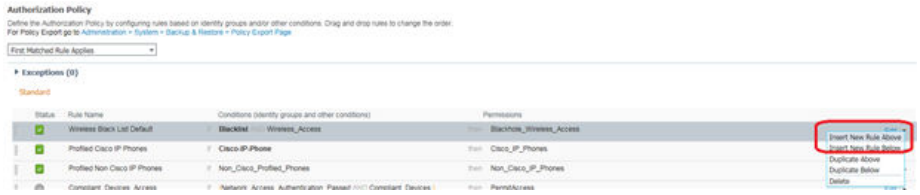


Step 5: Configure/Create Authorization Policy

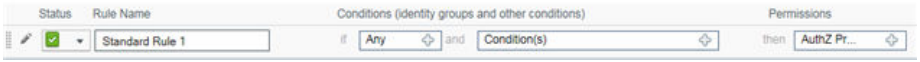
1. Access Policy>Authorization to see policy listing



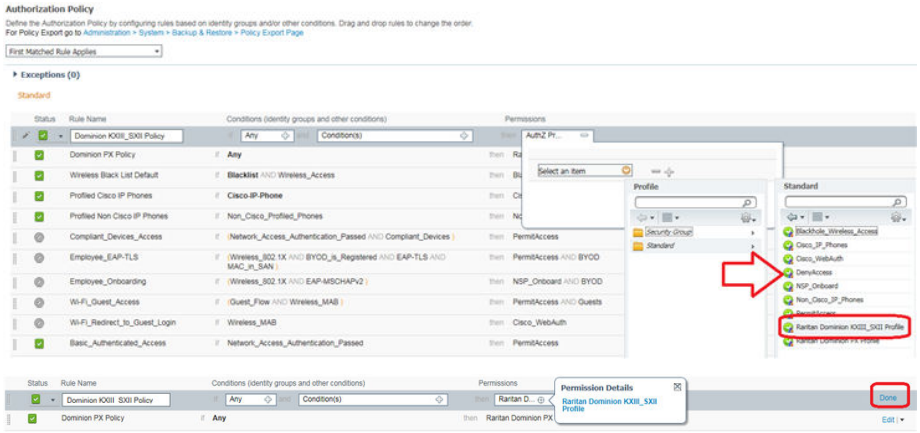
2. Next, click Edit dropdown in the first row and select Insert New Rule Above.



New first row is added.



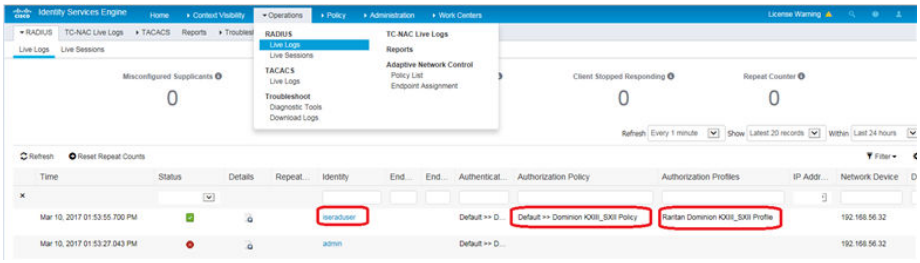
3. Specify appropriate Policy name and Click on add ( ) in Permission text box. Select Standard and from Submenu should appear with list of available profiles. Select Raritan Dominion KXIII_SXII Profile and click Done..



4. Click Save to create policy.

Troubleshooting Tips

1. Verify from Live Logs under Operations> RADIUS that correct Authorization Policy is being applied. Click Details icon to see more information



2. User authorization may fail if incorrect policy is applied. Check the following:
   - Moving policy higher up in the order (in case of multiple policy sets)
   - More appropriate conditions in policy coupled with device type and location when adding KXIII/SXII as a network device in Cisco ISE

Specifications

Hardware

Dimensions and Physical Specifications

Dominion KX III model	Description	Power & heat dissipation	Dimensions (WxDxH)	Weight	Operating temp	Humidity
DKX3-108	• 8 server ports • 1 remote user • 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz	17.3" x 13.15'' x 1.73''	8.60lbs	0º - 45º C	0-85 % RH

Dominion KX III model	Description	Power & heat dissipation	Dimensions (WxDxH)	Weight	Operating temp	Humidity
		1.8A 60W 52 KCAL	439x334x44mm	3.9kg	32º - 113º F	
DKX3-116	• 16 server ports • 1 remote user • 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''	8.60lbs	0º - 45º C	0-85 % RH
			439x334x44mm	3.9kg	32º - 113º F	
DKX3-132	• 32 server ports • 1 remote user • 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''	8.60lbs	0º - 45º C	0-85 % RH
			439x334x44mm	3.9kg	32º - 113º F	
DKX3-216	• 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	
DKX3-232	• 32 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	
DKX3-416	• 16 server ports • 4 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	
DKX3-432	• 32 server ports • 4 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	
DKX3-464	• 64 server ports • 4 remote users • 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.3" x 3.5"	12.39lbs	0º - 45º C	0-85 % RH
			439x338x89mm	5.62kg	32º - 113º F	
DKX3-808	• 8 server ports • 8 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''	9.96lbs	0º - 45º C	0-85 % RH
			439x334x44mm	4.52kg	32º - 113º F	

Dominion KX III model	Description	Power & heat dissipation	Dimensions (WxDxH)	Weight	Operating temp	Humidity
DKX3-816	• 16 server ports • 8 remote users • 1 local port for use at the rack		440mm x 334mm x 44mm; 17.3" x 13.1" x 1.7"	6kg; 13.2lbs	0 - 50°C	0 - 85% RH
DKX3-832	• 32 server ports • 8 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''	9.96lbs	0º - 45º C	0-85 % RH
			439x334x44mm	4.52kg	32º - 113º F	
DKX3-864	• 64 server ports • 8 remote users • 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.3" x 3.5"	12.39lbs	0º - 45º C	0-85 % RH
			439x338x89mm	5.62kg	32º - 113º F	

Supported Target Server Video Resolutions

When using digital CIMs, you set the target's video resolution to match your monitor's native display resolution. The native display resolution is set when configuring ports for digital CIMs (see: Configure the CIM Target Settings).

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
- 1280x800@60Hz
- 1280x960@60Hz
- 1280x960@85Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1280x1024@85Hz
- 1360x768@60Hz
- 1366x768@60Hz
- 1368x768@60Hz
- 1400x1050@60Hz
- 1440x900@60Hz
- 1600x900 @60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@50Hz
- 1920x1080@60Hz
- 1920x1200@60Hz (Requires Reduced Blanking Time)

  For 1920x1200@60Hz, you must use a digital CIM and set the CIM's preferred resolution to 1920x1200@60Hz.

KX III 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
- 800x480@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:

Target server video resolution	Maximum distance
1024x768@60Hz (and below)	150' (45 m)
1280x1024@60Hz	100' (30 m)
1280×720@60Hz	75' (22 m)
1600x1200@60Hz	50' (15 m)
1920x1080@60Hz	50' (15 m)

See: Supported Target Server Video Resolutions (on page 178) for the video resolutions supported by the KX III.

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 Module (CIMs) Specifications

Digital CIMs support Display Data Channels (DDC) and Enhanced Extended Display Identification Data (E-EDID). However, they do not support HDCP (high bandwidth digital copy protection) or embedded audio.

Note: Both plugs must be plugged in for the HDMI and DVI CIMs.

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-DVUSB	Dual USB CIM for: • OS virtual media • Smartcard/CAC • Audio • Absolute Mouse Synchronization 	• 3.5" x 1.7" x 0.8" • 90 x 42 x 19mm	• 0.15lb • 0.07kg
D2CIM-DVUSB-MDP	Dual mini USB CIM for: • OS virtual media • Smartcard/CAC • Audio • Absolute Mouse Synchronization 	• 4.1" x 1.7" x 0.8" • 105 x 42 x 19mm	• 0.1lb • 0.052kg

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-VUSB	USB CIM for: • OS virtual media • Absolute Mouse Synchronization 	• 3.5" x 1.7" x 0.8" • 90 x 42 x 19mm	• 0.11lb • 0.052kg
D2CIM-VUSB-USBC	USB CIM for: • USB-C ports on Macs and PCs • USB keyboard, mouse, and virtual media • DisplayPort video • No Audio or Smartcard 	• 4.1" x 1.7" x 0.7" • 105 x 42 x 19mm	• 0.11lb • 0.05kg
D2CIM-DVUSB-DP	Digital CIM that provides digital-to-analog conversion and support for: • OS virtual media • Smartcard/CAC • Audio • Absolute and Relative Mouse Synchronization 	• 4.1" x 1.7" x 0.8" • 105 x 42 x 19mm	• 0.19lb • 0.85kg

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-DVUSB-HDMI	Digital CIM that provides digital-to-analog conversion and support for: • OS virtual media • Smartcard/CAC • Audio • Absolute and Relative Mouse Synchronization 	• 4.1" x 1.7" x 0.7" • 105 x 42 x 19mm	• 0.2lb • 0.09kg
D2CIM-DVUSB-DVI	Digital CIM that provides digital-to-analog conversion and support for: • OS virtual media • Smartcard/CAC • Audio • Absolute and Relative Mouse Synchronization 	• 4.1" x 1.7" x 0.8" • 105 x 42 x 19mm	• 0.25lb • 0.115kg
DCIM-PS2	CIM for PS2 	• 3" x 1.3" x 0.6" • 76 x 33 x 15mm	• 0.15lb • 0.07kg

CIM model	Description	Dimensions (WxDxH)	Weight
DCIM-USBG2	CIM for USB and Sun USB 	• 3" x 1.3" x 0.6" • 76 x 33 x 15mm	• 0.11lb • 0.05kg

Supported Digital Video CIMs for Mac

Use a digital video CIM to connect to the following Mac® ports:

Mac port	CIM
USB-C	D2CIM-VUSB-USBC
DVI	D2CIM-DVUSB-DVI
HDMI	D2CIM-DVUSB-HDMI
DisplayPort or Thunderbolt	D2CIM-DVUSB-DP

If the Mac's HDMI or DisplayPort video has a mini connector, a passive adapter cable may be required to connect to the full sized HDMI and DisplayPort plugs on the digital CIMs.

Alternatively, use the Mac VGA adapter with the D2CIM-VUSB or D2CIM-DVUSB. Note that this may be less reliable and the video quality may suffer.

For information on established modes supported by the KX III2.5.0 (and later) for Mac, see: Digital CIM Established and Standard Modes (on page 185).

Digital CIM Timing Modes

Following are the default timing modes that are used when the KX III communicates with a video source via a digital CIM.

The timing mode that is used is dependent on the native resolution of the video source.

- 1024x768@60Hz
- 1024x768@70Hz
- 1152x864@60Hz
- 1280x720@60Hz
- 1280x800@60HZ
- 1280x960@60Hz

- 1280x1024@60Hz (default resolution applied to digital CIMs)
- 1360x768@60Hz
- 1400x1050@60Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@50Hz
- 1920x1080@60Hz
- 1920x1200@60Hz

See: Configuring CIM Ports for more information.

Digital CIM Established and Standard Modes

The following additional established and standard resolutions and timing modes are supported by the KX III.

Digital CIM Established Modes

- 720x400@70Hz IBM, VGA
- 640x480@60Hz IBM, VGA
- 640x480@67Hz Apple Mac® II
- 640x480@72Hz VESA
- 640x480@75Hz VESA
- 800x600@56Hz VESA
- 800x600@60Hz VESA
- 800x600@72Hz VESA
- 800x600@75Hz VESA
- 832x624@75Hz Apple Mac II
- 1024x768@60Hz VESA
- 1024x768@70Hz VESA
- 1024x768@75Hz VESA
- 1280x1024@75Hz VESA
- 1152x870@75Hz Apple Mac II

Digital CIM Standard Modes

- 1152x864@75Hz VESA
- 1280x960@60Hz VESA
- 1280x1024@60Hz VESA
- 1360x768@60Hz VESA
- 1400x1050@60Hz VESA
- 1440x900@60Hz VESA

- 1600x1200 @60Hz VESA
- 1680x1050@60Hz VESA
- 1920x1080@60Hz VESA

DVI Compatibility Mode

DVI Compatibility Mode may be required if you are using an HDMI CIM to connect to a Dell Optiplex target with an Intel video card, or a Mac® Mini with an HDMI video port.

Selecting this mode ensures a good video quality from the targets.

See: Configuring CIM Ports in online help.

Supported Remote Connections

Remote connection	Details
Network	10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet
Protocols	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Network Speed Settings

KX III network speed setting							
Network switch port setting		**Auto**	**1000/Full**	**100/Full**	**100/Half**	**10/Full**	**10/Half**
	Auto	Highest Available Speed	1000/Full	KX III: 100/Full Switch: 100/Half	100/Half	KX III: 10/Full Switch: 10/Half	10/Half
	1000/ Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
	100/ Full	KX III: 100/Half Switch: 100/Full	KX III: 100/Half Switch: 100/Full	100/Full	KX III: 100/Half Switch: 100/Full	No Communication	No Communication
	100/ Half	100/Half	100/Half	KX III: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/ Full	KX III: 10/ Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	KX III: 10/Half Switch: 10/Full
	10/ Half	10/Half	No Communication	No Communication	No Communication	KX III: 10/Full Switch: 10/Half	10/Half

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 KX III behavior deviates from expected behavior

---

Note: For reliable network communication, configure the KX III and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure the KX III 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 KX III:

Video resolution	Cable length
1024x768@60Hz	50' (15.24 m)
1280x1024@60Hz	50' (15.24 m)
1600x1200@60Hz	30' (9.14 m)

Smart Card Minimum System Requirements

Local Port Requirements

The basic interoperability requirement for local port attachment to the KX III 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).
- A digital CIM or D2CIM-DVUSB (Dual-VM 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.

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 KX III 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

Operating system	Required PC/SC
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- 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 pcsc daemon (resource manager in framework) is restarted, restart the browser

Supported Smart Card Readers

Type	Vendor	Model	Verified
USB	SCM Microsystems	SCR331	Verified on local and remote
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	Verified on local and remote

Type	Vendor	Model	Verified
USB	SCM Microsystems	SCR331	Verified on local and remote
USB	ActivIdentity	ActivIdentity USB Reader v3.0	Verified on local and remote
USB	Gemalto®	GemPC USB-SW	Verified on local and remote
USB Keyboard/Card reader combo	Dell®	USB Smart Card Reader Keyboard	Verified on local and remote
USB Keyboard/Card reader combo	Cherry GmbH	G83-6744 SmartBoard	Verified on local and remote
USB reader for SIM-sized cards	Omnikey	6121	Verified on local and remote
Integrated (Dell Latitude D620)	O2Micro	OZ776	Remote only
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	Remote only
PCMCIA	SCM Microsystems	SCR243	Remote only

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, it's function cannot be guaranteed.

Type	Vendor	Model	Notes
USB Keyboard/Card reader Combo	HP®	ED707A	No interrupt endpoint => not compatible with Microsoft® driver
USB Keyboard/Card reader Combo	SCM Microsystems	SCR338	Proprietary card reader implementation (not CCID-compliant)
USB Token	Aladdin®	eToken PRO™	Proprietary implementation

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.

Audio format	Network bandwidth requirement
44.1 KHz, 16bit stereo	176 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 audio/video.

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

- 2 Virtual Media devices
- 1 Virtual Media + 1 smart card reader
- 1 Virtual Media + 1 audio device (w. playback and capture interfaces)
- 1 smart card reader + 1 audio device (w. playback and capture interfaces)

Certified Modems

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

KX III Supported Keyboard Languages

The KX III 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 KX III Local Console functions. For more information about non-US keyboards, see Informational Notes (on page 197).

Note: It is strongly recommended that you use system-config-keyboard to change languages if you are working in a Linux environment.

Language	Regions	Keyboard layout
US English	United States of America and most of English-speaking countries: for example, Canada, Australia, and New Zealand.	US Keyboard layout
US English International	United States of America and most of English-speaking countries: for example, Netherlands	US Keyboard layout
UK English	United Kingdom	UK layout keyboard
Chinese Traditional	Hong Kong S. A. R., Republic of China (Taiwan)	Chinese Traditional
Chinese Simplified	Mainland of the People's Republic of China	Chinese Simplified
Korean	South Korea	Dubeolsik Hangul
Japanese	Japan	JIS Keyboard
French	France	French (AZERTY) layout keyboard.

Language	Regions	Keyboard layout
German	Germany and Austria	German keyboard (QWERTZ layout)
French	Belgium	Belgian
Norwegian	Norway	Norwegian
Danish	Denmark	Danish
Swedish	Sweden	Swedish
Hungarian	Hungary	Hungarian
Slovenian	Slovenia	Slovenian
Italian	Italy	Italian
Spanish	Spain and most Spanish speaking countries	Spanish
Portuguese	Portugal	Portuguese

Mac Mini BIOS Keystroke Commands

The following BIOS commands have been tested on Intel-based Mac® Mini target servers and Mac Lion® servers running Mac Snow Leopard®. The servers were attached to a KX III with D2CIM-DVUSB and D2CIM-VUSB CIMs. See below for the supported keys and any notes.

Keystroke	Description	Virtual Media CIM	Dual Virtual Media CIM	Mac Lion Server HDMI CIM
Press C during startup	Start up from a bootable CD or DVD, such as the Mac OS X Install disc	Yes	Yes	Yes
Press D during startup	Start up in Apple Hardware Test (AHT)	Yes May need BIOS Mac profile for the mouse to work	Yes May need BIOS Mac profile for mouse to work	Yes May need BIOS Mac profile for the mouse to work
Press Option- Command-P-R until you hear startup sound a second time.	Reset NVRAM		Yes	Yes
Press Option during startup	Start up in Startup Manager, where you can select a Mac OS X volume to start from	Yes	Yes	Yes
Press Eject, F12, or hold the mouse button	Ejects any removable media, such as an optical disc	Yes	Yes	

Keystroke	Description	Virtual Media CIM	Dual Virtual Media CIM	Mac Lion Server HDMI CIM
Press N during startup	Start up from a compatible network server (NetBoot)	Yes	Yes	Yes
Press T during startup	Start up in Target Disk mode			Yes
Press Shift during startup	Start up in Safe Boot mode and temporarily disable login items	Yes	Yes	Known issue with LION to boot to safe mode. "Safe Mode" in red does not appear for Lion
Press Command-V during startup	Start up in Verbose mode.admin	Yes	Yes	Yes
Press Command-S during startup	Start up in Single-User mode	Yes	Yes	Yes
Press Option-N during startup	Start from a NetBoot server using the default boot image	Yes	Yes	Yes
Press Command-R during startup	Start from Lion Recovery1	N/A	N/A	Yes

Using a Windows Keyboard to Access Mac Targets

A Windows® keyboard can be used to access a Mac® connected to a KX III. 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)

* 5000: CC-SG and KXUS access (configurable)

* 22: SSH access (if enabled, configurable)

* 68: DHCP access (if DHCP is enabled)

► *Listening UDP Ports:*

* 162: SNMP access (if SNMP Agent is enabled)

* 5001: CC_SG event notification (if under CC-SG management)

► *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)

* 5001: CC_SG event notification (if under CC-SG management, configurable)

* 1812: RADIUS authentication (if enabled, configurable)

* 1813: RADIUS authentication (if enabled, configurable)

Software

Supported Operating Systems, Browsers and Java Versions

► *Java:*

Azul's open JDK/JRE version 8 and above is supported at the time of this release.

Future Java versions should work correctly assuming no incompatible changes are made by the Java developers. For any issues, please contact Technical Support.

- For best results, we recommend that Java Plug-in Caching is not enabled.
- For greater security and fewer Java and browser warning messages, Raritan recommends customers upload a SSL certificate to each KX III switch.
- Customers need to affirmatively click through all security warnings for the Raritan Java applets to load. See www.raritan.com/java for more information.

Note: See Java Requirements for Azul's open JDK/JRE support.

► *Browsers:*

Supported browsers, see the Release Notes for latest supported versions:

- Microsoft Edge
- Firefox
- Chrome
- Safari

For more details on compatible browsers for your OS, see the table below.

The Active KVM Client (AKC), the native Windows Client, requires Microsoft Edge, WebView2 and Microsoft .NET Framework versions 4.5 & above, and is supported on Windows desktops.

Note: These support statements do not apply to the KX III when used with CC-SG. Check the CC-SG Release Notes and Compatibility Matrix.

Operating Systems	Browsers	Java
Windows 11	Windows Edge Chrome Firefox	Azul's OpenJDK/JRE Java 8 or later for VKCs Java 8 or later for VKCs
openSUSE® 15	Firefox	
Fedora® 42 and 43	Firefox	
Red Hat 7.5	Firefox	
Mac 15.7.2, 26.0 and 26.1	Safari Chrome Firefox	

JRE Requirements and Browser Considerations for Mac

Java Runtime Environment Requirements for Mac

Install Azul's OpenJDK/JRE Java on PCs and Macs® when using the Virtual KVM Client (VKC) to access target devices via KX III.

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 Azul's OpenJDK/JRE 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 KX III.

Certain versions of Safari® block Java for security reasons. Use Firefox® instead in this case.

Additionally, you may be required to navigate through a number of messages. Select 'Do Not Block' if these messages are displayed.

Multi-Language Keyboard JRE Requirement

In order for multi-language keyboards to work in the KX III 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 KX III audit log and syslog:

- Access Login - A user has logged in to the KX III
- Access Logout - A user has logged out of the KX III
- 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.
- End CC Control - CC-SG management ended
- 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
- 802.1X Authentication Failed, CA Certificate uploaded for 802.1X authentication, Client Certificate uploaded for 802.1X authentication, Client Key uploaded for 802.1X authentication

BSMI Certification

設備名稱：KVM-over-IP 數位切換器 Equipment name　　型號（型式）：DKX3系列 (系列型號參見次頁) Type designation (Type)

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
電路板	—	○	○	○	○	○
電源供應器	—	○	○	○	○	○
機殼	○	○	○	○	○	○
面板	○	○	○	○	○	○
其他配件	○	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note 1：“Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2：“○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝—〞係指該項限用物質為排除項目。

Note 3：The “—” indicates that the restricted substance corresponds to the exemption.

系列型號:

DKX3-108	DKX3-116	DKX3-132
DKX3-216	DKX3-232	DKX3-416
DKX3-432	DKX3-464	DKX3-808
DKX3-832	DKX3-864	

Informational Notes

Overview

This section includes important notes on KX III usage. Future updates will be documented and available online through the Help link in the KX III Remote Console interface.

Note: Some topics in this section reference other multiple Raritan appliances because various appliances are impacted by the information.

Java Runtime Environment (JRE) Notes

Java Not Loading Properly on Mac

If you are using a Mac® and see the following message when connecting to a device from the KX III Port Access Table, Java™ is not loaded properly:

"Error while getting the list of open targets, please try again in a few seconds".

If this occurs, check your Java installation from this website: https://www.azul.com/downloads/?package=jdk#zulu

If your Java applet is inactive, it can be enabled from this page. If it is not installed correctly, a message lets you know and you can then reinstall Java.

AKC Download Server Certification Validation IPv6 Support Notes

If you are connecting to a KX III standalone device and support for AKC download server certificate validation is enabled, the valid IPv6 format to generate the certificate is either:

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` when there is a leading 0
  or
- `CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]` when there is no zero compression

Dual Stack Login Performance Issues

If you are using the KX III in a dual stack configuration, it is important you configured the domain system (DNS) correctly in the KX III in order to avoid delays when logging in.

See: Tips for Adding a Web Browser Interface for information on configuring your DNS in KX III.

CIM Notes

Windows 3-Button Mouse on Linux Targets

When using a 3-button mouse on a Windows® client connecting to a Linux® target, the left mouse button may get mapped to the center button of the Windows client 3-button mouse.

Target Video Picture Not Centered (Mouse Out of Synch)

At certain resolutions when using an HDMI or DVI CIM with the KX III:

- The video display may not be centered properly - black rectangles can be seen at the edges of the screen
- The mouse on the target may appear to be slightly out of synch

If either or both of these occur, you may be able to correct this by adjusting the display scaling options from the target computer's video controller software.

For example, if your target computer uses the Catalyst Control Center video controller, adjust the Underscan/Overscan setting as needed.

Powerstrip is not detected

When the PowerCIM-PDU is disconnected physically from the KX3, the PDU is still listed in the PowerStrip Device drop-down list with a "Powerstrip is not detected, please check!" message that does not disappear.

► *To solve:*

In the port configuration page for the port, click Reset To Default.

Virtual Media Notes

Cannot Connect to Drives from Linux Clients

If you cannot connect to a virtual media drive on a target server when you connect from a client running Linux® Fedora™ 18 with Java™ 1.8, disable SELinux in Fedora 18 on the client to resolve the problem.

Virtual Media via VKC and AKC in a Windows Environment

Following is a list of virtual media types users can access via VKC and AKC when running in a Windows environment.

Client	Administrator and Standard User
AKC and VKC	Access to: • Removable drives • CD/DVD drives • ISO images • Remote ISO images

Virtual Media Not Refreshed After Files Added

After a virtual media drive has been mounted, if you add a file(s) to that drive, those files may not be immediately visible on the target server. Disconnect and then reconnect the virtual media connection.

Virtual Media Linux Drive Listed Twice

For KX III, users who are logged in to Linux™ clients as root users, the drives are listed twice in the Local Drive drop-down.

For example, you will see eg /dev/sdc and eg /dev/sdc1 where the first drive is the boot sector and the second drive is the first partition on the disk.

Disconnecting Mac and Linux Virtual Media USB Drives

In a Linux® or Mac® environment:

- For Linux users, if there is /dev/sdb and /dev/sdb1, the client only uses /dev/sdb1 and advertise it as removable disk
- /dev/sdb is not available for the user.
- For Linux users, if there is /dev/sdb but no /dev/sdb1, /dev/sdb is used as a removable device
- For Mac users, /dev/disk1 and /dev/disk1s1 is used

Target BIOS Boot Time with Virtual Media

The BIOS for certain targets may take longer to boot if media is mounted virtually at the target.

► *To shorten the boot time:*

1. Close the Virtual KVM Client to completely release the virtual media drives.
2. Restart the target.

Virtual Media Connection Failures Using High Speed for Virtual Media Connections

Under certain circumstances it may be necessary to select the "Use Full Speed for Virtual Media CIM" when a target has problems with "High Speed USB" connections or when the target is experiencing USB protocol errors caused by signal degradation due to additional connectors and cables (for example, a connection to a blade server via a dongle).

USB Port and Profile Notes

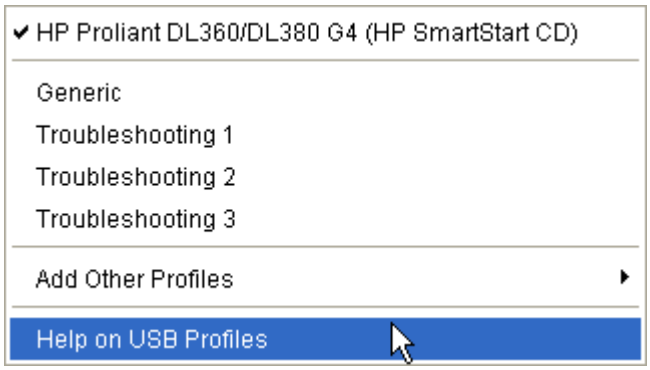
VM-CIMs and DL360 USB Ports

HP® DL360 servers have one USB port on the back of the device and another on the front of the device. With the DL360, both ports cannot be used at the same time. Therefore, a dual VM-CIM cannot be used on DL360 servers.

However, as a workaround, a USB2 hub can be attached to the USB port on the back of the device and a dual VM-CIM can be attached to the hub.

Help Choosing USB Profiles

When you are connected to a KVM target server via the Virtual KVM Client (VKC), you can view information about USB profiles via the Help on USB Profiles command on the USB Profile menu.



USB profile help appears in the USB Profile Help window. For detailed information about specific USB profiles, see Available USB Profiles.

A standard selection of USB configuration profiles are provided for a wide range of operating system and BIOS level server implementations. These are intended to provide an optimal match between remote USB device and target server configurations.

The 'Generic' profile meets the needs of most commonly deployed target server configurations.

Additional profiles are made available to meet the specific needs of other commonly deployed server configurations (for example, Linux®, Mac OS X®).

There are also a number of profiles (designated by platform name and BIOS revision) that have been tailored to enhance the virtual media function compatibility with the target server, for example, when operating at the BIOS level.

'Other Profiles' provides access to other profiles available on the system. Profiles selected from this list will be added to the USB Profile Menu. This includes a set of 'trouble-shooting' profiles intended to help identify configuration limitations.

The USB Profile Menu selections are configurable via accessing the target settings in the KVM Port Access and Configuration page

Should none of the standard USB profiles provided meet your target server requirements, Technical Support can work with you to arrive at a solution tailored for that target.

1. Check the most recent release notes to see if a solution is already available for your configuration.
2. If not, please provide the following information when contacting Technical Support:
   a. Target server information, manufacturer, model, BIOS, manufacturer, and version.
   b. The intended use (e.g. redirecting an image to reload a server's operating system from CD).

Changing a USB Profile when Using a Smart Card Reader

There may be certain circumstances under which you will need to change the USB profile for a target server. For example, you may need to change the connection speed to "Use Full Speed for Virtual Media CIM" when the target has problems with the "High Speed USB" connection speed.

When a profile is changed, you may receive a New Hardware Detected message and be required to log in to the target with administrative privileges to reinstall the USB driver. This is only likely to occur the first few times the target sees the new settings for the USB device. Afterward, the target will select the driver correctly.

Video Mode and Resolution Notes

Video Image Appears Dark when Using a Mac

If you are using a Mac® with an HDMI video port and the video seems too dark, enable DVI Compatibility Mode on the CIM to help resolve the issue.

See: Configuring CIM Ports

Video Shrinks after Adjusting Target Clock

On HP® Proliant® DL380p G8 target servers, certain resolutions cause the target video to shrink. This is caused when the server's clock attempts to auto-adjust and detects the wrong active line length.

Depending on the resolution the target is set to, this occurs when connecting to the HP target from the KX III Remote Console or Local Port, or both the Remote Console and Local Port. This issue was detected at the following resolutions:

Target resolution	Issue seen on Local Port	Issue seen from Remote Console
1440x900@60Hz	Yes	Yes
1400x1050@60Hz	No	Yes
1152x864@60Hz	No	Yes

Black Stripe/Bar(s) Displayed on the Local Port

Certain servers and video resolutions may display on the local port with small black bars at the edge of the screen.

If this occurs:

1. Try a different resolution, or
2. If using a digital CIM, then change the Display Native Resolution on the Port Configuration page to another resolution, or
3. If using the HDMI CIM, use the DVI Compatibility Mode.

Contact Raritan Technical Support for additional assistance.

Sun Composite Synch Video

Sun™ composite synch video is not supported.

SUSE/VESA Video Modes

The SuSE X.org configuration tool SaX2 generates video modes using modeline entries in the X.org configuration file. These video modes do not correspond exactly with VESA video mode timing (even when a VESA monitor is selected). The KX III, on the other hand, relies on exact VESA mode timing for proper synchronization. This disparity can result in black borders, missing sections of the picture, and noise.

► *To configure the SUSE video display:*

1. The generated configuration file /etc/X11/xorg.conf includes a Monitor section with an option named UseModes. For example,
   UseModes "Modes[0]"
2. Either comment out this line (using #) or delete it completely.
3. Restart the X server.

With this change, the internal video mode timing from the X server is used and corresponds exactly with the VESA video mode timing, resulting in the proper video display on the KX III.

Keyboard Notes

French Keyboard

Caret Symbol (Linux Clients Only)

The Virtual KVM Client (VKC) do not process the key combination of Alt Gr + 9 as the caret symbol (^) when using French keyboards with Linux® clients.

► *To obtain the caret symbol:*

From a French keyboard, press the ^ key (to the right of the P key), then immediately press the space bar.

Alternatively, create a macro consisting of the following commands:

1. Press Right Alt
2. Press 9.
3. Release 9.
4. Release Right Alt.

Note: These procedures do not apply to the circumflex accent (above vowels). In all cases, the ^ key (to the right of the P key) works on French keyboards to create the circumflex accent when used in combination with another character.

Numeric Keypad

From the Virtual KVM Client (VKC), the numeric keypad symbols display as follows when using a French keyboard:

Numeric keypad symbol	Displays as
/	;
.	;

Tilde Symbol

From the Virtual KVM Client (VKC), the key combination of Alt Gr + 2 does not produce the tilde (~) symbol when using a French keyboard.

► *To obtain the tilde symbol:*

Create a macro consisting of the following commands:

- Press right Alt
- Press 2
- Release 2
- Release right Alt

Keyboard Language Preference (Fedora Linux Clients)

Because the JAVA™ JRE™ on Linux® has problems generating the correct KeyEvents for foreign-language keyboards configured using System Preferences, it is recommended that you configure foreign keyboards using the methods described in the following table.

Language	Configuration method
US Intl	Default
UK	System Settings (Control Center)
French	Keyboard Indicator
German	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Swiss-German	System Settings (Control Center)
Norwegian	Keyboard Indicator
Swedish	Keyboard Indicator
Danish	Keyboard Indicator
Japanese	System Settings (Control Center)
Korean	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Italian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

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

There are several methods that can be used to set the keyboard language preference on Fedora® Linux clients. The following method must be used in order for the keys to be mapped correctly from the Virtual KVM Client (VKC).

► *To set the keyboard language using System Settings:*

1. From the toolbar, choose System > Preferences > Keyboard.
2. Open the Layouts tab.
3. Add or select the appropriate language.
4. Click Close.

► *To set the keyboard language using the Keyboard Indicator:*

1. Right-click the Task Bar and choose Add to Panel.
2. In the Add to Panel dialog, right-click the Keyboard Indicator and from the menu choose Open Keyboard Preferences.
3. In the Keyboard Preferences dialog, click the Layouts tab.
4. Add and remove languages as necessary.

Macros Not Saving on Linux Targets

If you receive the following error message when you create and then save a macro on a target server running Linux® Fedora™ 18 with Java™ 1.7.0 (update 45 and later), disable SELinux in Fedora 18 on the target server to resolve the problem.

```
"An error occurred attempting to write the new keyboard macros. Macro
was not added"
```

Mac Keyboard Keys Not Supported for Remote Access

When a Mac® is used as the client, the following keys on the Mac® keyboard are not captured by the Java™ Runtime Environment (JRE™):

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

As a result, the Virtual KVM Client (VKC) are unable to process these keys from a Mac client's keyboard.

Mouse Notes

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target device running Fedora® 7, if the target and local mouse pointers lose synchronization, changing the mouse mode from or to Intelligent or Standard may improve synchronization.

Single mouse mode may also provide for better control.

► *To resynchronize the mouse cursors:*

- Use the Synchronize Mouse option from the Virtual KVM Client (VKC).

Single Mouse Mode when Connecting to a Target Under CC-SG Control

When using Firefox® to connect to a KX III target under CC-SG control using DCIM-PS2 or DCIM-USBG2, if you change to Single Mouse Mode in the Virtual KVM Client (VKC), the VKC window will no longer be the focus window and the mouse will not respond.

If this occurs, left click on the mouse or press Alt+Tab to return the focus to the VKC window.

Mouse Sync Issues in Mac OS

In Mac OS, if mouse sync is an issue at some resolutions, use USB profile "General" and Absolute mouse mode.

Audio

Audio Playback and Capture Issues

Features that May Interrupt an Audio Connection

If you use any of the following features while connected to an audio device, your audio connection may be interrupted. These features are not recommended if you are connected to an audio device:

- Video Auto-Sense
- Extensive use of the local port
- Adding users

Issues when Using a Capture Device and Playback Device Simultaneously on a Target

On some targets, the simultaneous connection of capture devices and playback devices may not work due to the USB hub controller and how it manages the USB ports. Consider selecting an audio format that requires less bandwidth.

If this does not resolve the issue, connect the D2CIM-DVUSB CIM's keyboard and mouse connector to a different port on the target. If this does not solve the problem, connect the device to a USB hub and connect the hub to the target.

Audio in a Linux Environment

The following are known issues when using the audio feature in a Linux® environment.

- Linux® users, use the default audio device for playback. Sound may not come through if a non-default sound card is selected.
- SuSE 11 clients require Javas_1_6_0-sun-alsa (ALSA support for java-1_6_0-sun) to be installed via YaST.
- For Logitech® headsets with a built in a mic, only the Mono Capture option is available.
- In order to display the device, if you are running SUSE 11 and an ALSA driver, log out of KX III, then log back in.
- Note: If you connect and disconnect the audio device a number of times, the device may be listed several times vs. just once as it should.

Audio in a Windows Environment

On Windows® 64-bit clients, only one playback device is listed on the Connect Audio panel when accessing the device through the Virtual KVM Client (VKC).

The audio device is the default device, and is listed on the Connect Audio panel as Java Sound Audio Engine.

Smart Card Notes

Smart Card Connections to Fedora Servers

If you are using a smart card to connect to a Linux® Fedora® server via Virtual KVM Client (VKC) upgrade the pcsc-lite library to 1.4.102-3 or above.

CC-SG Notes

Virtual KVM Client Version Not Known from CC-SG Proxy Mode

When the Virtual KVM Client (VKC) is launched from CommandCenter Secure Gateway (CC-SG) in proxy mode, the VKC version is unknown.

In the About Raritan Virtual KVM Client dialog, the version is displayed as “Version Unknown”.

Moving Between Ports on a Device

If you move between ports on the same Raritan device and resume management within one minute, CC-SG may display an error message.

If you resume management, the display will be updated.

Browser Notes

Resolving Issues with Firefox Freezing when Using Fedora

If you are accessing Firefox® and are using a Fedora® server, Firefox may freeze when it is opening.

To resolve this issue, install the libnpjp2.so Java™ plug-in on the server.

Frequently Asked Questions

General FAQs

Question	Answer
What is Dominion KX III?	Dominion KX III is a third-generation digital KVM (keyboard, video, mouse) switch that enables one, two, four or eight IT administrators to access and control 8, 16, 32 or 64 servers over the network with BIOS-level functionality. Dominion KX III is completely hardware- and OS-independent; users can troubleshoot and reconfigure servers even when servers are down. At the rack, Dominion KX III provides the same functionality, convenience, and space and cost savings as traditional analog KVM switches. However, Dominion KX III also integrates the industry's highest performing KVM-over-IP technology, allowing multiple administrators to access server KVM consoles from any networked workstation as well as from the iPhone® and iPad®.
How is KX III different from KX II ?	The KX III is the next generation version of the KX II. Featuring a modern hardware design with increased computing power and storage, the KX III provides KVM-over-IP access for IT administration, as well as high performance IP access for broadcast applications. KX III includes virtually all KX II features with the following advancements: The KX III's new video processing engine supports a broad range of applications from traditional computer applications to the most dynamic broadcast applications requiring 30 frames-per-second 1920x1080 video, 24 bit color, digital audio, dual monitors and DVI, HDMI, DisplayPort and VGA video. With the industry's first DVI-based local port, the KX III's common user interface provides new levels of productivity and performance for at-the-rack administration and server access. All KX III models feature a tiering port to connect multiple Dominion KX III switches together and access the attached servers. Up to 1024 servers can be accessed via a consolidated port list. KX III supports all Dominion and Paragon II CIMs supported by KX II.

Question	Answer
How does Dominion KX III differ from remote control software?	When using Dominion KX III remotely, the interface, at first glance, may seem similar to remote control software such as pcAnywhere™, Windows® Terminal Services/ Remote Desktop, VNC, etc. However, because Dominion KX III is not a software but a hardware solution, it's much more powerful: Hardware- and OS-independent – Dominion KX III can be used to manage servers running many popular OSs, including Intel®, Sun®, PowerPC running Windows, Linux®, Solaris™, etc. State-independent/Agentless – Dominion KX IIKX IIII does not require the managed server OS to be up and running, nor does it require any special software to be installed on the managed server. Out-of-band – Even if the managed server's own network connection is unavailable, it can still be managed through Dominion KX III. BIOS-level access – Even if the server is hung at boot up, requires booting to safe mode, or requires system BIOS parameters to be altered, Dominion KX III still works flawlessly to enable these configurations to be made.
Can the Dominion KX III be rack mounted?	Yes. The Dominion KX III ships standard with 19" rack mount brackets. It can also be reverse rack mounted so the server ports face forward.
How large is the Dominion KX III?	Dominion KX III is only 1U high (except the KX3-864 and KX3-464, which are 2U), fits in a standard 19" rack mount and is only 11.4" (29 cm) deep. The Dominion KX3-832 and KX3-864 are 13.8" (36 cm) deep.

Remote Access

Question	Answer
How many users can remotely access servers on each Dominion KX III?	Dominion KX III models offer remote connections for up to eight users per user channel to simultaneously access and control a unique target server. For one-channel appliances like the DKX3-116, up to eight remote users can access and control a single target server. For two-channel appliances, like the DKX3-216, up to eight users can access and control the server on channel one and up to another eight users on channel two. For four-channel appliances, up to eight users per channel, for a total of 32 (8 x 4) users, can access and control four servers. Likewise, for the eight-channel appliances, up to eight users can access a single server, up to an overall maximum of 32 users across the eight channels.
Can I remotely access servers from my iPhone or iPad?	Yes. Users can access servers connected to the KX III using their iPhone or iPad. Mobile access is provided through Mobile Access Client, which requires the use of CommandCenter Secure Gateway (CC-SG).
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.

Question	Answer
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 Dominion KX III from a client, what hardware, software or network configuration is required?	Because Dominion KX III is completely Web-accessible, it doesn't require customers to install proprietary software on clients used for access. Dominion KX III can be accessed through major Web browsers, including: Edge® and Firefox®. Dominion KX III can be accessed on Windows®, Linux® and Mac® desktops, via Raritan's Windows Client, and the Java™-based Virtual KVM Client™. Dominion KX III administrators can also perform remote management (set passwords and security, rename servers, change IP address, etc.) using a convenient browser-based interface.

<table>
<tr><th>Question</th><th>Answer</th></tr>
<tr><td>What is the file size of the applet that’s used to access Dominion KX III? How long does it take to retrieve?</td><td>The Virtual KVM Client (VKC) applet used to access Dominion KX III is approximately 500KB in size. The following chart describes the time required to retrieve Dominion KX III’s applet at different network speeds:
<table>
<tr><td>100Mbps</td><td>Theoretical 100Mbit network speed</td><td>.05 seconds</td></tr>
<tr><td>60Mbps</td><td>Likely practical 100Mbit network speed</td><td>.08 seconds</td></tr>
<tr><td>10Mbps</td><td>Theoretical 10Mbit network speed</td><td>.4 seconds</td></tr>
<tr><td>6Mbps</td><td>Likely practical 10Mbit network speed</td><td>.8 seconds</td></tr>
</table></td></tr>
</table>

Question	Answer
Do you have a Windows KVM Client?	Yes. We have a native .NET Windows Client called the Raritan Active KVM Client (AKC). See Active KVM Client (AKC) (on page 75)
Do you have a non-Windows KVM Client?	Yes. The Virtual KVM Client (VKC) allows non-Windows users to connect to target servers in the data center. See Virtual KVM Client (VKC and VKCs) Help (on page 41)
Do your KVM Clients have multi-language support?	Yes. The Dominion KX III's remote HTML User Interface and the KVM Clients support the Japanese, Simplified Chinese and Traditional Chinese languages. This is available stand-alone as well as through CC-SG.
Do your KVM Clients support dual LCD monitors?	Yes. For customers wishing to enhance their productivity by using multiple LCD monitors on their desktops, the Dominion KX III can launch KVM sessions to multiple monitors, either in full screen or standard modes.
Do you support servers with dual video cards?	Yes, dual video cards are supported with an extended desktop configuration available to the remote user.
How do I access servers connected to Dominion KX III if the network ever becomes unavailable?	You can access servers at the rack or via modem. Dominion KX III offers a dedicated modem port for attaching an external modem.

Universal Virtual Media

Question	Answer
Which Dominion KX III models support virtual media?	All Dominion KX III models support virtual media. It is available stand-alone and through CommandCenter® Secure Gateway, Raritan's centralized management appliance.
Which types of virtual media does the Dominion KX III support?	Dominion KX III supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives and ISO images.

Question	Answer
What is required for virtual media?	A Dominion KX III virtual media CIM is required. There are two VGA-based CIMs: a D2CIM-VUSB or D2CIM-DVUSB. The D2CIM-VUSB has a single USB connector and is for customers who will use virtual media at the OS level. The D2CIM-DVUSB has dual USB connectors and should be purchased by customers who wish to utilize virtual media at the BIOS level. The D2CIM-DVUSB is also required for smart card authentication, tiering/cascading and digital audio. Both support virtual media sessions to target servers supporting the USB 2.0 interface. Available in economical 32 and 64 quantity CIM packages, these CIMs support Absolute Mouse Synchronization™ as well as remote firmware updates. Our CIMs have traditionally supported analog VGA video. Three new dual virtual media CIMs support digital video formats, including DVI, HDMI and DisplayPort. These are the D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI and D2CIM-DVUSB-DP.
Is virtual media secure?	Yes. Virtual media sessions are secured using 256-bit AES or 128-bit AES encryption.
Does virtual media really support audio?	Yes. Audio playback and recording to a server connected to the Dominion KX III 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. A digital CIM or D2CIM-DVUSB dual virtual media CIM is required.
What is a USB profile?	Certain servers require a specifically configured USB interface for USB-based services such as virtual media. The USB profile tailors the KX III's USB interface to the server to accommodate these server-specific characteristics.
Why would I use a USB profile?	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 Mac and Linux servers.
How is a USB profile used?	Individual ports or groups of ports can be configured by the administrator to use a specific USB profile in the KX III's port configuration page. A USB profile can also be selected in the KX III Client when required. See the user guide for more information.
Do I always need to set a USB profile when I use virtual media?	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.
What profiles are available? Where can I find more information?	Consult the user guide for the available profiles and for more information.

Bandwidth and KVM-over-IP Performance

Question	Answer
How is bandwidth used in KVM-over-IP systems?	Dominion KX III offers totally new video processing that provides flexible, high performance video, efficient use of bandwidth and anytime/anywhere access via LAN, WAN or Internet. The Dominion KX III 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 client to create the remote session to the user. The KX III 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 to the server's video display screen. If there are no changes to the video – the user is not interacting with the server – there is generally little to 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.
How does bandwidth affect KVM-over-IP performance?	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 Dominion KX III has been optimized to provide strong performance in a wide variety of environments.
What factors affect bandwidth?	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, the KVM Client Connection Properties, client PC resources and video card noise.
How much bandwidth does KX III use for common tasks?	Bandwidth primarily depends on the user's task and actions. The more the server's video screen changes, the more bandwidth is utilized.

Question	Answer
How do I optimize performance and bandwidth?	KX III 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. Optimize For. Use this setting to configure the video engine for standard IT/ computer applications or for video/broadcast applications. Compression. 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. 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)
I want to connect over the Internet. What type of performance should I expect?	It depends on the bandwidth and latency of the Internet connection between your remote client and the KX III. 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.
I have a high bandwidth environment. How can I optimize performance?	The default settings will work well. You can move the Connection Properties settings to the left for increased video performance.
What is the maximum remote (over IP) video resolution supported?	The Dominion KX III is the first and only KVM-over-IP switch to support full high definition (HD) remote video resolution – 1920x1080 at frame rates up to 30 frames per second with digital audio. In addition, popular widescreen formats are supported, including 1600x1200, 1680x1050 and 1440x900, so remote users can work with today's higher resolution monitors.
How much bandwidth is used for audio?	It depends on the type of audio format used, but to listen to CD quality audio, approximately 1.5 Mbps is used.
What about servers with DVI ports?	Servers with DVI ports that support DVI-A (analog) and DVI-I (integrated analog and digital) can use Raritan's ADVI-VGA inexpensive, passive adapter to convert the server's DVI port to a VGA plug that can be connected to a KX III CIM's VGA plug. Servers with DVI ports that support DVI-I or DVI-D (digital) can use the new D2CIM-DVUSB-DVI CIM.

IPv6 Networking

Question	Answer
What is IPv6?	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.
Why does KX III support IPv6 networking?	U.S. government agencies and the Department of Defense are now mandated to purchase IPv6-compatible products. In addition, many enterprises and foreign countries, such as China, will be transitioning to IPv6 over the next several years.
What is "dual stack" and why is it required?	Dual stack is the ability to simultaneously support IPv4 and IPv6 protocols. Given the gradual transition from IPv4 to IPv6, dual stack is a fundamental requirement for IPv6 support.
How do I enable IPv6 on the KX III?	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.
What if I have an external server with an IPv6 address that I want to use with my KX III?	The KX III can access external servers via their IPv6 addresses, for example, an SNMP manager, syslog server or LDAP server. Using the KX III's dual-stack architecture, these external servers can be accessed via: (1) an IPv4 address, (2) IPv6 address or (3) hostname. So, the KX III supports the mixed IPv4/IPv6 environment many customers will have.
What if my network doesn't support IPv6?	The KX III'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.
Where can I get more information on IPv6?	See www.ipv6.org for general information on IPv6. The KX III user guide describes the KX III's support for IPv6.

Servers

Question	Answer
Does KX III depend on a Windows server to operate?	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), KX III is designed to be completely independent from any external server.
What should I do to prepare a server for connection to KX III?	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.

Question	Answer
What about mouse synchronization?	In the past, KVM-over-IP mouse synchronization was a frustrating experience. The KX III'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.
What comes in the KX III box?	The following is included: (1) KX III appliance, (2) Quick Setup Guide, (3) standard 19" rack mount brackets, (5) localized AC line cord and (6) and other documentation.

Installation

Question	Answer
Besides the appliance itself, what do I need to order to install Dominion KX III?	Each server that connects to Dominion KX III requires a Dominion or Paragon computer interface module (CIM), an adapter that connects directly to the keyboard, video and mouse ports of the server.
Which kind of Cat5 cabling should be used in my installation?	Dominion KX III can use any standard UTP (unshielded twisted pair) cabling, whether Cat5, Cat5e or Cat6. Often in our manuals and marketing literature, Raritan will simply say "Cat5" cabling for short. In actuality, any brand UTP cable will suffice for Dominion KX III.
Which types of servers and PCs can be connected to Dominion KX III?	Dominion KX III 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 DSAM.
How do I connect servers to Dominion KX III?	Servers that connect to the Dominion KX III require a Dominion CIM, which connects directly to the keyboard, video and mouse ports of the server. Then, connect each CIM to Dominion KX III using standard UTP (unshielded twisted pair) cable such as Cat5, Cat5e or Cat6.
How far can my servers be from Dominion KX III?	In general, servers can be up to 150 feet (45 m) away from Dominion KX III, depending on the type of server. (See Target Server Video Resolution - Supported Connection Distances and Refresh Rates (on page 180)) For the D2CIM-VUSB CIMs that supports virtual media and Absolute Mouse Synchronization, a 100-foot (30 m) range is recommended.
Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to Dominion KX III from locking up when I switch away from them?	Each Dominion computer interface module (DCIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan's KME technology is data center grade, battle-tested and far more reliable than that found in lower-end KVM switches: it incorporates more than 15 years of experience and has been deployed to millions of servers worldwide.

Question	Answer
Are there any agents that must be installed on servers connected to Dominion KX III?	Servers connected to Dominion KX III do not require any software agents to be installed because Dominion KX III connects directly via hardware to the servers' keyboard, video and mouse ports.
How many servers can be connected to each Dominion KX III appliance?	Dominion KX III models range from 8, 16 or 32 server ports in a 1U chassis, to 64 server ports in a 2U chassis. This is the industry's highest digital KVM switch port density.
What happens if I disconnect a server from Dominion KX III and reconnect it to another Dominion KX III appliance, or connect it to a different port on the same Dominion KX III appliance?	Dominion KX III 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 and the optional CommandCenter Secure Gateway management appliance.
How do I connect a serially controlled (RS-232) device, such as a Cisco router/switch to Dominion KX III?	Connecting a KX III and a Dominion Serial Access Module (DSAM) provides serial access for the KX III. The DSAM is a 2- or 4 port serial module that derives power from the KX III.

Local Port - KX III

Question	Answer
Can I access my servers directly from the rack?	Yes. At the rack, Dominion KX III functions just like a traditional KVM switch – allowing control of up to 64 servers using a single keyboard, monitor and mouse. You can switch between servers by the browser based user interface or via a hotkey.
Can I consolidate the local ports of multiple KX IIIs?	Yes. You can connect the local ports of multiple KX III switches to another KX III using the "tiering" feature of the KX III. You can then access the servers connected to your KX III appliances from a single point in the data center via a consolidated port list.
When I am using the local port, do I prevent other users from accessing servers remotely?	No. The Dominion KX III local port has a 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.
Can I use a USB keyboard or mouse at the local port?	Yes. The Dominion KX III has USB keyboard and mouse ports on the local port. Dominion KX III switches do not have PS/2 local ports. Customers with PS/2 keyboards and mice should utilize a PS/2 to USB adapter.
Is there an onscreen display (OSD) for local, at-the-rack access?	Yes, but Dominion KX III's at-the-rack access goes way beyond conventional OSDs. Featuring the industry's first browser-based interface for at-the-rack access, Dominion KX III's local port uses the same interface for local and remote access. Moreover, most administrative functions are available at the rack.

Question	Answer
How do I select between servers while using the local port?	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.
How do I ensure that only authorized users can access servers from the local port?	Users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that: If the Dominion KX III 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, Dominion KX III fails over to its own internal authentication database. Dominion KX III has its own stand-alone authentication, enabling instant, out-of-the-box installation.

Blade Servers

Question	Answer
Can I connect blade servers to the Dominion KX III?	Yes. Dominion KX III supports popular blade server models from the leading blade server manufacturers: HP®, IBM®, Dell® and Cisco®.
Which blade servers are supported?	The following models are supported: Dell PowerEdge® 1855, 1955 and M1000e; HP BladeSystem c3000 and c7000; IBM BladeCenter® H, E and S; and Cisco UCS B-Series.
Which CIM should I use?	It depends on the type of KVM ports on the specific make and model of the blade server you are using. The following CIMs are supported: DCIM-PS2, DCIM-USBG2, D2CIM-VUSB and D2CIM-DVUSB.
Which types of access and control are available?	The Dominion KX III provides automated and secure KVM access: (1) at the rack, (2) remotely over IP, (3) via CommandCenter and (4) by modem.
Do I have to use hotkeys to switch between blades?	Some blade servers require you to use hotkeys to switch between blades. With the Dominion KX III, you don't have to use these hotkeys. Just click on the name of the blade server, and the Dominion KX III will automatically switch to that blade without the explicit use of the hotkey.
Can I access the blade server's management module?	Yes. You can define the URL of the management module and access it from the Dominion KX III or from our CommandCenter Secure Gateway. If configured, one-click access is available.
How many blade servers can I connect to a Dominion KX III?	For performance and reliability reasons, you can connect up to eight blade chassis to a Dominion KX III, regardless of model. Raritan recommends connecting up to two times the number of remote connections supported by the device. For example, with a KX3-216 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.

Question	Answer
I'm an enterprise customer using CommandCenter Secure Gateway. Can I access blade servers via CommandCenter Secure Gateway?	Yes. Once blade servers are configured on the Dominion KX III, the CommandCenter Secure Gateway user can access them via KVM connections. In addition, the blade servers are organized by chassis as well as CommandCenter Secure Gateway custom views.
What if I also want in-band or embedded KVM access?	In-band and embedded access to blade servers can be configured within CommandCenter Secure Gateway.
I'm running VMware® on some of my blade servers. Is this supported?	Yes. With CommandCenter Secure Gateway, you can display and access virtual machines running on blade servers.
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 CIM – D2CIM-VUSB or D2CIM-DVUSB – 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 and some Dell blade servers, a CIM can be connected to each blade, so Absolute Mouse Synchronization is supported.
Is blade access secure?	Yes. Blade access uses all of the standard Dominion KX III 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.
Does the Dominion KSX II or the KX III-101 support blade servers?	At this time, these products do not support blade servers.

Extended Local Port

Question	Answer
What is the extended local port?	The Dominion KX2-808, KX2-832 and KX2-864 featured an extended local port. The corresponding Dominion KX III models do not have an extended local port. Instead all KX III models have a tiering port. To extend the KX III's digital local port, you can use the Raritan Cat5 Reach DVI product for local and remote access up to 500 meters. See Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality (on page 159)

Dual Power Supplies

Question	Answer
Does KX III have a dual power option?	Yes. All KX III 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 KX III will automatically switch to the other.

Question	Answer
Does the power supply used by KX III automatically detect voltage settings?	Yes. KX III's power supply can be used in AC voltage ranges from 100–240 volts, at 50–60 Hz.
If a power supply or input fails, will I be notified?	The KX III 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 KX remote client user interface. If configured by the administrator, then SNMP or syslog events will be generated.

Intelligent Power Distribution Unit (PDU) Control

Question	Answer
What type of remote power control capabilities does Dominion KX III offer?	Raritan's intelligent PDUs can be connected to the Dominion KX III to provide power control of target servers and other equipment. For servers, after a simple one-time configuration step, just click on the server name to power on, off or to recycle a hung server.
What type of power strips does Dominion KX III support?	Raritan's Dominion PX™ and Remote Power Control (RPC) power strips. These come in many outlet, connector and amp variations. Note that you should not connect the PM series of power strips to the Dominion KX III as these power strips do not provide outlet-level switching.
How many PDUs can be connected to a Dominion KX III?	Up to eight PDUs can be connected to a Dominion KX III appliance.
How do I connect the PDU to the Dominion KX III?	The D2CIM-PWR is used to connect the power strip to the Dominion KX III. The D2CIM-PWR must be purchased separately; it does not come with the PDU.
Does Dominion KX III support servers with multiple power supplies?	Yes. Dominion KX III can be easily configured to support servers with multiple power supplies connected to multiple power strips. Four power supplies can be connected per target server.
Does the Dominion KX III display statistics and measurements from the PDU?	Yes. PDU-level power statistics, including power, current and voltage, are retrieved from the PDU and displayed to the user.
Does remote power control require any special configuration of attached servers?	Some servers ship with default BIOS settings such that the server does not automatically restart after losing and regaining power. For these servers, see the server's documentation to change this setting.
What happens when I recycle power to a server?	Note that this is the physical equivalent of unplugging the server from the AC power line, and reinserting the plug.

Ethernet and IP Networking

Question	Answer
What is the speed of Dominion KX III's Ethernet interfaces?	Dominion KX III supports gigabit as well as 10/100 Ethernet. KX III supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto detected or manually set).
Can I access Dominion KX III over a wireless connection?	Yes. Dominion KX III not only uses standard Ethernet, but also very conservative bandwidth with very high quality video. Thus, if a wireless client has network connectivity to a Dominion KX III, servers can be configured and managed at the BIOS level wirelessly.
Does the Dominion KX III offer dual gigabit Ethernet ports to provide redundant failover or load balancing?	Yes. Dominion KX III features dual gigabit Ethernet ports to provide redundant failover capabilities. Should the primary Ethernet port (or the switch/router to which it is connected) fail, Dominion KX III will failover to the secondary network port with the same IP address – ensuring that server operations are not disrupted. Note that automatic failover must be enabled by the administrator.
Can I use Dominion KX III with a VPN?	Yes. Dominion KX III uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Traffic can be easily tunneled through standard VPNs.
Can I use KX III with a proxy server?	Yes. KX III can be used with a SOCKS proxy server, assuming the remote client PC is configured appropriately. Contact the user documentation or online help for more information.
How many TCP ports must be open on my firewall in order to enable network access to Dominion KX III?	Two ports are required: TCP port 5000 to discover other Dominion appliances and for communication between Raritan appliances and CC-SG; and, of course, port 443 for HTTPS communication.
Are these ports configurable?	Yes. Dominion KX III's TCP ports are configurable by the administrator.
Can Dominion KX III be used with Citrix®?	Dominion KX III may work with remote access products like Citrix if configured appropriately, but Raritan cannot guarantee it will work with acceptable performance. Customers should realize that products like Citrix utilize video redirection technologies similar in concept to digital KVM switches so that two KVM-over-IP technologies are being used simultaneously.
Can the Dominion KX III use DHCP?	DHCP addressing can be used; however, Raritan recommends fixed addressing since the Dominion KX III is an infrastructure appliance and can be accessed and administered more effectively with a fixed IP address.

Question	Answer
I’m having problems connecting to the Dominion KX III over my IP network. What could be the problem?	The Dominion KX III relies on your LAN/WAN network. Some possible problems include: • Ethernet auto-negotiation. On some networks, 10/100 auto-negotiation does not work properly, and the Dominion KX III appliance must be set to 100 Mb/full duplex or the appropriate choice for its network. • Duplicate IP address. If the IP address of the Dominion KX III is the same as another appliance, network connectivity may be inconsistent. • Port 5000 conflicts. If another appliance is using port 5000, the Dominion KX III default port must be changed (or the other appliance must be changed). • When changing the IP address of a Dominion KX III, or swapping in a new Dominion KX III, sufficient time must be allowed for its IP and Mac® addresses to be known throughout the Layer 2 and Layer 3 networks.

Local Port Consolidation, Tiering and Cascading

Question	Answer
How do I physically connect multiple Dominion KX III appliances together into one solution?	To physically connect multiple KX III appliances together for consolidated local access, you can connect the Tiering ports of multiple "tiered" (or "cascaded") KX III switches to a "base" KX III using the Tiering port of the KX III. You can then access the servers connected to your KX III appliances from a single point in the data center via a consolidated port list. The Tiering port must be used to connect the tiered KX III 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 KX IIIs can be accessed via a hierarchical port list or via search (with wildcards). Two levels of tiering are supported; up to 1024 appliances can be accessed in a tiered configuration. Remote power control is also supported. Virtual media, smart card and blade server access via tiered access will be supported in a future release. Of course these features are available when accessed via a standard remote connection. While remote IP server access via the consolidated port list is available as a convenience, remote accessing a tiered server from CommandCenter or via the KX III the server is connected to, is recommended for optimal performance.

Question	Answer
Do I have to physically connect Dominion KX III appliances together?	Multiple Dominion KX III appliances do not need to be physically connected together. Instead, each Dominion KX III appliance connects to the network, and they automatically work together as a single solution if deployed with Raritan's CommandCenter Secure Gateway (CC-SG) management appliance. CC-SG acts as a single access point for remote access and management. CC-SG offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update and a single authentication and authorization database. Customers using CC-SG for centralized remote access can make good use of the KX III's tiering (cascading) feature to consolidate the local ports of multiple KX III switches and locally access up to 1024 servers from a single console when in the data center.
Is CC-SG required?	For customers wanting stand-alone usage (without a central management system), multiple Dominion KX III appliances still interoperate and scale together via the IP network. Multiple Dominion KX III switches can be accessed from the KX III Web-based user interface.
Can I connect an existing analog KVM switch to Dominion KX III?	Yes. Analog KVM switches can be connected to one of Dominion KX III's server ports. Simply use a USB computer interface module (CIM), and attach it to the user ports of the existing analog KVM switch. Analog KVM switches supporting hotkey-based switching on their local ports can be tiered to a Dominion KX III switch and switched via a consolidated port list, both remotely and in the data center. Please note that analog KVM switches vary in their specifications and Raritan cannot guarantee the interoperability of any particular third-party analog KVM switch. Contact Raritan technical support for further information.

Computer Interface Modules (CIMs)

Question	Answer
What type of video is supported by your CIMs?	Our CIMs have traditionally supported analog VGA video. Three new CIMs support digital video formats, including DVI, HDMI and DisplayPort. These are the D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI and D2CIM-DVUSB-DP.
Can I use computer interface modules (CIMs) from Paragon, Raritan's analog matrix KVM switch, with Dominion KX III?	Yes. Certain Paragon computer interface modules (CIMs) may work with Dominion KX IIKX IIII. (Please check the Raritan Dominion KX III Release Notes on the website for the latest list of certified CIMs.) However, because Paragon CIMs cost more than Dominion KX III CIMs (as they incorporate technology for video transmission of up to 1,000 feet [304 m]), it is not generally advisable to purchase Paragon CIMs for use with Dominion KX III. Also note that when connected to Dominion KX III, Paragon CIMs transmit video at a distance of up to 150 feet (46 m), the same as Dominion KX III CIMs – not at 1,000 feet (304 m), as they do when connected to Paragon.

Question	Answer
Does Dominion KX III support Paragon Dual CIMs?	Yes. The Dominion KX III supports Paragon II Dual CIMs (P2CIM-APS2DUAL and P2CIM-AUSBDUAL), which can connect servers in the data center to two different Dominion KX III switches. If one KX III switch is not available, the server can be accessed through the second KX III switch, providing redundant access and doubling the level of remote KVM access. Please note these are Paragon CIMs, so they do not support the KX III advanced features such as virtual media, absolute mouse, audio, etc.

Security

Question	Answer
Is the KX III FIPS 140-3 Certified?	The KX III uses an embedded FIPS 140-3 validated cryptographic module running on a Linux platform per FIPS 140-3 implementation guidelines. This cryptographic module is used for encryption of KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.
What kind of encryption does KX III use?	KX III 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 KX III that is not completely secured by encryption.
Does KX III support AES encryption as recommended by the U.S. government's NIST and FIPS standards?	Yes. The KX III utilizes the Advanced Encryption Standard (AES) for added security. 256-bit and 128-bit AES is available. 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.
Does KX III allow encryption of video data? Or does it only encrypt keyboard and mouse data?	Unlike competing solutions, which only encrypt keyboard and mouse data, KX III does not compromise security – it allows encryption of keyboard, mouse, video and virtual media data.
How does KX III integrate with external authentication servers such as Active Directory, RADIUS or LDAP?	Through a very simple configuration, KX III can be set to forward all authentication requests to an external server such as LDAP, Active Directory or RADIUS. For each authenticated user, KX III receives from the authentication server the user group to which that user belongs. KX III then determines the user's access permissions depending on the user group to which he or she belongs.
How are usernames and passwords stored?	Should KX III's internal authentication capabilities be used, all sensitive information, such as usernames and passwords, is stored in an encrypted format. Literally no one, including Raritan technical support or product engineering departments, can retrieve those usernames and passwords.

Question	Answer
Does KX III support strong passwords?	Yes. The KX III 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.
Can I upload my own digital certificate to the KX III?	Yes. Customers can upload self-signed or certificate authority-provided digital certificates to the KX III for enhanced authentication and secure communication.
Does the KX III support a configurable security banner?	Yes. For government, military and other security-conscious customers requiring a security message before user login, the KX III can display a user-configurable banner message and optionally require acceptance.
My security policy does not allow the use of standard TCP port numbers. Can I change them?	Yes. For customers wishing to avoid the standard TCP/IP port numbers to increase security, the KX III allows the administrator to configure alternate port numbers.

Smart Cards and CAC Authentication

Question	Answer
Does KX III support smart card and CAC authentication?	Yes. Smart cards and DoD common access cards (CAC) authentication to target servers is supported.
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 multitechnology, multipurpose card; the goal is to have a single identification card. For more information, see the FIPS 201 standards.
Which KX III models support smart cards/ CAC?	All KX III models are supported. The KX III-101 models do not currently support smart cards and CAC.
Do enterprise and SMB customers use smart cards, too?	Yes. However, the most aggressive deployment of smart cards is in the U.S. federal government.
Which CIMs support smart card/CAC?	The D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP and D2CIM-DVUSB-MDP are the required CIMs.
Which smart card readers are supported?	The required reader standards are USB CCID and PC/SC. Consult the user documentation for a list of certified readers and more information.
Can smart card/CAC authentication work on the local port and via CommandCenter?	Yes. Smart card/CAC authentication works on both the local port and via CommandCenter. For the local port, connect a compatible smart card reader to the USB port of the KX III.

Manageability

Question	Answer
Can KX III be remotely managed and configured via Web browser?	Yes. KX III can be completely configured remotely via Web browser. Note that this does require that the workstation have an appropriate Java Runtime Environment (JRE) version installed. Besides the initial setting of KX III's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and KX III's default IP address, you can even configure the initial settings via Web browser.)
Can I back up and restore KX III's configuration?	Yes. KX III's appliance and user configurations can be completely backed up for later restoration in the event of a catastrophe. KX III's backup and restore functionality can be used remotely over the network, or through your Web browser.
What auditing or logging does KX III offer?	For complete accountability, KX III logs all major user events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user logout, user access of a particular server, unsuccessful login, configuration changes, etc.
Can KX III integrate with syslog?	Yes. In addition to KX III's own internal logging capabilities, KX III can send all logged events to a centralized syslog server.
Can KX III integrate with SNMP?	Yes. In addition to KX III's own internal logging capabilities, KX III can send SNMP traps to SNMP management systems. SNMP v2 and v3 are supported.
Can an administrator log-off a user?	Yes, administrators can view which users are logged into which ports and can log-off a user from a specific port or from the appliance if required.
Can KX III's internal clock be synchronized with a timeserver?	Yes. KX III 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).

Documentation and Support

Question	Answer
Is online help available?	Yes. Online help is available from the KX III user interface, and at raritan.com with the documentation. Online help includes KX III administration and end user information on using the Remote Console, Virtual KVM Client (VKC) Active KVM Client (AKC) and Local Console, as well KX III specifications, informational notes, using KX III with Paragon II, connecting KX III to the Cat5 Reach DVI, connecting KX III to the T1700-LED, and so on.
Where do I find documentation on the Dominion KX III?	The documentation is available at raritan.com. The documentation is listed by firmware release.

Question	Answer
What documentation is available?	A Quick Setup Guide, online help, a PDF version of the help in the form of an Administrators Guide and a Users Guide, as well as Release Notes and other information are available.
What CIM should I use for a particular server?	Consult the CIM Guide available with the KX III documentation. Note that DVI, HDMI and DisplayPort video standards are supported with the digital video CIMs.
How long is the hardware warranty for the KX III?	The Dominion KX III comes with a standard two-year warranty, which can be extended to 5 years of warranty coverage.

Miscellaneous

Question	Answer
What is Dominion KX III's default IP address?	192.168.0.192
What is Dominion KX III's default username and password?	The Dominion KX III's default username and password are admin/raritan. However, for the highest level of security, the Dominion KX III forces the administrator to change the Dominion KX III default administrative username and password when the appliance is first booted up. Username is not case sensitive.
I changed and subsequently forgot Dominion KX III's administrative password; can you retrieve it for me?	Dominion KX III contains a hardware reset button that can be used to factory reset the appliance, which will reset the administrative password on the appliance to the default password.
How do I migrate from the Dominion KX II to Dominion KX III?	In general, KX II customers can continue to use their existing switches for many years. As their data centers expand, customers can purchase and use the new KX III models. Raritan's centralized management appliance, CommandCenter Secure Gateway (CC-SG) Release 6.0 supports KX II and KX III switches seamlessly.
Will my existing KX II CIMs work with Dominion KX III switches?	Yes. Existing KX II CIMs will work with the Dominion KX III switch. In addition, select Paragon CIMs will work with the KX III. This provides an easy migration to KX III for Paragon II customers who wish to switch to KVM over IP. However, you may want to consider the D2CIM-VUSB and D2CIM-DVUSB CIMs that support virtual media, audio and Absolute Mouse Synchronization. Additionally, digital video CIMs supporting DVI, HDMI, and Display Port are also available.

Appendix A Third Party Licenses

Licenses - Ccid

OpenCT, a middleware framework for smart card terminals.

Copyright (c) 2003, Olaf Kirch <okir@suse.de>

Copyright (c) 2003, Andreas Jellinghaus <aj@dungeon.inka.de>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the authors nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FORANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - Clish

This package contains code which is copyrighted to multiple sources. The initial public release of this software was developed by Graeme McKerrell whilst in the employment of 3Com Europe Ltd.

Copyright (c) 2005, 3Com Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of 3Com Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Newport Networks Ltd.

The 0.6-0.7 releases of this software was developed by Graeme McKerrell whilst in the employment of Newport Networks Ltd.

As well as enhancing the existing code the following new modules were developed.

Copyright (c) 2005,2006, Newport Networks Ltd

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Newport Networks Ltd nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

tinyxml

Yves Berquin

As of release 0.6 the tinyxml library is included (unchanged) as part of the distribution.

tinyxml (v2.5.1)

http://www.sourceforge.net/projects/tinyxml

Original file by Yves Berquin.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

GNU binutils

As of release 0.7.1 libbfd can be used to resolve symbols forstacktraces. This feature can be turned off if linking with GPL code is problematic, using "configure --without-gpl".

The Binary File Descriptor library is part of GNU binutils

http://www.gnu.org/software/binutils/

The following file is licensed under the GPLv2.

This file is part of the CLISH project http://clish.sourceforge.net/

The code in this file is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2

This code is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Derived from addr2line.c in the GNU binutils package by Ulrich.Lauther@mchp.siemens.de

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Licenses - Dropbear

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2015 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

curve25519-donna:

/* Copyright 2008, Google Inc.

* All rights reserved.

*

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

*

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* curve25519-donna: Curve25519 elliptic curve, public key function

* http://code.google.com/p/curve25519-donna/

* Adam Langley <agl@imperialviolet.org>

* Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to>

* More information about curve25519 can be found here

* http://cr.yp.to/ecdh.html

* djb's sample implementation of curve25519 is written in a special assembly language called qhasm and uses the floating point registers.

* This is, almost, a clean room reimplementation from the curve25519 paper. It uses many of the tricks described therein. Only the crecip function is taken from the sample implementation.

Licenses - Iperf

iperf, Copyright (c) 2014-2017, The Regents of the University of California, through Lawrence Berkeley National Laboratory (subject to receipt of any required approvals from the U.S. Dept. of Energy). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/ or other materials provided with the distribution.

Neither the name of the University of California, Lawrence Berkeley National Laboratory, U.S. Dept. of Energy nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

You are under no obligation whatsoever to provide any bug fixes, patches, or upgrades to the features, functionality or performance of the source code ("Enhancements") to anyone; however, if you choose to make your Enhancements available either publicly, or directly to Lawrence Berkeley National Laboratory, without imposing a separate written license agreement for such Enhancements, then you hereby grant the following license: a non-exclusive, royalty-free perpetual license to install, use, modify, prepare derivative works, incorporate into other computer software, distribute, and sublicense such enhancements or derivative works thereof, in binary and source code form.

=====

This software contains source code (src/cjson.{c,h}) that is:

Copyright (c) 2009 Dave Gamble

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

This software contains source code (src/net.{c,h}) that is:

This software was developed as part of a project at MIT.

Copyright (c) 2005-2007 Russ Cox, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

Contains parts of an earlier library that has:

The authors of this software are Rob Pike, Sape Mullender, and Russ Cox

Copyright (c) 2003 by Lucent Technologies.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

=====

This software contains source code (src/net.c) that is:

Copyright (c) 2001 Eric Jackson <ericj@monkey.org>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This software contains source code (src/queue.h) that is:

Copyright (c) 1991, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

@(#)queue.h 8.5 (Berkeley) 8/20/94

=====

This software contains source code (src/units.{c.h}) that is:

Copyright (c) 1999,2000,2001,2002,2003

The Board of Trustees of the University of Illinois

All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software (Iperf) and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

Redistributions of source code must retain the above

copyright notice, this list of conditions and the following disclaimers.

Redistributions in binary form must reproduce the above

copyright notice, this list of conditions and the following disclaimers in the documentation and/or other materials provided with the distribution.

Neither the names of the University of Illinois, NCSA, nor the names of its contributors may be used to endorse or promote products derived from this Software without specific prior written permission.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE CONTIBUTORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

National Laboratory for Applied Network Research

National Center for Supercomputing Applications

University of Illinois at Urbana-Champaign

http://www.ncsa.uiuc.edu

stdio.c by Mark Gates <mgates@nlanr.net> and Ajay Tirumalla <tirumala@ncsa.uiuc.edu>

input and output numbers, converting with kilo, mega, giga

=====

This software contains source code (src/portable_endian.h) that is:

"License": Public Domain

I, Mathias Panzenböck, place this file hereby into the public domain. Use it at your own risk for whatever you like.

=====

Licenses - LIBXML2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Licenses - Net-SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2013, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 10: Lennart Poettering copyright notice (BSD-like) -----

Copyright 2010 Lennart Poettering

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Part 11: IETF copyright notice (BSD) -----

Copyright (c) 2013 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Internet Society, IETF or IETF Trust, nor the names of specific contributors, may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 12: Arista Networks copyright notice (BSD) ----

Copyright (c) 2013, Arista Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Arista Networks, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 13: VMware, Inc. copyright notice (BSD) -----

Copyright (c) 2016, VMware, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of VMware, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 14: USC/Information Sciences Institute copyright notice (BSD) -----

Copyright (c) 2017-2018, Information Sciences Institute

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Information Sciences Institue nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - Open LDAP

Copyright 1998-2019 The OpenLDAP Foundation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and/or subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>.

This work also contains materials derived from public sources. Additional information about OpenLDAP can be obtained at <http://www.openldap.org/>.

Portions Copyright 1998-2012 Kurt D. Zeilenga.

Portions Copyright 1998-2006 Net Boolean Incorporated.

Portions Copyright 2001-2006 IBM Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted only as authorized by the OpenLDAP

Public License.

Portions Copyright 1999-2008 Howard Y.H. Chu.

Portions Copyright 1999-2008 Symas Corporation.

Portions Copyright 1998-2003 Hallvard B. Furuseth.

Portions Copyright 2007-2011 Gavin Henry.

Portions Copyright 2007-2011 Suretec Systems Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided "as is'' without express or implied warranty.

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided ``as is'' without express or implied warranty.

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,

DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Licenses - OpenSSL

LICENSE ISSUES

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts.

OpenSSL License

Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young

(eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public License.]

Licenses - WPA Supplicant and Hostapd

Copyright (c) 2002-2019, Jouni Malinen <j@w1.fi> and contributors

All Rights Reserved.

These programs are licensed under the BSD license (the one with advertisement clause removed).

If you are submitting changes to the project, please see CONTRIBUTIONS file for more instructions.

This package may include either wpa_supplicant, hostapd, or both. See README file respective subdirectories (wpa_supplicant/README or hostapd/README) for more details.

Source code files were moved around in v0.6.x releases and compared to earlier releases, the programs are now built by first going to a subdirectory (wpa_supplicant or hostapd) and creating build configuration (.config) and running 'make' there (for Linux/BSD/cygwin builds).

License

This software may be distributed, used, and modified under the terms of BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index

A

About the Cat5 Reach DVI 159

Absolute Mouse Synchronization 55, 93

Access a Virtual Media Drive on a Client Computer 35

Access a Virtual Media Image File 36

Access and Display Favorites 146

Access Connection Properties 43

Accessing a Target Server 149

Active KVM Client (AKC) 75

Active System Partition 38

Active System Partitions 37

Add a Macro to the Toolbar 87

Add New Macro 86

Adding Attributes to the Class 165

Additional Security Warnings 18

Adjust Audio Settings 74

Adjust Full Screen Window Size to Target Resolution 61

Adjusting Capture and Playback Buffer Size (Audio Settings) 73

Adjusting Video Settings 52

AKC Download Server Certification Validation IPv6 Support Notes 198

AKC Supported Browsers 76

AKC Supported Microsoft .NET Framework 75

AKC Supported Operating Systems 75

Allow Cookies 76

Allow Pop-Ups 16

Audio 206

Audio in a Linux Environment 207

Audio in a Mac Environment 190

Audio in a Windows Environment 207

Audio Level 70, 189

Audio Menu 105

Audio Playback and Capture Issues 206

Audio Playback and Capture Recommendations and Requirements 70, 189

Audio Settings 106

Authentication When Accessing a Smart Card Reader 67

Auto Sense 96

Auto-Sense Video Settings 52

B

Bandwidth and KVM-over-IP Performance 214

Bandwidth Requirements 71, 190

Black Stripe/Bar(s) Displayed on the Local Port 202

Blade Chassis - Port Access Page 25

Blade Servers 219

Browser Notes 208

Browser Tips for HSC 125, 137

BSMI Certification 197

Build a New Macro 48

C

Calibrating Color 52

Cannot Connect to Drives from Linux Clients 199

Caret Symbol (Linux Clients Only) 203

CC-SG Notes 207

Certified Modems 191

Changing a Password 145

Changing a USB Profile when Using a Smart Card Reader 201

CIM Notes 198

CIMs Required for Virtual Media 33

Cisco ISE for RADIUS Users 168

Clear Video Settings Cache 52, 100

Client Launch Settings 61

Collect a Diagnostic Snapshot 64

Collecting a Diagnostic Snapshot of the Target 63

Color Calibration 97

Command Line Interface High-Level Commands 125

Command Line Interface Shortcuts 125

Computer Interface Modules (CIMs) 224

Conditions when Read/Write is Not Available 34

Configure DSAM Serial Ports 118

Configure Local Console Scan Settings 154
Configure Port Scan 63
Configuring Connection Properties 42
Configuring Port Scan Settings in VKC/VKCS and AKC 63
Connect 27
Connect Audio 105
Connect Cat5 Reach DVI and Cat5 Reach DVI 159
Connect Drive Permissions (Linux) 38
Connect Drive Permissions (Mac) 38
Connect DSAM 116
Connect Files and Folders 101
Connect ISO 103
Connect Key Examples 150
Connect to a Digital Audio Device 72
Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC) 76, 42
Connect to DSAM Serial Target via SSH 128
Connect to DSAM Serial Target with URL Direct Port Access 128
Connect to DSAM Serial Targets in Port Access Page 127
Connect to Virtual Media 67
Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality 159
Connecting and Disconnecting from a Digital Audio Device 72
Connecting to Multiple Targets from a Single Remote Client 71
Connection Info 81
Connection Information 45
Connection Properties 79
Construct Macro From Text 49
Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional) 21
Copy and Paste and Copy All 132
Creating a New Attribute 164
Cursor Shape 57

D

Default Connection Properties 79
Default Connection Property Settings - Optimized for Best Performance 43
Default Login - Change the Password 16
Delete a Macro 87
Dell Chassis Cable Lengths and Video Resolutions 187
Device certificate requirement for AKC 76
Digital Audio 69
Digital Audio VKC and AKC Icons 70
Digital CIM Established and Standard Modes 185
Digital CIM Established Modes 185
Digital CIM Standard Modes 185
Digital CIM Timing Modes 184
Dimensions and Physical Specifications 176
Disable 'Protected Mode' 76
Disconnect 28
Disconnect from an Audio Device 73
Disconnect from Virtual Media Drives 37
Disconnecting Mac and Linux Virtual Media USB Drives 199
Discovering Devices on the KX III Subnet 147
Discovering Devices on the Local Subnet 146
DKX3-808 Fast Switching 29
Documentation and Support 227
Dominion User Station 138
Drive Partitions 38, 38
DSAM LED Operation 116
Dual Mouse Modes 55
Dual Port Video Groups - Port Access Page 25
Dual Power Supplies 220
Dual Stack Login Performance Issues 198
DVI Compatibility Mode 186

E

Editing rciusergroup Attributes for User Members 166
Emulator 128
Enable Favorites 146
Enter Intelligent Mouse Mode 56
Ethernet and IP Networking 222

Events Captured in the Audit Log and Syslog 196
Example 1: Import the Certificate into the Browser 19
Example 2: Add the KX III to Trusted Sites and Import the Certificate 20
Export Macros 51
Extended Local Port 220

F

French Keyboard 203
Frequently Asked Questions 208
From LDAP/LDAPS 162
From Microsoft Active Directory 162
Front View 14
Full Screen Mode 66

G

General FAQs 208
General Settings 58
Get Started Using KX III 16

H

Hardware 12, 176
Help Choosing USB Profiles 200
HSC Functions 128
HTML KVM Client (HKC) 77
HTML Serial Console (HSC) Help 128

I

Import and Export Macros 89
Import Macros 50
Importing and Exporting Macros 50
Include KX III IP Address in 'Trusted Sites Zone' 76
Informational Notes 197
Install and Configure KX III 16
Install Certificate on Apple iOS Device 107
Installation 217
Installing a Certificate 19
Intelligent 93
Intelligent Mouse Mode 55
Intelligent Mouse Synchronization Conditions 56, 95
Intelligent Power Distribution Unit (PDU) Control 221
Introduction 12
IPv6 Networking 216

J

Java Not Loading Properly on Mac 197
Java Runtime Environment (JRE) Notes 197
Java Validation and Access Warning 17
JRE Requirements and Browser Considerations for Mac 195

K

Keyboard 47
Keyboard Access on Mobile 111
Keyboard and Mouse Menu 83
Keyboard Language Preference (Fedora Linux Clients) 204
Keyboard Layout 83
Keyboard Limitations 60
Keyboard Macros 48
Keyboard Notes 203
Known Issues for Macros 90
KVM Client Applications 15
KVM Client Launching 40
KVM Clients 40
KX III Device Photos and Features 12
KX III Interface and Navigation 24
KX III Local Console 149
KX III Local Console Factory Reset 157
KX III Local Console Interface 31
KX III Remote Console 141
KX III Remote Console Interface 24
KX III Supported Keyboard Languages 191
KX III Supported Local Port DVI Resolutions 179
KX III Virtual Media Prerequisites 32

L

Left Panel 29
Licenses - Ccid 229
Licenses - Clish 229
Licenses - Dropbear 233

Licenses - Iperf 234
Licenses - LIBXML2 237
Licenses - Net-SNMP 237
Licenses - Open LDAP 242
Licenses - OpenSSL 243
Licenses - WPA Supplicant and Hostapd 244
Limitations on Apple iOS Devices 113
Local Console Smart Card Access 154
Local Console USB Profile Options 157
Local Console Video Resolution Behavior 149
Local Port - KX III 218
Local Port Auto-Sense (Video Refresh) - Default Hot Key 150
Local Port Consolidation, Tiering and Cascading 223
Local Port Hot Keys and Connect Keys 150
Local Port Requirements 187
Logging In to KX III 23

M

Mac Keyboard Keys Not Supported for Remote Access 205
Mac Mini BIOS Keystroke Commands 192
Macro Editor 84
Macros Not Saving on Linux Targets 205
Manage HKC iOS Client Keyboard Macros 111
Manageability 227
Managing Favorites 145
Mapped Drives 37
Miscellaneous 228
Mount a Smart Card Reader 68
Mounting CD-ROM/DVD-ROM/ISO Images 36
Mouse Modes 92
Mouse Notes 206
Mouse Options 54
Mouse Pointer Synchronization (Fedora) 206
Mouse Sync 94
Mouse Sync Issues in Mac OS 206
Mouse Synchronization Tips 57
Moving Between Ports on a Device 207
Multi-Language Keyboard JRE Requirement 196

N

Network Speed Settings 186
Noise Filter 45, 81
Number of Supported Audio/Virtual Media and Smartcard Connections 190
Number of Supported Virtual Media Drives 34
Numeric Keypad 203

O

Online Help 15
Operating System Audio Playback Support 72
Operating the User Station 139
Optimize for: Selections 41
Overview 75, 138, 141, 197, 32

P

Package Contents 12
PC Share Mode and Privacy Settings when Using Smart Cards 68
Photos 14
Port Access Page (Remote Console Display) 24
Port Action Menu 27
Power Control Menu 107
Power Control Using VKC, VKCS, and AKC 74
Power Cycle 29
Power Cycle a Target 136
Power Off 29
Power Off a Target 136
Power On 28
Power on a Target 135
Power Status 134
Powerstrip is not detected 198
Prerequisites for Using AKC 76
Prerequisites for Using Virtual Media 32

R

Recommendations for Audio Connections when PC Share Mode is Enabled 70, 190
Recommended Minimum Active KVM Client (AKC) Requirements 75
Recommended Minimum Virtual KVM Client (VKC) Requirements 41
Refresh Screen 95

Refreshing the Screen 51
Remote Access 209
Remote Client Requirements 188
Remote Linux Client Requirements 188
Remote PC VM Prerequisites 33
Remote/Local Console Interfaces and User Station 14
Resetting the KX III Using the Reset Button 157
Resolving Issues with Firefox Freezing when Using Fedora 208
Return to the Local Console from a Target Device - Default Hot Key 150
Returning User Group Information 161
Root User Permission Requirement 38

S

Saving Audio Settings 71
Scale Video 66
Scan for Targets 144
Scan for Targets - Local Console 154
Scanning Port Slide Show - Local Console 152
Scanning Ports - Local Console 152
Scanning Ports - Remote Console 141
Scanning Ports Slide Show - Remote Console 141
Screenshot 96
Screenshot from Target Command (Target Screenshot) 54
Security 225
Security Warnings and Validation Messages 16
Send Ctrl+Alt+Del Macro 47
Send LeftAlt+Tab (Switch Between Open Windows on a Target Server) 48
Send Macro 83
Send Smart Card Remove and Reinsert Notifications 69
Send Text File 133
Send Text to Target 48, 92
Serial Access With Dominion Serial Access Module 115
Serial Port Keyword List 121
Servers 216
Set Scan Tab 27
Setting CIM Keyboard/Mouse Options 48
Setting the Registry to Permit Write Operations to the Schema 162
Settings to Configure on Cisco ISE 170
Settings to Configure on Raritan Product 169
Simultaneous Users 150
Single 94
Single Mouse Mode 58
Single Mouse Mode when Connecting to a Target Under CC-SG Control 206
Smart Card Connections to Fedora Servers 207
Smart Card Minimum System Requirements 187
Smart Card Minimum System Requirements, CIMs and Supported/Unsupported Smart Card Readers 67
Smart Card Notes 207
Smart Card Reader Detected 68
Smart Cards 67
Smart Cards and CAC Authentication 226
Software 13, 194
Special Sun Key Combinations 151
Specifications 176
Standard 93
Standard Mouse Mode 56
Step 1: Add Raritan Network Devices 170
Step 2: Create/Edit User 171
Step 3: Configure Allowed Authentication Protocol Service (PAP/CHAP/MS-CHAP) 172
Step 4: Create Authorization Profile 173
Step 5: Configure/Create Authorization Policy 175
Sun Composite Synch Video 202
Supported CLI Commands 121
Supported Computer Interface Module (CIMs) Specifications 181
Supported Digital Video CIMs for Mac 184
Supported Escape Key Characters 125
Supported Number of Ports and Remote Users per Model 14
Supported Operating Systems, Browsers and Java Versions 194
Supported Paragon II CIMS and Configurations
Supported Remote Connections 186
Supported Smart Card Readers 188
Supported Target Server Video Resolutions 178

Supported Tasks Via Virtual Media 33
Supported USB Device Combinations 117
Supported Virtual Media Operating Systems 34
Supported Virtual Media Types 34
SUSE/VESA Video Modes 202
Switch From 27
Synchronize Your Mouse 57

T

Target BIOS Boot Time with Virtual Media 200
Target Server Requirements 187
Target Server Video Resolution - Supported Connection Distances and Refresh Rates 180
Target Server VM Prerequisites 33
Target Status Indicators During Port Scanning - Local Console 154
Target Status Indicators During Port Scanning - Remote Console 142
Target Video Picture Not Centered (Mouse Out of Synch) 198
TCP and UDP Ports Used 193
Text to macro 90
Third Party Licenses 229
Tiered Devices - Port Access Page 25
Tilde Symbol 204
Tool Options 58
Tools Menu 111
Tools: Start and Stop Logging 134
Touch Mouse Functions 110
Troubleshooting Tips 176

U

Universal Virtual Media 212
Unmount (Remove) a Smart Card Reader 69
Unsupported Smart Card Readers 189
Update a Smart Card Reader 69
Updating the LDAP Schema 161
Updating the Schema Cache 166
Upgrade DSAM Firmware 121
USB Port and Profile Notes 200
USB Profile 82
USB Profiles 46
User Station Photo and Features 138
Using a Smart Card at the Local Port 156
Using a Windows Keyboard to Access Mac Targets 193
Using HKC on Apple iOS Devices 107
Using Scan Port Options 143

V

Version Information 74
Video Image Appears Dark when Using a Mac 201
Video Menu 95
Video Mode 44, 80
Video Mode and Resolution Notes 201
Video Properties 51
Video Settings 97
Video Shrinks after Adjusting Target Clock 202
View by Group Tab 26
View by Search Tab 26
View by Serial Tab 26
View DSAM Serial Ports 117
View Menu 100
View Options 64
View Status Bar 65
View Toolbar 64
Virtual KVM Client (VKC and VKCs) Help 41
Virtual KVM Client Java Requirements 41
Virtual KVM Client Version Not Known from CC-SG Proxy Mode 207
Virtual Media 32, 35
Virtual Media Connection Failures Using High Speed for Virtual Media Connections 200
Virtual Media File Server Setup (File Server ISO Images Only) 39
Virtual Media in a Linux Environment 37
Virtual Media in a Mac Environment 38
Virtual Media Linux Drive Listed Twice 199
Virtual Media Menu 101
Virtual Media Not Refreshed After Files Added 199
Virtual Media Notes 199
Virtual Media via VKC and AKC in a Windows Environment 199
VM-CIMs and DL360 USB Ports 200

W

What's new in the KX III User Guide 11
Windows 3-Button Mouse on Linux Targets 198