Dominion KX3G2 User Guide

DKX3G2-A1-v4.0
March 2025
Release 4.0.0

Contents

Raritan.
A brand of legrand

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.

Raritan
A brand of legrand

Safety

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances. See Specifications in User Guide.
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, such as power strips (other than direct connections), to the branch circuit.

Welcome

The second-generation Dominion KXIII is an enterprise-class, secure, KVM-over-IP switch that provides multiple users with remote BIOS-level control of 8 to 64 servers. DKX3G2 comes with standard features such as DVI/HDMI/DisplayPort digital and analog video, audio, virtual media, smart card/CAC, and mobile access. Deploy DKX3G2 individually, or with Raritan's Command Center Secure Gateway (CC-SG).

Features of DKX3G2:

- HDMI display support for local ports
- It supports 32:9 Video Switch
- It contains 2GB DDR3 RAM to provide faster data processing capability

Introduction

The <ProdcutName> 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, and smart card/CAC.

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

In This Chapter

Package Contents

Each DKX3G2 ships as a fully-configured stand-alone product in a standard 1U or 2U form with 19" rackmount chassis.

- 1 - DKX3G2 device
- 1 - Rackmount kit
- 2 - AC power cords
- 1 - Set of 4 rubber feet (for desktop use)

Device Photos and Features

Hardware

- Integrated KVM-over-IP remote access
- 1U or 2U rack-mountable (brackets included)
- One M5 grounding screw on the back panel
- Dual power supplies with failover; autoswitching power supply with power failure warning
- Supported 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
- DCIM-USBG2

- Required for PS2:
  - DCIM-PS2
- HDMI monitor support from the HDMI local port
- Remote access and power management from an iPhone® or iPad®
- 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
  - 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
- Centralized access security
- Integrated power control
- Power LED with dual color LED bar with RED and WHITE
- LED indicators for dual power status, network activity, and remote user status
- Hardware Reset button
- Front panel StatusLED turns green when DKX3G2 boots up successfully and available to use
- Front panel Status LED turns blue when DKX3G2 firmware upgrades
- Front panel Status LED turns blue when DKX3G2 firmware upgrade happens via USB stick
- Front panel Status LED blinks blue when DKX3G2 firmware upgrade completes via USB stick but pending reboot

Supported Number of Ports and Remote Users per Model

Model	Ports	Remote users
DKX3-816	16	8
DKX3-864	64	8
DKX3-832	32	8
DKX3-808	8	8
DKX3-464	64	4
DKX3-432	32	4
DKX3-416	16	4
DKX3-232	32	2
DKX3-216	16	2

Model	Ports	Remote users
DKX3-132	32	1
DKX3-116	16	1
DKX3-108	8	1

Software

- Virtual media support in Windows®, Mac® and Linux® environments*
- Absolute Mouse Synchronization*

---

*Note: Virtual media and Absolute Mouse Synchronization require use of virtual CIMS. See: Hardware (on page 10)

- 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 and ServerTech Pro4x
- Support for remote IP access from the new <ProdcutName> User Station
- Support for access to serial targets using the Dominion Serial Access Module (DSAM)

Photos

Front View

Rear View - Features

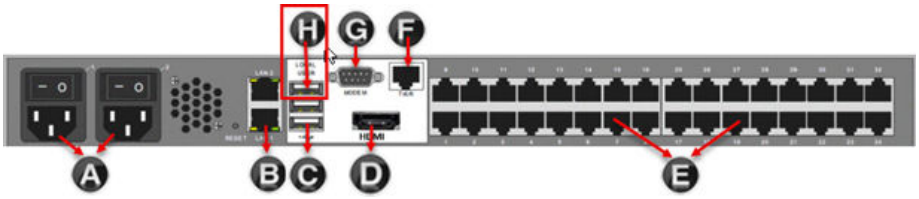


Diagram key	
A	Dual Power AC 100V/240V
B	Dual 10/100/1000 Ethernet access
C	Local USB ports
D	HDMI port
E	KVM ports for UTP Cabling (Cat5/5e/6)
F	Tier port for tiering devices
G	Serial Admin Port
H	Dominion Serial Access Module USB port (optional)

Remote/Local Console Interfaces and User Station

Use the Remote Console interface to configure and manage the DKX3G2 over a network connection.

Use the Local Console interface to access the DKX3G2 while at the rack.

See: DKX3G2 Remote Console Interface (on page 116), DKX3G2 Local Console Interface respectively.

The Dominion User Station provides an alternative interface for IP access to the DKX3G2's target servers. See: Dominion User Station.

KVM Client Applications

DKX3G2 works with -

- Active KVM Client (AKC) - Default client, Windows only. Microsoft .NET® 4.5 or above, Microsoft Edge WebView2 required to use DKX3G2 with the Microsoft Windows®-based Active KVM Client (AKC). See Active KVM Client (AKC)
- Virtual KVM Client (VKC) -Java™1.8 is required to use the Java-based Virtual KVM Client (VKC). See Virtual KVM Client (VKC) Help
- HTML KVM Client (HKC) - Runs on Linux, Mac, and Windows without .Net. Supports Edge, Firefox, Chrome and Safari browsers. See HTML KVM Client (HKC) Help.

Online Help

DKX3G2 online help is considered your primary help resource.

KVM Client help is provided as part of DKX3G2 online help.

Online help is accompanied by the DKX3G2 Quick Setup Guide, which is included with your DKX3G2 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 DKX3G2 administrator help sections.

See the DKX3G2 Release Notes for important information on the current release before you begin using the DKX3G2.

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

Get Started

This section walks you through high-level tasks to start using DKX3G2.

In This Chapter

Initial Configuration

Equipment Setup

Rack Mounting

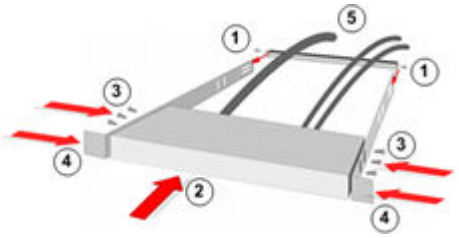
The DKX3G2 can be mounted in 1U (1.75", 4.4 cm) of vertical space in a standard 19" rack.

Note: Diagram may not depict your exact device. The mounting instructions are specific to your device.

► *To configure forward mount:*

The steps correspond to the numbers shown in the front rackmount diagrams.

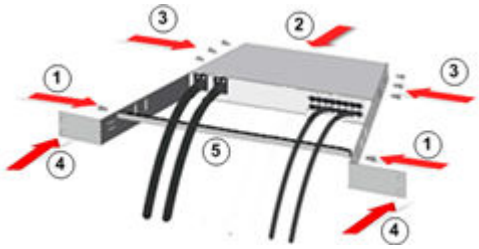
1. Secure the cable-support bar to the back end of the side brackets using two of the included screws.
2. Slide the DKX3G2 between the side brackets, with its rear panel facing the cable-support bar, until its front panel is flush with the “ears” of the side brackets.
3. Secure the DKX3G2 to the side brackets using the remaining included screws (three on each side).
4. Mount the entire assembly in your rack, and secure the side brackets' ears to the rack's front rails with your own screws, bolts, cage nuts, and so on.
5. When connecting cables to the rear panel, drape them over the cable-support bar.



► *To configure rear mount:*

The steps correspond to the numbers shown in the rear rackmount diagrams.

1. Secure the cable-support bar to the front end of the side brackets, near the side brackets' “ears,” using two of the included screws.
2. Slide the DKX3G2 between the side brackets, with its rear panel facing the cable-support bar, until its front panel is flush with the back edges of the side brackets.
3. Secure the DKX3G2 to the side brackets using the remaining included screws (three on each side).
4. Mount the entire assembly in your rack and secure the side brackets' ears to the rack's front rails with your own screws, bolts, cage nuts, and so on.
5. When connecting cables to the rear panel, drape them over the cable-support bar.



Connecting the Equipment

AC Power:

Use the power cords that came with DKX3G2. Use both cords with AC power outlets for dual-power failover protection.

Network Ports:

Connect a standard Ethernet cable from the LAN1 network port to an Ethernet switch, hub, or router.

To enable the failover or isolation mode capabilities, connect a standard Ethernet cable from the LAN2 network port to an Ethernet switch, hub, or router.

USB Ports:

Connect a USB keyboard and mouse to the respective Local User port on the back of DKX3G2.

The Local User port provides direct access for initial network configuration and target connections. After network setup, all further configuration can be performed from remote logins to the device

If you're also using Dominion Serial Access Modules (DSAM), reserve the top USB port on the rear of the unit for connecting DSAM.

HDMI Port:

HDMI cable is used to connect to a local monitor.

Target servers:

Connect the keyboard, mouse and video plugs on the CIM to the corresponding ports on the target server.

Connect the CIM to an available target server port on the back of the DKX3G2 via a Cat5/5e/6 cable.

Dominion Serial Access Module (DSAM):

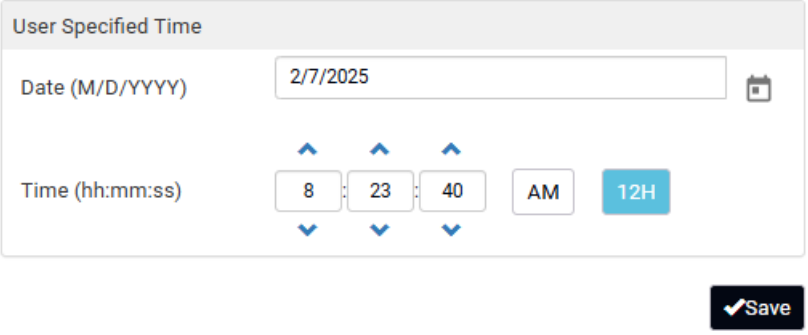
Connecting a DKX3G2 and a Dominion Serial Access Module (DSAM) provides access to devices such as LAN switches and routers that have a RS-232 serial port.

1. Connect the DSAM unit's USB cable to the top USB port on the rear of the KX III device. Connect additional DSAM units to any other USB port.
2. Connect the serial devices to the serial ports on the DSAM unit.

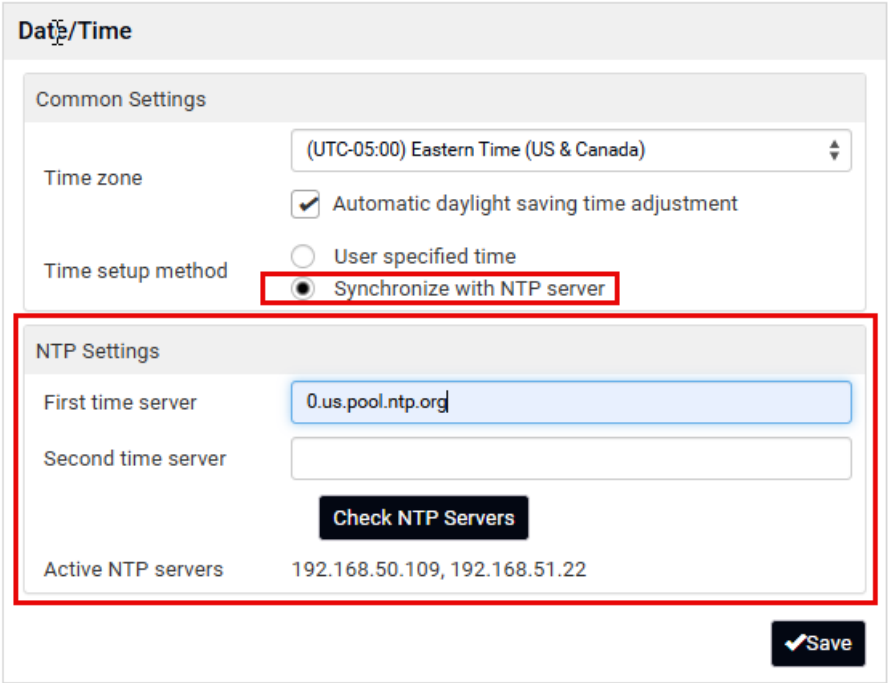
Configure Date/Time Settings

There are two ways to do this:

- Manually set the date and time.



- Synchronize the date and time with a Network Time Protocol (NTP) server.



Note: NTP security is added to the DKX3G2, which allows it to request the date and time with or without authentication. If the NTP server is configured to use authentication, it will accept the request along with the authentication key, and send back the date and time along with digital information of the authentication key. The DKX3G2 will verify the digital information and will use the date and time if the key matches; otherwise discard the received information.

► *To configure date/time settings:*

1. Choose Device Settings > Date/Time to open the Date/Time Settings page.
2. Choose your time zone from the Time Zone drop-down list.
3. Adjust for daylight savings time by checking the "Adjust for daylight savings time" checkbox.
4. Choose the method to use to set the date and time:
   - User Specified Time - use this option to input the date and time manually. For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).
   - Synchronize with NTP Server - use this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
5. For the Synchronize with NTP Server option:
   - Enter the IP address of the Primary Time server, Authentication Type, ID, key Format and key value.
   - Enter the IP address of the Secondary Time server, Authentication Type, ID, key Format and key value Optional

Note: If DHCP is selected for the Network Settings on the Network page, the NTP server IP address is automatically retrieved from the DHCP server by default. Manually enter the NTP server IP address by selecting the Override DHCP checkbox.

6. Click OK.

Create and Install an SSL Certificate

It is strongly recommended to install your own SSL Certificate in each DKX3G2 device. This security best practice reduces the number of browser and Java™ warning messages, and avoids man-in-the-middle attacks. It also prevents future Java versions and browser versions from blocking access to your DKX3G2 device.

For information on creating and installing SSL certificates, see DKX3G2 Online Help.

Configuring the DKX3G2

You are forced to change the password at first login to a strong password as you connect via local port. After the password update you assign its IP address.

The DKX3G2 device is shipped with the following default settings.

Default login:

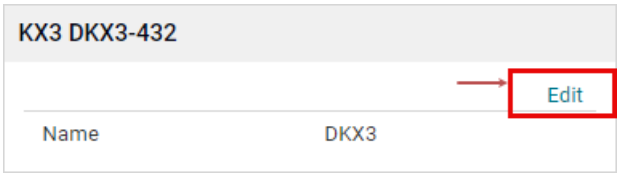
- Username = `admin`
- Password = `raritan`
- IP address = DHCP

All other steps can be performed either from the Local Console, or the via Remote Console in a web browser using the DKX3G2's IP address.

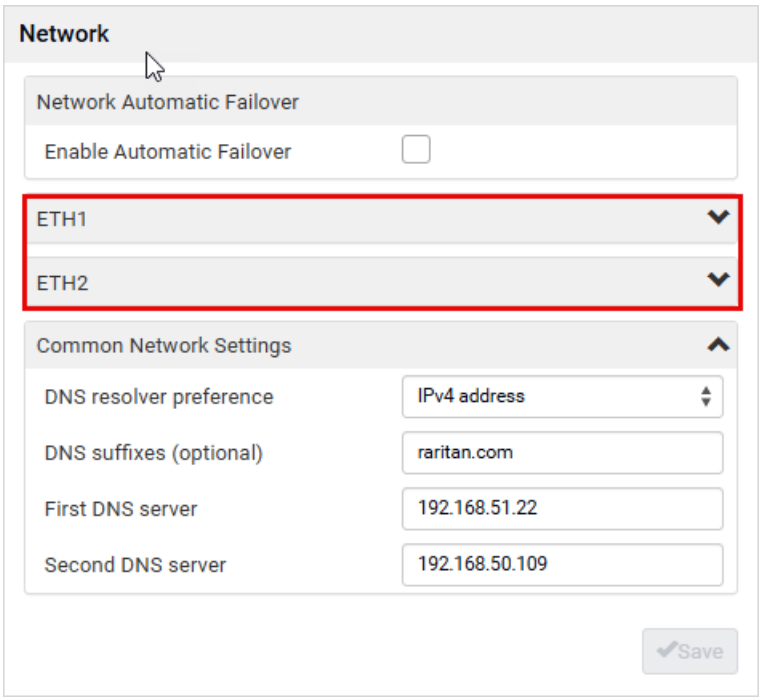
Important: For backup and business continuity purposes, it is strongly recommended you create a backup administrator username and password, and keep that information in a secure location.

► *To configure device name:*

1. Connect remotely to the DKX3G2 via it's IP address.
2. Log in with newly set password.
3. Choose Device Information and click on Edit.



4. Specify a meaningful Device Name for your DKX3G2 device.
   - Up to 32 alphanumeric and valid special characters, no spaces between characters.
5. Next, configure the IP address and DNS settings on Network.



Configuring Network Firewall Settings

TCP Port 5000:

Enable remote access to DKX3G2 by allowing network and firewall communication on TCP Port 5000.

TCP Port 443:

- Allow access to TCP Port 443 (Standard HTTPS) so you can access DKX3G2 via a web browser.

TCP Port 80:

Allow access to TCP Port 80 (Standard HTTP) to enable automatic redirection of HTTP requests to HTTPS.

Configuring KVM Target Servers

Absolute mouse mode:

Absolute mouse mode is recommended to minimize mouse settings on target servers.

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.

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

Target Server Video Resolutions:

See: Supported Target Server Video Resolutions (on page 311) in Online Help.

Choose Failover or Isolation Mode

Configure DKX3G2 for Dual LAN Failover Mode: In failover mode, LAN status is used to determine which LAN port is used in failover. LAN port #1 is switched as default. If the switched LAN port status is down, then the other LAN port will be switched to until a LAN port whose status is on is found.

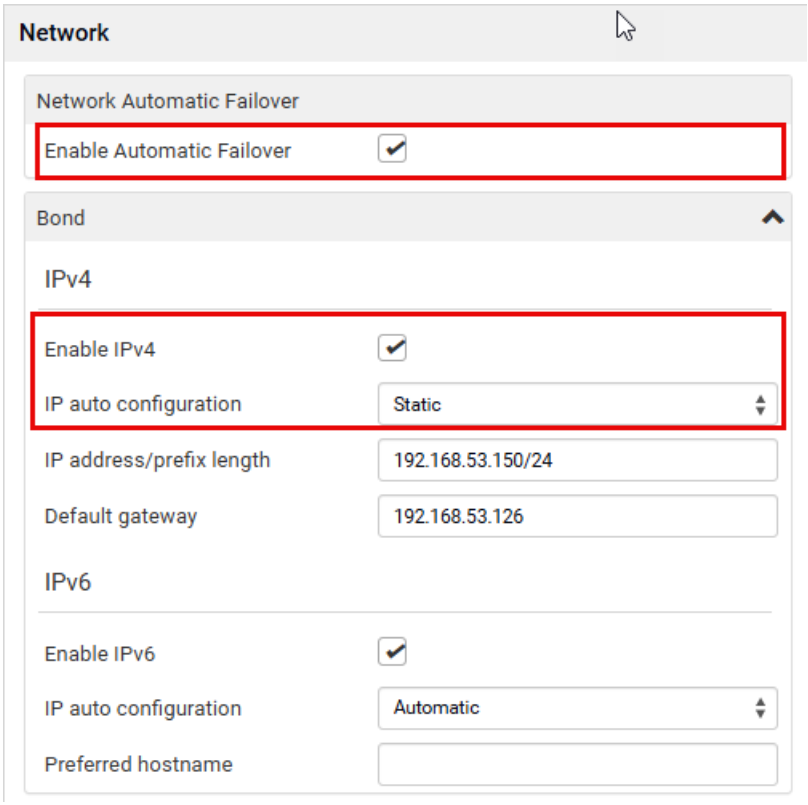
Configure DKX3G2 for Dual LAN Isolation Mode: In isolation mode the two LAN ports are configured with different IP addresses. They can be in the same or different subnets. Once <ProdcutName>is isolation mode failover can not be configured.

Configure DKX3G2 for Dual LAN Failover Mode

LAN1 and LAN2 share the same IP address or different IP addresss within the same subnet to support automatic failover.

LAN1 is the primary port. If LAN1 fails, LAN2 is used to access DKX3G2.

1. Select Device Settings > Network to open the Device Network Settings page.
2. Select the "Enable Automatic Failover" to enable failover.
3. Expand Bond section, which has IPV4 and IPV6 setup. By default Enable IPV4 and Enable IPV6 are checked.
4. Set the IP Auto Configuration to Static in the IPv4 section.
5. Manually specify the network parameters by entering the Default Gateway.
6. Enter the IPv4 IP Address/Prefix.
7. Click Save and Apply Settings.
8. The LAN1 settings are applied to LAN2 if failover occurs.
9. Repeat steps 4 to 7 for IPV6 setup or disable by unchecking "Enable IPV6" checkbox.



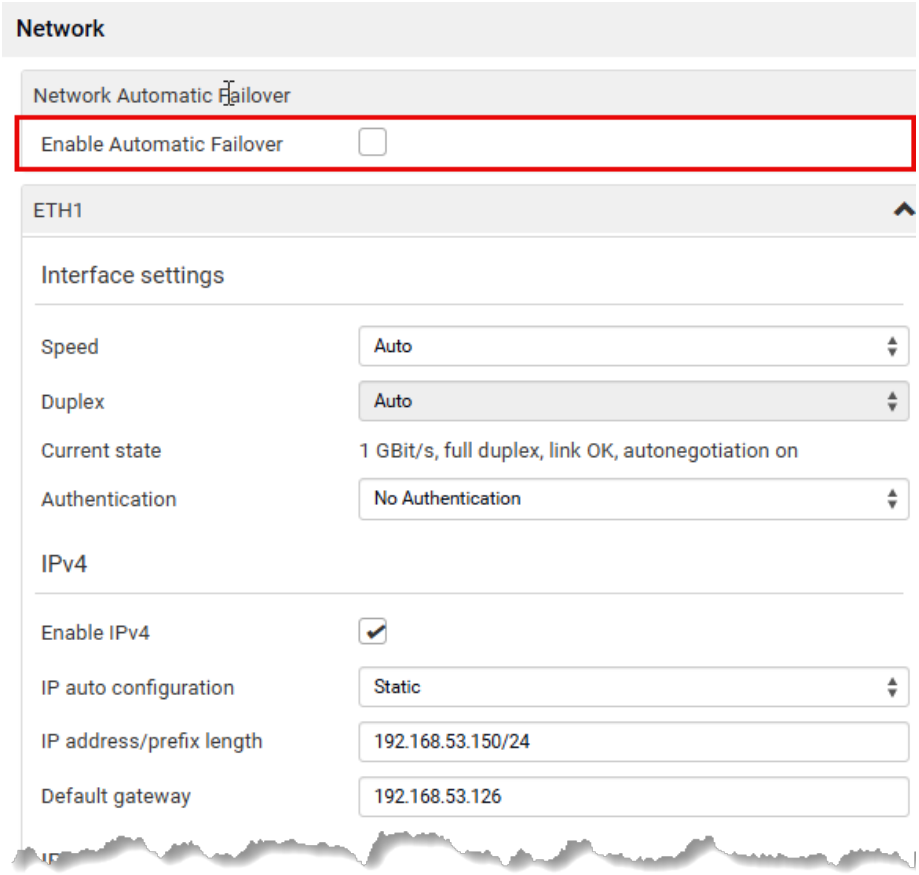
Configure DKX3G2 for Dual LAN Isolation Mode

Isolation mode allows you to access each LAN port independently using different IP addresses.

Note: Failover is not supported in this mode.

---

1. Select Device Settings > Network to open the Device Network Settings page.
2. Ensure the "Enable Automatic Failover" checkbox is not selected.
3. Set the IP Auto Configuration to Static in the IPv4 section.



4. If needed, manually specify the network parameters by entering the Default Gateway and then complete the steps that follow.
5. Enter the IP address you want to use to connect to the DKX3G2 LAN1.
6. Enter the LAN2 IPv4 Default Gateway.
7. In the LAN2 IPv4 section, set the IP Auto Configuration to Static.
8. Enter the IP address you want to use to connect to the DKX3G2 LAN2.
9. Enter the LAN2 IPv4 Default Gateway.
10. Complete the IPv6 sections, if applicable.
11. Select the IP Auto Configuration.

If Static is selected, you must manually specify -

- Global/Unique IP Address - this is the IP address assigned to DKX3G2.
- Prefix Length - this is the number of bits used in the IPv6 address.
- Gateway IP Address.

Select *Router Discovery* to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

Note that the following additional, read-only information appears in this section -

- Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.
- Zone ID - Identifies the device the address is associated with. Read-Only

12. Select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary address is used if the primary DNS server connection is lost due to an outage.

Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when DKX3G2 is configured in DHCP mode

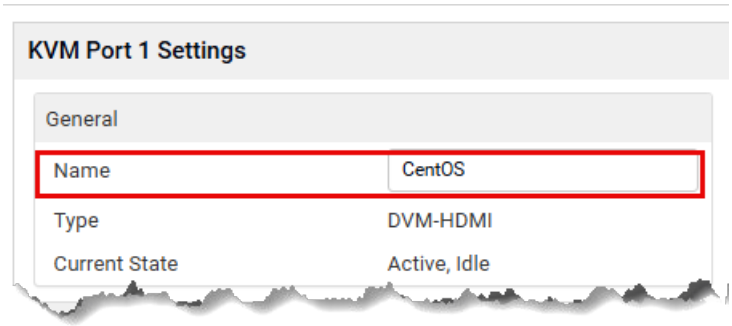
---

13. Set the LAN 1/LAN 2 Interface Speed and Duplex, and the LAN 1/LAN 2 MTU.
    - Valid range for MTU is 576 - 1500.
14. When finished, click OK.

Your DKX3G2 device is now accessible via the LAN1 IP address and the LAN2 IP address.

Name Your Target Servers

1. Connect all of the target servers if you have not already done so.
2. Select KVM Ports > then click the settings of Port of the target servers named after remote login.



3. Enter a name for the server up to 32 alphanumeric and special characters. Click OK.

Power Supply Autodetection

DKX3G2 provides dual power supplies.

When both power supplies are connected, and Power Supply Auto Detection is remotely configured:

- DKX3G2 automatically detects both power supplies.
- DKX3G2 notifies you about their status.
- On the Power Supply Setup page the Powerln1 Auto Detect and Powerln2 Auto Detect checkboxes are automatically selected.

If you are using only one power supply, you can enable automatic detection for only the power supply in use.

When only one power input is connected, the Power LED on the front of the DKX3G2 device is Red when the checkbox is selected for an unconnected power supply, and Blue when the checkbox is not selected for an unconnected power supply.

► *To enable automatic detection for the power supply in use:*

1. Select Device Settings > Power Supply Setup.
   - Select the PowerIn1 Auto Detect option if you are plugging power input into power supply number one.

     (The left-most power supply at the back of the device when you are facing rear of the device.)

Or

   - Select the PowerIn2 Auto Detect option if you are plugging power input into power supply number two.

     (The right-most power supply at the back of the device when you are facing rear of the device.)
2. Click OK.

Rear View - Features

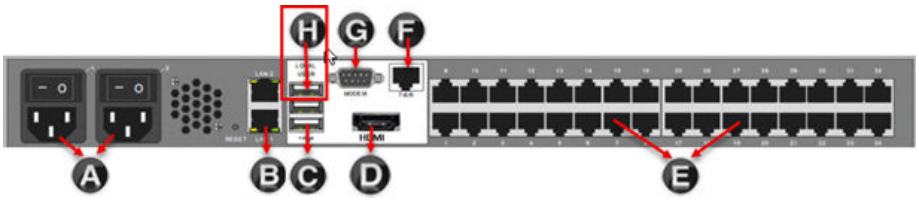


Diagram key	
A	Dual Power AC 100V/240V
B	Dual 10/100/1000 Ethernet access
C	Local USB ports
D	HDMI port
E	KVM ports for UTP Cabling (Cat5/5e/6)

Diagram key	
F	Tier port for tiering devices
G	Serial Admin Port
H	Dominion Serial Access Module USB port (optional)

Default Login - Change the Password

The DKX3G2 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 = DHCP

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 DKX3G2 Remote Console.

Security Warnings and Validation Messages

When logging in to DKX3G2, 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 26)
- If you choose to use the Virtual KVM Client (VKC/VKCS), you may see Java™ security warnings and requests to validate DKX3G2.
  See: Java Validation and Access Warning (on page 27) and Installing a Certificate (on page 27).

Note! Use the HTML KVM Client (HKC) instead to avoid Java. The HKC is Java-Free. See: KVM Client Launching (on page 42).

Additional Security Warnings

Even after an SSL certificate is installed in the DKX3G2, depending on your browser and security settings, additional security warnings may be displayed when you log in to DKX3G2.

It is necessary to accept these warnings to launch the DKX3G2 Remote Console.

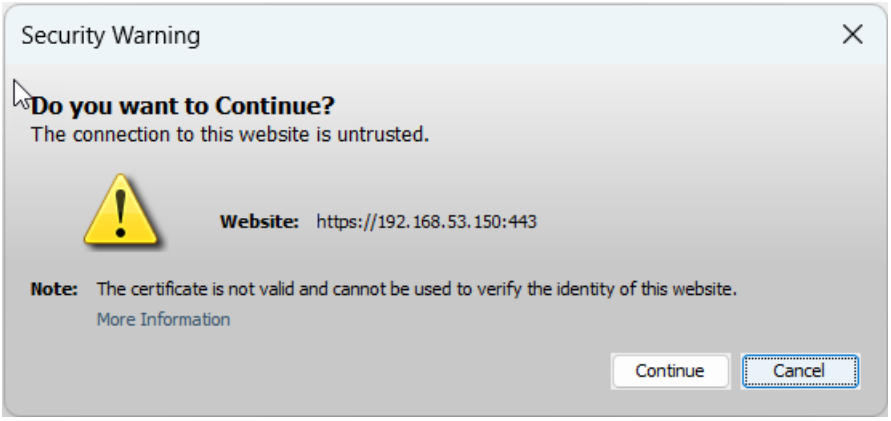
Reduce the number of warning messages during subsequent log ins by checking the following options on the security and certificate warning messages:

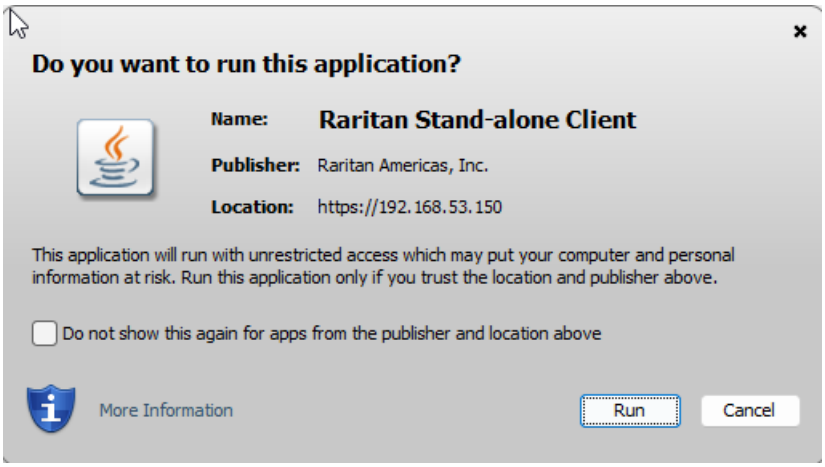
- In the future, do not show this warning
- Always trust content from this publisher

Java Validation and Access Warning

When logging in to DKX3G2 using the Java-based client, Java prompts you to validate DKX3G2, and to allow access to the application.

Installing an SSL certificate in each DKX3G2 device is recommended to reduce Java warnings, and enhance security. See SSL Certificates





Installing a Certificate

You may be prompted by the browser to accept and validate the DKX3G2's SSL certificate.

Depending on your browser and security settings, additional security warnings may be displayed when you log in to DKX3G2.

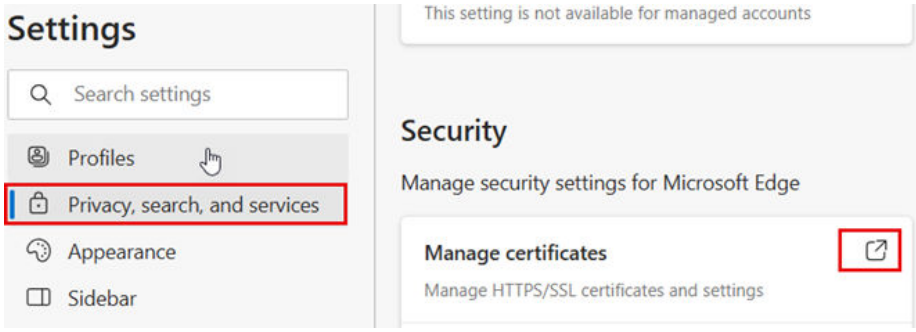
It is necessary to accept these warnings to launch the DKX3G2 Remote Console. For more information, see Security Warnings and Validation Messages.

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.

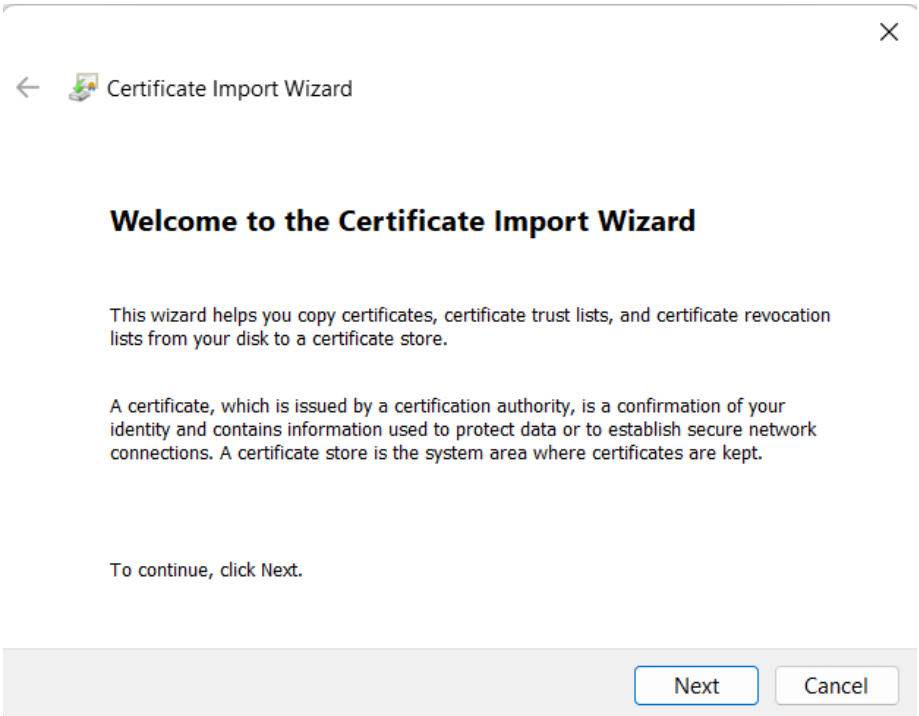
Example 1: Import the Certificate into the Browser

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

1. Open Microsoft Edge browser, then log in to DKX3G2.
2. Click on the dots in the top right corner > Go the Settings
3. Now click on the Privacy, search and services on the left-hand side menu
4. Scroll down until you find Security then click on Manage certificates
5. Click on Import.



6. The Certificate Import Wizard opens and walks you through each step.
7. File to Import - Browse to locate the Certificate



8. Certificate Store - Select the location to store the Certificate
9. Click Finish on the last step of the Wizard.
10. The Certificate is imported. Close the success message.
11. Click OK to apply the changes, then close and reopen the browser.

Example 2: Add the DKX3G2 to Trusted Sites and Import the Certificate

In this example, the DKX3G2's URL is added as a Trusted Site, and the Self Signed Certificate is added as part of the process.

1. Open Control Panel, then launch the Internet Options. Internet Properties window opens up.
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 DKX3G2 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 Control Panel, then laun ,ch the Internet Options. Internet Properties window opens up.
2. Click the Content tab.
3. Click Certificates.
4. Select the certificate>click View
5. Click Certificate Details for more information. You are prompted to install the certificate. Follow the wizard steps.

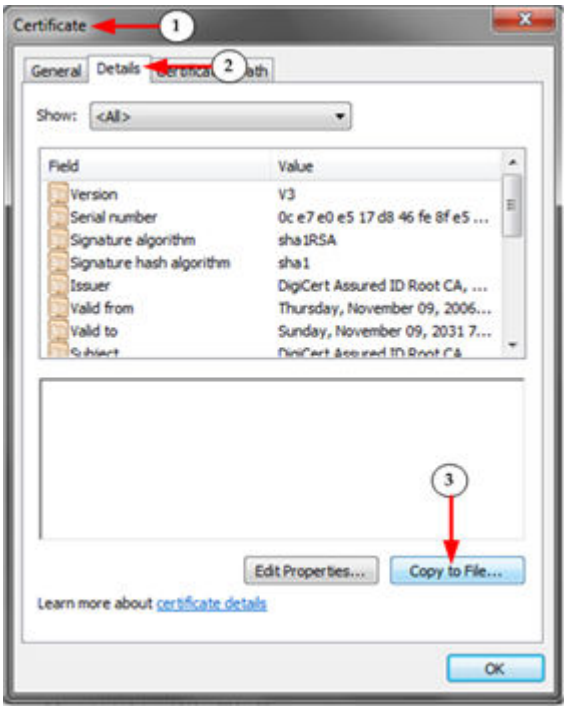
For details see, Example 1: Import the Certificate into the Browser.

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

DKX3G2 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.

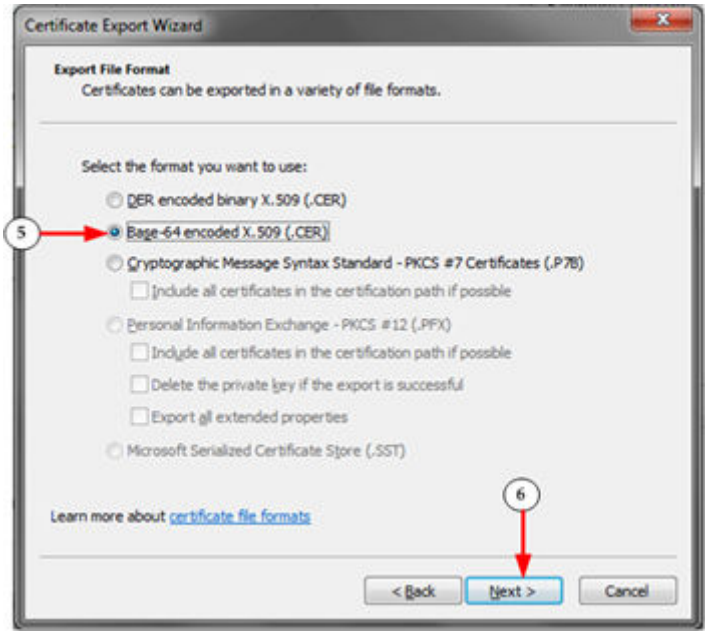


1. Locate the DEGHKVM0001.cer binary file on your Windows machine.

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 DKX3G2.

Logging In to DKX3G2

Log in to your DKX3G2 Remote Console from any workstation with network connectivity. See the Release Notes for supported browser versions.

Logging in and using DKX3G2 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.

1. To log in via Remote Console:
2. Launch a supported web browser, and enter the IP address assigned to the DKX3G2.
3. A default client is launched based on your PC and browser settings. See KVM Client. You can also choose a client by entering the URL directly. See KVM Client Launching.
4. Enter your username and password, then click Login.
5. Accept the user agreement (if applicable). If security warnings appear, click to accept.

Virtual Media

In This Chapter

Overview

All DKX3G2 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 DKX3G2 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

DKX3G2 Virtual Media Prerequisites

- For users requiring access to virtual media, the DKX3G2 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, Virtual Media Share must also be enabled in the KVM 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.

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.

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 is to use virtual media:

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

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.

Mounting Local Drives

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

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

Note: Some browsers may restrict access to local drives, folders or files and may not grant administrative permission.

Supported Virtual Media Types

The following virtual media types are supported for Windows®, Mac® and Linux™ clients when using AKC and VKC/VKCS.

- Internal and external hard drives
- Internal and USB-mounted CD and DVD drives
- USB mass storage devices
- ISO images (disk images)
- IMG files
- DMG files
- ISO9660 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

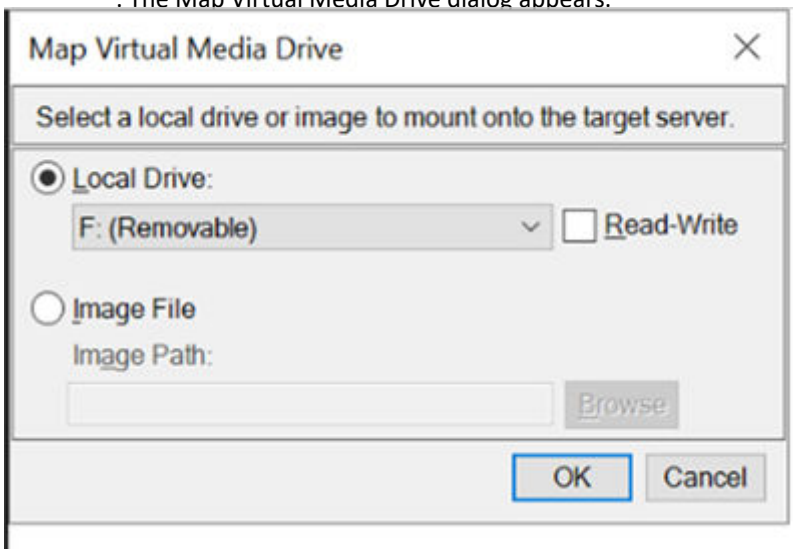
Virtual Media

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

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

1. From the KVM client, choose Virtual Media > Connect CD-ROM/ISO Image, or click the Connect CD ROM/ISO button  . The Map Virtual Media CD/ISO Image dialog appears.
2. For internal and external CD-ROM or DVD-ROM drives:
   a. Choose the Local CD/DVD Drive option.
   b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.
   c. Click 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 1: If you are working with files on a Linux® target, use the Linux Sync command after the files are copied using virtual media in order to view the copied files. Files may not appear until a sync is performed.

Note 2: If you are using the Windows operating system®, Removable Disk is not displayed by default in the Window's My Computer folder when you mount a Local CD/DVD Drive or Local or Remote ISO Image. To view the Local CD/DVD Drive or Local or Remote ISO Image in this folder, select Tools > Folder Options > View and deselect "Hide empty drives in the Computer folder".

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.

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 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. ISO9660 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 Virtual Media Shared Images 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.

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

1. Choose Device Settings/Virtual Media Shared Images from the remote console. The Virtual Media Shared Images setup page opens.
2. Click New to open the Add Shared Image page.
3. Enter information about the file server ISO images that you want to access.
   - IP Address/Hostname
   - Share Name
   - Image Path
   - Select Enable SAMBA v1.0 as applicable.
4. Click Add Shared Image.

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) 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

KVM Client	Name	URL to Force Launch
HTML KVM Client - Java-Free	HKC	<DKX3G2 IP Address>/hkc OR <DKX3G2 IP Address>/
Active KVM Client - Requires .NET	AKC	<DKX3G2 IP Address>/akc
Virtual KVM Client - Requires Java	VKCs	<DKX3G2 IP Address>/vkcs

Virtual KVM Client

To launch VKCS, enter https://<KX3- IP address>/vkcs in a browser.

Java Requirements

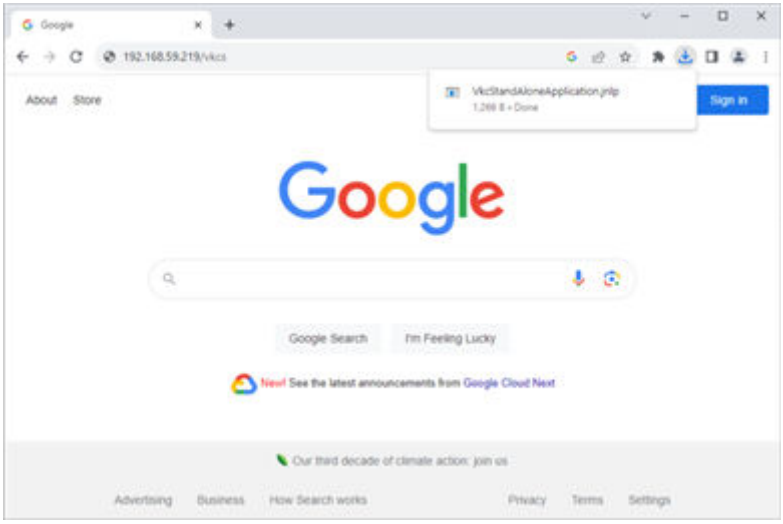
- A supported Java version is required. Check the release notes for latest supported version.
- If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

Note: On Windows Operating Systems use 64 bit JRE to get better performance.

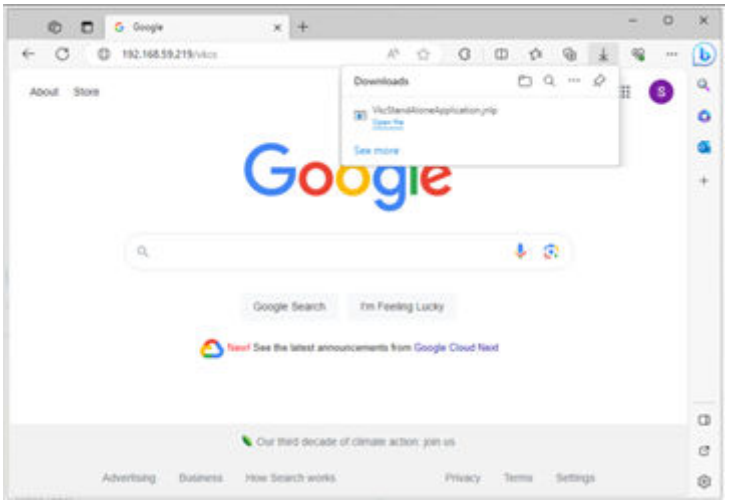
► *VKCS Launching:*

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".

Proxy Server Configuration

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

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

► *To configure the SOCKS proxy:*

1. On the remote client PC, select Control Panel > Internet Options.
   a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.
   b. Select 'Use a proxy server for your LAN'.
   c. Click Advanced. The Proxy Settings dialog opens.
   d. Configure the proxy servers for all protocols.
      IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

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

      ---

   e. Click OK at each dialog to apply the settings.
2. Next, configure the proxy settings for the Java™ applets:

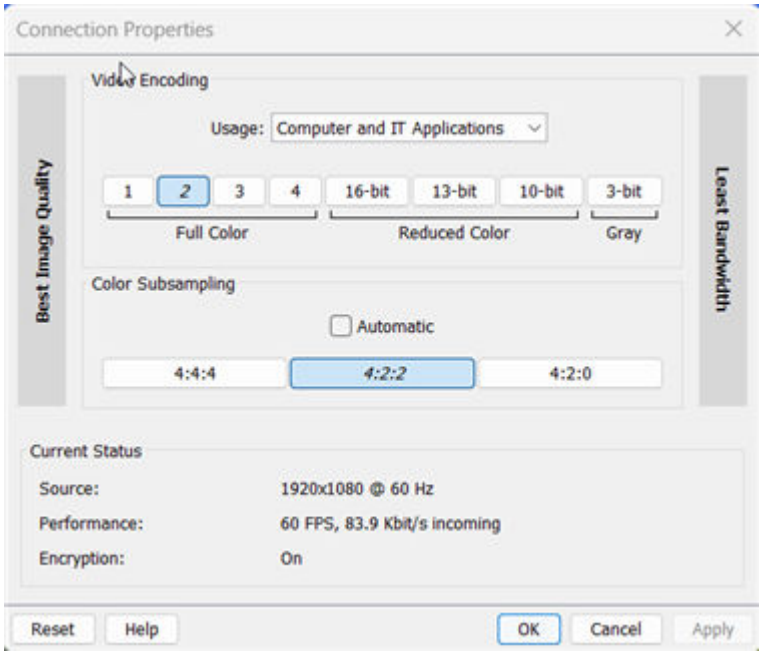
a. Select Control Panel > Java.
b. On the General tab, click Network Settings. The Network Settings dialog opens.
c. Select "Use Proxy Server".
d. Click Advanced. The Advanced Network Settings dialog opens.
e. Configure the proxy servers for all protocols.

   IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

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

Connection Properties

The Connection Properties dialog allows you to configure the video stream parameters to match your system capabilities with your performance needs.



► *Video Encoding*

This section selects the video encoding algorithm and quality setting.

- Usage: specify your general application area. This selection optimizes the available choices elsewhere in this dialog.
  - General Purpose Video: video content where smooth color reproduction is most important, such as movies, video games, and animations.
  - Computer and IT Applications: video content where text sharpness and clarity are important, such as computer graphical interfaces.
- Encoder Mode: Choose the encoder mode from the row of eight buttons. Options will vary depending on the Usage selection. In general, modes towards the left of the button bar offer higher image quality but consume higher bandwidth, and might cause frame rate to drop depending on network speed and/or client performance. Modes towards the right consume lower bandwidth at the cost of reduced image quality. In network- or client-constrained situations, modes towards the right may achieve better frame rates.

The default video mode is always "Full Color 2", which is a high-quality mode and works well for most uses in LAN environments. If needed, experiment with modes further towards the right to find the right balance of image quality and frame rate.

► *Color Subsampling*

Color subsampling reduces the color information in the encoded video stream.

- Automatic: Recommended. The optimal color subsampling mode will be enabled based on the selections in the video encoding section.
- 4:4:4: Highest quality at significant bandwidth cost. Usually not necessary except for some situations in graphical user interfaces.
- 4:2:2: Good blend of image quality and bandwidth.
- 4:2:0: Maximum savings of network bandwidth and client load. Works fine for most general-purpose applications that don't emphasize high-resolution lines or text.

► *Current Status*

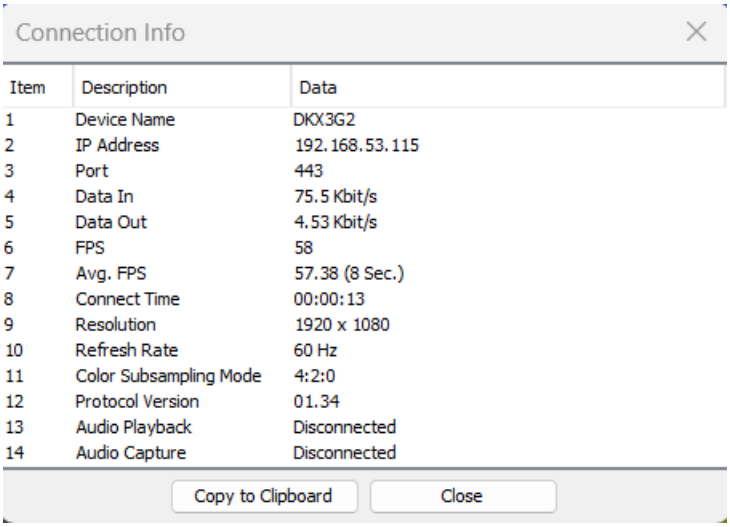
Current status includes real-time video performance statistics. As you change settings in the dialog, you can immediately see the effects on performance.

- Source: resolution and frame rate of the incoming video source.
- Performance: frames per second (FPS) being rendered in the client, and the data rate of the incoming video stream. These values are where you will see the effects of your video settings.
- Encryption: whether the video stream is encrypted or not. Encrypted streams usually have lower frame rates and lower bandwidth. Encryption is a global setting in security → KVM Security → "Apply Encryption Mode to KVM and Virtual Media".

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. To edit the connection properties, see: Connection Properties (on page 45).

- To view the Connection Info, choose Connection > Info...



Connection Info

Item	Description	Data
1	Device Name	DKX3G2
2	IP Address	192.168.53.115
3	Port	443
4	Data In	75.5 Kbit/s
5	Data Out	4.53 Kbit/s
6	FPS	58
7	Avg. FPS	57.38 (8 Sec.)
8	Connect Time	00:00:13
9	Resolution	1920 x 1080
10	Refresh Rate	60 Hz
11	Color Subsampling Mode	4:2:0
12	Protocol Version	01.34
13	Audio Playback	Disconnected
14	Audio Capture	Disconnected

Copy to Clipboard Close

USB Profile

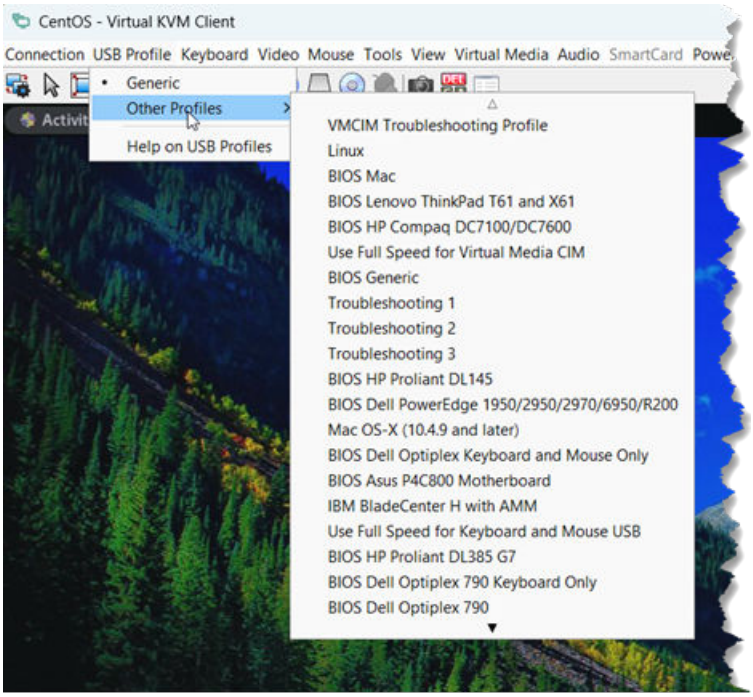
Select a USB profile that best applies to the KVM target server.

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

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

► *To set a USB profile for a target server:*

- Choose USB Profile, then choose Generic, or choose Other Profiles to select from a menu.



► *To view details on USB profiles:*

- Choose USB Profile > Help on USB Profiles.

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.

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.

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

Build a New Macro

► *To build a macro:*

1. Click Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Click Add. The Add Keyboard Macro dialog appears.
3. Type a name for the macro in the Keyboard Macro Name field. This name appears in the Keyboard menu after it is created.
4. From the Hot-Key Combination field, select a keyboard combination from the drop-down list. This allows you to execute the macro with a predefined keystroke. Optional
5. In the Keys to Press drop-down list, select each key you would like to use to emulate the keystrokes that is used to perform the command. Select the keys in the order by which they are to be pressed. After each selection, select Add Key. As each key is selected, it appears in the Macro Sequence field and a Release Key command is automatically added after each selection.

For example, create a macro to close a window by selecting Left 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.

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

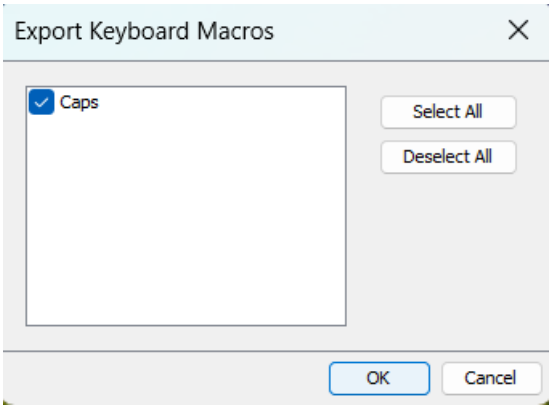
- Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are skipped as well.
- Click Cancel to stop the import.
- Alternatively, click Rename to rename the macro and import it. If Rename is selected, the Rename Macro dialog appears. Enter a new name 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 hot key that already exists, the hot key 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

Refreshing the Screen

The Refresh Screen command forces a refresh of the video screen

- Choose Video > Refresh Screen, or click the Refresh Screen button  in the toolbar.

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.

Auto Sense Video Settings

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 Video Settings.

A message stating that the auto adjustment is in progress appears.

Calibrate Color

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.

► *To calibrate color:*

- Choose Video > Calibrate Color.
  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.

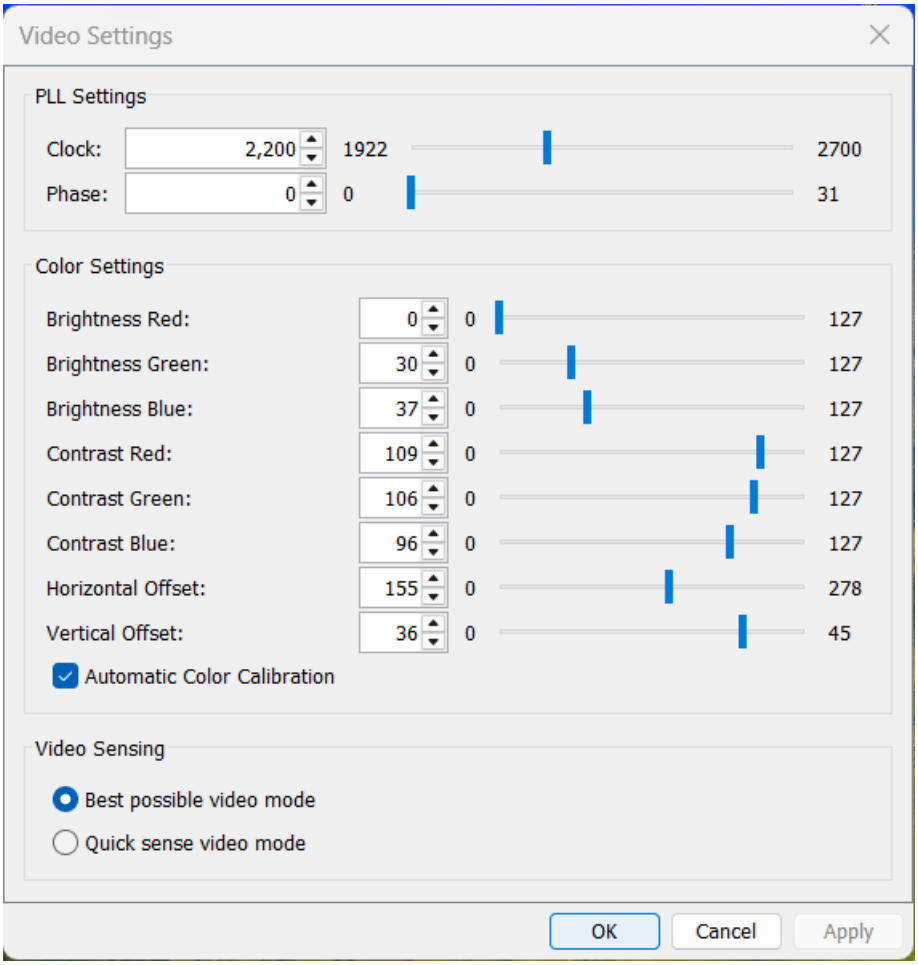
      Contrast Blue - Controls the blue signal.

      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.

Screen Shot from Target

You can take a screen from the target and save it on your local machine.

► *To take a screen shot:*

Choose Video >Screen Shot from Target.

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 DKX3G2 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.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when other modes don't work.

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

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 is the default mouse mode.

► *To enter Absolute Mouse Synchronization:*

- Choose Mouse > Absolute from the KVM client.

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. Use intelligent mouse mode if absolute mouse mode is not supported on the target.

Enter Intelligent Mouse Mode

► *To enter intelligent mouse mode:*

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

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

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- 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. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
3. Open a terminal window.
4. Enter the following command: xset mouse 1 1
5. Close the terminal window.
6. 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.

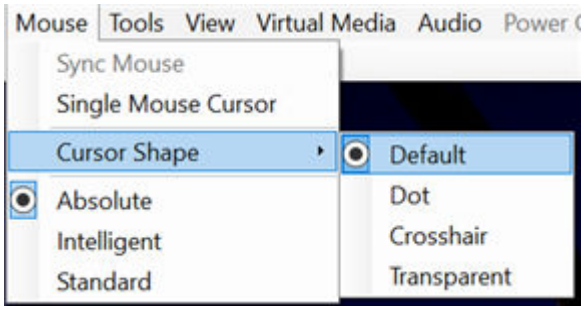
Note: This option is available only in Standard and Intelligent mouse modes.

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.

► *To change the cursor shape:*

- Choose Mouse > Cursor Shape, then select from the list.
  - Default which is an arrow
  - Dot
  - Crosshair
  - Transparent



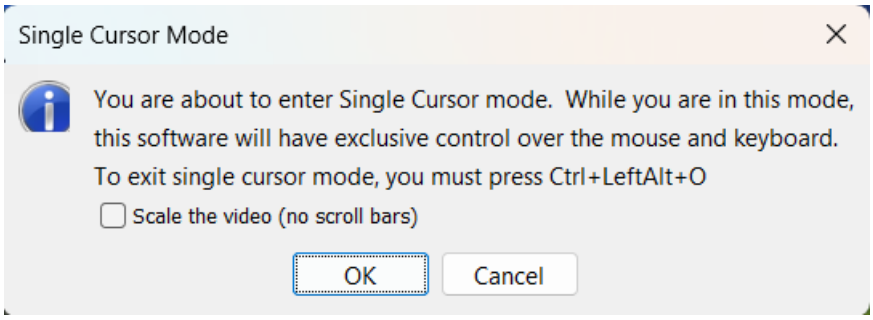
Single Mouse Cursor

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.

Tools

General Settings

To set the tools options:

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.
- 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 for details and examples.
- In Mac OS/VKCs launches only, Let Full Screen Window Cover the Main Menu Bar and the Dock is enabled by default. Use this setting to prevent the Java menubar from hiding the VKCs menubar when running VKCs in full-screen mode on Mac.
- Select Disable Menu in Full Screen to hide the menu options in Full screen mode if you do not want to see it.
- Choose the Keyboard Type from the drop-down list (if necessary):
  - Danish (Denmark)
  - English (UK)
  - English US/International
  - French (Belgium)
  - French (France)
  - German (Germany)
  - German (Switzerland)
  - Hungarian
  - Italian (Italy)
  - Japanese
  - Korean (Korea)
  - Norwegian (Norway)
  - Portuguese (Portugal)
  - Slovenian
  - Spanish (Spain)
  - Swedish (Sweden)
  - Translation: French - US
  - Translation: French - US International

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

2. 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 hot key 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 hot key 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 hot key used to toggle in and out of scaling mode.

- Disconnect from Target - Hotkey.

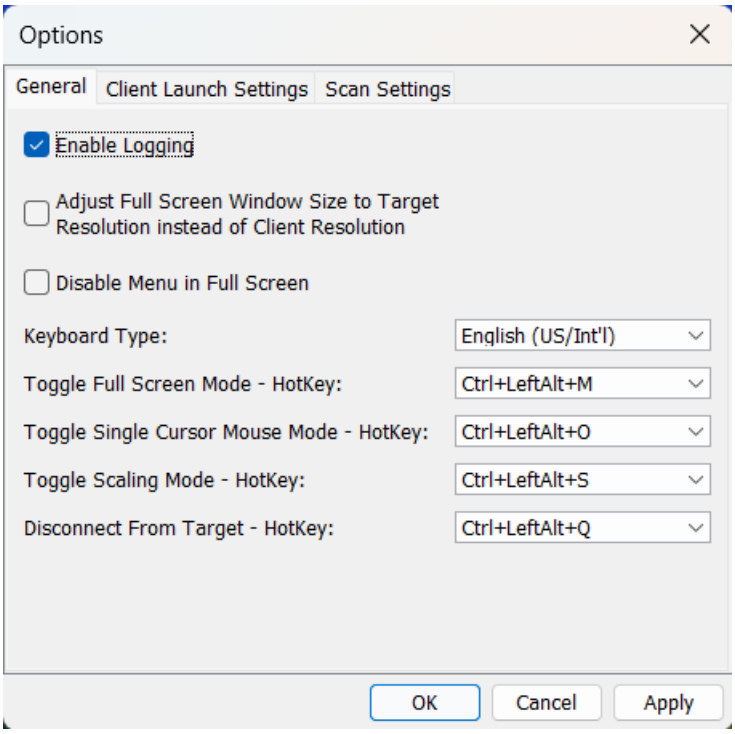
  Enable this hotkey to allow users to quickly disconnect from the target.

3. Click OK.

Note: 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.



Keyboard Limitations

Turkish Keyboards

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

Slovenian Keyboards

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

Language Configuration on Linux

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

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. DKX3G2 supports up-to 1920x1200 resolution.

Client Launch Settings

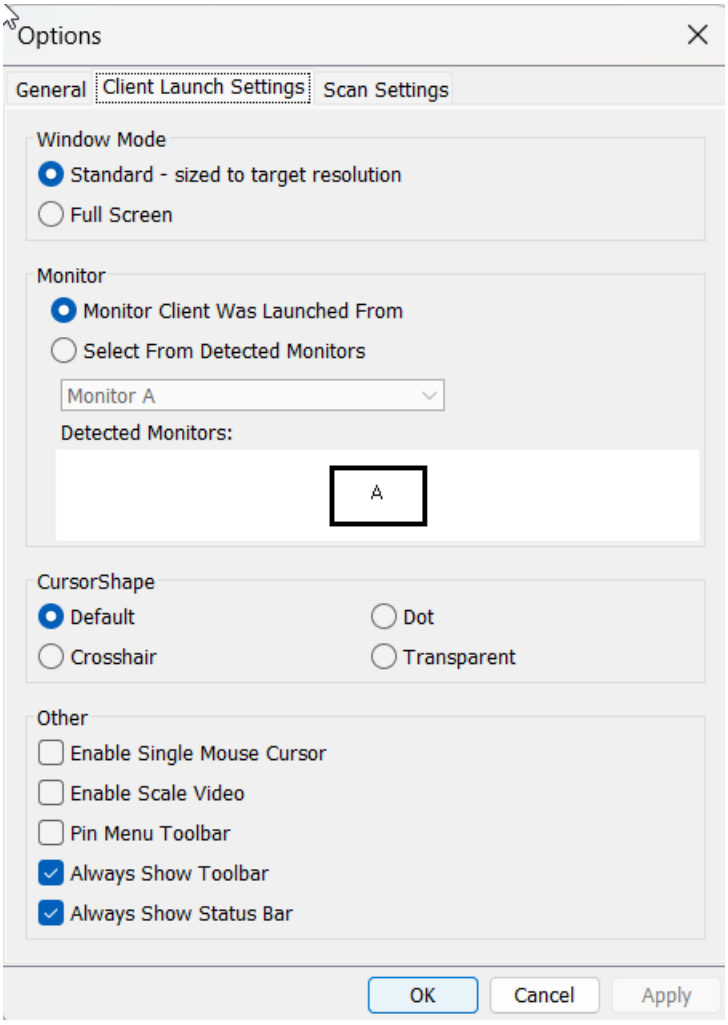
► *To configure client launch settings:*

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.

- 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 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.

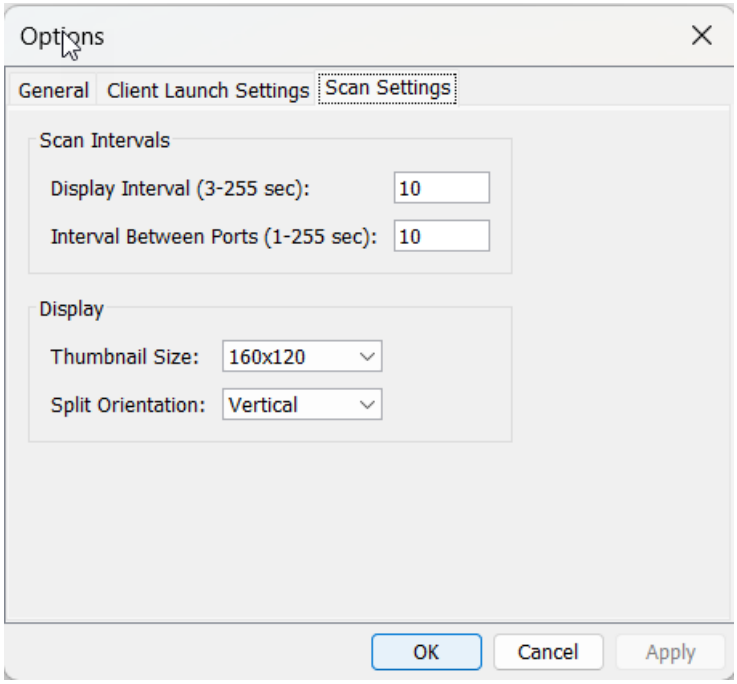
3. Click OK.



Scan Settings

► *To Configure Scan Settings*

1. Click Tools > Options. The Options dialog appears.
2. Select Scan Settings tab.
3. Type the duration for display intervals and intervals between the ports
4. Select the size for thumbnail display and orientation.
5. Click OK.



Collecting a Diagnostics 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:

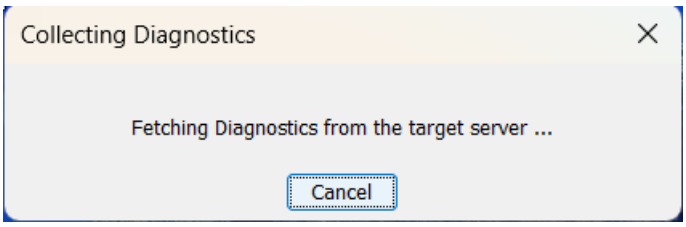
  These are the client logs.

  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 Diagnostics Snapshot

► *To capture a diagnostic snapshot:*

1. Connect to a target and then click Tools -> Collect a Diagnostics Snapshot. Several messages are displayed as the information is collected.



2. You are prompted to save the Zip file containing the diagnostics files
3. The zip file containing the diagnostics files is saved as per your selection.

View Options

View Toolbar

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

► *To toggle the display of the toolbar (on and off):*

- Choose View > View Toolbar.

View Status Bar

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

► *To hide the status bar:*

- Click View > Status Bar to deselect it.

► *To restore the status bar:*

- Click View > Status Bar to select it.

Scaling

Scaling your target window allows you to view the entire contents of the target server window.

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

► *To toggle scaling (on and off):*

- Choose View > Scaling.

Full Screen Mode

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

The hot key used for exiting this mode is specified in the Options dialog, see Tool Options.

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.

► *To enter full screen mode:*

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

► *To exit full screen mode:*

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

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

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

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

Virtual Media

This feature allows you to access storage media such as CD-ROMs, flash memory and external drives anywhere on the network as if they are directly attached to that server's USB port See:Virtual Media (KX3/LX2) for more details.

Digital Audio

The DKX3G2 supports audio playback via D2CIM-DVUSB variants.

Supported Audio Device Formats

The DKX3G2 supports one playback and capture device and one record device on a target at a time. The following audio device formats are supported:

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

Digital Audio VKC and AKC Icons

Audio icons	Icon name	Description
	Speaker	These icons are located in status bar at the bottom of the client window. Green, blinking waves indicate an audio playback session is currently streaming. A black speaker icon is displayed when the session is muted. The icon is grayed out when no audio is connected.
	Microphone	These icons are located in the status bar at the bottom of the client window. Red, blinking waves indicate an audio capture session is currently underway. The Speaker icon, indicating a playback session is streaming, is also displayed when a session is underway. A black Microphone icon is displayed when the session is muted. When the Microphone icon is grayed out, no audio is connected.

Audio Playback and Capture Recommendations and Requirements

Audio Level

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

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

Recommendations for Audio Connections when PC Share Mode is Enabled

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

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

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

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

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

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

Bandwidth Requirements

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

Audio format	Network bandwidth requirement
44.1 KHz, 16bit stereo	176 KB/s
44.1 KHz, 16bit mono	88.2 KB/s
22.05 KHz, 16bit stereo	88.2 KB/s
22.05 KHz, 16bit mono	44.1 KB/s
11.025 KHz, 16bit stereo	44.1 KB/s
11.025 KHz, 16bit mono	22.05 KB/s

In practice, the bandwidth used when an audio device connects to a target is higher due to the keyboard and video data consumed when opening and using an audio application on the target.

A general recommendation is to have at least a 1.5MB connection before running 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 DKX3G2 device basis.

Once the audio devices settings are configured and saved on the DKX3G2, the same settings are applied to it.

See: Connecting and Disconnecting from a Digital Audio Device (on page 69) for information on connecting to and configuring an audio device, and Adjusting Buffer Size (Audio Settings) for information on audio device buffer settings.

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

So, when a user joins an audio session, the target machine settings are used.

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 69) 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 capture supported by:	Audio playback supported by:
Windows®	• Active KVM Client (AKC) • Virtual KVM Client (VKC)	• Active KVM Client (AKC) • Virtual KVM Client (VKC) • HTML KVM Client (HKC)
Linux®	• Virtual KVM Client (VKC)	• Virtual KVM Client (VKC) • HTML KVM Client (HKC)
Mac®	• Virtual KVM Client (VKC)	• Virtual KVM Client (VKC) • HTML KVM Client (HKC)

Connecting and Disconnecting from a Digital Audio Device

Audio device settings are applied on a per DKX3G2 device basis.

Once the audio devices settings are configured and saved on the DKX3G2, the same settings are applied to it.

See: Saving Audio Settings (on page 68) 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 67), Audio Playback and Capture Recommendations and Requirements (on page 321) 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
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 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.

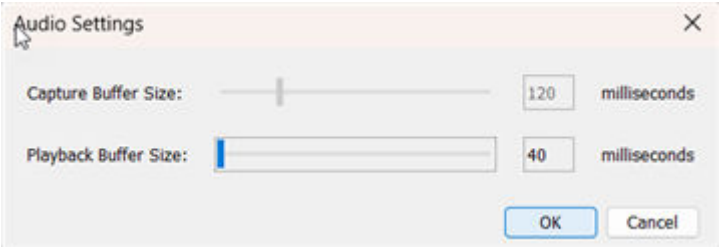
The buffer size can be adjusted whenever needed, including during an audio session.

Audio settings are configured in .

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.



Smart Card

Using the DKX3G2, 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.

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

Smart cards are supported on AKC and VKC remote clients.

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 Requirements (on page 320)
- Supported Computer Interface Module (CIMs) Specifications
- Supported Smart Card Readers (on page 321)

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

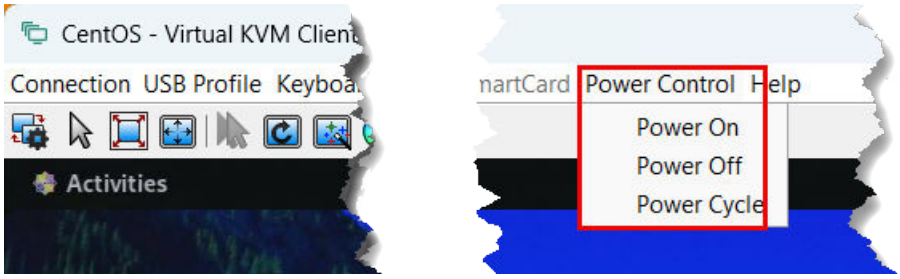
► *To unmount a smart card reader:*

- Select the smart card reader to be unmounted and click the Unmount button.

Power Control

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.

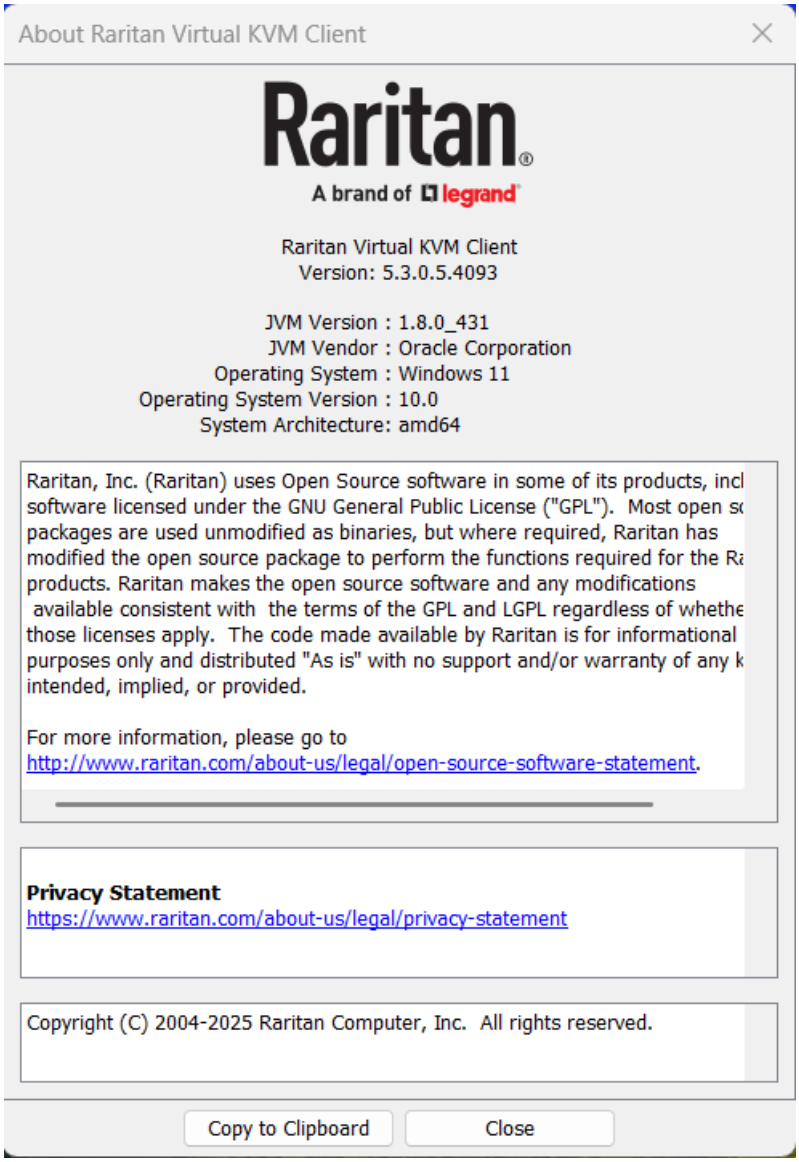
The menu option is disabled if you do not have permission for power control, and when outlets are not associated with the port.



Version Information

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

- Choose Help > About Raritan Virtual KVM Client.



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..

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 DKX3G2.

AKC is compatible with the following platforms:

- Windows 10 and 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

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.
- To use AKC in Chrome make sure the ClickOnce plugin is installed. To enable ClickOnce in Edge: Type edge://flags in the browser, search for ClickOnce support, set to enabled and restart the browser.

Edge Chromium versions

The Edge Chromium browser has experimental ClickOnce support which must be enabled for AKC. The browser will not detect support for ClickOnce, so you will still need to download AKC manually.

- To enable ClickOnce in Edge: Type edge://flags in the browser, search for ClickOnce support, set to enabled and restart the browser.
- To download AKC manually: Go to the DKX3G2 URL, for example https://(KX-IP-Hostname)/akc then select "Please click here" on the message showing that ClickOnce support has not been detected.

Proxy Server Configuration

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

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

► *To configure the SOCKS proxy:*

1. On the remote client PC, select Control Panel > Internet Options.

a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.
b. Select 'Use a proxy server for your LAN'.
c. Click Advanced. The Proxy Settings dialog opens.
d. Configure the proxy servers for all protocols.
   IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

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

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

2. Next, configure the proxy settings for the Java™ applets:
   a. Select Control Panel > Java.
   b. On the General tab, click Network Settings. The Network Settings dialog opens.
   c. Select "Use Proxy Server".
   d. Click Advanced. The Advanced Network Settings dialog opens.
   e. Configure the proxy servers for all protocols.
      IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

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

Browser Tips for AKC

- If AKC fails to launch and displays an application error, you may need to delete the ClickOnce cache. https://docs.microsoft.com/en-us/troubleshoot/dotnet/framework/clickonce-application-fails-update

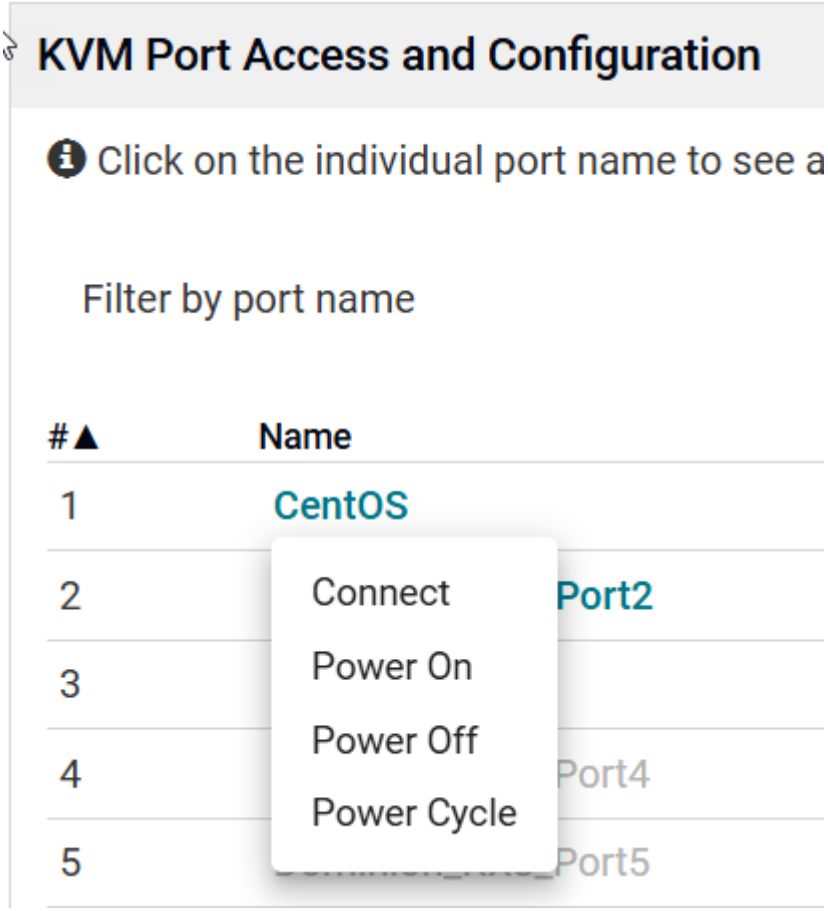
Connect to a Target

Once you have logged on to the DKX3G2 Remote Console, access target servers via the AKC client.

► *To connect to an available server:*

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

Click Connect.



See Port Action Menu 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 42) for a full matrix of clients.

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

► *Supported Features:*

- Connection Properties
- USB Profiles
- Video Settings

- Input Settings
- Audio Playback
- Virtual Media
- Dual Video Targets
- 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 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.
- HKC is a default client and to launch just use http://IP Address>in any browser.
- From Chrome running on Linux, to get ´ ` or ^, the key needs to be hit three times, or twice followed by a space.

Connection Properties

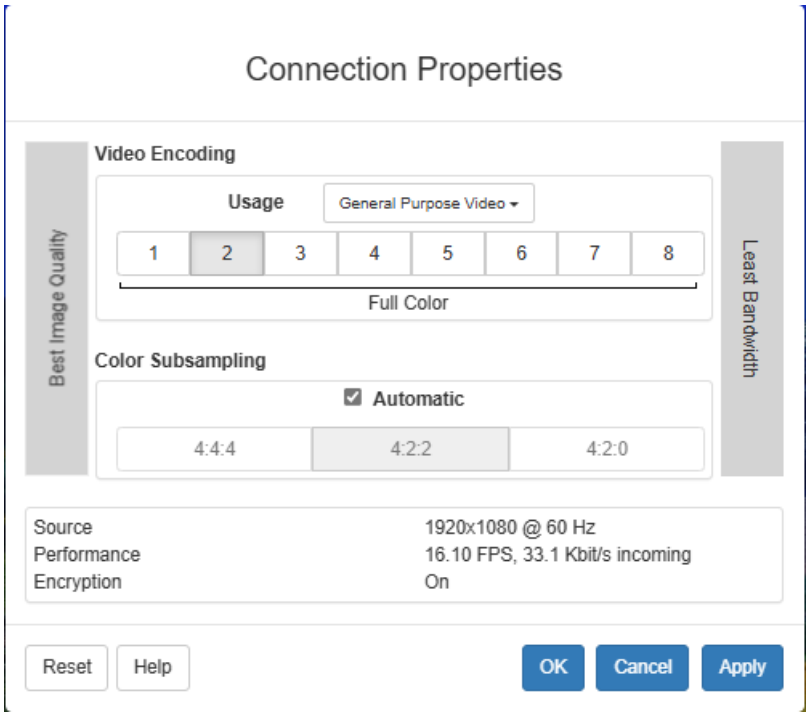
Connection properties manage streaming video performance over remote connections to target servers.

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 Connection > Connection Properties.



- Video Encoding
- This section selects the video encoding algorithm and quality setting.
- Usage: specify your general application area. This selection optimizes the available choices elsewhere in this dialog.
- General Purpose Video: video content where smooth color reproduction is most important, such as movies, video games, and animations.

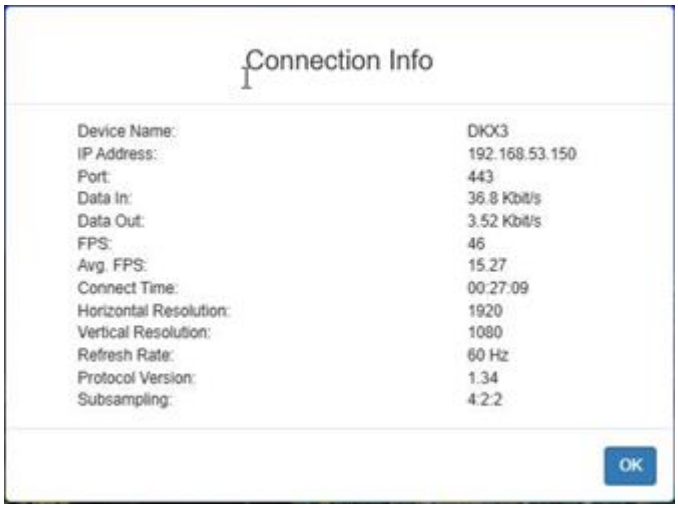
- Computer and IT Applications: video content where text sharpness and clarity are important, such as computer graphical interfaces.
- Encoder Mode: Choose the encoder mode from the row of eight buttons. Options will vary depending on the Usage selection. In general, modes towards the left of the button bar offer higher image quality but consume higher bandwidth, and might cause frame rate to drop depending on network speed and/or client performance. Modes towards the right consume lower bandwidth at the cost of reduced image quality. In network- or client-constrained situations, modes towards the right may achieve better frame rates.
- The default video mode is always "Full Color 2", which is a high-quality mode and works well for most uses in LAN environments. If needed, experiment with modes further towards the right to find the right balance of image quality and frame rate.
- Color Subsampling
- Color subsampling reduces the color information in the encoded video stream.
- Automatic: Recommended. The optimal color subsampling mode will be enabled based on the selections in the video encoding section.
- 4:4:4: Highest quality at significant bandwidth cost. Usually not necessary except for some situations in graphical user interfaces.
- 4:2:2: Good blend of image quality and bandwidth.
- 4:2:0: Maximum savings of network bandwidth and client load. Works fine for most general-purpose applications that don't emphasize high-resolution lines or text.
- Current Status
- Current status includes real-time video performance statistics. As you change settings in the dialog, you can immediately see the effects on performance.
- Source: resolution and frame rate of the incoming video source.
- Performance: frames per second (FPS) being rendered in the client, and the data rate of the incoming video stream. These values are where you will see the effects of your video settings.
- Encryption: whether the video stream is encrypted or not. Encrypted streams usually have lower frame rates and lower bandwidth. Encryption is a global setting in security → KVM Security → "Apply Encryption Mode to KVM and Virtual Media".

Connection Info

Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed. See: Connection Properties (on page 80) to configure.

- 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:

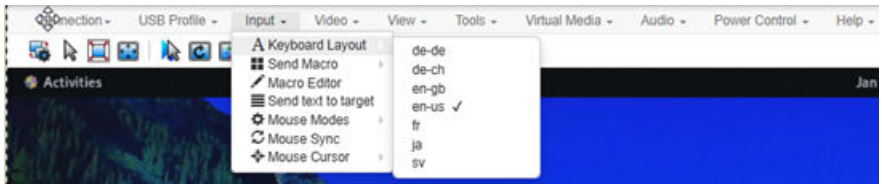
Choose USB Profile > Help on USB Profiles.

Input 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

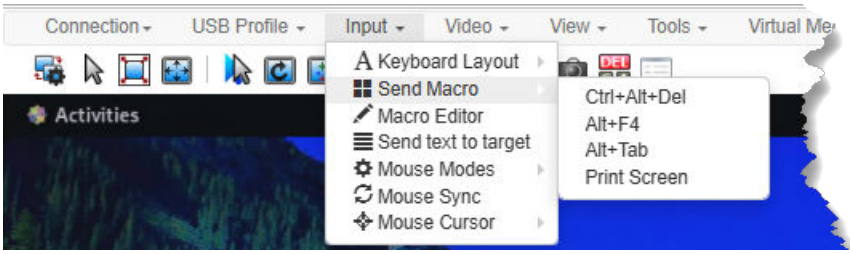


Send Macro

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.



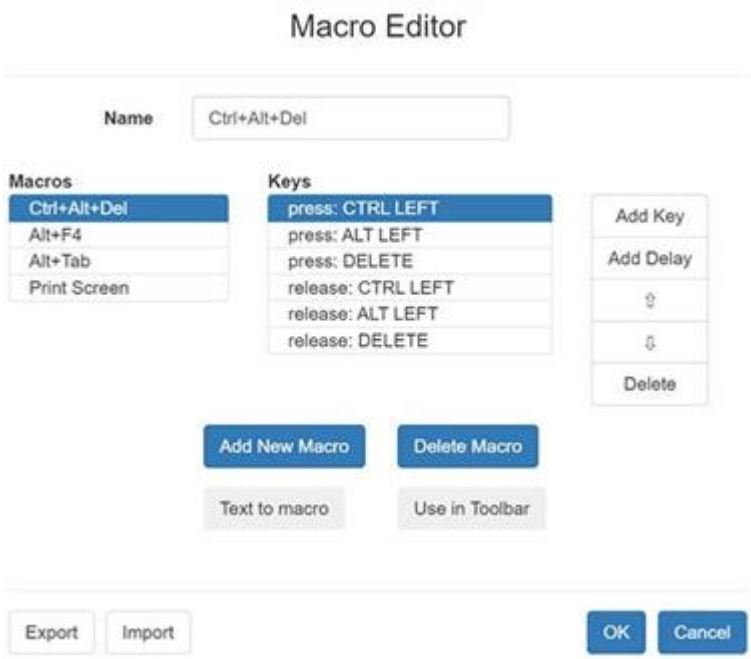
Macro Editor

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 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 DKX3G2, your macros will only be available on the browser and DKX3G2 where they were created. To reuse your macros in another DKX3G2 device, you can import and export the macro files. See Import and Export Macros.

► *To Access the Macro Editor:*

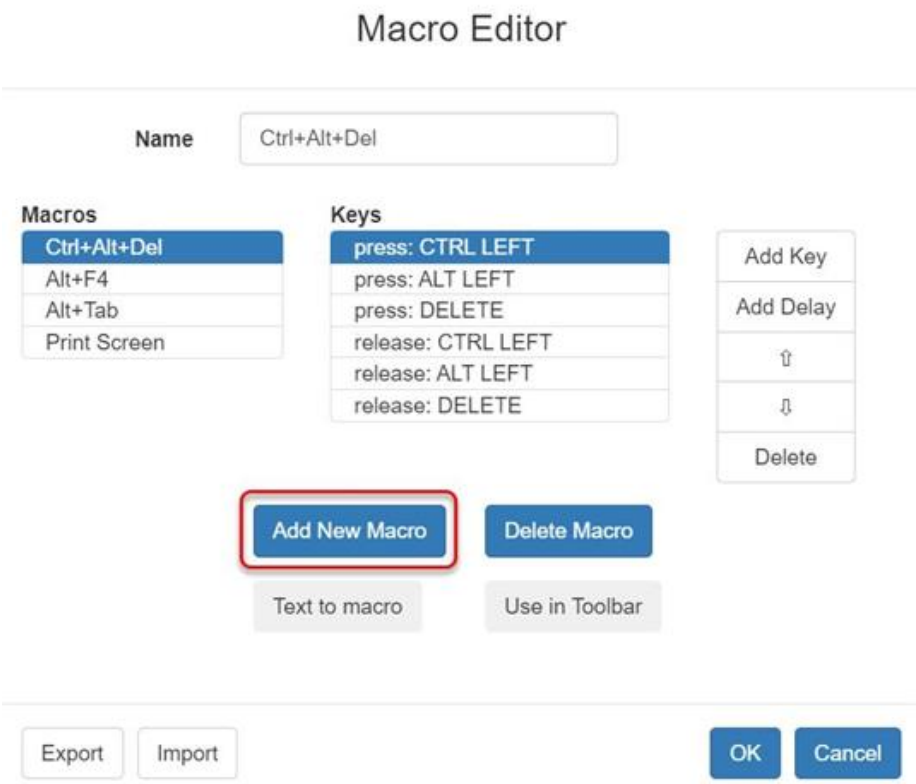
- Choose Inputs > Macro Editor.
- Select a macro from the Macros list to view the key combination.



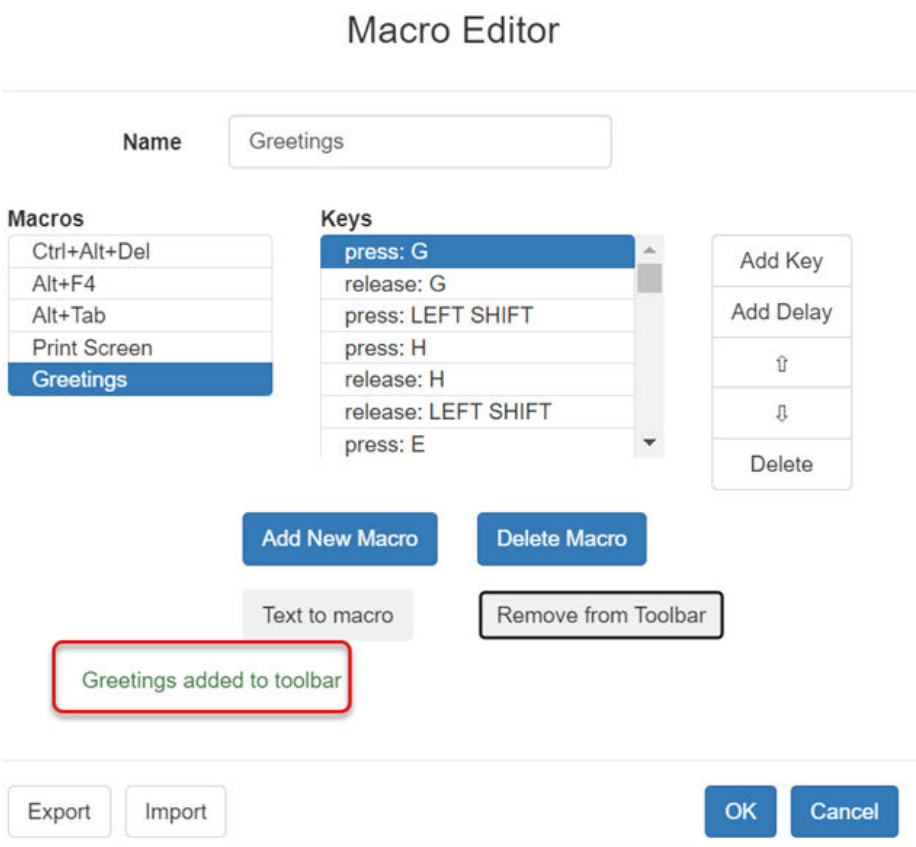
Add New Macro

► *To add a new macro:*

1. Choose Input > 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 for more details.

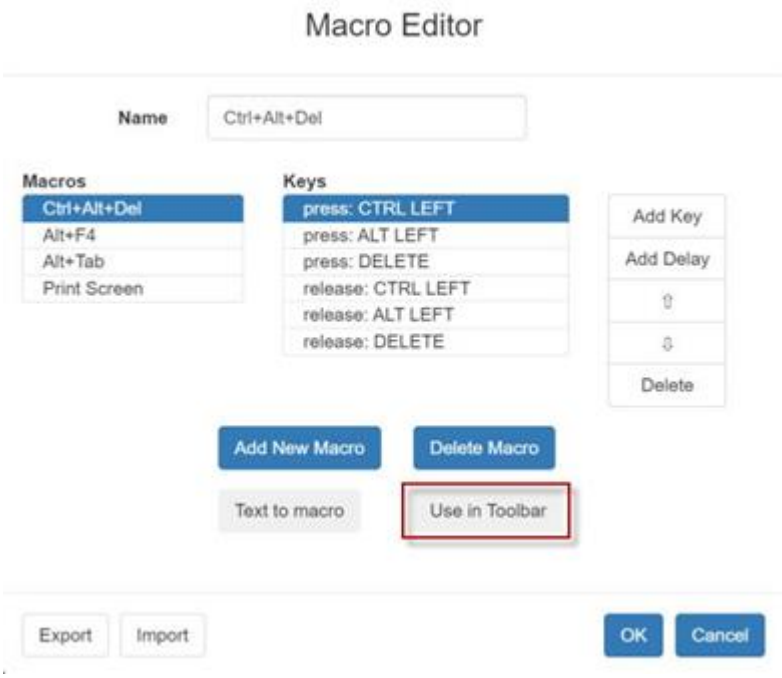


Add a Macro to the Toolbar

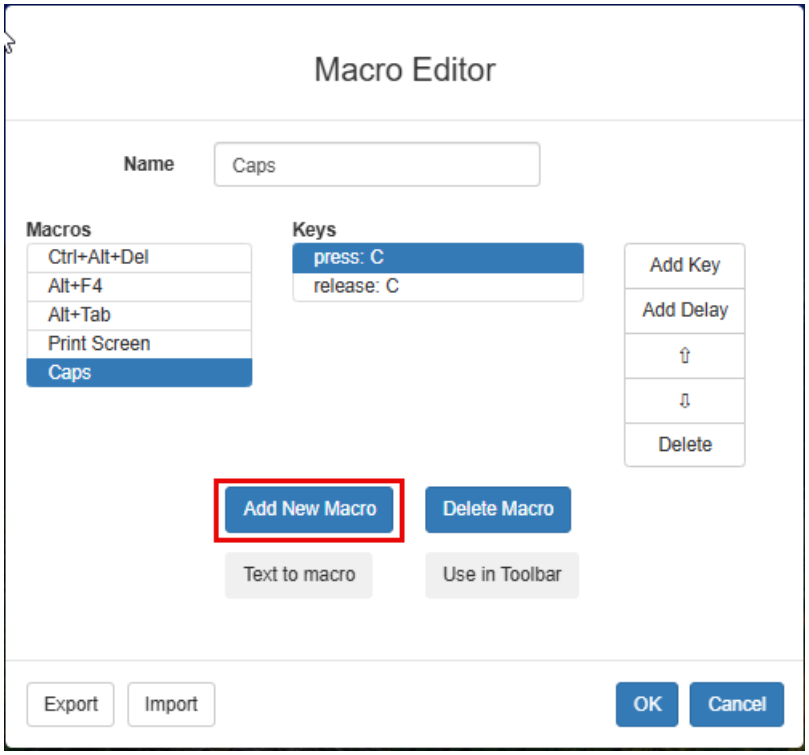
You can add a single macro to your HKC toolbar, so that you can use the macro by clicking an icon.

► *To add a macro to the toolbar:*

1. Choose Inputs > 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.
   - To remove the macro from the toolbar, click Remove from Toolbar, or select a different macro and click Use in Toolbar.

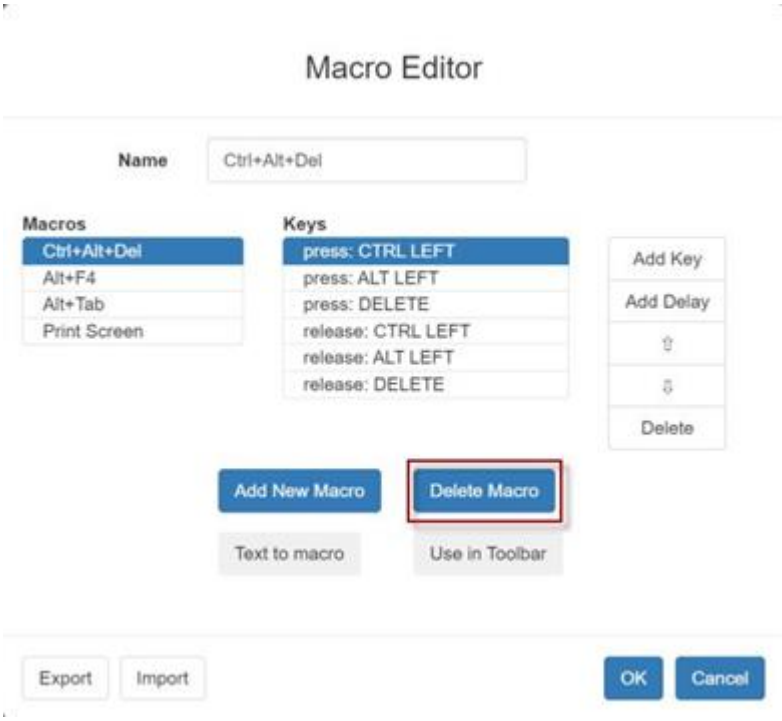


5. Click OK and exit the Macro Editor.

Delete a Macro

► *To delete a macro:*

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



Import and Export Macros

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one DKX3G2, your macros will only be available on the browser and DKX3G2 where they were created. To reuse your macros in another DKX3G2 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.

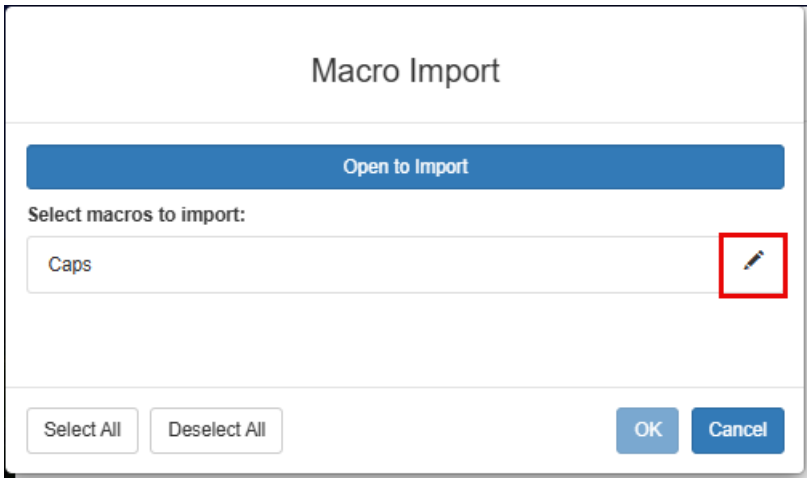
Macros are exported to an xml file named "usermacros.xml". Files are saved in your browser's default download location. Default macros are not exported.

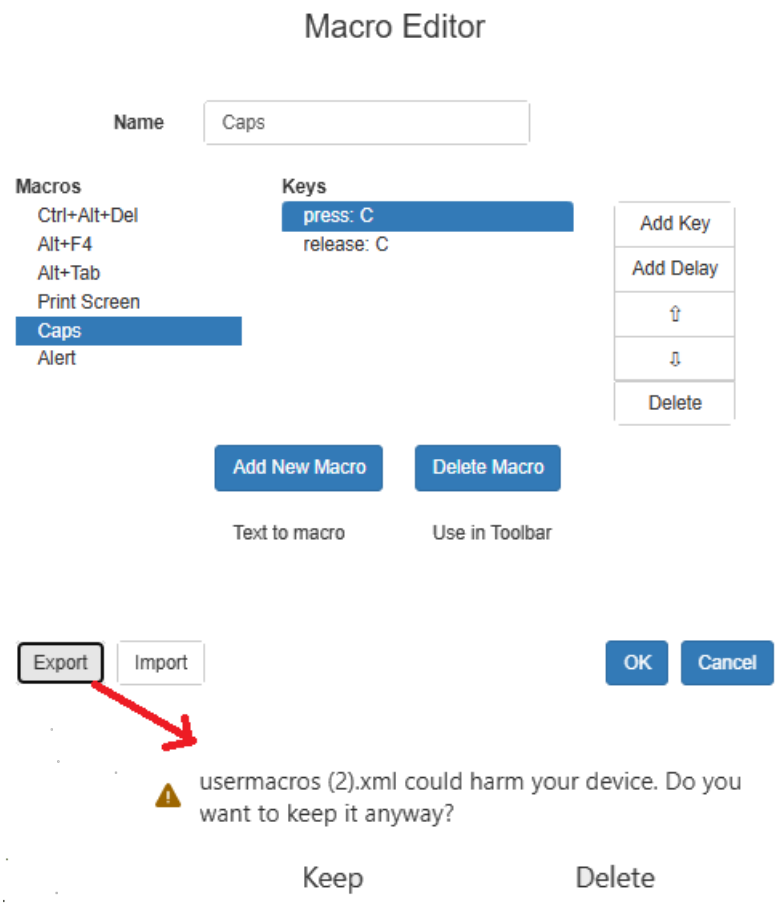
Note: When exporting macros from Edge browser, a Down arrow is briefly displayed at the bottom of the KVM window and a file named "unconfirmed.crdownload" is saved to the default download directory. To use this file as a macro input file, rename it with a .xml extension.

► *To export and import macros:*

1. Choose Input > Macro Editor. The list of macros created for your browser and DKX3G2 displays in the Macro Editor dialog.
2. To export the list, click the Export button, then save the file.
3. Log in to the DKX3G2 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.



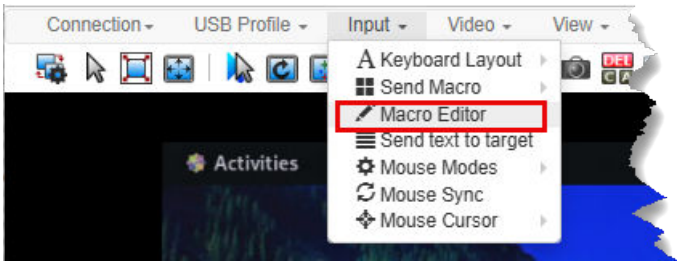


Text to Macros

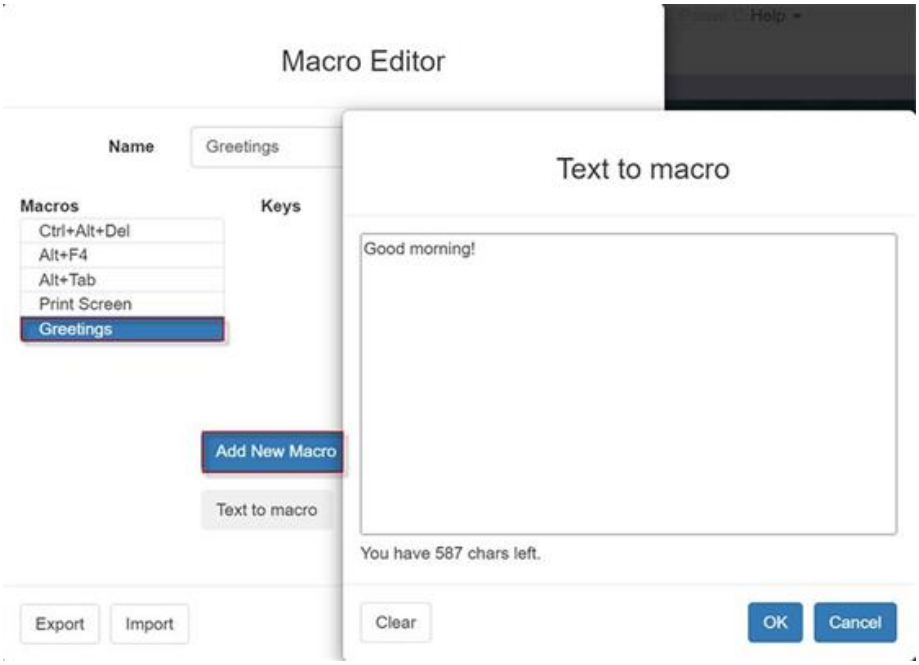
Text to macros will enable you to work more efficiently by producing frequently used phrases and paragraphs with a single command. Create a new macro and then assign text to it.

► *To add text to a macro:*

1. Choose Input > Macro Editor.



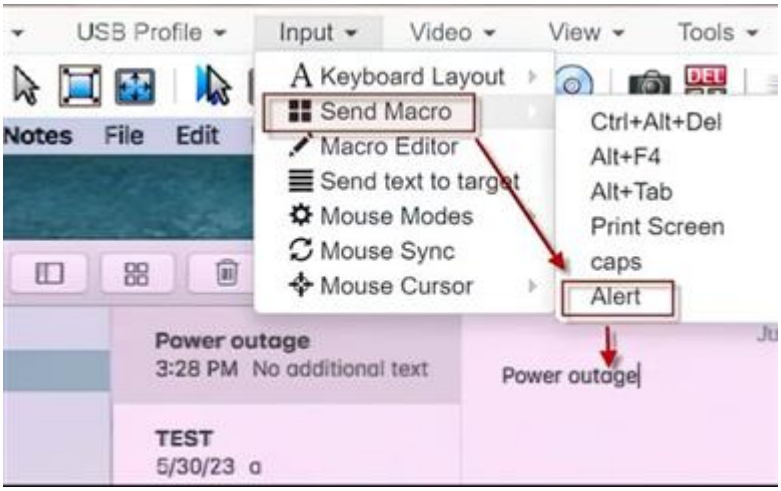
2. Select to add new macro and enter a macro name.
3. Click Text to macro.



1. Enter text in the text box and then click OK to save.
2. 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.



Known Issues for Macros

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

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 Input > 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 DKX3G2 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.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when other modes don't work.

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

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.

Mouse Cursor

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

To change the cursor shape see: Cursor Shape (on page 57)

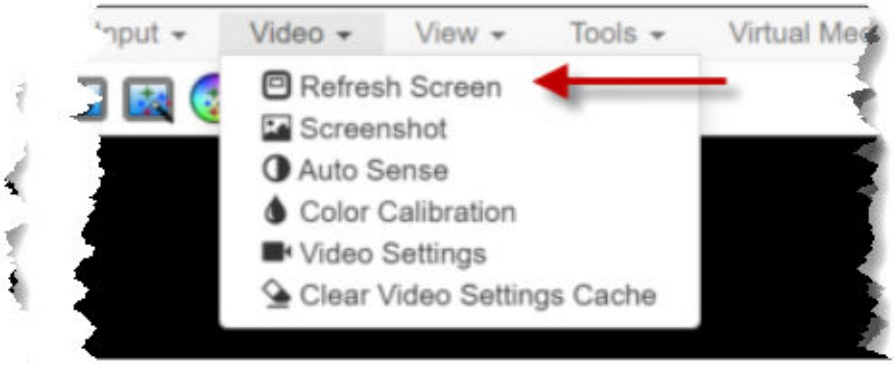
Video Menu

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:*

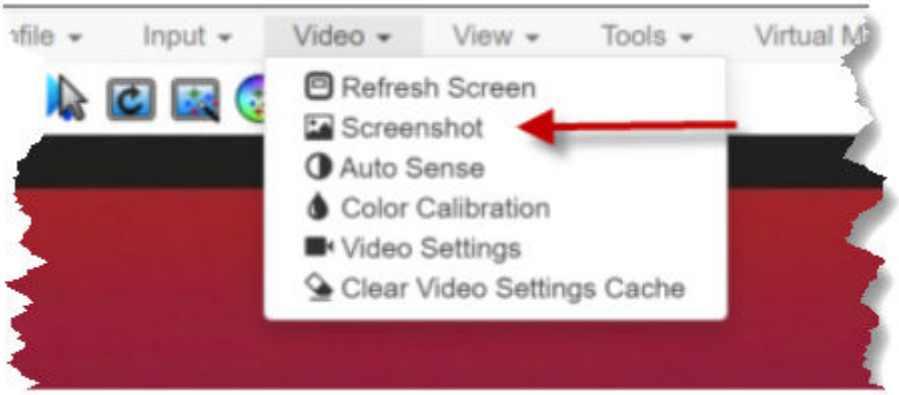
- Choose Video > Refresh Video.
- 

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.

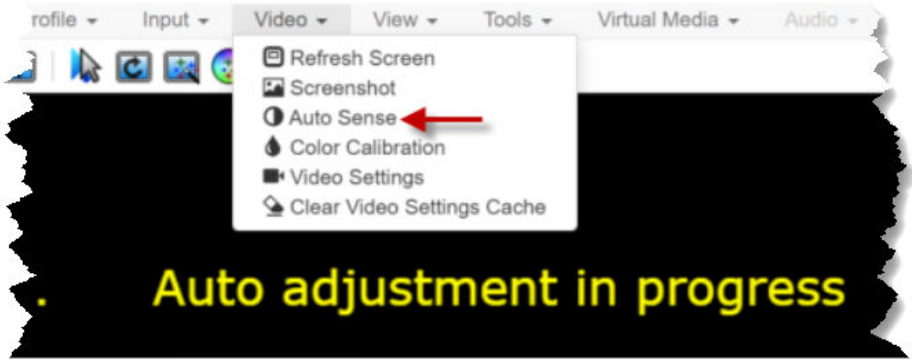


Auto Sense

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

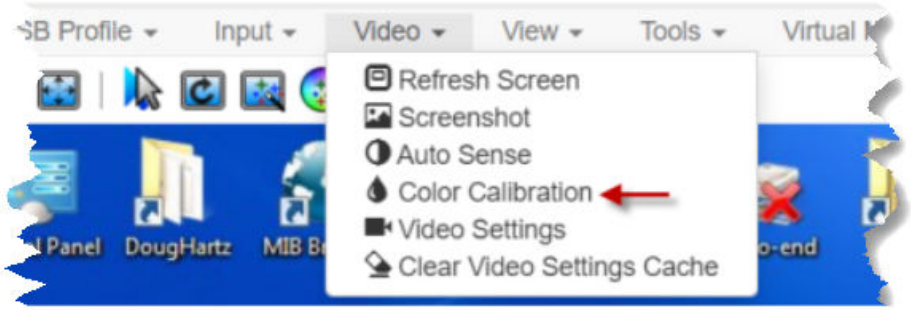
The Color Calibration command optimizes the color levels, such as hue, brightness, and saturation, of the transmitted video images.

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.

► *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.

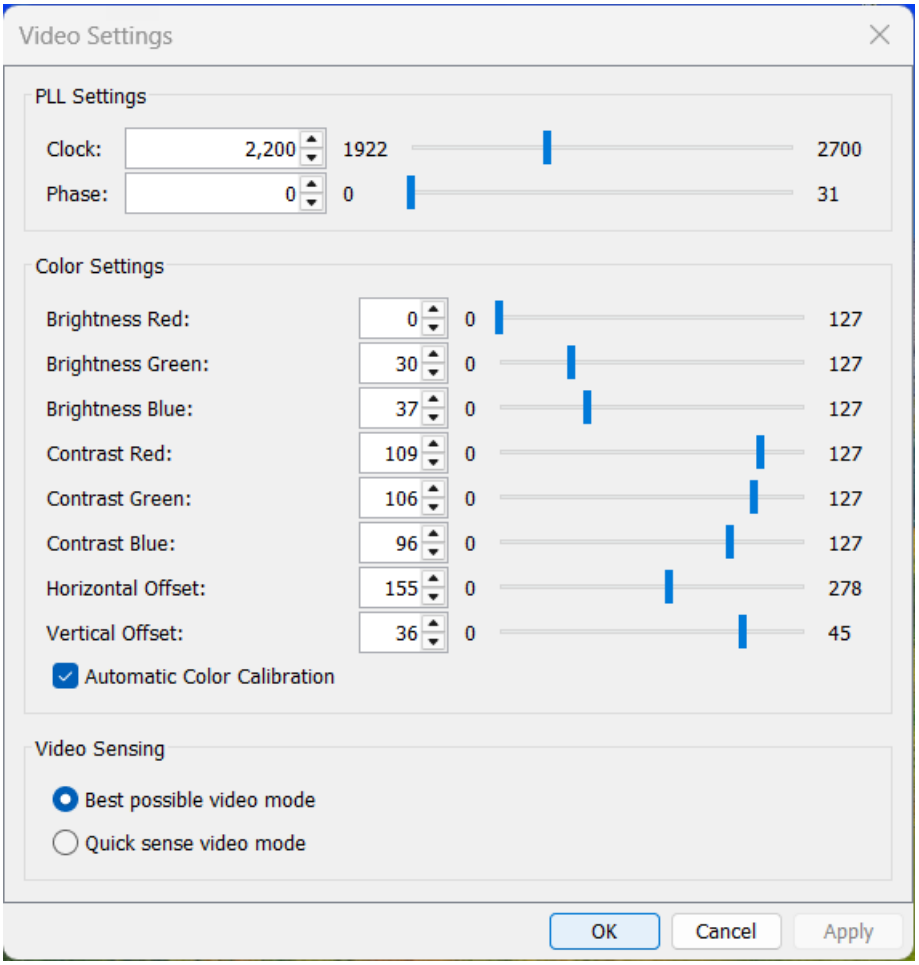
      Contrast Blue - Controls the blue signal.

      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.

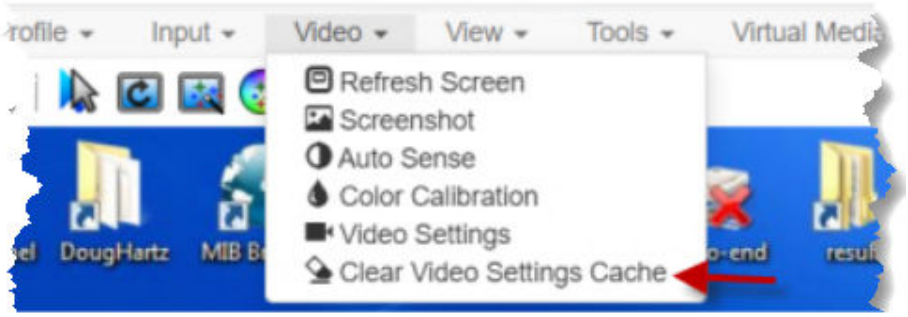


Clear Video Settings Cache

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.

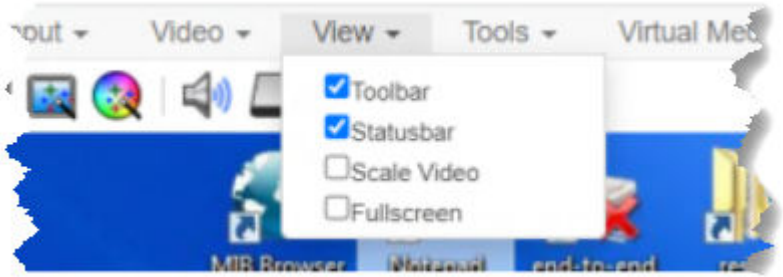
► *To clear the video settings cache:*

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



View Menu

The View Menu contains options to customize your HKC display.



► *Toolbar and Statusbar:*

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

► *Scale Video:*

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

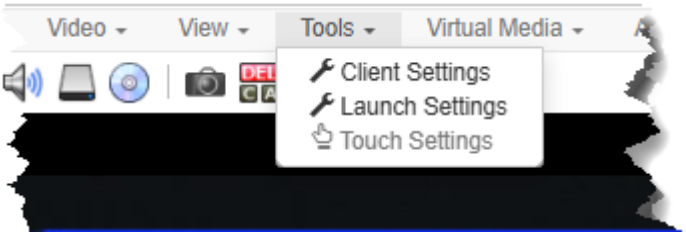
► *Fullscreen:*

Fullscreen sets the target window to the size of your full screen, removing your client from the view.

- Press Esc to exit fullscreen.

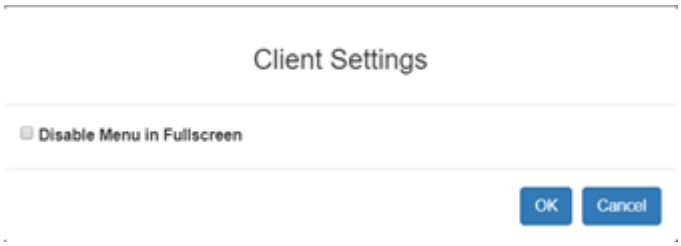
Tools Menu

The Tools menu contains options for HKC target connection settings.



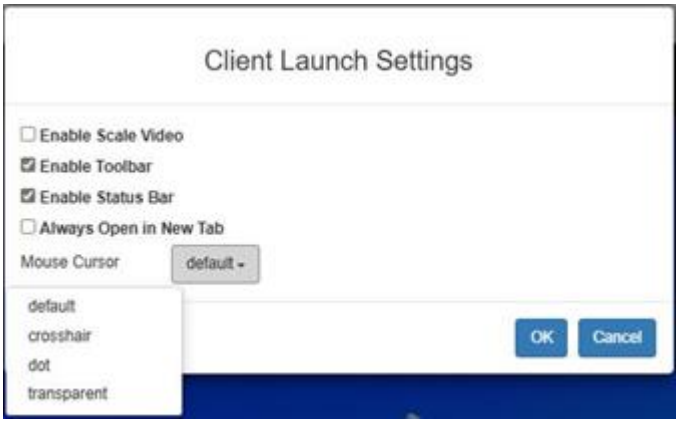
► *Client Settings:*

- 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, Enable Toolbar, Enable Statusbar, Enable Always Open in New tab and Mouse Cursor at target launch.



Note: Launch settings are applied on a per DKX3G2 device basis.

The option "Always Open in New Tab" only applies to KVM target connections, serial connections are still opened in a new browser window. Additionally option does not apply to KVM targets opened from a CC-SG browser

If user connects an audio device to a target opened in a tab and then clicks on another tab in the same browser, audio is muted

► *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.

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

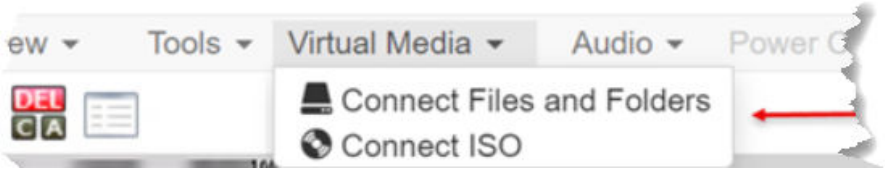
The Connect Files and Folders command provides an area to drag and drop files or folders that you want to connect by means of virtual media.

Supported browsers: Chrome, Firefox, Safari, Edge.

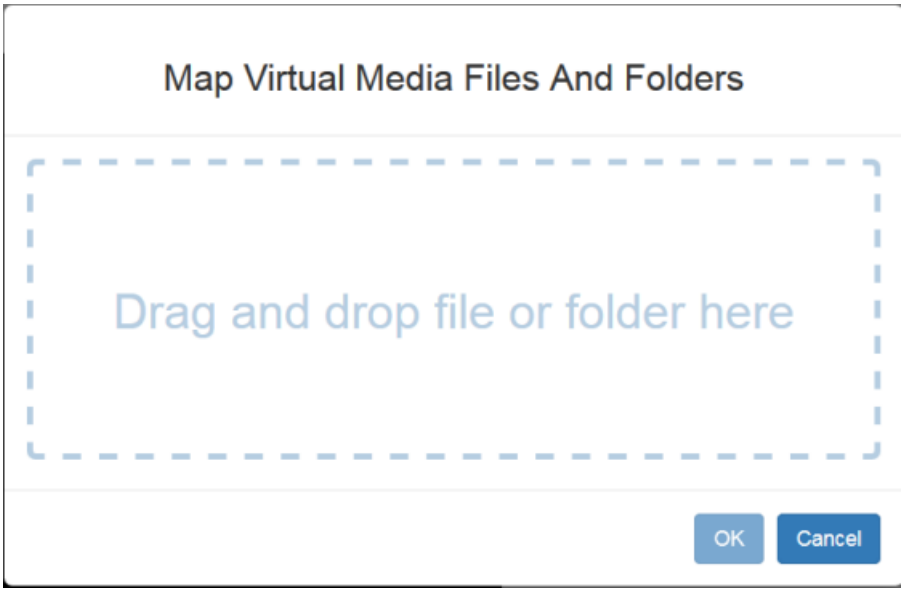
File size limit: 4GB per file

► *To connect files and folders:*

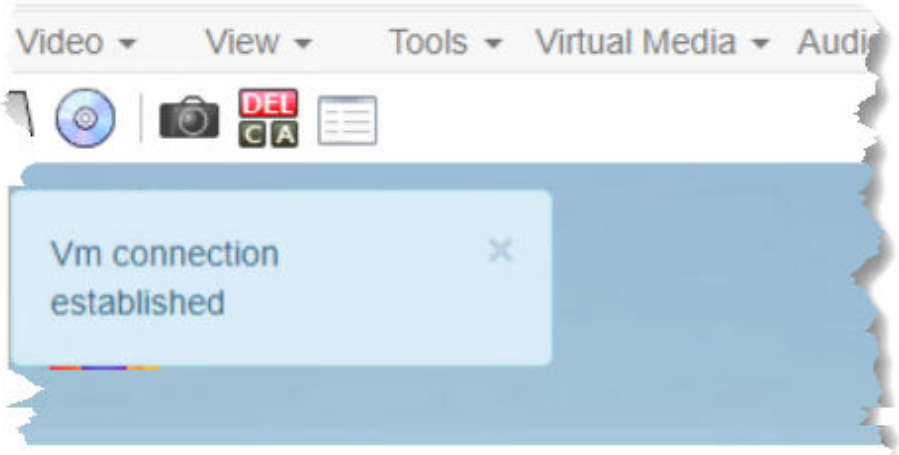
1. Choose Virtual Media > Connect Files and Folders. Or, click the matching icon in toolbar.



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

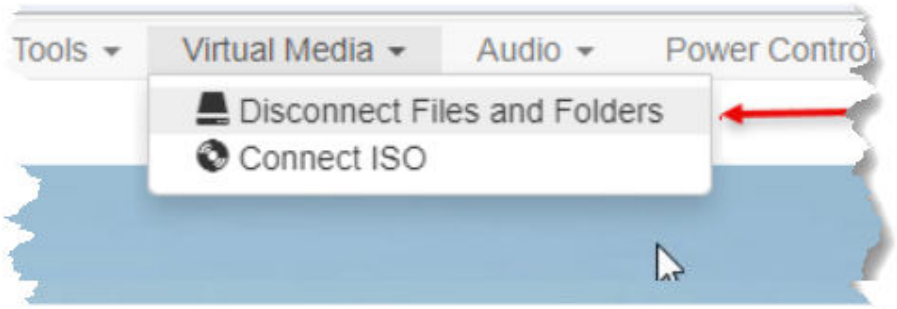


3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.



► *To disconnect files and folders:*

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



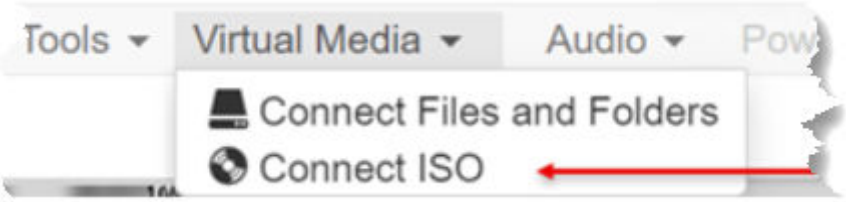
Connect ISO

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.

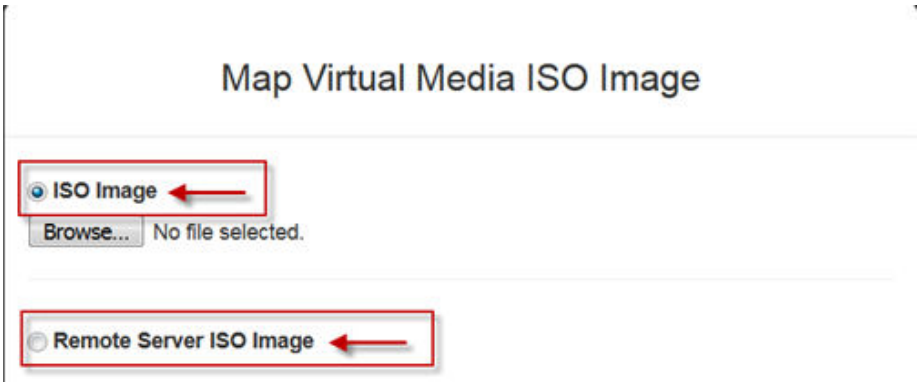
Note: If connection to your SAMBA server is lost while transferring files from your image file to the target, keyboard and mouse control will be lost for several minutes, but will recover.

► *To map virtual media image files:*

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



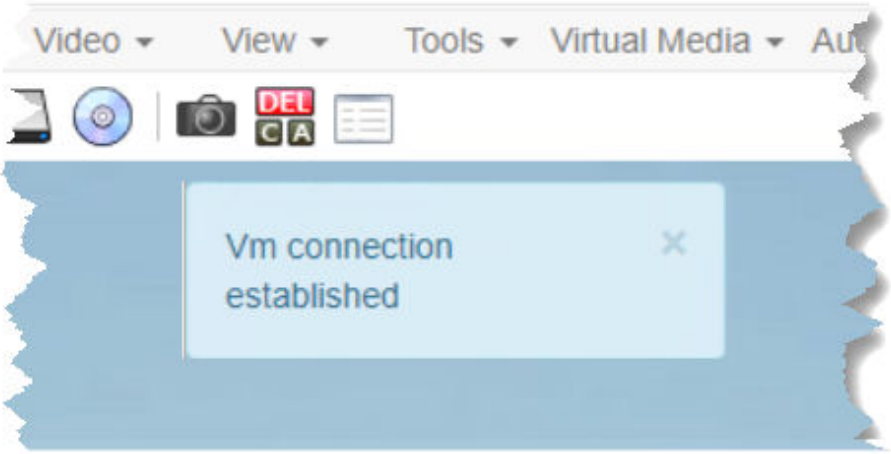
2. Select the option for your file's location:



- 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 Browse button.

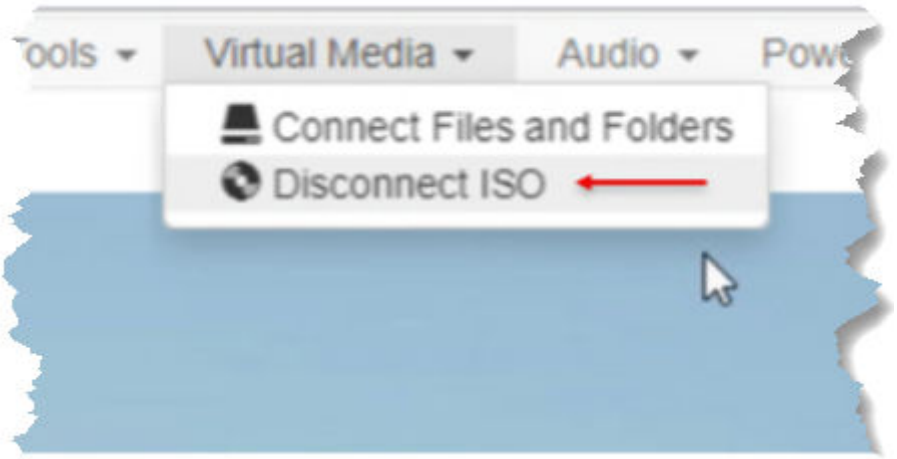
- Select Remote Server ISO Image for ISO files on a remote server. Remote ISO files must be pre-configured by an administrator for the mapping to appear here. See Virtual Media File Server Setup (File Server ISO Images Only). Select the Hostname, then select the image file from the Image list. Enter 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.

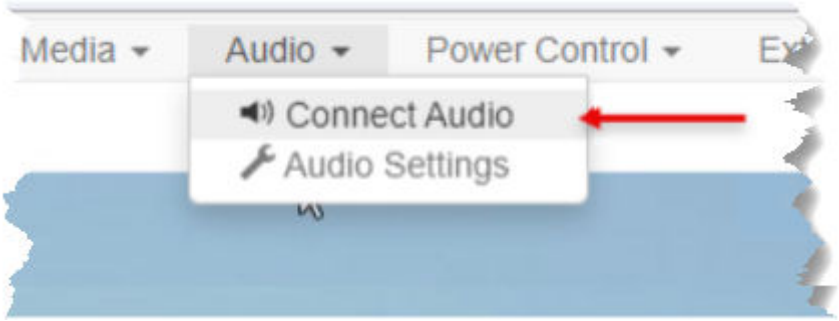
Supported audio sample rates differ depending on your connecting device and browser:

- On Windows Edge - 11,025, 22,050 and 44,100 Hz
- On Mac/Windows and Linux Chrome - 11,025, 22,050 and 44,100 Hz
- On Mac/Windows and Linux Firefox only 44.1 kHz available
- On Mac Safari - only 44.1 kHz available
- On IOS devices - only 44.1 kHz available

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

► *To connect audio:*

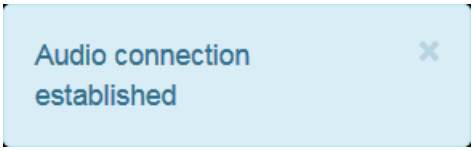
1. Choose Audio > Connect Audio, or click the matching icon in the toolbar.



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

3. Select the Format.

4. Select the "Mount selected playback device automatically on connection to target" checkbox to enable the option. This setting will connect audio automatically the next time you connect to the target.
5. Click OK. A success message appears.



► *To disconnect audio:*

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

Audio Settings

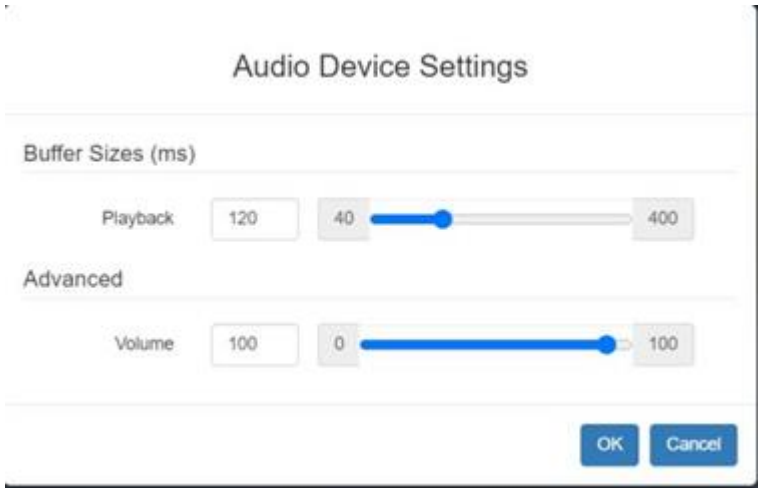
The Audio Settings option is enabled when audio is connected. Use the Audio Settings to set the buffer and volume.

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 (on page 73)

Using HKC on Apple iOS Devices

DKX3G2 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 114).

Install Certificate on Apple iOS Device

You must install a CA-signed certificate on your Apple iOS device before you can connect to DKX3G2. 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".

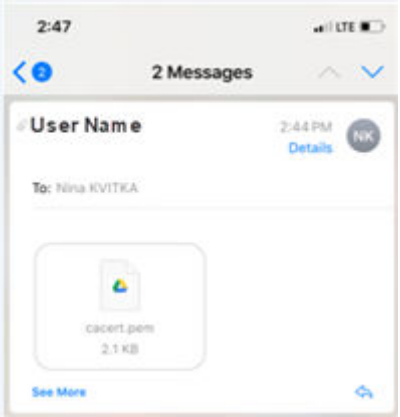
When creating certificates, the certificate Common name should match the IP address/Hostname used to connect to the device.

Install both the DKX3G2 certificate and the CA certificate used to sign the DKX3G2 certificate.

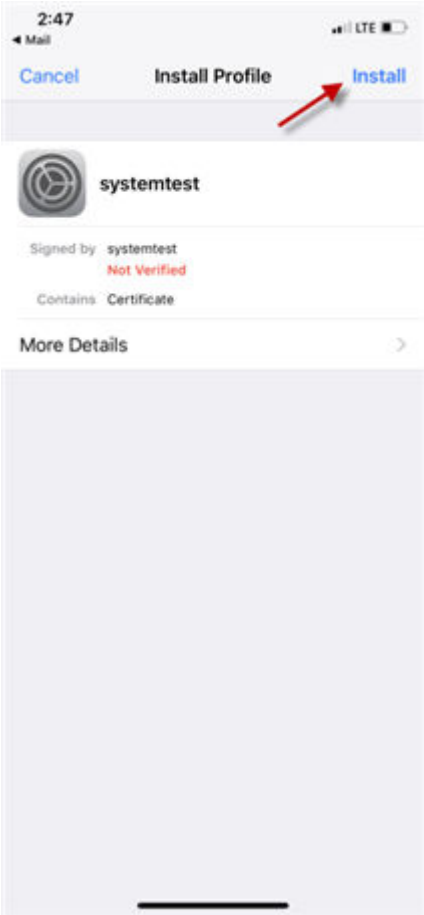
Note: If you have issues launching connections from IOS devices, check that the certificate meets Apple requirements: https://support.apple.com/en-us/HT210176

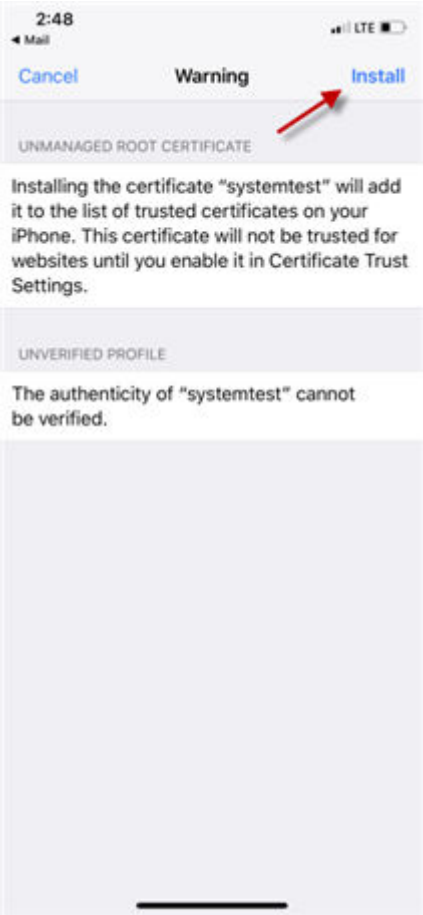
► *To install the certificate on an IOS device:*

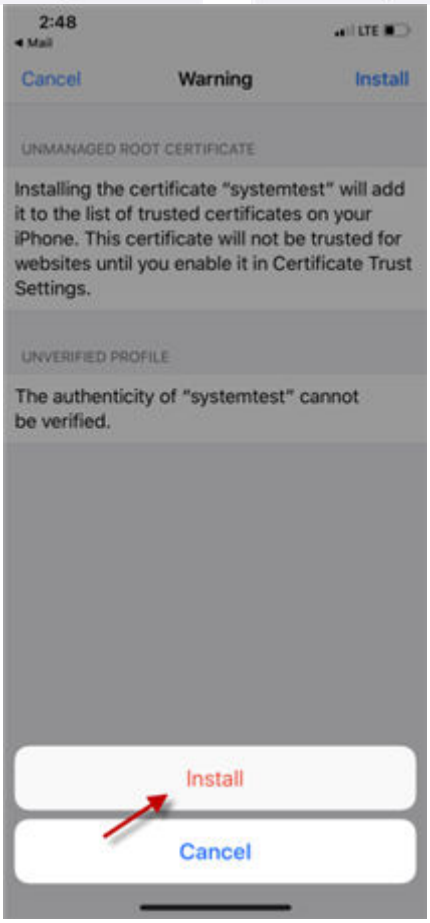
1. Email the certificate file to an email account that can be opened on the iOS device. Open the email and tap the attachment.



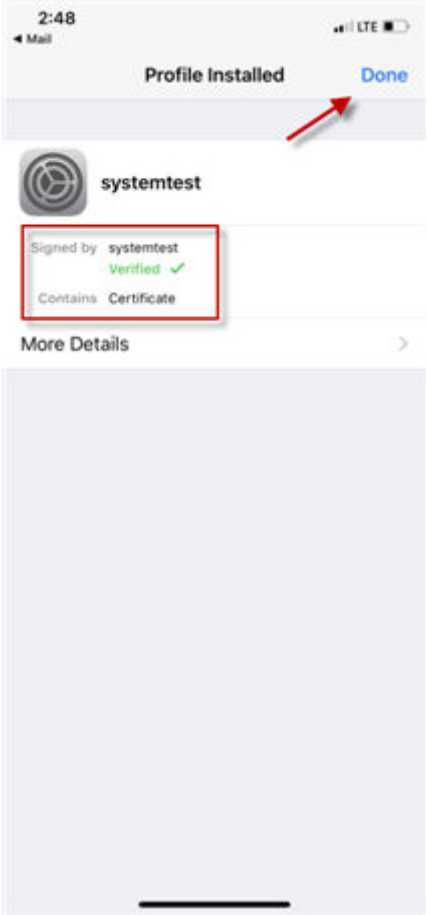
2. The certificate downloads as a "profile" that you have to install. You can have only one profile ready to install at a time. For example, if you download a profile and don't install it, and then download a second profile, only the second profile is available to be installed. If a profile is not installed 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.


2:47
Mail
LTE
Cancel
Install Profile
Install
systemtest
Signed by systemtest
Not Verified
Contains Certificate
More Details

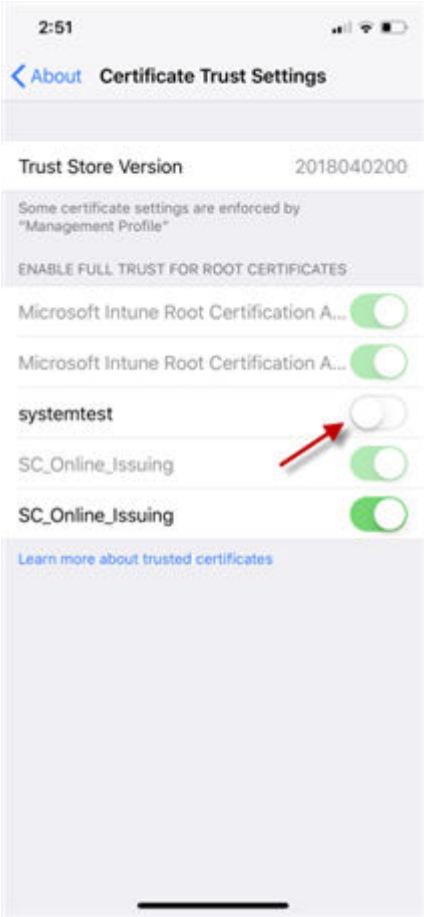

2:48
Mail
LTE
Cancel
Warning
Install
UNMANAGED ROOT CERTIFICATE
Installing the certificate "systemtest" will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.
UNVERIFIED PROFILE
The authenticity of "systemtest" cannot be verified.


2:48
Mail
LTE
Cancel
Warning
Install
UNMANAGED ROOT CERTIFICATE
Installing the certificate "systemtest" will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.
UNVERIFIED PROFILE
The authenticity of "systemtest" cannot be verified.
Install
Cancel

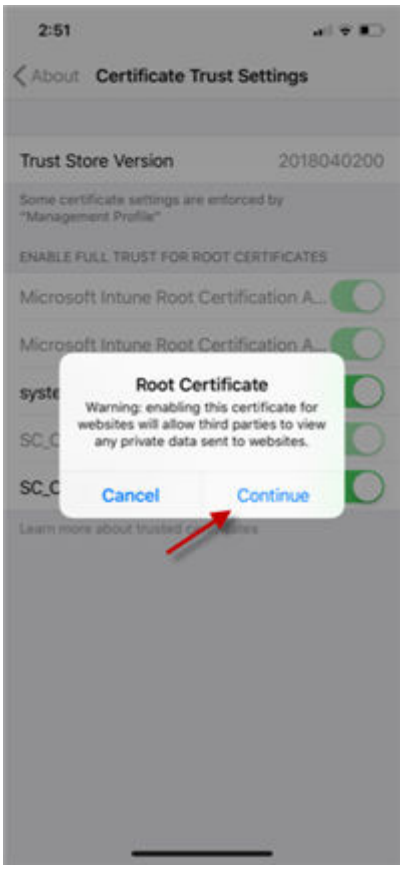
5. When complete the certificate is marked Verified. Tap Done.

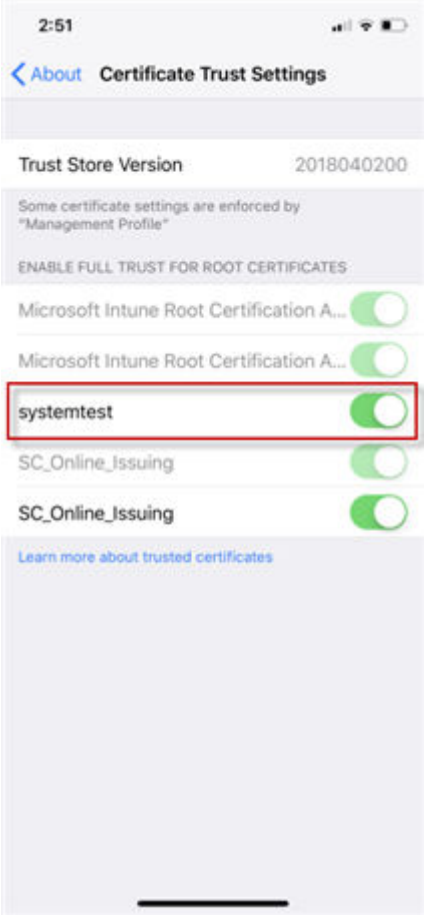


6. To enable the certificate, go to Settings > General > About, then scroll all the way down. Tap Certificate Trust Settings.



7. Tap the certificate that was installed earlier to enable. A warning appears. Tap Continue to enable. The certificate slider displays green for enabled.





Touch Mouse Functions

Use the touchscreen equivalent for each mouse function. Some touch settings are configurable. See: Tools Menu (on page 113).

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 and Import and Export Macros.

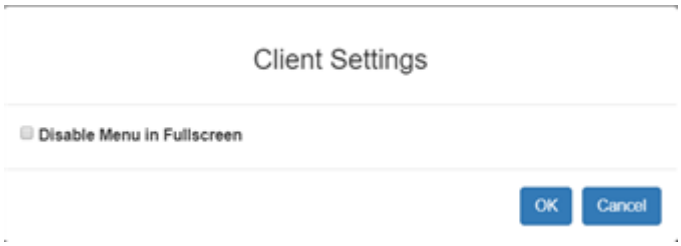
Note: To import macros when using an Apple iOS device, first export the file from HKC using a PC client. Add the file to a Cloud location to access from the IOS device for import.

Tools Menu

The Tools menu contains options for HKC target connection settings.

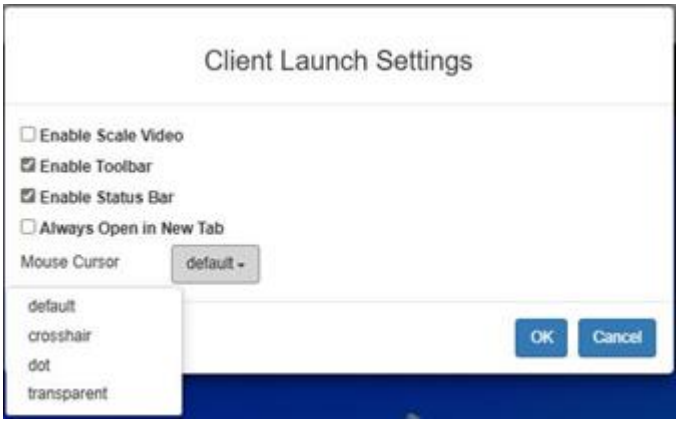
► *Client Settings:*

- 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, Enable Toolbar, Enable Statusbar and Mouse Cursor at target launch.



► *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 112).
- 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

Interface and Navigation

The DKX3G2 Remote Console is web-based graphical user interfaces.

Use the Remote Console interface to configure and manage the DKX3G2 over a network connection.

Use the Local Console interface to access the DKX3G2 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.

In This Chapter

DKX3G2 Remote Console Interface

- The DKX3G2 Remote Console is a browser-based graphical user interface that enables you to log in to and remotely manage targets connected to the DKX3G2. It provides a network connection to your KVM target servers, opening a KVM Client window upon login. In contrast, the DKX3G2 Local Console offers limited functionality, allowing users to connect to the targets and configure network setup.

Overview

When you log in to the DKX3G2 using a network connection, you access the Remote Console. The first page accessed is the Port Access page.

See: Logging In to DKX3G2 (on page 31) and KVM Ports (on page 116)

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

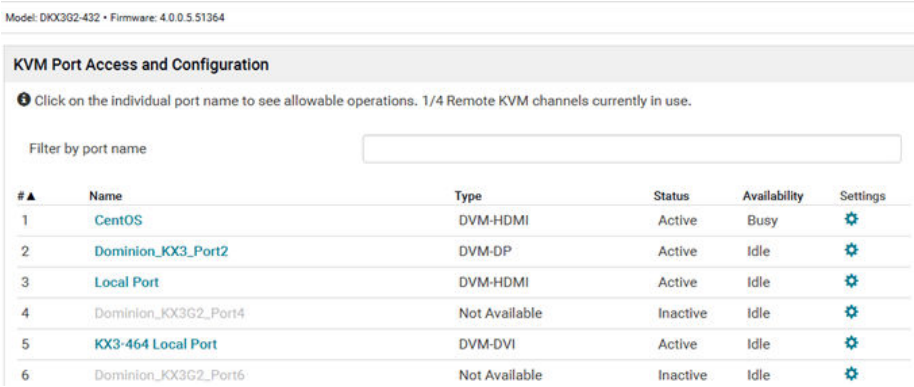
For more in the Remote Console interface elements, see: DKX3G2 Remote Console Interface (on page 116)

KVM Ports

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

Ports connected to KVM target servers are displayed in blue. Left mouse click on any of these ports to open the Port Action menu. For more information, see: Port Action Menu.

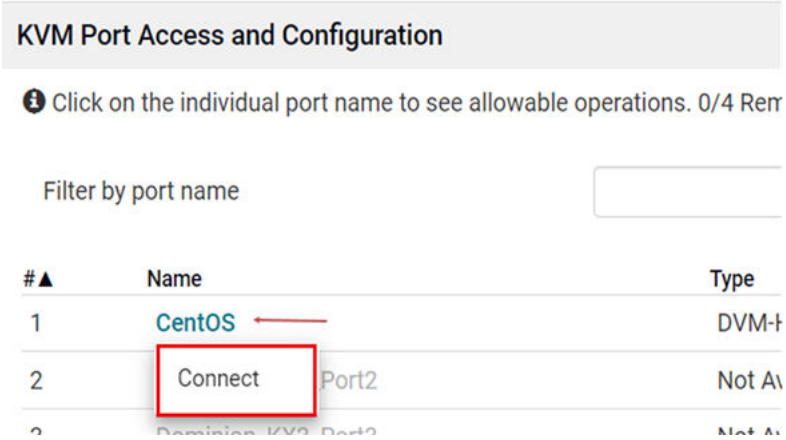
If a DKX3G2 port has no CIM connected or is connected to a CIM with no name, a default port name of Dominion_Model Name_PortNumber is assigned to the port. PortNumber is the number of the DKX3G2 physical port.



You can sort by Port Number, Port Name, Type, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading.

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 DKX3G2 Remote Console, a new KVM Client page appears.
- For the DKX3G2 Local Console, the display switches to the target server, and switches away from the local user interface.
- On the local port, the DKX3G2 Local Console interface must be visible in order to perform the switch.
- Hot key switching is also available from the local port.

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.

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 DKX3G2 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 (on page 73)

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 (on page 73)

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 (on page 73)

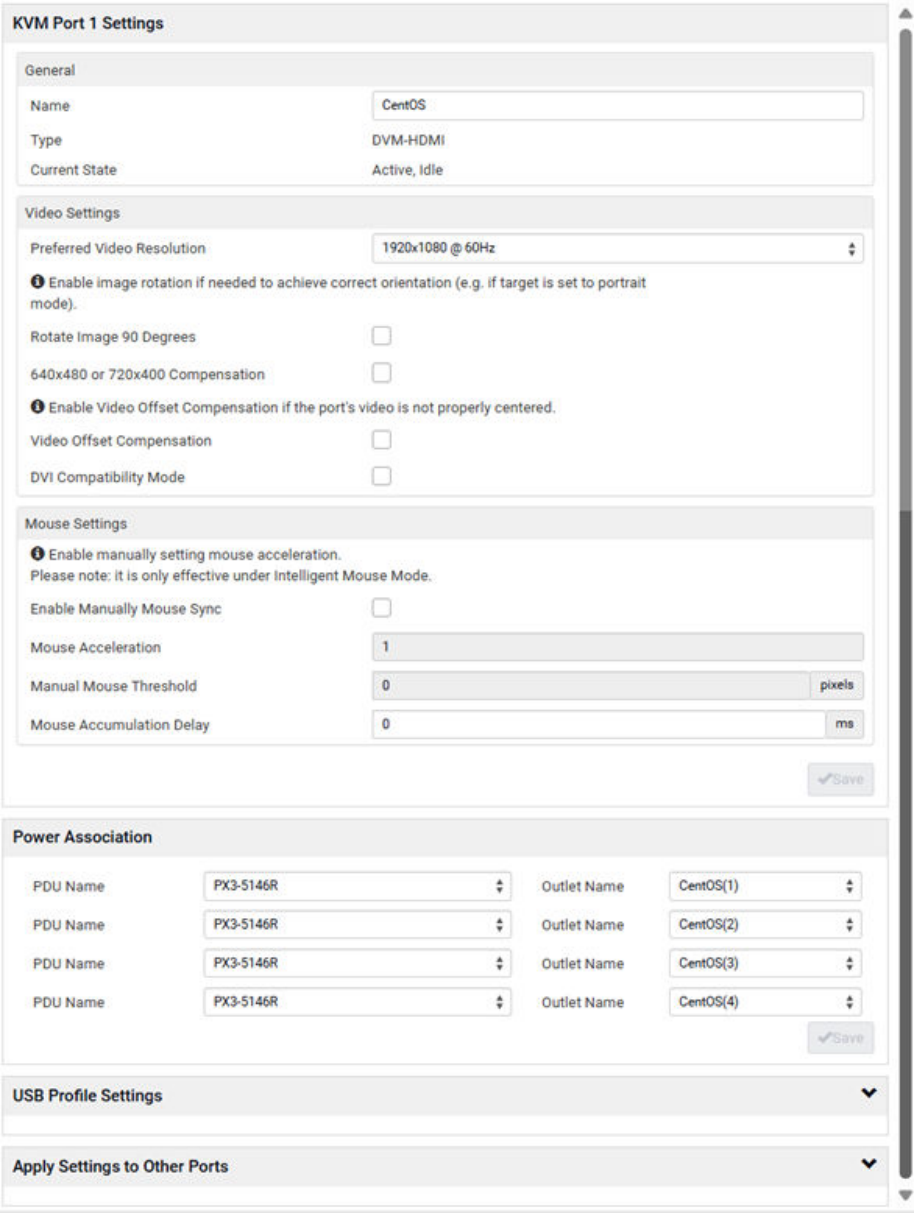
Port Configuration

► *To access a port settings:*

1. Login to the DKX3G2 > select KVM Ports. The KVM Port Access and Configuration Page opens.

This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

2. Click the Settings icon for the port you want to edit.



KVM Port Settings

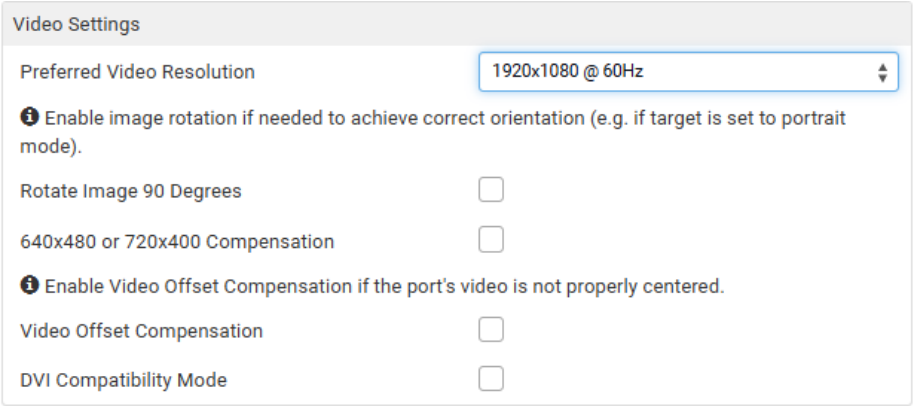
► *KVM Port Settings:*

General Settings:

- To rename the KVM port: enter a new name and click Save.
- View the Type of Port
- View the Current Port Status:
  - Active, Idle
  - Active, Busy: Connected, but PC Share is disabled. See: KVM Security.
  - Active, Connected: Connected, and PC Share is enabled.

Video Settings:

- Select the Preferred Video Resolution: Important! To change the video resolution on the target server, change the Preferred Video Resolution to the new resolution. This should change the resolution when you connect to the target; if not, you can then also change the resolution on the target server.
  - See: Supported Preferred Video Resolutions (on page 121) for a list of all supported resolutions.
- Select Rotate Image 90 Degrees and change the target's display orientation to obtain the proper video orientation between landscape and portrait modes.
- Select 640x480 or 720x400 Compensation if you are experiencing display issues when the target is using this resolution.
- Select Video Offset Compensation if the video appears off center on your target.
- Enable DVI Compatibility Mode for the target server to correct this.

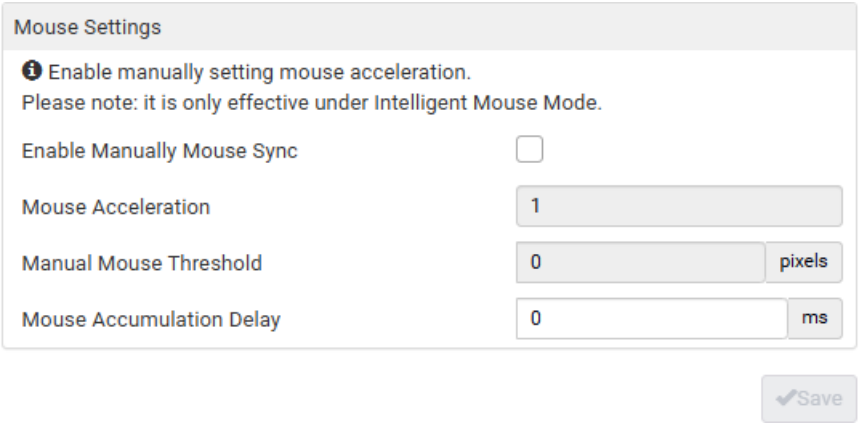


- Click Save to apply all settings.

Mouse Settings

You can manually set mouse parameters which allows mouse sync if mouse cursor is not detected due to target screen color or video noise.

Note: It is only effective under Intelligent Mouse Mode.



- Select Enable Manually Mouse Sync - If this feature is enabled, you can control the mouse sync. By default this setting is disabled.
- Set the Mouse Acceleration value - This value is used to adjust mouse steps. The default setting is 1.00.
- Set Manual Mouse Threshold value - This value is used to control acceleration when mouse movement is bigger than the threshold value. By default this value is set to 0 pixels.
- Set Mouse Accumulation Delay - This value is used to reduce mouse packets if the mouse movements are lagging on the target. The available range is from 0 to 200ms. The default is set to 0 ms.
- Click Save to apply all settings.

Supported Preferred Video Resolutions

Each supported video resolutions it can offer. The server will generally choose the largest resolution and refresh rate that it can support.

- 1024x768 @ 60HZ
- 1024x768 @ 70HZ
- 1152x864 @ 60HZ
- 1280x720 @ 60HZ
- 1280x800 @ 60HZ
- 1280x960 @ 60HZ
- 1280x1024 @ 60HZ
- 1360x768 @ 60HZ
- 1400x1050 @ 60HZ
- 1440x900 @ 60HZ
- 1600x900 @60HZ
- 1600x1200 @60HZ
- 1920x1080 @50HZ
- 1920x1080 @60HZ
- 1920x1200 @60HZ

Port Configuration: Port Power Association

Port association can be done once a power strip is added to the DKX3G2. See: Adding PDUs. You can configure up to four power associations on each target. The outlets may be on the same or different PDUs.

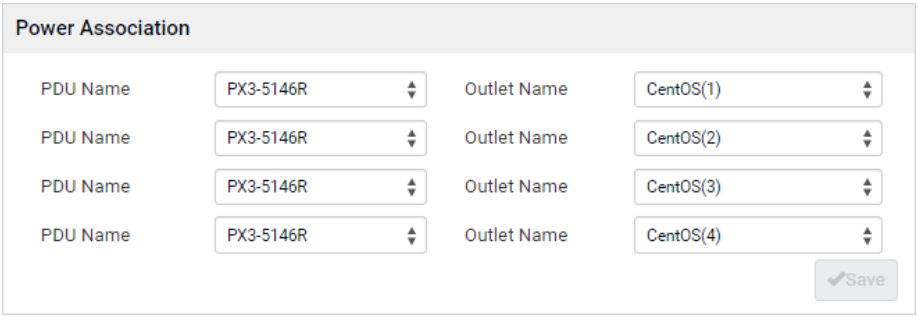
Note: Power association will not be visible if a PDU has not been added to the DKX3G2.

► *To configure Power Associations:*

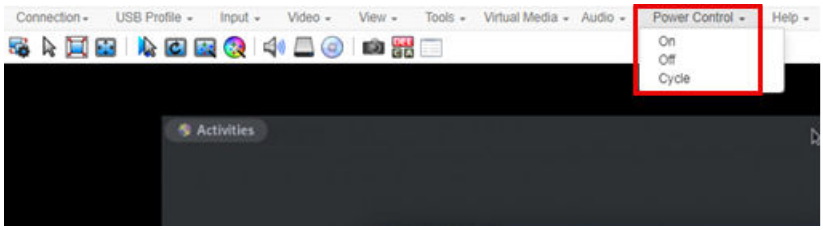
1. Login in to the DKX3G2 > select KVM Ports. The KVM Port Access and Configuration Page opens.

This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

2. Click the Settings icon for the port you want to edit.
3. On Port Settings page scroll down to Power Association.
4. In the PDU Name fields, select from the drop down list of configured PDUs.
5. In the Outlet Name fields, select the outlet from each PDU you want to associate with this target.
6. Leave extra fields blank or select none.
7. Click Save.



8. Once Power Association is saved, you will see power controls on the KVM Port Access page.



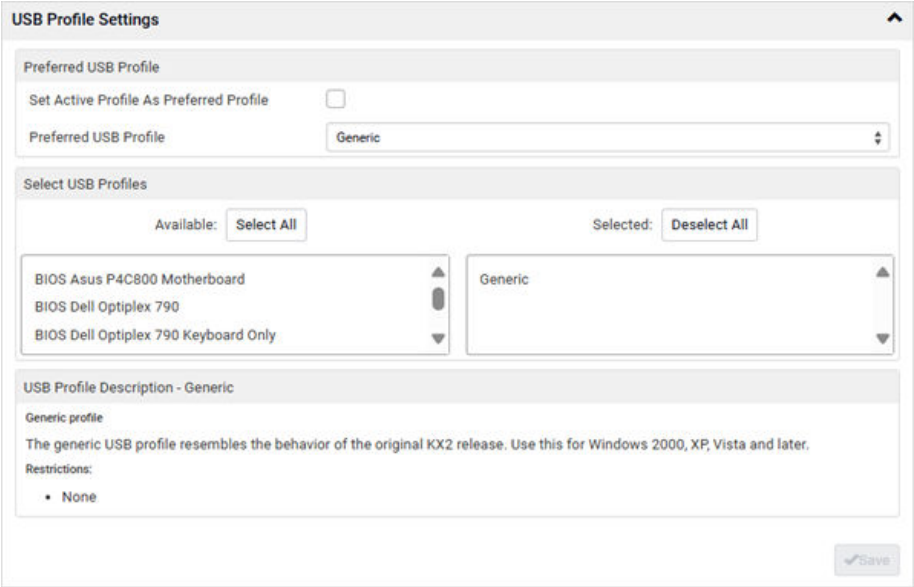
Port Configuration: USB Profile Settings

You can choose the available USB profiles for a port under the Select USB Profiles section. The USB profiles chosen become the profiles available to the user when connecting to a KVM target server from the port. For information about USB profiles, see: USB Profiles.

Note: To set USB profiles for a port, you must have a supported CIM connected with firmware compatible with the current firmware version of the DKX3G2. See: Upgrading CIMs.

The profiles available to assign to a port appear in the Available list on the left. The profiles selected for use with a port appear in the Selected list on the right. When you select a profile in either list, a description of the profile and its use appears in the Profile Description field.

In addition to selecting a set of profiles to make available for a KVM port, you can also specify the preferred profile for the port and apply the settings from one port to other KVM ports.



► *To select the USB profiles for a KVM port:*

1. Login in to the DKX3G2 > select KVM Ports. The KVM Port Access and Configuration Page opens.

This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

2. Click the Settings icon for the port you want to edit.
3. On Port Settings page scroll down to USB Profile Settings.
4. In the Select USB Profiles section, select a USB profile from the Available list and double click to move it to the Selected section. Repeat the same to move others.
5. To select all you can click Select All button. This will move all the available profiles to Selected section.
6. Click Save. The selected profiles appear in the Selected list. These are the profiles that can be used for the KVM target server connected to the port.

► *To specify a preferred USB profile:*

1. If check box Set Active Profile As Preferred Profile is selected, this preferred USB profile is also used as active profile.

► *To remove selected USB profiles:*

1. In the Select USB Profiles for Port section, select a profile from the Selected list , double click. This will move the profile to the Available pane.
2. You can also click Deselect All to remove all the profiles from selected section.
3. Click Save. The selected profiles appear in the Available list. These profiles are no longer available for a KVM target server connected to this port.

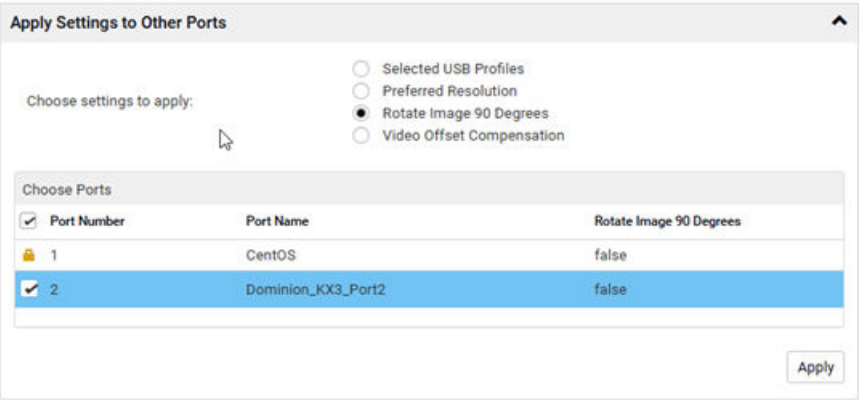
Apply Settings to Other Ports

► *To apply a settings to multiple ports:*

1. In the Apply Settings to Other Ports section,choose one from the following settings:

- Selected USB Profiles
- Preferred Resolution
- Rotate Image 90 Degrees
- Video Offset Compensation

1. To select all KVM ports, click Select All or check the ones you want.
2. Click Apply.

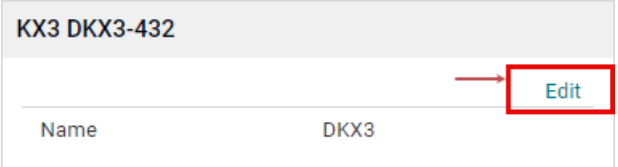


Device Information

Click Device Information to view name, system, and network details about your DKX3G2. In this page you can also rename your device, and view open source license information.

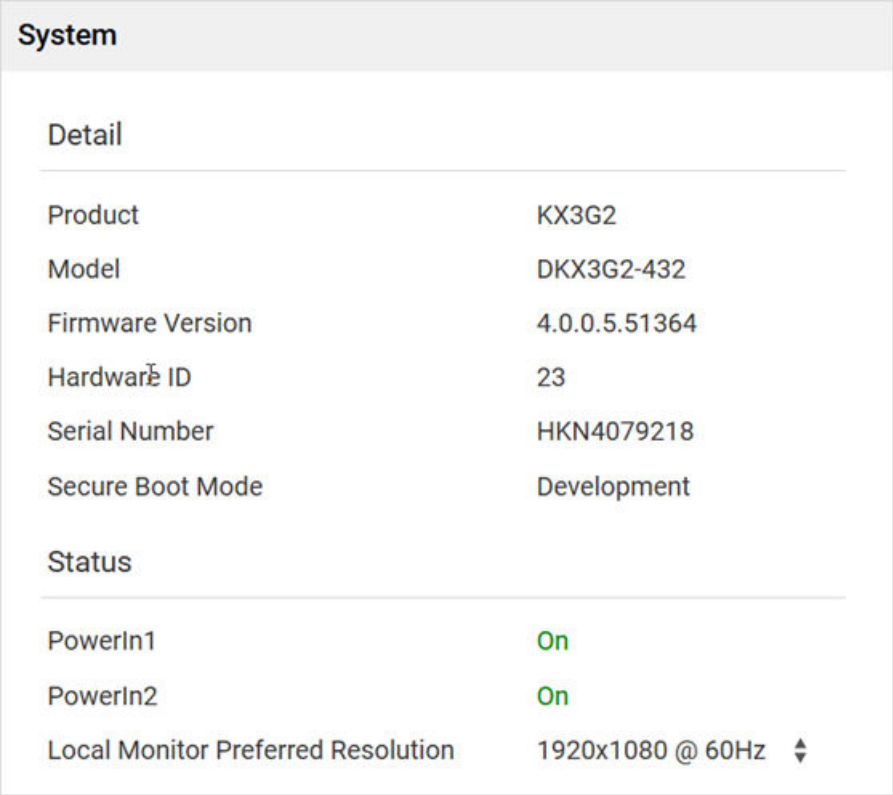
► *To edit your device name:*

- Click Device Information, then click Edit to enter a new name. Click Save.



► *To view system details and status:*

- System Details: View the product name, model, firmware version, hardware ID, and serial number.
- System Status: View the power detection status, and local monitor status.



► *To view network details:*

- View the network details as currently configured: IPv4/IPV6 address, MAC address, Link state, DNS servers, DNS suffixes, DNS resolver preference, IPv4/IPv6 routes, MTU and Authentication state.

Note: DKX3G2 determines LAN port status by physical connection.

Network

Common

DNS servers	192.168.51.22, 192.168.50.109
DNS suffixes	raritan.com
DNS resolver preference	IPv4 address
IPv4 routes	Default via 192.168.53.126 (ETH1) Default via 192.168.62.126 (ETH2) 192.168.53.0/24 dev ETH1 192.168.62.0/23 dev ETH2
IPv6 routes	fd07:2fa:6cff:2020::/64 dev ETH1 fd07:2fa:6cff:2021::/64 dev ETH1 fd07:2fa:6cff:2030::/64 dev ETH2 fe80::/64 dev ETH2 fe80::/64 dev ETH1 Default via fe80::209:fff:fe09:1 (ETH2) Default via fe80::209:fff:fe09:1 (ETH1)

Bond

ETH1

MAC address	00:0d:5d:00:03:38
Link state	1 GBit/s, full duplex, link OK, autonegotiation on
MTU	1500
Authentication state	disabled
IPv4 address	192.168.53.150/24
IPv6 addresses	fd07:2fa:6cff:2020:f53d:d176:bbc1:f5ee (unique local) fe80::92f2:7d4e:69a5:61fb (link local)

ETH2

MAC address	00:0d:5d:00:03:39
Link state	1 GBit/s, full duplex, link OK, autonegotiation on
MTU	1500
Authentication state	disabled
IPv4 address	192.168.63.44/23
IPv6 addresses	fd07:2fa:6cff:2030:d4d6:c749:7fbe:d40e (unique local) fe80::6a7a:5625:af95:4b36 (link local)

► *To view CIM details:*

- When a CIM is attached, view the hardware details: port number name, type, hardware version, firmware version and serial number.

CIM Information

Port	Name	Type	Hardware Version	Firmware Version	Serial Number
1	CentOS	DVM-HDMI	5000	5A9F	HUX2500005

► *To view open source license notification and privacy statement:*

Open Source License Notification

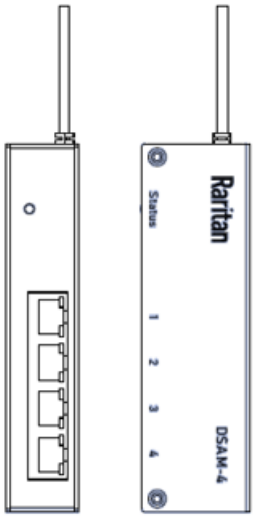
Raritan, Inc. (Raritan) uses Open Source software in some of its products, including software licensed under the GNU General Public License ("GPL"). Most open source packages are used unmodified as binaries, but where required, Raritan has modified the open source package to perform the functions required for the Raritan products. Raritan makes the open source software and any modifications available consistent with the terms of the GPL and LGPL regardless of whether those licenses apply. The code made available by Raritan is for informational purposes only and distributed "As is" with no support and/or warranty of any kind intended, implied, or provided.

For more information, please go to http://www.raritan.com/about-us/legal/open-source-software-statement.

Privacy Statement

https://www.raritan.com/about-us/legal/privacy-statement

Serial Access with Dominion Serial Access (DSAM) Module



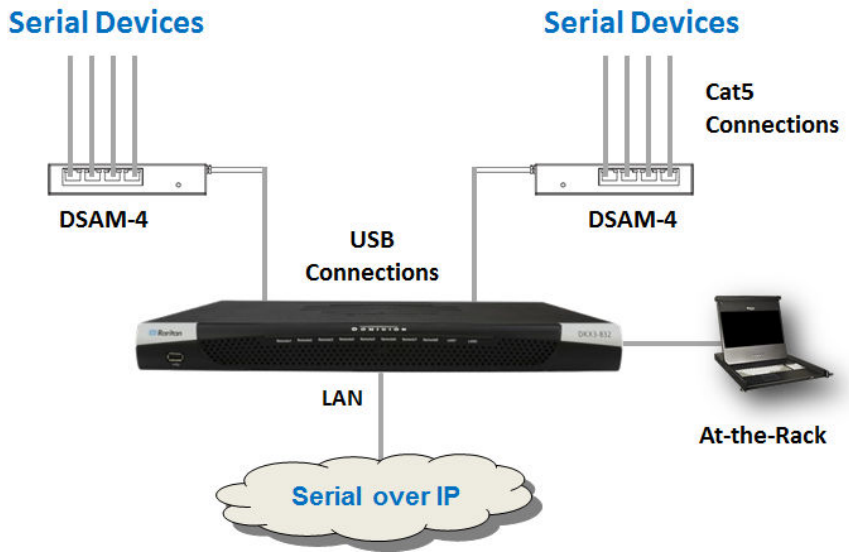
Connecting a DKX3G2 and a Dominion Serial Access Module (DSAM) provides access to devices such as LAN switches and routers that have a RS-232 serial port.

The DSAM is a 2- or 4 port serial module that derives power from the DKX3G2.

Connect a maximum of 2 DSAM modules to the DKX3G2 using USB cables. DSAM can be mounted in a 0U configuration.

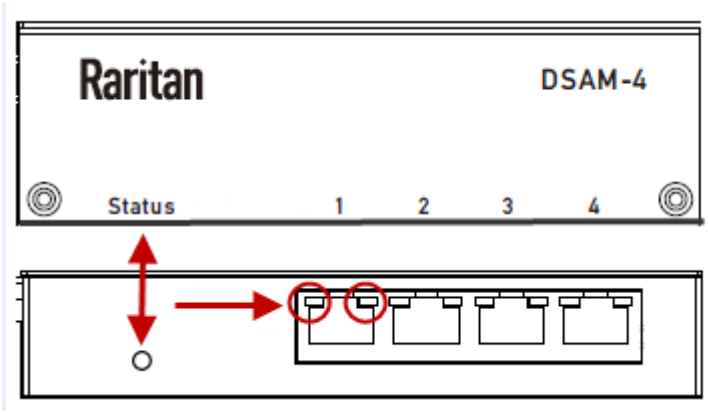
Connect DSAM Device

1. Connect the DSAM unit's USB cable to the TOP USB port on the rear of DKX3G2 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 DKX3G2.
- Blue LED - Slow blink: DSAM controlled by DKX3G2.
- 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

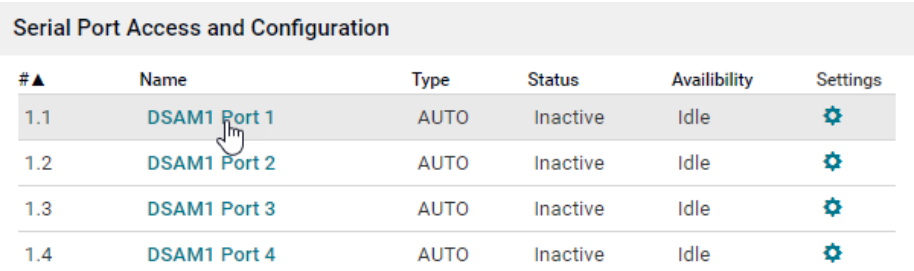
DSAM Serial Ports

When a DSAM unit is connected to the DKX3G2, DSAM Serial Ports is seen on the menu options.

► *To access Serial Ports:*

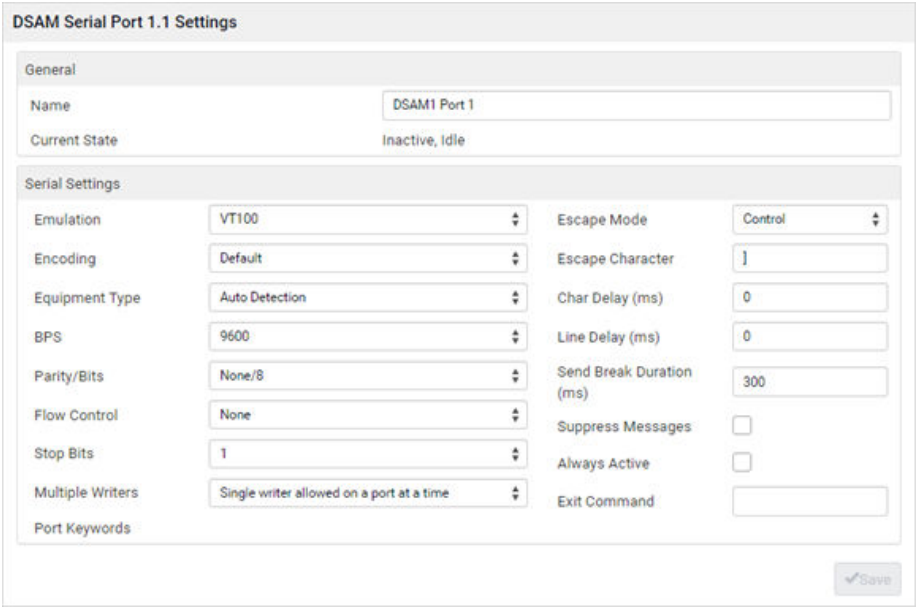
1. Login in to the DKX3G2 > select DSAM Serial Ports. The Serial Port Access and Configuration Page opens.

This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.



► *To configure Serial Port Settings*

1. Click the Settings icon for the port you want to edit.
2. DSAM Serial Port settings page appears.



3. 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
4. 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
   - 8BIT-ASCII
   - ISO8859-1
   - ISO8859-15
   - UTF-8
   - Shift-JIS
   - EUC-JP
   - EUC-KR
5. In the Equipment Type field, indicate whether you want the DKX3G2 to automatically detect a physical connection to the target. The default is Auto Detection.

Force DTE causes DKX3G2 to act as a piece of data terminal detection equipment to detect targets connected to it.

Force DCE causes DKX3G2 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. DKX3G2 does not support autodetection of both DCE and DTE on the same port.

---

6. 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
7. Select the Parity/Bits from the Parity Bits drop-down menu.
8. Select the Flow Control from the Flow Control drop-down menu.
9. Select the Stop Bits from the Stop Bits drop-down menu.
10. 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.
11. To configure the delay between when lines of text are sent via the port, enter it in the Line Delay field.
12. Configure the sendbreak duration by entering the send break time in the Send Break Duration field. The send break is configurable from 0ms - 1000ms.
13. Select an option to allow single or multiple writers on a port at one time in the Multiple Writers field.
14. 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 .

---

15. If you do not want messages displayed to users connecting to DKX3G2 via Direct Port Access, select the Suppress Message checkbox.
16. 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.

17. Type the character in the Escape Character field. The default for the DKX3G2 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.

18. 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.

19. Click OK.

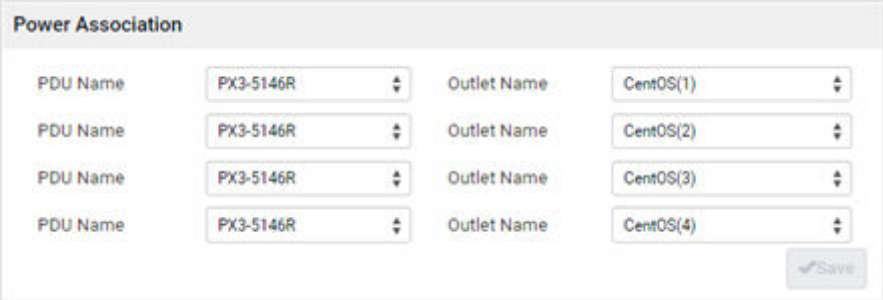
Power Association

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 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.

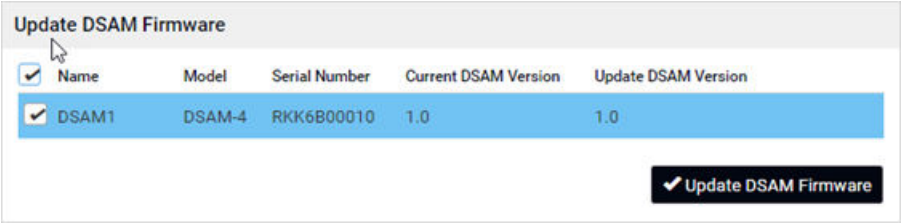
Click OK.

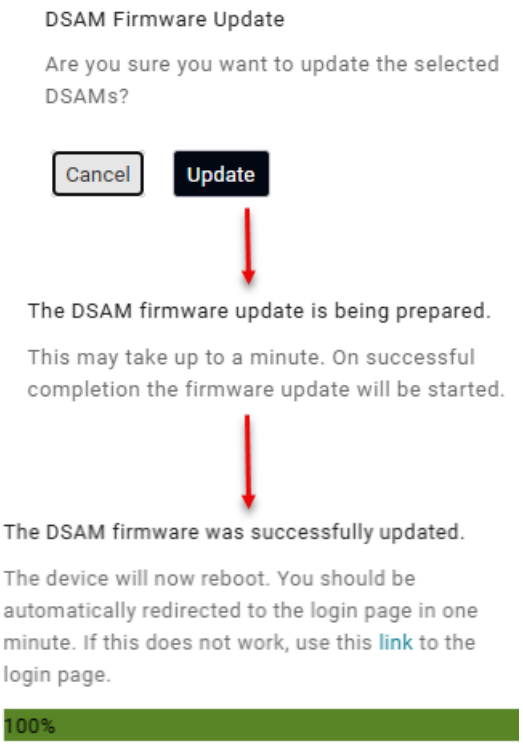
Update DSAM Firmware

DSAM firmware is upgraded automatically during DKX3G2 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 >Update DSAM Firmware.
2. Select the checkboxes for the DSAM units you want to upgrade to the Upgrade DSAM Version listed.
3. Click update DSAM Firmware, then click Update to confirm. A progress message appears.
4. When firmware upgrade completes, a success message appears and the device automatically reboots.





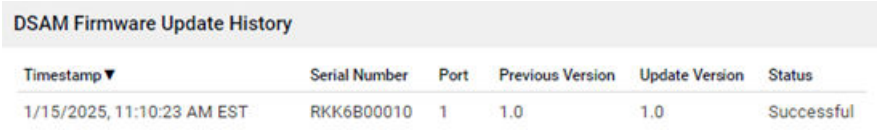
DSAM Firmware History

The DKX3G2 provides information about upgrades performed.

► *To view the DSAM firmware update history:*

- Choose Maintenance > DSAM Firmware History. The DSAM Firmware Update History page opens. Each firmware update event consists of:

- Update date and time
- Serial Number of DSAM
- Port where DSAM is connected
- Previous firmware version
- Update firmware version
- Status



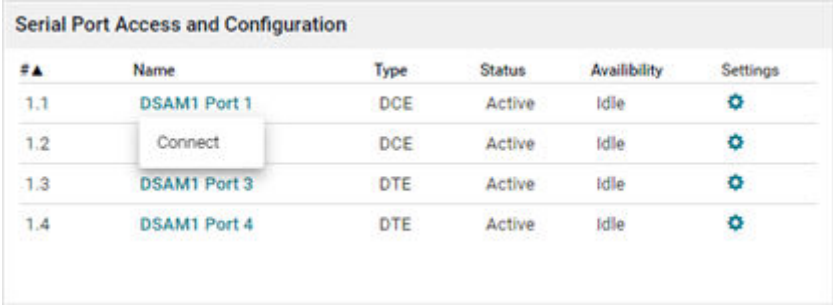
DSAM Firmware Update History

Timestamp ▼	Serial Number	Port	Previous Version	Update Version	Status
1/15/2025, 11:10:23 AM EST	RKK6B00010	1	1.0	1.0	Successful

Connect DSAM Serial Targets

► *To connect to DSAM serial targets:*

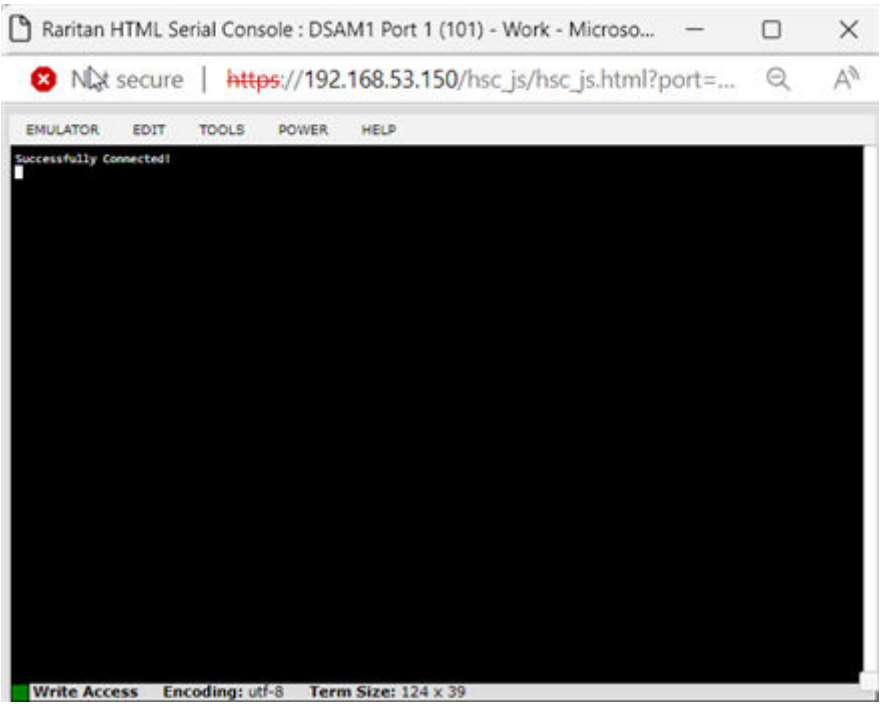
1. In the Port Access page, click the View By Serial tab to view the serial targets.
2. Click the port name you want to connect to. Click Connect.



Serial Port Access and Configuration

# ▲	Name	Type	Status	Availibility	Settings
1.1	DSAM1 Port 1	DCE	Active	Idle	
1.2	Connect	DCE	Active	Idle	
1.3	DSAM1 Port 3	DTE	Active	Idle	
1.4	DSAM1 Port 4	DTE	Active	Idle	

3. The HTML Serial Console (HSC) window opens. See: HTML Serial Console (HSC) Help (on page 136)



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 > Network Services > SSH, then select the Enable SSH checkbox.
2. Launch SSH client in client PC to connect to DKX3G2.
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.

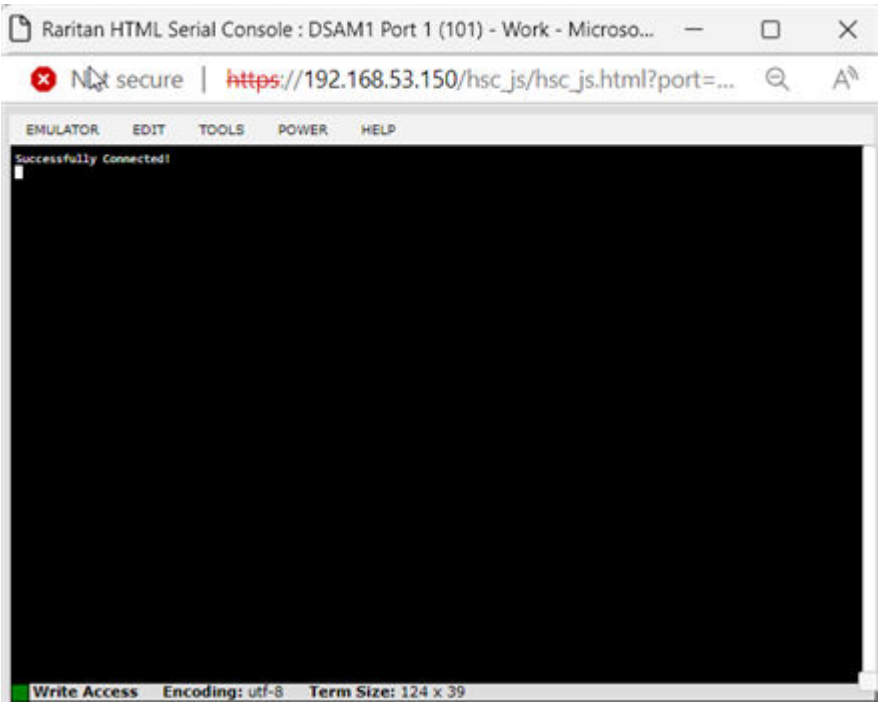
Browser Tips for HSC

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.

HTML Serial Console (HSC) Help

You can connect to serial targets using HSC. HSC is supported with several Raritan products that offer serial connections. Not all products support all HSC features. Differences are noted.

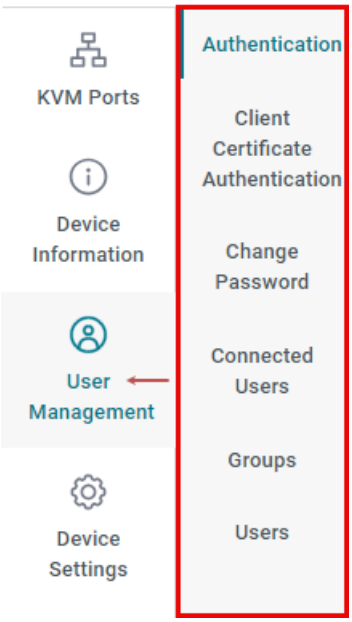


User Management

DKX3G2 can be configured for local or remote authentication. To prepare for configuring external authentication, see: Gathering LDAP/Radius Information (on page 138).

DKX3G2 is shipped with one built-in administrator account: admin, which is ideal for initial login and system administration. You cannot delete 'admin' or change its permissions, but you can change the username and password. For other security settings related to user management, see: Security.

Click User Management to view the submenu options.



Gathering LDAP/Radius Information

You must have the following information about your authentication and authorization (AA) server settings to configure external authentication. See: LDAP Configuration. If you are not familiar with these settings, consult your AA server administrator for help.

► *LDAP authentication:*

- The IP address or hostname of the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*
    - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- The required type of LDAP Security (None, TLS, StartTLS).
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)
- If the Group lookup using memberOf attribute is not selected, use following additional filters for group search.

- Group member attribute
- Group entry object class
- Group search subfilter

► *Radius authentication:*

- The IP address or host name of the Radius server
- The type of Radius Authentication used by the Radius server (PAP, CHAP or MS CHAPV2)
- Shared secret for a secure communication
- UDP authentication port and accounting port used by the Radius server

Configuring Authentication

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

The DKX3G2 supports :

- Local user database on the DKX3G2
- LDAP
- Radius

By default, the DKX3G2 is configured for local authentication. If you use this method, you only need to create user accounts.

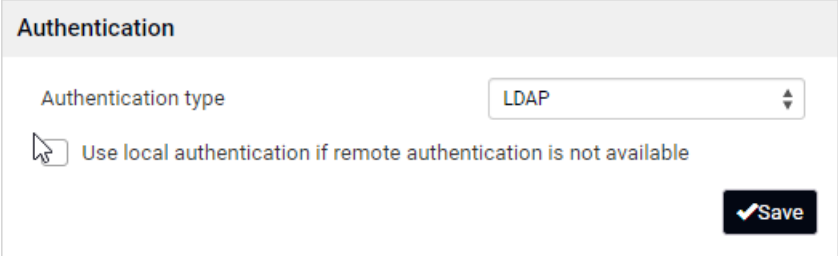
If you prefer external authentication, you must provide the DKX3G2 with information about the external Authentication and Authorization (AA) server.

If you would like local authentication to be available as a backup method when external authentication is not available, create user accounts on the DKX3G2 in addition to providing the external AA server data. Note that local and external authentication cannot be used simultaneously. When configured for external authentication, all DKX3G2 users must have an account on the external AA server. Local-authentication-only users will have no access when external authentication is enabled, except for the admin, who can always access the DKX3G2.

► *To select authentication type:*

1. Click User Management > Authentication.
2. Select Authentication Type:
   - Local
   - LDAP
   - Radius
3. Select the "Use Local authentication when Remote Authentication is not available" checkbox to allow local authentication as a backup method when external authentication is not available, such as when the server is down.
4. Click Save. The authentication type is enabled.

For help with adding your external servers, see: LDAP Authentication (on page 140) and Radius Authentication (on page 146). For help with adding users, see: Users and Groups.



LDAP Authentication

Gather the information you need to add your LDAP servers to DKX3G2. For help, see: Gathering LDAP/ Radius Information (on page 138).

► *To add LDAP servers:*

1. Click User Management > Authentication.
2. Select LDAP as authentication type and LDAP server section becomes available.
3. In the LDAP section, click New. Enter your LDAP details.

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your LDAP/LDAPS server. • Without encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if encryption is enabled.
Copy settings from existing LDAP server	This checkbox appears only when there are existing AA server settings on the DKX3G2. To duplicate any existing AA server's settings, refer to the duplicating procedure below.
Type of LDAP Server	Choose one of the following options: • OpenLDAP • Microsoft Active Directory. .
Security	Determine whether you would like to use TLS encryption, which allows the DKX3G2 to communicate securely with the LDAPS server. Three options are available: • StartTLS • TLS • None
Port (None/ StartTLS)	• The default Port is 389, or specify another port.
Port (TLS)	Configurable only when "TLS" is selected in the Security field. The default port is 636, or specify another port.

Field/setting	Description
Enable verification of LDAP Server Certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the DKX3G2 prior to the connection. If the certificate validation fails, the connection is refused.
CA Certificate	Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click Browse to select and install the certificate file. • Click Show to view the installed certificate's content. • Click Remove to delete the installed certificate if it is inappropriate. *Note: If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.*
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous Bind	Use this checkbox to enable or disable anonymous bind. • To use anonymous bind, select this checkbox. • When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
Bind DN	Required after deselecting the Anonymous Bind checkbox. Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind Password, Confirm Bind Password	Required after deselecting the Anonymous Bind checkbox. Enter the Bind password.
Base DN for Search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. • Example: `ou=dev,dc=example,dc=com`
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. • Usually it is the `uid`.
User Entry Object Class	The object class for user entries. • Usually it is `inetOrgPerson`.
User Search Subfilter	Search criteria for finding LDAP user objects within the directory tree.
Group lookup using memberOf attribute	Use this checkbox to enable or disable group lookup. • Based on memberOf attribute group will be find.

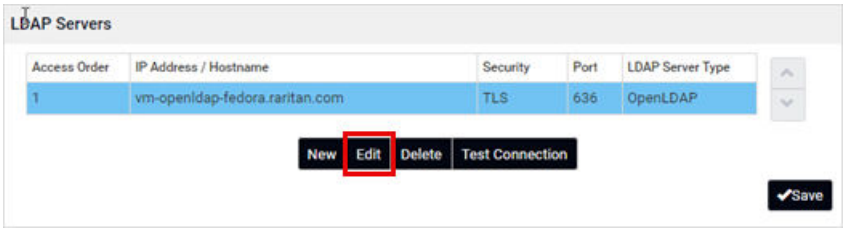
Field/setting	Description
Group Member Attribute	Group attribute that contains DNs of member users (only if memberOf is not used).
Group entry object class	Object class denoting group objects (only if memberOf is not used).
Group search subfilter	Additional filter to lookup group objects (only if memberOf is not used).
Active Directory Domain	The name of the Active Directory Domain. • Example: `testldap.com`

4. Click Test Connection to check if DKX3G2 can connect with the server.
5. Click Add Server. The new LDAP server is listed on the Authentication page. To add more servers, repeat the same steps. If you have multiple servers, use the arrow buttons to set their order, then click Save.
6. To start using these settings, make sure LDAP is selected and saved in the Authentication Type field. See: Configuring Authentication.

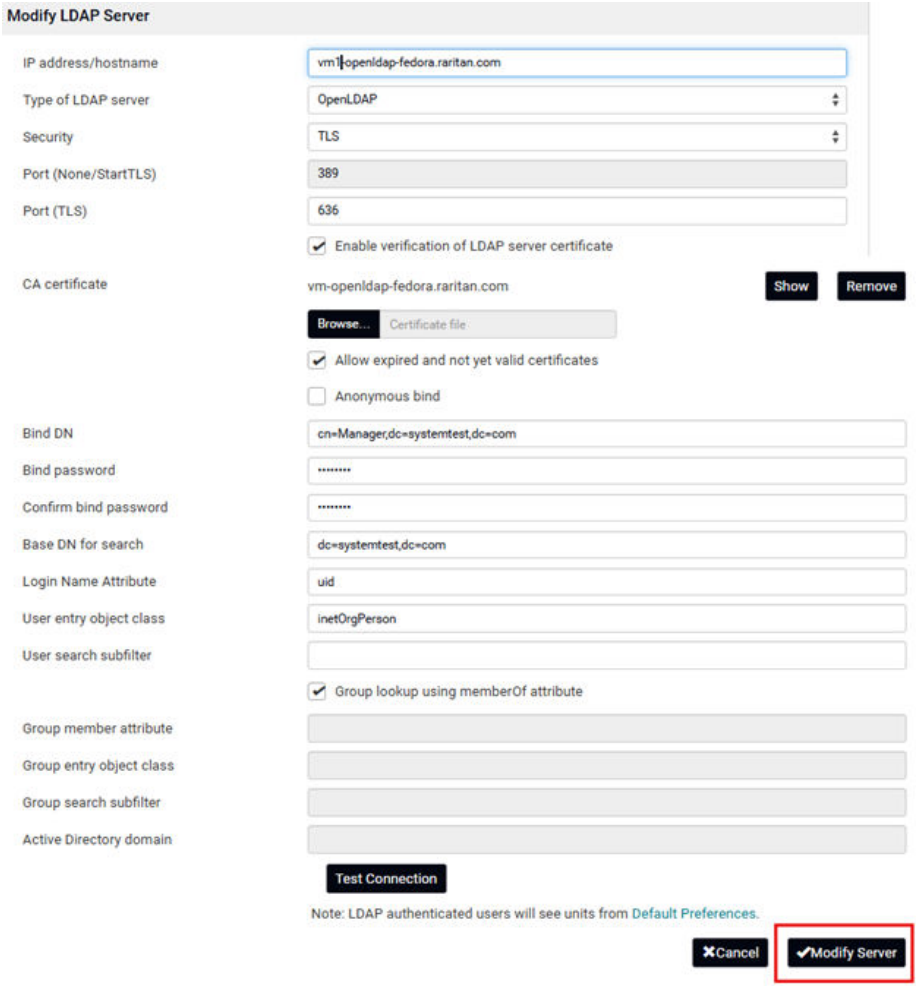
Edit and Delete LDAP Server

► *To Edit LDAP server:*

1. Click User Management > Authentication.
2. Select LDAP server to modify.
3. Click Edit.

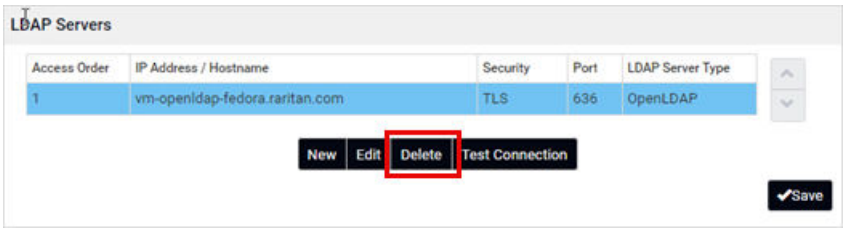


4. Modify LDAP Server opens up.
5. Make updates and click Modify Server.
6. Click Save to confirm.

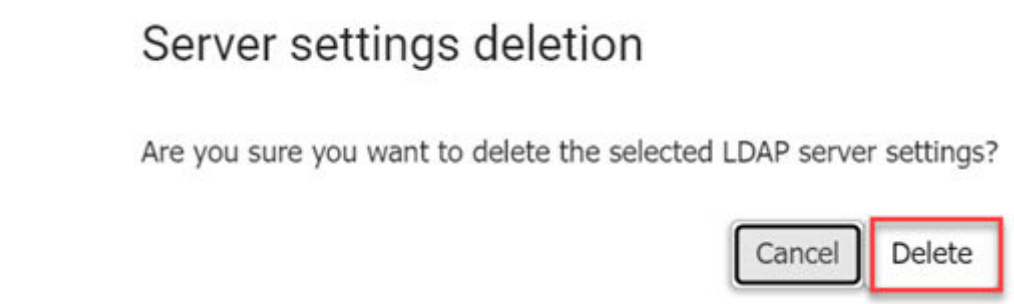


► *To Delete LDAP servers:*

1. Click User Management > Authentication.
2. Select LDAP server to delete.
3. Click Delete.



4. Click Delete to confirm.
5. Click Save to finalize the changes.



Configure Group on the DKX3G2

A group on the DKX3G2 determines the permissions. You must create the groups whose names are identical to the user groups created for the DKX3G2 on the AD server or authorization will fail. See: Configure User Groups on the AD Server. Therefore, we will create the groups named *KX_User* and *KX_Admin* on the DKX3G2. In this example, we will create two user groups with different permissions. Each group will consist of two user accounts available on the AD server.

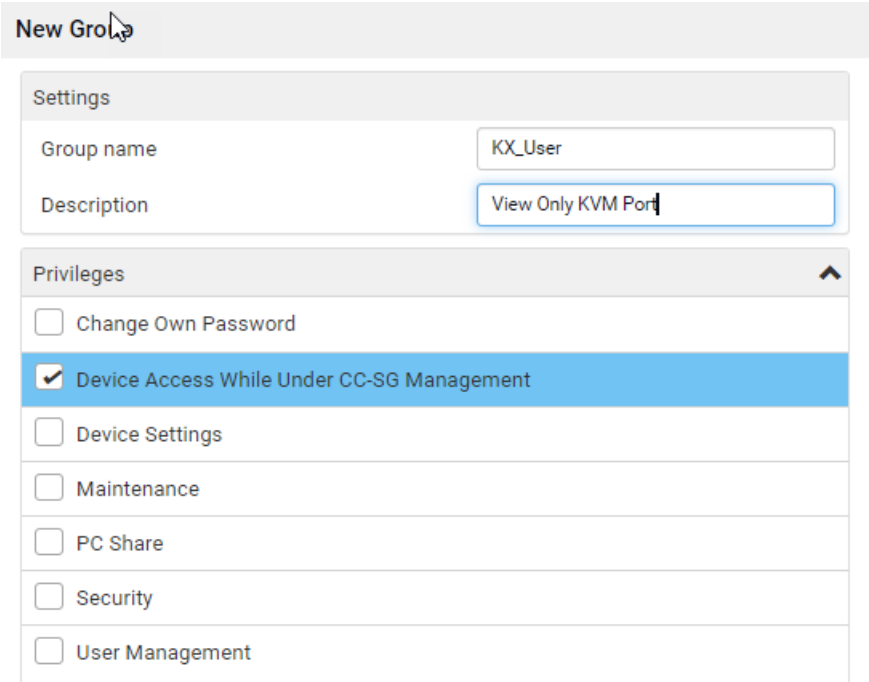
User group	User accounts (members)
KX_User	usera
	kxuser2
KX_Admin	userb
	kxuser

Group permissions:

- The KX_User group will have only view permission to kvm port.
- The KX_Admin group will have full privileges and all the permissions to the kvm port.

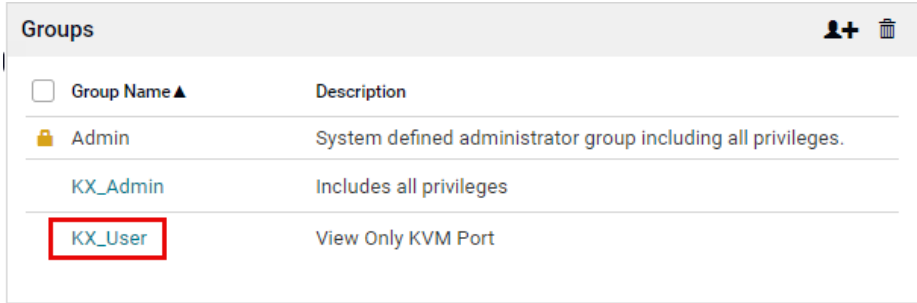
► *To create the KX_User group with appropriate permissions assigned:*

1. Choose User Management > Groups.
2. Click  to add a new group.
   a. Type KX_User in the Group Name field.
   b. Type a description for the KX_User group in the Description field. In this example, we type "View Only KVM Port" to describe the group.
   c. In the Privileges list, select Device Access While Under CC-SG Management. This will allow user to view the KVM port even when the device is under CC-SG control.



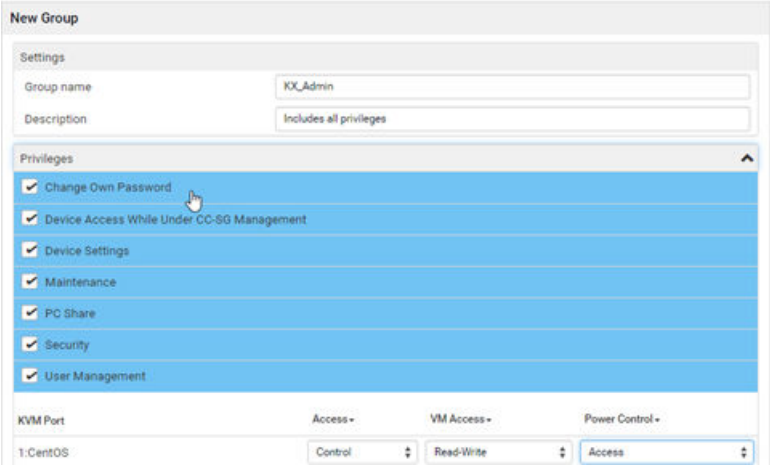
d. Click Save.

3. The KX_User group is created.



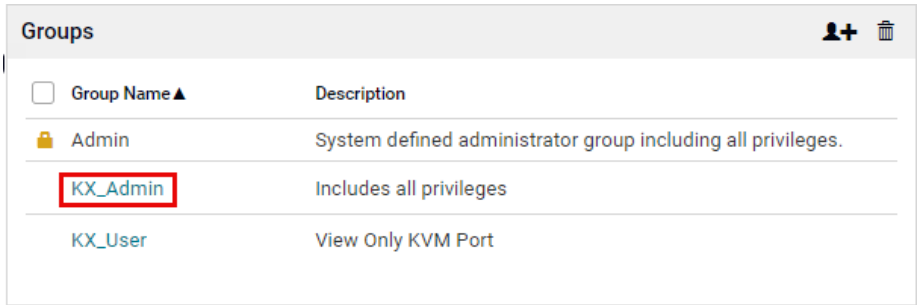
► *To create the KX_Admin group with full permissions assigned:*

1. Click  to add another group.
   a. Type KX_Admin in the Group Name field.
   b. Type a description for te KX_Admin group in the Description field. In this example, we type "Includes all privileges" to describe the group.
   c. In the Privileges list, select all Privileges. This allows users to configure or change DKX3G2 settings.
   d. For KVM Port give full Control Access, Read-Write VM Access, and full Power Control.



e. Click Save.

2. The KX_Admin group is created.



Radius Authentication

Gather the information you need to add your Radius servers to DKX3G2. For help, see: Gathering LDAP/Radius Information (on page 138).

Note: All authentication methods are insecure. It is strongly recommended to use RADIUS only in a secure networking environment. A warning displays for all methods.

► *To add Radius servers:*

1. Click User Management > Authentication.
2. Select Radius in Authentication type section, click New. Enter your Radius details.

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your Radius server.

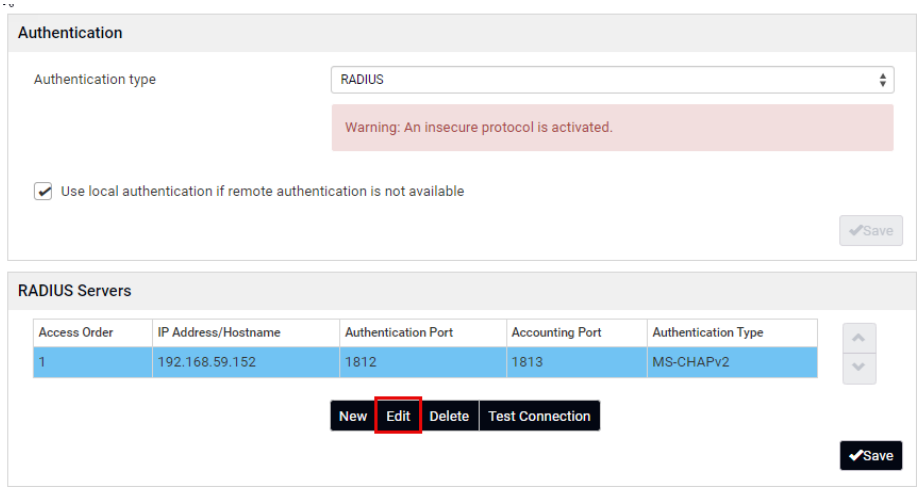
Field/setting	Description
Type of RADIUS Authentication	Select an authentication protocol. • PAP (Password Authentication Protocol) • MS-CHAP v2 (Microsoft's Point-to-Point Tunneling Protocol) • CHAP (Challenge Handshake Authentication Protocol) CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.
Authentication Port, Accounting Port	The defaults are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared Secret, Confirm Shared Secret	The shared secret is necessary to protect communication with the Radius server.
Message Authenticator attribute	This enables the Message-Authenticator attribute in Access-Request replies

3. Click Test Connection to check if DKX3G2 can connect with the server.
4. Click Add Server. The new Radius server is listed on the Authentication page. To add more servers, repeat the same steps. If you have multiple servers, use the arrow buttons to set their order, then click Save.
5. To start using these settings, make sure Radius is selected and saved in the Authentication Type field. See: Configuring Authentication.

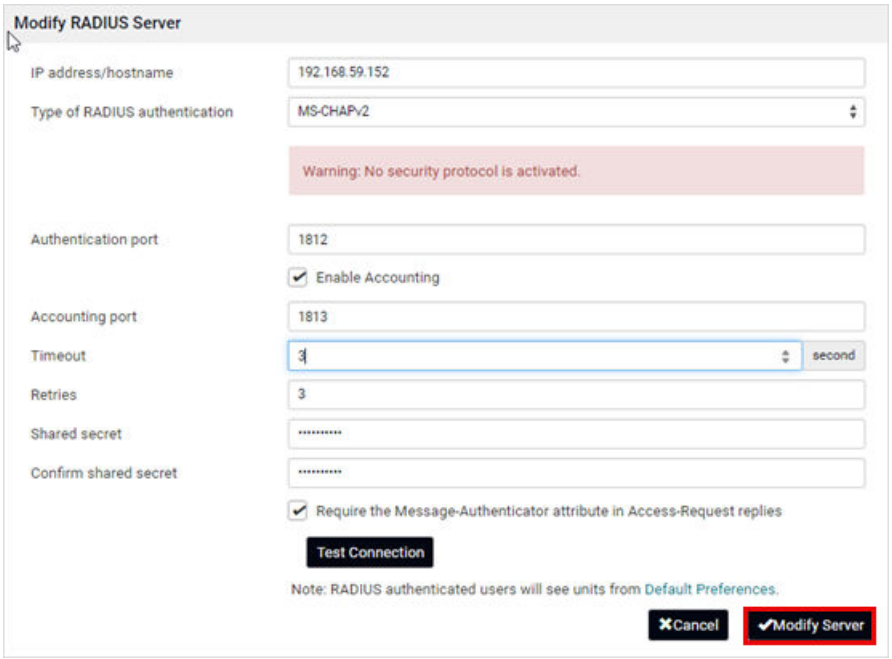
Edit and Delete Radius Server

► *To Edit Radius server:*

1. Click User Management > Authentication.
2. Select Radius server to modify.
3. Click Edit.

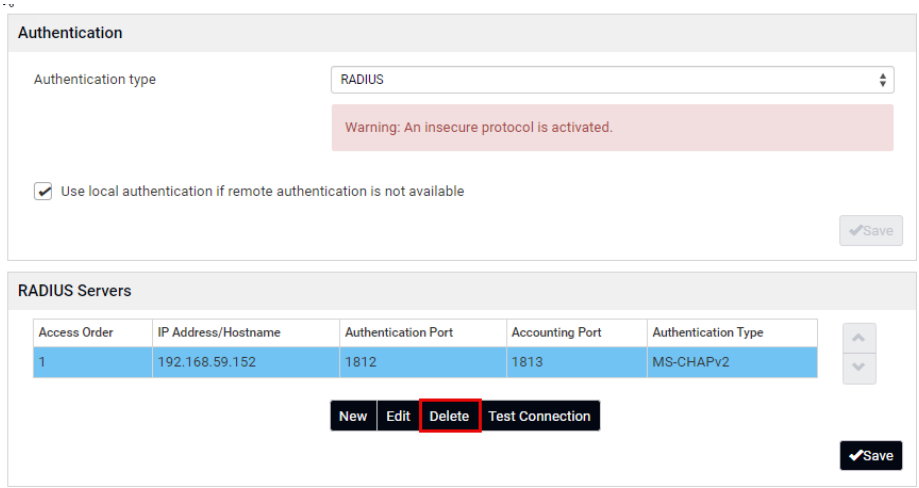


4. Modify Radius Server opens up.
5. Make updates and click Modify Server.
6. Click Save to finalize the changes.

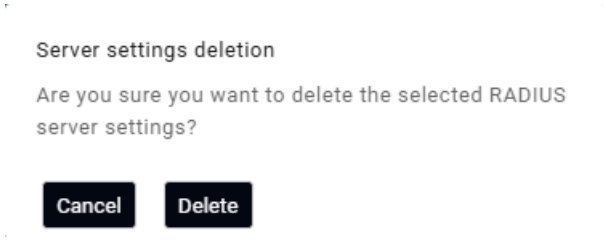


► *To Delete Radius servers:*

1. Click User Management > Authentication.
2. Select Radius server to delete.
3. Click Delete.



4. Click Delete to confirm.
5. Click Save to finalize the changes.



Returning User Group Information via RADIUS

`Raritan:G{GROUP_NAME}`

When a RADIUS authentication attempt succeeds, the DKX3G2 determines the permissions for a given user based on the permissions of the user's group.

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS FILTER-ID. The FILTER-ID should be formatted as follows: Raritan:G{*GROUP_NAME*} where *GROUP_NAME* is a string denoting the name of the group to which the user belongs.

RADIUS Using RSA SecurID Hardware Tokens

DKX3G2 supports RSA SecurID Hardware Tokens used with a RADIUS server for two factor authentication

Users will specify their RADIUS password followed by the token ID without a delimiter between.

► *For example:*

- password = apple
- token = 1234
- User enters: apple1234

Or, configure the RADIUS server to use only hardware token and no passwords. Users will specify the token ID only.

Disabling External Authentication

► *To disable external authentication:*

1. Click User Management > Authentication.
2. In the Authentication Type, select Local.
3. Click Save.

Client Certificate Authentication

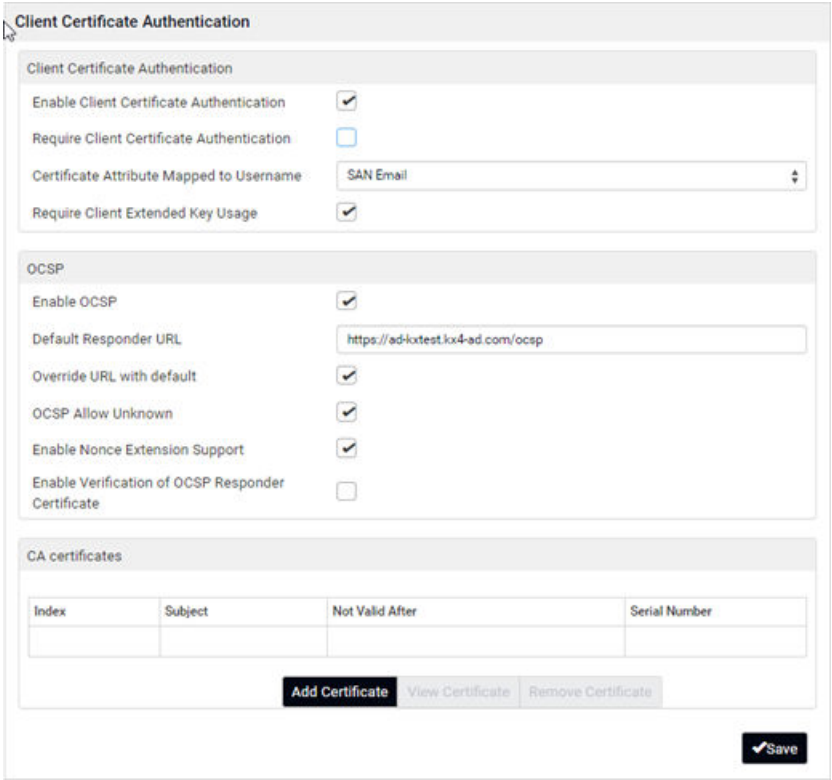
When enabled, Client Certificate Authentication applies to smart card and certificate authentication.

All Client Certificate Authentication settings are disabled by default.

IMPORTANT: Selecting "Require Client Authentication" will lock out standard username/password access to the web interface. Do not enable this setting until you have tested all other settings to verify successful authentication.

OCSP is supported as methods to validate certificates against a certificate authority.

► *To configure client certificate authentication settings:*



1. Click User Management > Client Certificate Authentication.
2. Enabling/Disabling:
   - Enable Client Certificate Authentication: Select this checkbox to enable client certificates for authentication. When enabled, client certificate authentication will be in effect for smart card authentication and PKI certificate authentication.
   - Require Client Certificate Authentication: IMPORTANT - Test and verify all other client certificate settings before using this setting. Removes the ability to authenticate on HTTPS connections via username/password. All access must be authenticated using client certificates, whether by smart card or certificates in the browser.
3. Require Extended Key Usage: Extended Key Usage enforces that the certificate's public key is being used for it’s intended purpose of authentication. When this setting is selected, login will be unsuccessful for certificates without extended key usage or those determined to be intended for purposes other than authentication.
4. Certificate Attribute Mapped to Username: Select the certificate attributes that should be used as the DKX3G2 user's login name. The login determines which group the user is in.
   - Common Name
   - emailAddress
   - Other Name
   - DNS Name
   - SAN Email
   - URI
   - UID

5. OCSP: Enable OCSP to use this method to validate certificates against a certificate authority.
   - Default Responder URL: Enter a default responder URL to be used if the certificate does not contain an OCSP server.
   - Override URL with Default: Restricts all OCSP communications to the URL entered in Default Responder URL.
   - OCSP Allow Unknown: Possible certificate statuses are Good, Revoked, or Unknown. When selected, DKX3G2 will still allow access for certificates with an Unknown status. When not selected, access will only be allowed for certificates with a Good status.
   - Enable Nonce Extension Support: Sends a nonce with the OCSP protocol to help prevent timing attacks. This requires support on the OCSP server side. Make sure that date/time is synced between DKX3G2 and the OCSP server.
   - Enable Verification of OCSP Responder Certificate: Ensure that the OCSP response is signed with a trusted CA key. This requires either that the OCSP server send the CA certificate it uses in the OCSP response data, or that the CA certificate for the OCSP server is added into the Certificate Repository.
6. Make sure you haven't selected Require Client Certificate Authentication unless you have already verified your access with these settings, or you have access to the DKX3G2 local port.
7. Click OK to save.

Change Your Password

► *To change your password:*

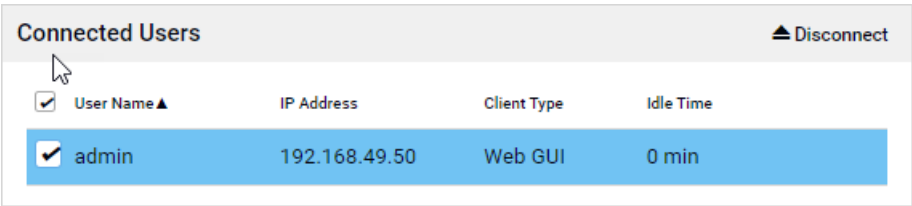
1. Click User Management > Change Password.
2. Enter your old password, then enter your new password twice. Click Save.

Connected Users

You can check which users have logged in to the DKX3G2 and their status. You can see the list of connected users without any special permission, but to terminate any user's connection, you must be administrator.

► *To view and manage connected users:*

1. Click User Management > Connected Users. A list of logged-in users displays.



Column	Description
User name	The login name of each connected user.

Column	Description
IP Address	The IP address of each user's host. For the login via a local connection (USB), <local> is displayed instead of an IP address.
Client Type	Web GUI: Refers to the web interface. CLI: Serial (local, such as USB connection) or SSH RDM: CC-SG or User Station
Idle Time	The length of time for which a user remains idle.

a. Select the user or users and then click Disconnect.
b. Click Disconnect on the confirmation message. The user is forced to log out.

Groups

All users must have a user account, containing the login name and password. Multiple users can log in simultaneously using the same login name. The admin user is created by default, and cannot be deleted, but you can change the username.

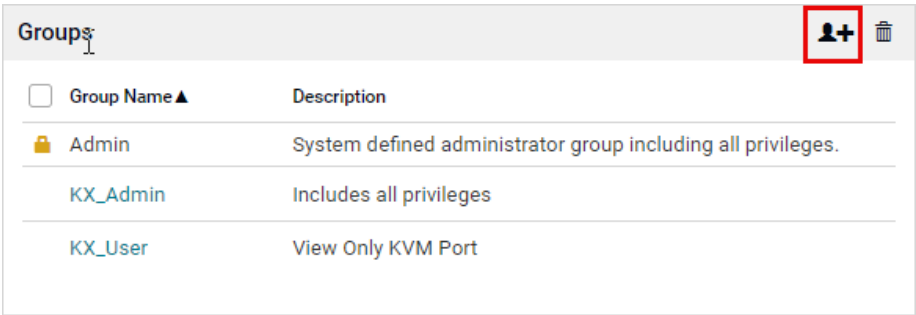
Privileges are assigned at the Group level, so you must also add groups, and assign your users to Groups. An admin group is created by default and has exclusive privileges. See: Admin Group Special Privileges.

When a user is assigned to multiple groups with different privilege levels, the highest-level of access specified is allowed to the user.

User group privilege changes take effect for the users in the group at the next login.

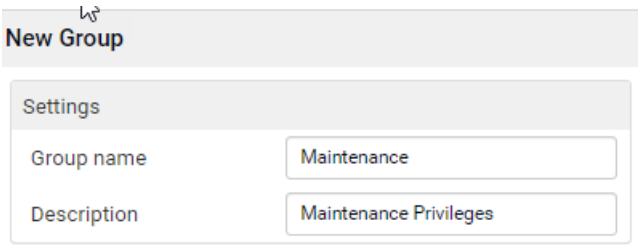
► *To add groups:*

1. Click User Management > Groups, then click the add group icon 

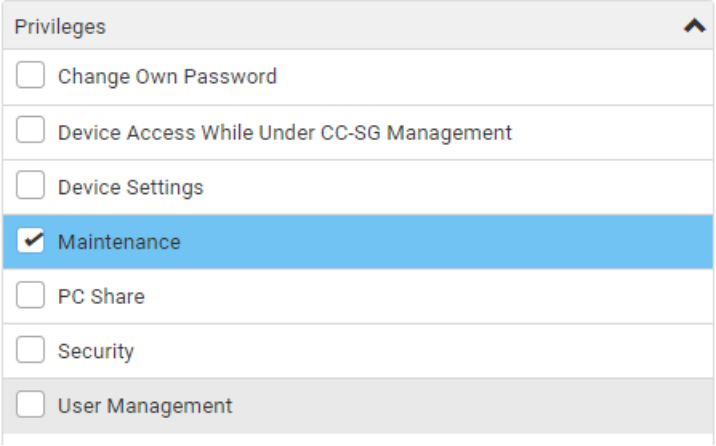


2. Complete the New Group information:

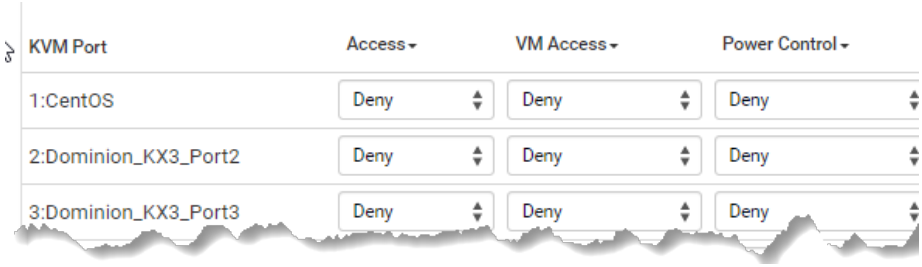
Field/setting	Description
Group Name	• 1 to 32 characters • Case sensitive • Spaces are permitted.
Description	• Enter a description of the group's role. • Up to 64 characters.



1. Select the Privileges assigned to this group. All tasks noted here as exclusions are available exclusively to the admin group. See: Admin Group Special Privileges.
   - Change Own Password: Allows users to change their own password.
   - Device Access While Under CC-SG Management: Allows users to directly access the DKX3G2 using an IP address when Local Access is enabled for the device in CC-SG. When a device is accessed directly while it is under CC-SG management, access and connection activity is logged on the DKX3G2. User authentication is performed based on DKX3G2 authentication settings.
   - Device Settings: All functions in the Device Settings menu except Enable and Configure SNMPv3
   - Maintenance: All functions in the Maintenance menu except Backup/Restore and Reset to Factory Defaults
   - PC Share: Simultaneous access to the same target by multiple users
   - Security: All functions in the Security menu
   - User Management: All functions in the User Management menu except Disconnect Users



2. Select the Access and VM privileges for the KVM Port.



- Access: Deny, View, Control
- VM Access: Deny, Read-only, Read-write
- Power Control: Access, Deny

Some privileges require certain access permission. If you do not set the needed permissions, an error will display.

3. When a DSAM unit is connected, the Serial Port section is available to select the Access privileges for the Serial Ports.
   - Access: Deny, View, Control

DSAM Serial Port	Access	Power Control
1.1:DSAM1 Port 1	View	Deny
1.2:DSAM1 Port 2	Control	Access
1.3:DSAM1 Port 3	Deny	Deny
1.4:DSAM1 Port 4	Deny	Deny

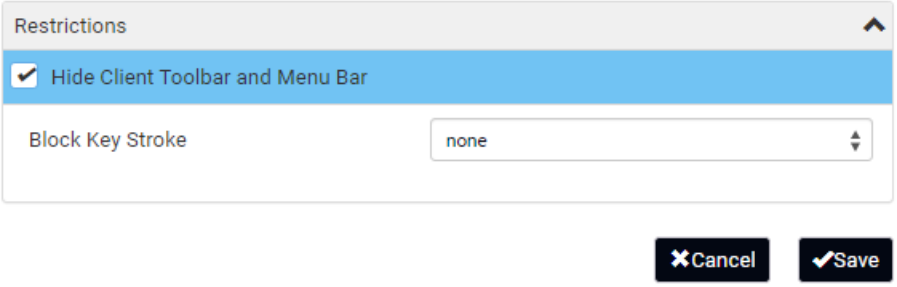
4. When PDUs are configured, the Power Control section is available to select the privileges to control power.
5. Power control: Access or Deny can be assigned to the KVM ports, the Serial ports or to the PDUs.

KVM Port	Access	VM Access	Power Control
1:Mac Mini	Deny	Deny	Deny

DSAM Serial Port	Access	Power Control
1.1:KX4-101-62219	Deny	Deny
1.2:KX4-101-62209	Deny	Deny

PDU Device	Power Control
PX3-5146R	Deny
PX2-2166R	Deny

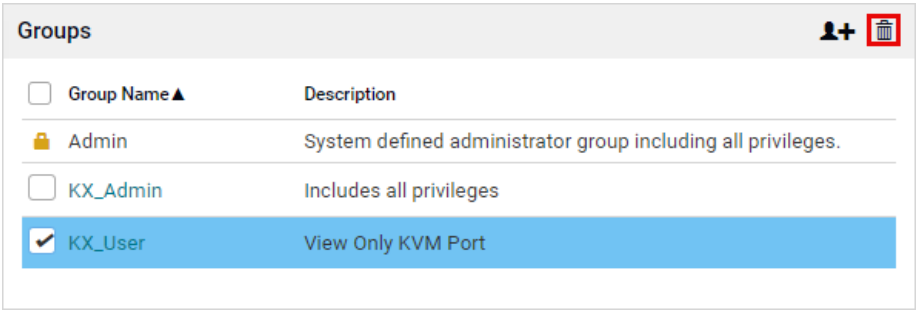
6. The Restrictions section has options for restricting client views and blocking keys.
   - Select Hide Client Toolbar and Menu Bar to remove these components from view for this group. Scaling and hotkeys for Single Mouse, Full-Screen, Scale Video and Disconnect from Target will be available.
   - In the Block Key Stroke field, select a keycode list to restrict the users in this group from using the keys in the list. See: Keycode List (on page 174).



7. Click Save. To assign these privileges and restrictions to users, select the group when you add or edit the user.

► *To delete a group:*

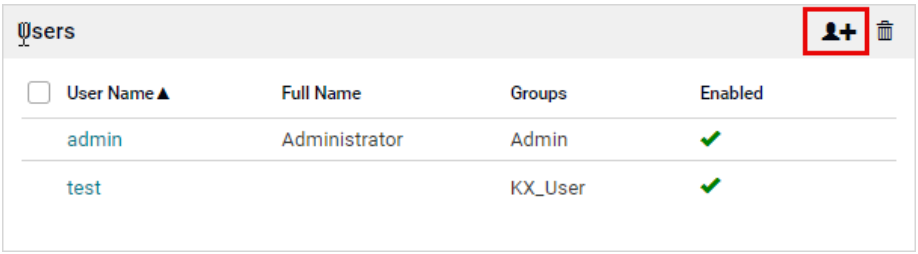
1. Click User Management > Groups, then click to select the group you want to delete.
2. Click trash icon  to delete and click Delete again to confirm.



Users

► *To add users:*

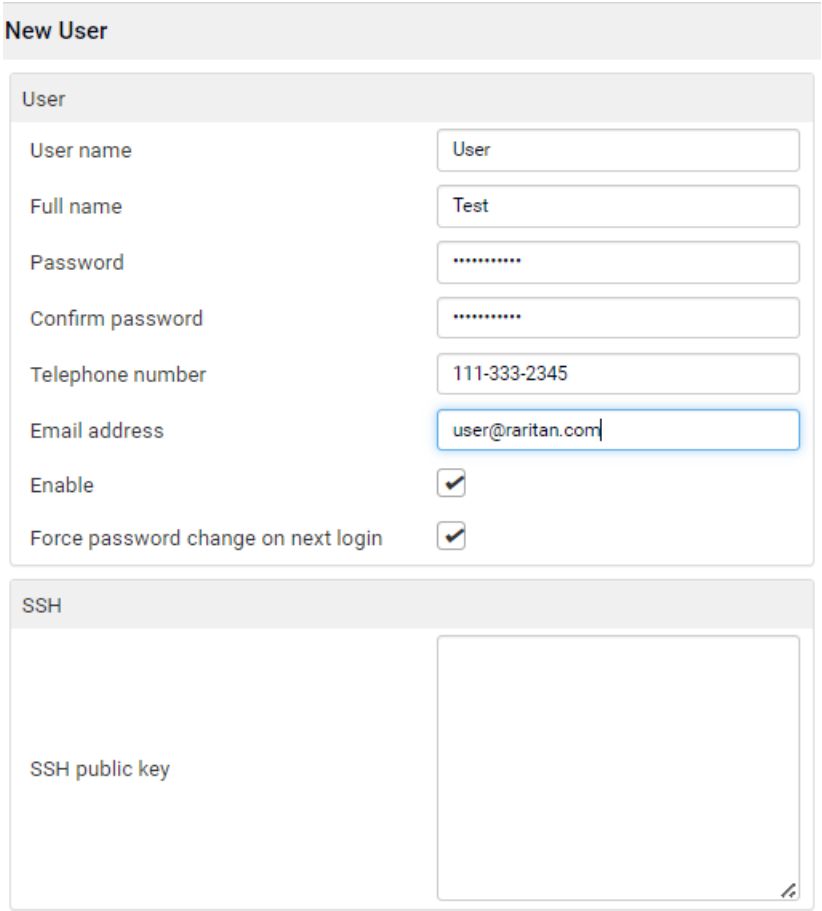
1. Click User Management > Users, then click the add user icon  .



2. Complete the User information:

Field/setting	Description
Username	The name the user enters to log in to the DKX3G2. • 4 to 64 characters • Case sensitive • Spaces, ":", "/" are NOT permitted.
Full Name	The user's first and last names. • Up to 64 characters
Password Confirm Password	• 4 to 64 characters • Case sensitive • Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address • Up to 128 characters • Case sensitive
Enable	When selected, the user can log in to the DKX3G2.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in.

3. SSH: The SSH public key is required when public key authentication for SSH is enabled. See: SSH Settings (on page 186)
4. Open the SSH public key with a text editor.
5. Copy and paste all content in the text editor into the SSH Public Key field.



6. SNMPv3: The SNMPv3 section appears when the user is part of the admin group. By default SNMPv3 is disabled, but can be enabled by selecting "Enable SNMPv3".

Field/ setting	Description
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user. Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See: Configuring SNMP Settings.
Security Level	Click the field to select a preferred security level from the list: • None: No authentication and no privacy. • Authentication: Authentication and no privacy. • Authentication & Privacy: Authentication and privacy. This is the default.

- Authentication Password: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

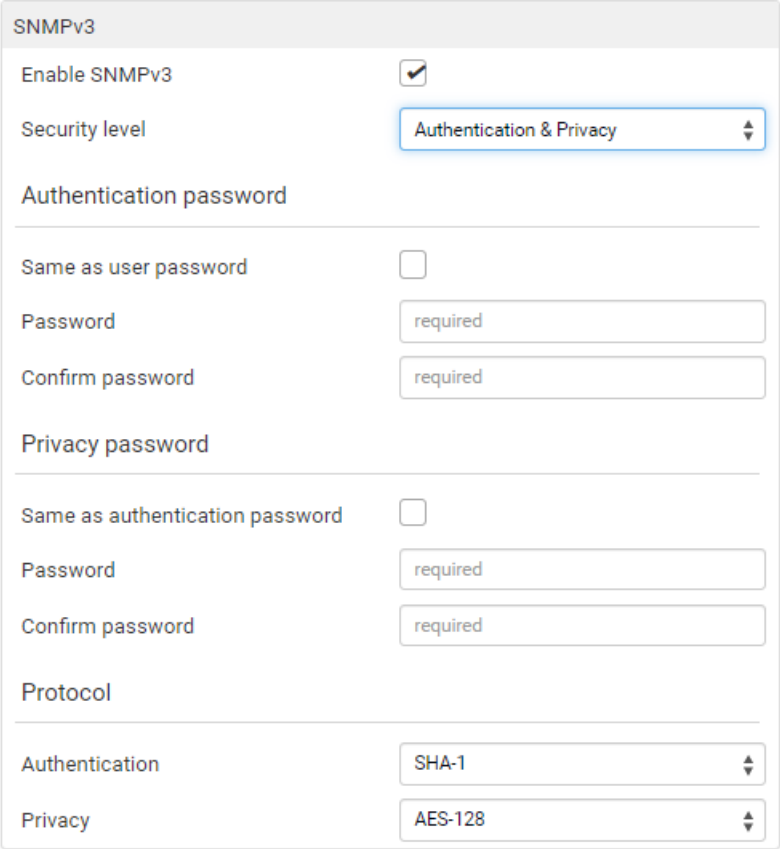
Field/setting	Description
Same as User Password	Select this checkbox if the authentication password is identical to the user's password. To specify a different authentication password, disable the checkbox.
Password, Confirm Password	Type the authentication password if the 'Same as User Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

- Privacy Password: This section is configurable only when 'Authentication & Privacy' is selected.

Field/setting	Description
Same as Authentication Password	Select this checkbox if the privacy password is identical to the authentication password. To specify a different privacy password, disable the checkbox.
Password, Confirm Password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

- Protocol: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

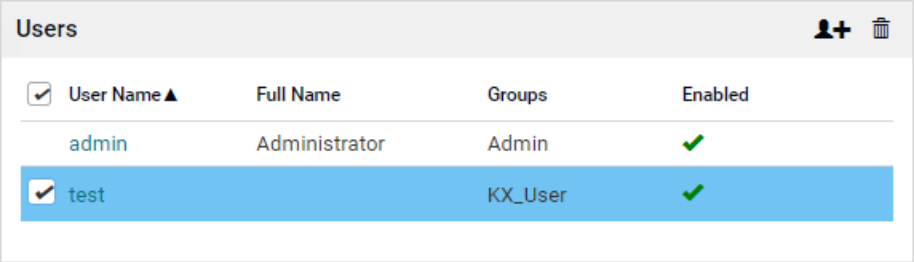
Field/setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: • MD5 • SHA-1 (default)
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: • DES • AES-128 (default)



1. Groups: Select the groups this user belongs to. Users have the privileges assigned to their groups.
2. Click Save.

► *To edit a user; change the admin username:*

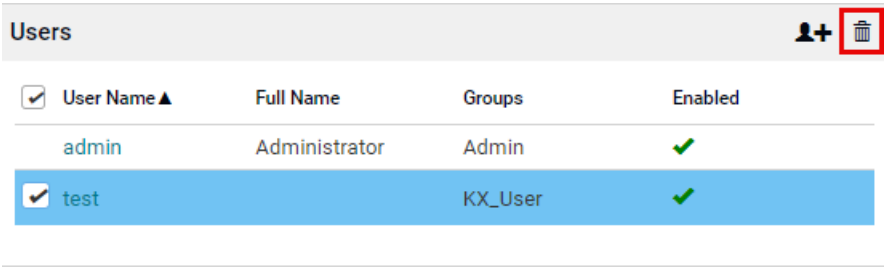
1. Click User Management > Users, then click to select the user you want to edit.



2. Change the user information as needed, then click Save.

► *To delete a user:*

1. Click User Management > Users, then click to select the user you want to delete.
2. Click trash icon  to delete and click Delete again to confirm.



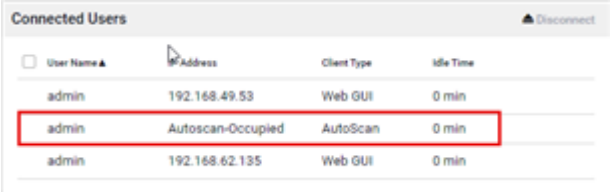
Device Settings

Auto Scan

The Auto Scan features uses the Local Port to automatically scan and capture a screenshot of your target video at a specified time interval. The local port is not accessible when this feature is enabled. Images are scaled and saved to a directory on your Network File Server. Image files are named after the port name, and saved as .JPG files. The image file is overwritten as each new capture is saved.

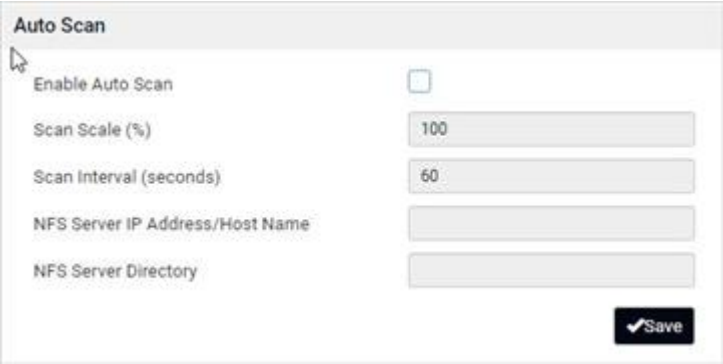
PC Share Mode should be enabled when using Auto Scan to ensure images can be captured and sent to the NFS server. When PC Share Mode is disabled, Auto Scan cannot capture a port image when the port is already occupied by another user. Go to Security > KVM Security to enable PC Share Mode.

While Auto Scan is enabled, the function will perform similarly to a connected user. In the User Management > Connected Users list, details are listed as shown here. The connection occupied by Auto Scan can be "disconnected" by disabling Auto Scan.



► *To configure auto scan settings:*

1. Choose Device Settings > Auto Scan.
2. Enable Auto Scan: Click the checkbox to enable the setting.
3. Scan Scale %: Saved images will be resized according to the scale percentage. 1%-100%.
4. Scan Interval (seconds): Enter the number of seconds between image captures. 60 seconds - 86400 seconds.
5. NFS Server IP Address/Host Name: Enter the network file server IPv4/IPv6 IP address or host name.
6. NFS Server Directory: Enter the directory on the network file server that will store the image file. For example, `/nfs/autoscan`.
7. Click Save to apply the settings.
8. When Auto Scan is enabled, view the status in the Device Info page. Go to Device Information, then check Auto Scan NFS in the System section.



► *Auto Scan NFS Status:*

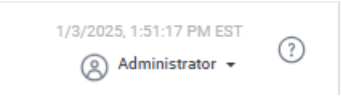
When Auto Scan is disabled, it does not appear in Device Info > Status. When enabled, possible status are:

- On
- Suspended
- Failed
- Connecting

Date and Time

Set the internal clock on the DKX3G2 manually, or link to a Network Time Protocol (NTP) server.

The DKX3G2 system date and time appears in the upper right corner of the web interface.

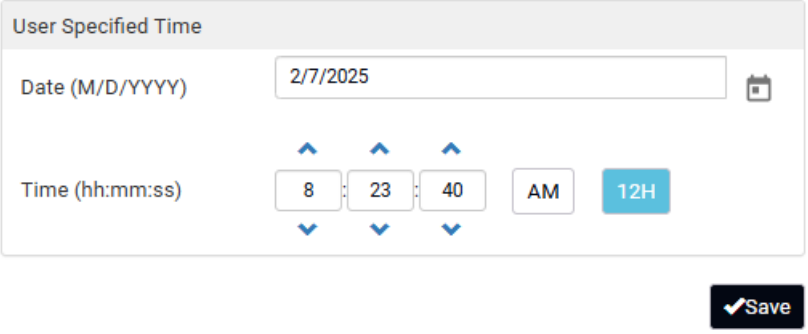


▶ *To set the date and time:*

1. Click Device Settings > Date/Time.
2. Select your Time Zone.
3. If your area participates in daylight saving time, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.
4. Select the Time Setup Method:
   - User Specified Time: Set the time manually.
   - Synchronize with NTP Server

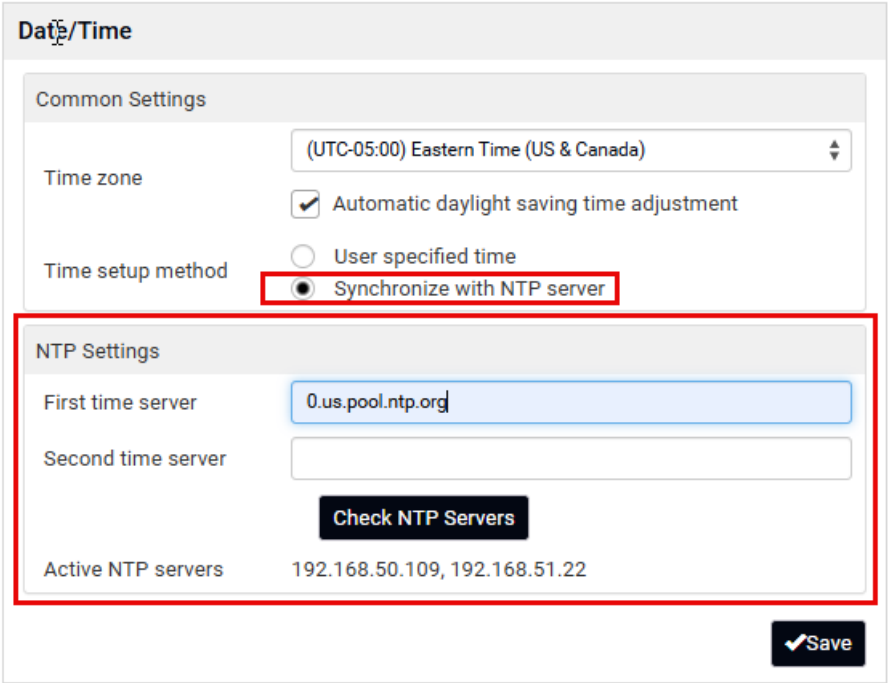
User Specified Time:

- Click the calendar icon to select the Date.
- Enter the time in Hours, Minutes and Seconds. Specify AM or PM. Click AM/PM to toggle the setting.
- Click Save.



Synchronize with NTP server:

- Select "Time setup method" as Synchronize with NTP server.
- By default the values of the primary NTP server in the First Time Server field and secondary NTP server as Second time server are not populated, however,active ntp servers may be obtained via DHCP/DHCPV6 or configured by the user.
- Click Check NTP Servers to verify the validity and accessibility of the NTP servers.

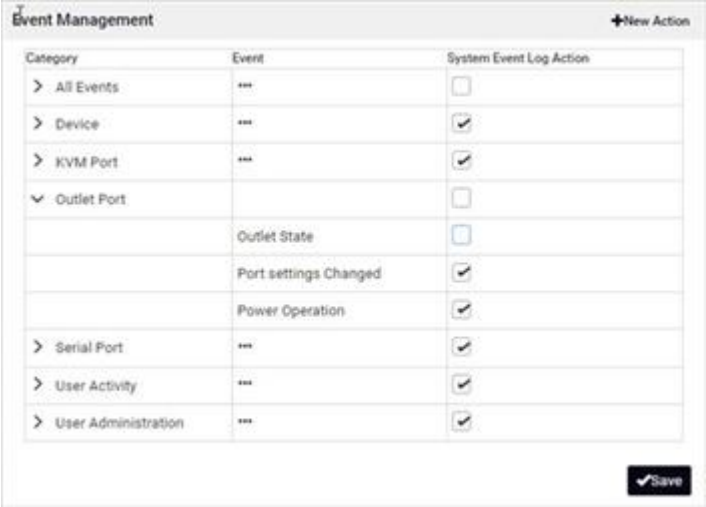


Event Management

All supported events are logged in the system log by default. You can also create additional actions for any event, including sending an email, sending an SNMP notification, and forwarding a syslog message.

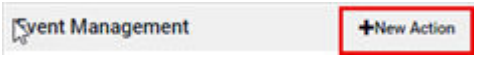
► *Configuring events and actions:*

1. Click Device Settings > Event Management.
2. The Event Management page shows events by Category. Click a category to view individual events.
3. Select the event check boxes to assign an action to an event. Click Save.
4. You can select the Power Operation event under Outlet Port and notify through email, syslog or snmp events.



► *To add an action:*

1. Click New Action.

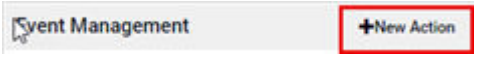


2. Assign a name to this action.
3. Select the desired action and configure it.
   - Email Actions: See: Send Email
   - SNMP Actions: See: SNMP Notifications
   - Syslog Actions: See: Syslog Messages
4. Click Create.

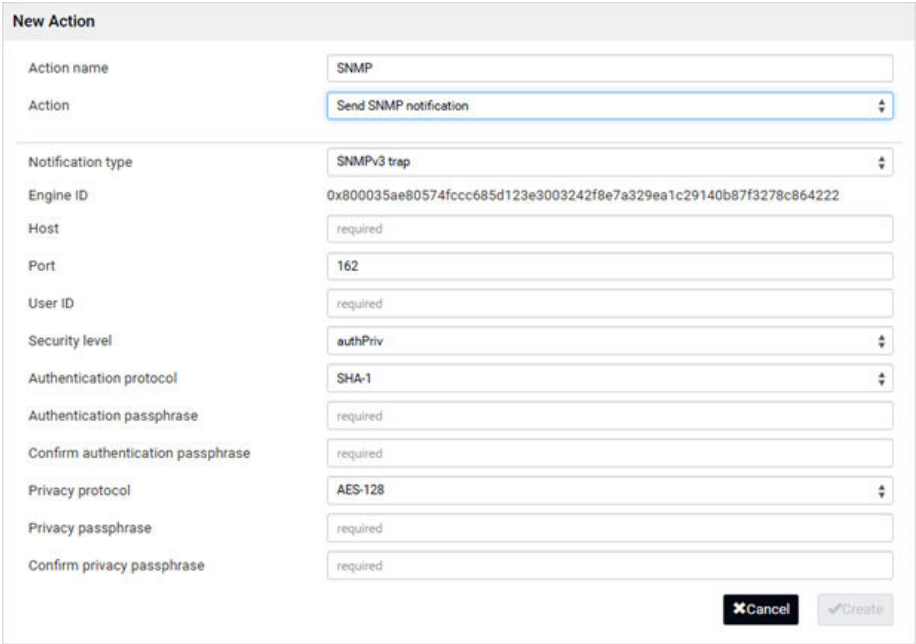
Configuring SNMP Action

► *To create new SNMP Action:*

1. Click Device Settings > Event Management.
2. Click New Action.



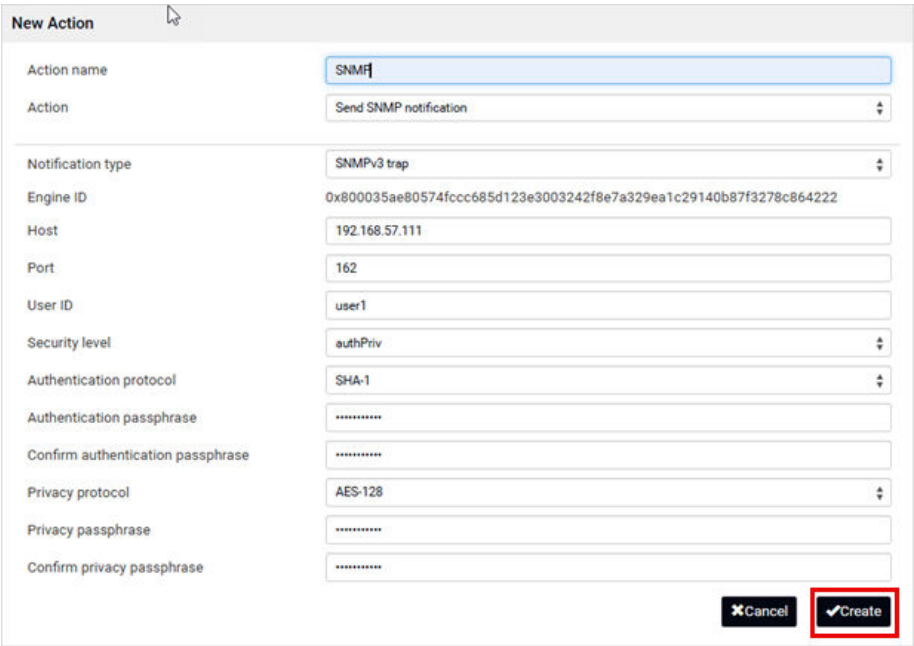
3. Assign a name to this action.
4. Select Send SNMP notification from the list.



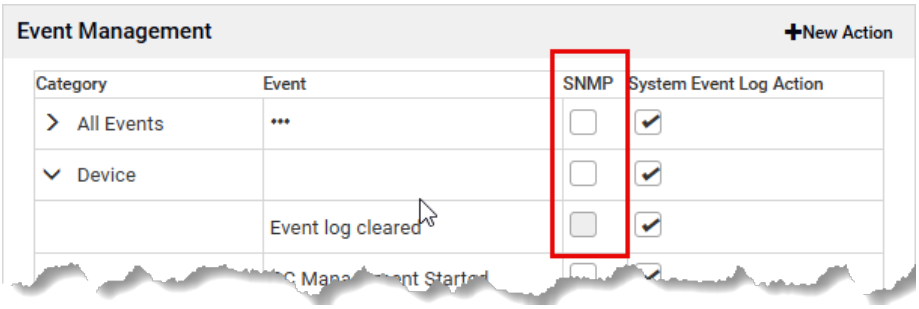
5. Enter the information as needed.

Field	Description
Notification type	Select a notification type. • SNMPv2 trap • SNMPv2 inform • SNMPv3 trap • SNMPV3 inform
Host	Type the host name or IP address of SNMP manager where the notification will be sent.
Port	Enter port number. Port number is used by SNMP manager. • Default port is 162
User ID	Type the user name. The userid or service account name of the entity communicating with the SNMP agent (up to 32 characters)
Security level	Select a security level. • authPriv • authNoPriv • noauthNopriv

Field	Description
Authentication protocol	Select an authentication protocol. • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Authentication passphrase	Type an authentication passphrase. • Minimum of 8 and maximum of 64 characters are allowed. Case sensitive.
Confirm Authentication passphrase	Retype the above Authentication passphrase.
Privacy protocol	Select a privacy protocol. • DES • AES-128 • AES-192 • AES-256 • AES-192 (3DES key extension) • AES-256 (3DES key extension)
Privacy passphrase	Type a Privacy passphrase. • Minimum of 8 and maximum of 64 characters are allowed. Case sensitive.
Confirm privacy passphrase	Retype the Privacy passphrase to confirm.



1. Click Create.



2. SNMP action is created and seen on the Event Management page.
3. Select the events for the SNMP notifications.See: complete list of SNMP Notifications (on page 169).
4. Click Save.

► *To edit existing SNMP notifications:*

1. Click Device Settings > Event Management.
2. The Event Management page opens. Check or uncheck the events as needed and click Save.

SNMP Notifications

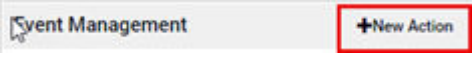
SNMP provides the ability to send notifications, to advise an administrator when one or more conditions have been met.

See: DKX3G2 Events (on page 171) for which notifications are generated.

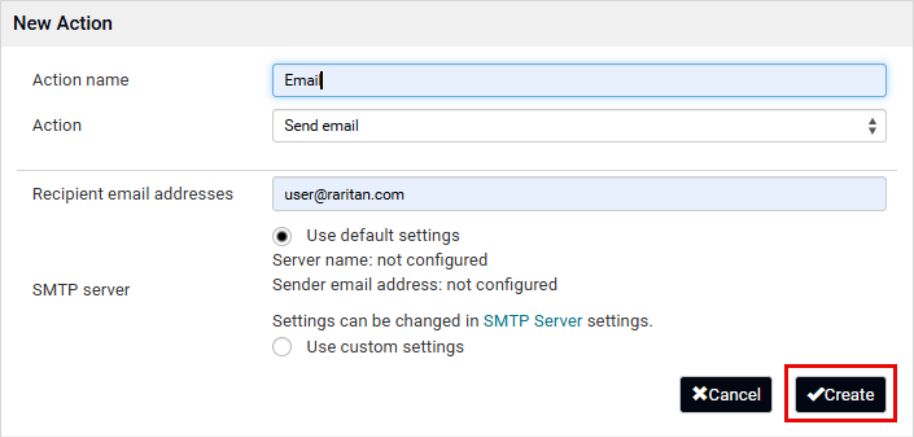
Configuring Email Action

► *To create new Email Notification Action:*

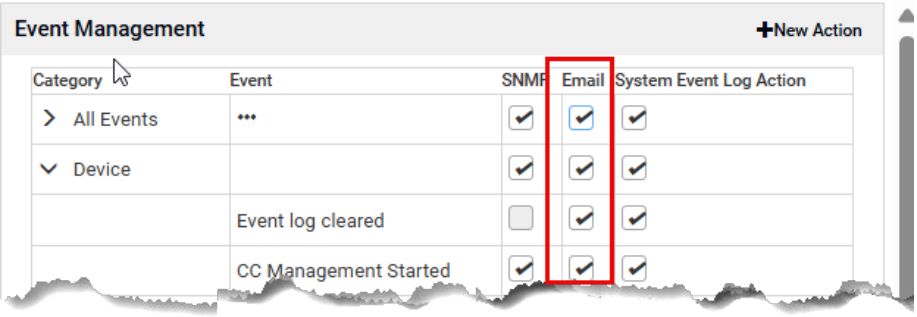
1. Click Device Settings > Event Management.
2. Click New Action.



3. Assign a name to this action.
4. Select action type Send email.
5. Type the recipient's email address in the 'Recipient email addresses' field. Use a comma to separate multiple email addresses.
6. "Use default settings" is checked for SMTP server. To use a different SMTP server, select the 'Use custom settings' radio button. Default messages are sent based on the event. To configure SMTP Server see:SMTP Server Settings (on page 184)
7. Click Create.



8. Email action is created and seen on the Event Management page.
9. Select the events for the email notifications. See: DKX3G2 Events (on page 171) for detail list.
10. Click Save.



► *To edit existing Email notifications:*

1. Click Device Settings > Event Management.
2. The Event Management page opens. Check or uncheck the events as needed and click Save.

DKX3G2 Events

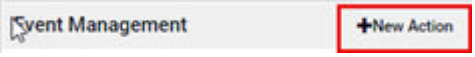
- Event log cleared - Event log was cleared
- CC Management Started - CC-SG management started
- CC Management Stopped - CC-SG management stopped
- CIM Firmware update completed - CIM Firmware update was completed
- CIM Firmware update started - CIM Firmware update was started
- Device clock changed - Device clock was changed
- Device settings restored - Device settings were restored
- Device settings saved - Device settings were backed up
- Device State changed - Device state was changed
- Device identification changed - Device name was modified
- DSAM Connected - A DSAM connected to DKX3G2
- DSAM Disconnected - A DSAM disconnected from DKX3G2
- DSAM Controller Recovery - DSAM controller was recovered
- DSAM Controller Reset - DSAM Controller was reset
- DSAM Firmware update completed - DSAM firmware update completed
- DSAM Firmware update started - DSAM firmware update started
- Ethernet failover - Ethernet failover occurred
- Firmware update completed - DKX3G2 firmware update completed
- Firmware update failed - DKX3G2 firmware update failed
- Firmware update started - DKX3G2 firmware update started
- Firmware validation failed - DKX3G2 firmware validation failed
- A LDAP error occurred - A LDAP error was occurred
- Local Port Out Disabled - Local port output disabled
- Local Port Out Enabled - Local port output enabled
- Network authentication result - Network authentication status
- Network interface link state is up - Network interface link state is up
- NFS Mount - NFS mount status (started/suspended/resumed/succeeded/failed)
- PDU Connected - A PDU connected to DKX3G2
- PDU Disconnected - A PDU disconnected from DKX3G2
- Power supply status changed - power supply status was changed
- Radius error occurred - A Radius error was occurred
- Sending SMTP message failed - Sending SMTP message failed
- Sending Syslog message failed - Sending Syslog message failed
- System reset - System reset
- System started - System started

- Network authentication result - Network authentication succeeded or failed
- KVM Port Connected - KVM Port was connected
- KVM Port Disconnected - KVM Port was disconnected
- KVM Port settings Changed - KVM Port settings changed
- Active USB Profile - Sending the information of active USB profile
- CIM Connected - A CIM connected to DKX3G2
- CIM Disconnected - A CIM disconnected to DKX3G2
- Port Audio Connected - Audio connected to DKX3G2 port
- Port Audio Disconnected - Audio connected to DKX3G2 port
- Port Smartcard Reader Connected - Smart card reader connected to DKX3G2 port
- Port Smartcard Reader Disconnected - Smart card reader disconnected to DKX3G2 port
- PortStatusChanged - Port status was changed
- Video Scan Started - Target scan was started
- Video Scan Stopped- Target scan was stopped
- VM Image Connected - A VM image was connected
- VM Image Disconnected - A VM image was disconnected
- Outlet Port State - Outlet port state of On/Off
- Outlet Port settings Changed - Outlet Port settings changed
- Outlet Port Power Operation - Outlet Port Power Operation (On/Off/Cycle)
- Serial Port Alert String - A keyword was detected
- Serial Port Connected – Serial port was connected
- Serial Port Disconnected - Serial port was disconnected
- Serial Port settings Changed - Serial port settings changed
- Serial Port status - Serial port status was changed
- User accepted the Restricted Service Agreement - User accepted/declined the restricted service agreement
- Authentication failure - Authentication was failed
- User logon state - User logged in/out
- Session timeout - Session was timed out
- User blocked - User was blocked
- Password changed - Password was changed.
- Password settings changed - Password settings were changed
- Restricted Service Agreement changed - Restricted Service Agreement was changed
- Group added - Group was added
- Group deleted - Group was deleted
- Group modified - Group was modified
- User added - User was added
- User deleted - User was deleted
- User modified - User was modified
- User renamed - User was renamed

Configuring Syslog Message Action

► *To create new Syslog Notification Action:*

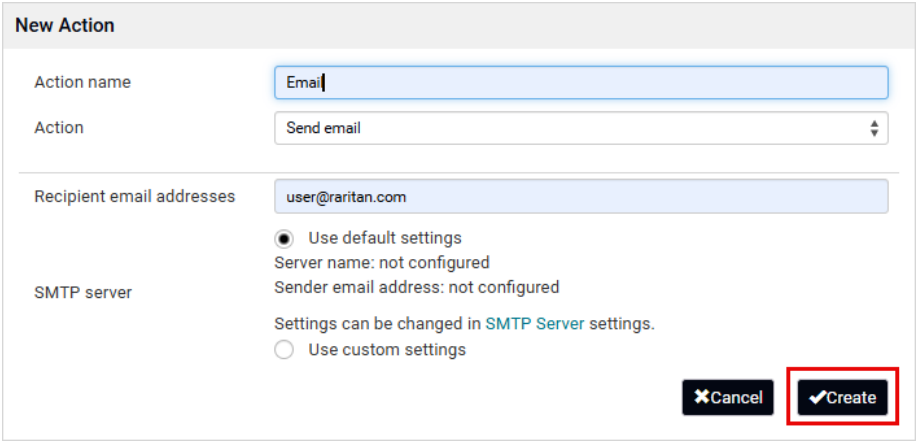
1. Click Device Settings > Event Management.
2. Click New Action.



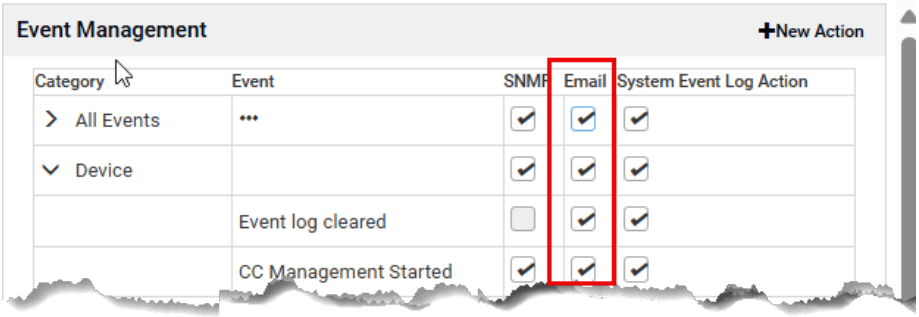
3. Assign a name to this action.
4. Select action type Syslog message.
5. Enter the information as needed.

Field	Description
Syslog server	Type syslog server host name or ipaddress
Host	Type the host name or IP address of SNMP manager where the notification will be sent.
Transport protocol	Select a transport protocol. • TCP • UDP • TCP+TLS
TCP port	Enter TCP port number • Default TCP port is 6514
CA Certificate	Upload CA Certificate using Browse. You can see the detail by pressing Show button or remove it by clicking Remove. By selecting "Allow expired and not yet valid certificates" options you will bypass the validity check of the certificate.

1. Click Create.



2. Syslog action is created and seen on the Event Management page.
3. Select the events for the syslog messages. See: DKX3G2 Events (on page 171) for detail list.
4. Click Save.



► *To edit existing Syslog messages events:*

1. Click Device Settings > Event Management.
2. The Event Management page opens. Check or uncheck the events as needed and click Save.

Keycode List

Use the Keycode List feature to create lists of keys you want to block from being used. Assign the list to a user group to block the group from using those keys. Keycode lists are created by keyboard language type. You are provided with a list of keys that can be blocked for each keyboard type.

When users are assigned more than one blocked keycode list, a given key will be available if it is not included on every keycode list. For example, a user is in groups with both List1 and List2 assigned. If List1 restricts F1, but List2 does not restrict F1, the user would be able to use F1

► *To add a new keycode list:*

1. Click Device Settings > Keycode List.
2. Click New.
3. Enter a Keyset Name to identify this list of keys to be blocked.

The keyset name is used when you assign the list to a user group. See: Users and Groups.

4. Select the Keyboard Type by language.
5. Select each Key you want to block from the Keys list, then click Add Key.

The added keys appear in the Keys Selected list. Click the Remove button to delete a key from the list.

6. When complete, click Add Keyset.

► *To edit a keycode list:*

1. Click Device Settings > Keycode List.
2. Click a keycode list by name to select it. The selected list is highlighted blue.
3. Click Edit to make changes to the list, and click Modify Keyset to save.

► *To delete a keycode list:*

1. Click Device Settings > Keycode List.
2. Click a keycode list by name to select it. The selected list is highlighted blue.
3. Click Delete to remove the list.

► *To block a user group from a keyset:*

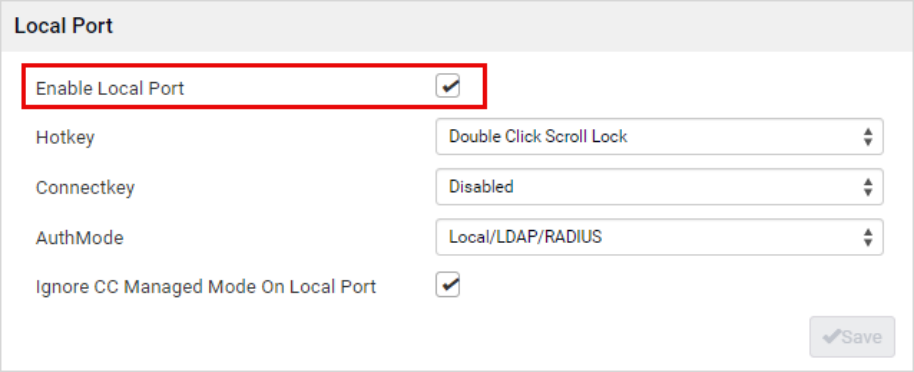
Select the keyset in the User Management > Group settings. See: Users and Groups.

Local Port

By default local port access is enabled which ensure continued access to the DKX3G2 via local port.

► *To configure Local Port settings:*

1. Click Device Settings > Local Port.
2. To enable or disable Local Port access, select or deselect the checkbox.

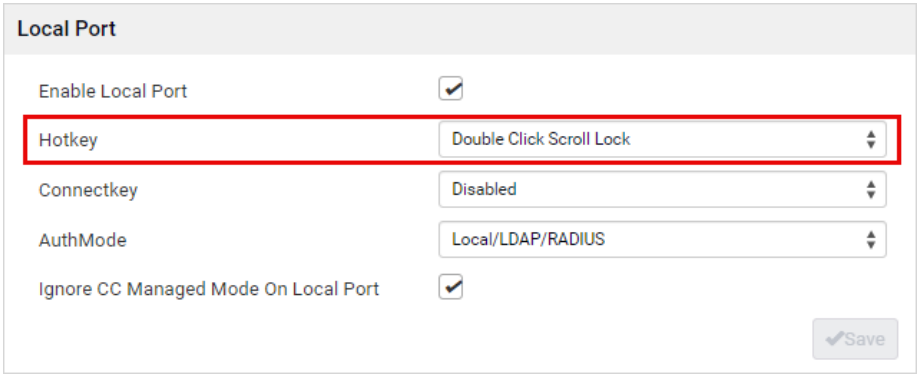


3. Click Save.

Note: Some changes you make to the settings on the Local Port Settings page requires you to restart the browser you are working in.

Select the Local Port Hotkey

- Choose the local port hotkey. The local port hotkey is used to return to the DKX3G2 Local Console interface when a target server interface is being viewed. The default is to Double Click Scroll Lock, but you can select any key combination from the drop-down list:



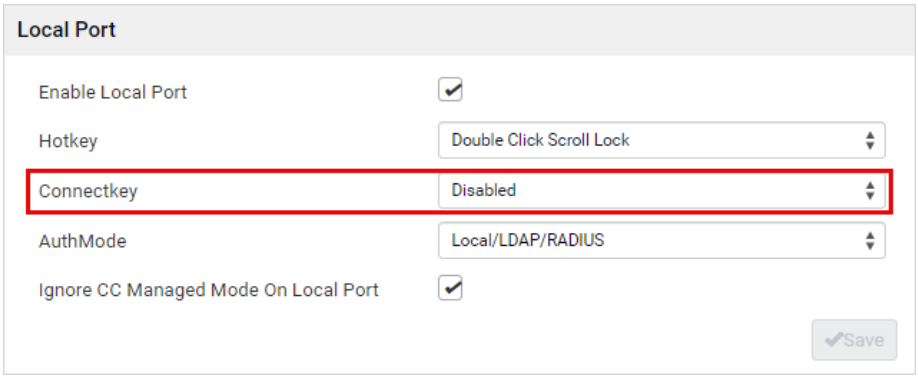
Hot key:	Take this action:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly

Hot key:	Take this action:
Double Click Left Ctrl key	Press the left Ctrl key twice quickly

Select the Local Port Connect Key

- Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target without returning to the GUI. Then use the hot key to disconnect and return to the local port GUI

Once the local port connect key is created, it will appear in the Navigation panel of the GUI so you can use it as a reference. See: Connect Key Examples for examples of connect key sequences.



Connect key:	Take this action to connect a port:
Left Alt Key	Press Left Alt key , press<port number> and release
Left Shift Key	Press Left Shift key , press<port number> and release
Let Ctrl Key	Press Left Ctrl key , press<port number> and release

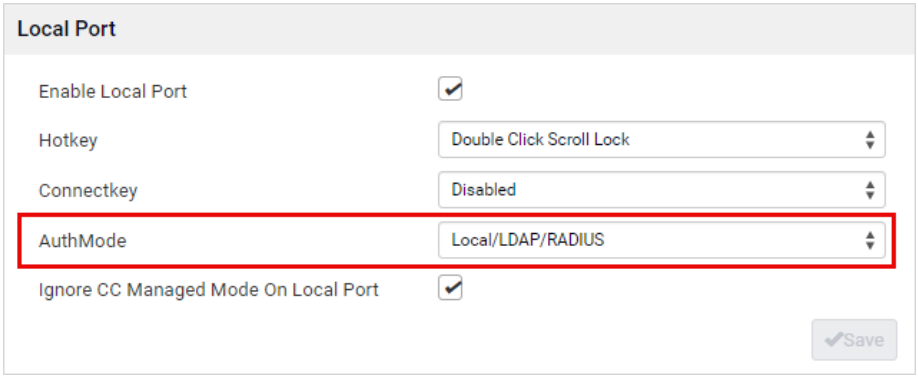
Connect and Hot Key Examples

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

Select the Local User Authentication

- Choose the type of local user authentication.
  - Local/LDAP/RADIUS. This is the recommended option.
  - None. There is no authentication for Local Console access.

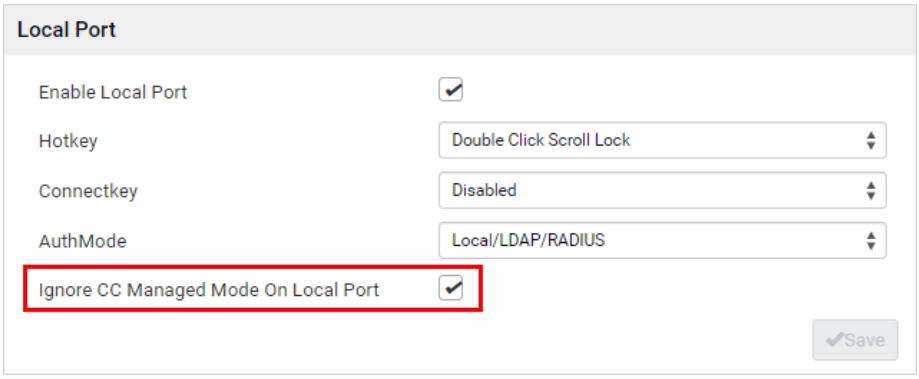
This option is recommended for secure environments only.



Select CC Managed Mode On Local Port

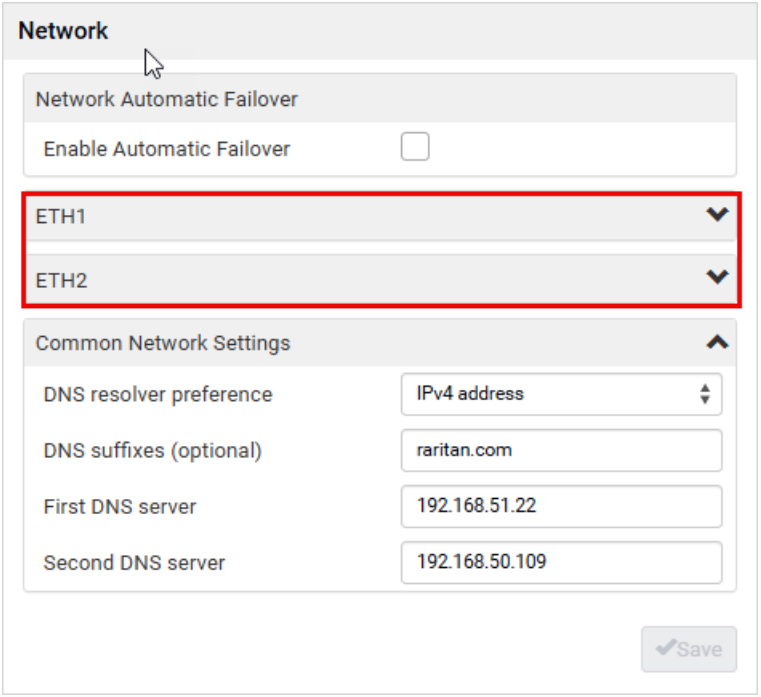
By default ignore CC Managed Mode is enabled which ensure continued access to the DKX3G2via local port.

- To enable or disable Ignore "CC Managed Mode on Local Port", select or deselect the checkbox.



Network

The default network setting is DHCP-enabled for IPv4. You can find your automatically assigned IP address in the Device Information page. See: Device Information. DKX3G2 supports 802.1X network authentication protocol.



Note: Network settings cannot be changed when the device is under CC-SG management.

► *IPv4 settings:*

Field/setting	***Description***
Enable IPv4	***Enable or disable the IPv4 protocol.***
IP auto configuration	***Select the method to configure IPv4 settings.*** • ***DHCP: Auto-configure IPv4 settings via DHCP servers.*** • ***Static: Manually configure the IPv4 settings.***

- DHCP settings: Optionally specify the preferred hostname, which must meet the following requirements:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot begin with a number
  - Cannot contain punctuation marks, spaces, and other symbols
  - Maximum 253 characters
- Static settings: Assign a static IPv4 address, which follows this syntax "IP address/prefix length".

  Example: *192.168.84.99/24*

► *IPv6 settings:*

Field/setting	***Description***
Enable IPv6	***Enable or disable the IPv6 protocol.***
IP auto configuration	***Select the method to configure IPv6 settings.*** • ***Automatic: Auto-configure IPv6 settings via DHCPv6.*** • ***Static: Manually configure the IPv6 settings.***

- Automatic settings: Optionally specify the preferred hostname, which must meet the above requirements.
- Static settings: Assign a static IPv6 address, which follows this syntax "IP address/prefix length".
  Example: *fd07:2fa:6cff:1111::0/64*

► *Interface Settings:*

Field	**Description**
Speed	• Select a LAN speed. • Auto: System determines the optimum LAN speed through auto-negotiation. • 10 MBit/s: Speed is always 10 Mbps. • 100 MBit/s: Speed is always 100 Mbps. • 1 GBit/s: Speed is always 1 Gbps (1000 Mbps).
Duplex	• Select a duplex mode. • Auto: The DKX3G2 selects the optimum transmission mode through auto-negotiation. • Full: Data is transmitted in both directions simultaneously. • Half: Data is transmitted in one direction (to or from the DKX3G2) at a time.
Current state	Show the LAN's current status, including the current speed and duplex mode.
Authentication	Select an authentication method. • *No Authentication:* No authentication data is required. • *EAP:* Use Protected Extensible Authentication Protocol. Enter required authentication data in the fields that appear.
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. • *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. • *TLS:* Authentication between the client and authentication server is performed using TLS certificates.

Field	Description
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. • *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. • *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Identity	This field appears when 'EAP' is selected. Type your user name.
Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. Type your password.
Client certificate, Client private key, Client private key password	This field appears when 'EAP', 'PEAP' and 'TLS' are all selected. PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. • Private keys in PKCS#1 and PKCS#8 formats are supported. • Client Private Key Password should be entered only when your private key is encrypted with a password. • To view the uploaded certificate, click Show Client Certificate. • To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
CA certificate	This field appears when 'EAP' is selected. A third-party CA certificate may or may not be needed. If needed, follow the steps below.

Field	Description
RADIUS authentication server name	This field appears when 'EAP' is selected. Type the name of the RADIUS server if it is present in the TLS certificate. • The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

Note: Auto-negotiation is disabled after setting both the speed and duplex settings of the DKX3G2 to NON-Auto values, which may result in a duplex mismatch.

- Available settings for the CA Certificate:

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see: TLS Certificate

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the DKX3G2 to verify the validity of the TLS certificate that will be installed. • For example, the certificate's validity period against the system time is checked.
Browse button	A client certificate is required for two scenarios: EAP+TLS, and EAP+PEAP+TLS. Click this button to import a certificate file. Then you can: • Click Show to view the certificate's content. • Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

► *Common Network Settings:*

Common Network Settings are OPTIONAL. If there are no specific local networking requirements, leave the default settings.

Field	Description
DNS resolver peference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. • IPv4 Address: Use the IPv4 addresses. • IPv6 Address: Use the IPv6 addresses.
DNS suffixes (optional)	Specify a DNS suffix name if needed.
First/Second DNS server	Manually specify static DNS server(s). • If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. • If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the DKX3G2 will use DHCP-assigned DNS servers.

► *Failover or Isolation Settings:*

To configure failover or isolation mode see: Choose Failover or Isolation Mode (on page 21)

Network Services

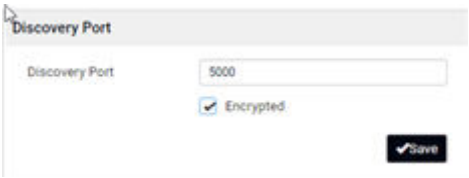
Discovery Port

DKX3G2 uses the default Discovery Port 5000 for communication with other Raritan products, such as User Station and CC-SG. You can change the port number if needed, but it cannot be changed while the device is under CC-SG management.

The device will transmit information about itself (make,model,firmware version,encryption) in clear text unless the encryption option is selected.

► *To change the default discovery port:*

1. Click Device Settings > Network Services > Discovery Port.
2. Enter the port number.
3. Select the Encrypted checkbox to encrypt the transmission of device information.
4. Click Save.



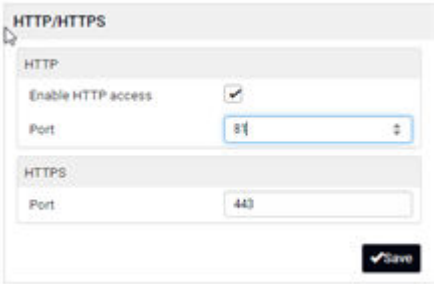
HTTP/HTTPS Ports

DKX3G2 uses the default HTTP/HTTPS ports 80/443. You can change the default if needed.

HTTP access will be redirected to HTTPS.

► *To change the default HTTP/HTTPS ports:*

1. Click Device Settings > Network Settings > HTTP/HTTPS Ports.
2. Select the HTTP Access checkbox if you need HTTP enabled.
3. Enter the port numbers then click Save.



1. The connection to the device will refresh with new HTTP/HTTPS port numbers. You must login again.

Note: Port forwarding with non standard https port works when HTTP port is disabled and a valid TLS certificate added into the "Trusted Root Certification Authorities" zone. The common name of the certificate must match the IP address or hostname of the device.

SMTP Server Settings

To send event emails, you must configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address. See: Event Management.

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See: Event Log.

► *To set SMTP server settings:*

1. Click Device Settings > Network Services > SMTP Server.
2. Enter the information needed.

Field	Description
IP address/host name	Type the name or IP address of the mail server.
Port	Type the port number. • Default is 25
Sender email address	Type an email address for the sender.
Number of sending retries	Type the number of email retries. • Default is 2 retries

Field	Description
Time between sending retries	Type the interval between email retries in minutes. • Default is 2 minutes.
Server requires authentication	Select this checkbox if your SMTP server requires password authentication, then enter the username and password.
User name Password	• 4 to 64 characters allowed. Case sensitive. • No spaces allowed in user name. • Spaces are allowed in password.
Enable SMTP over TLS (StartTLS)	Select this checkbox if your SMTP server supports TLS.

- Settings for the CA Certificate:

Field/setting	Description
Browse...	• Click Browse to import a certificate file. Then you can: • Click Show to view the certificate's content. • Click Remove to delete the installed certificate.
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period.

1. To test the settings:
   a. Enter a Recipient Email Address. Separate multiple email addresses with a comma.
   b. Click Send Test Email and verify emails are received.
2. Click Save.

Note: The DKX3G2 device's TLS-based protocols support AES 128 and 256-bit ciphers. The exact cipher to use is negotiated between the device and the client web browser. To force a specific cipher, check your client documentation for configuring AES settings.

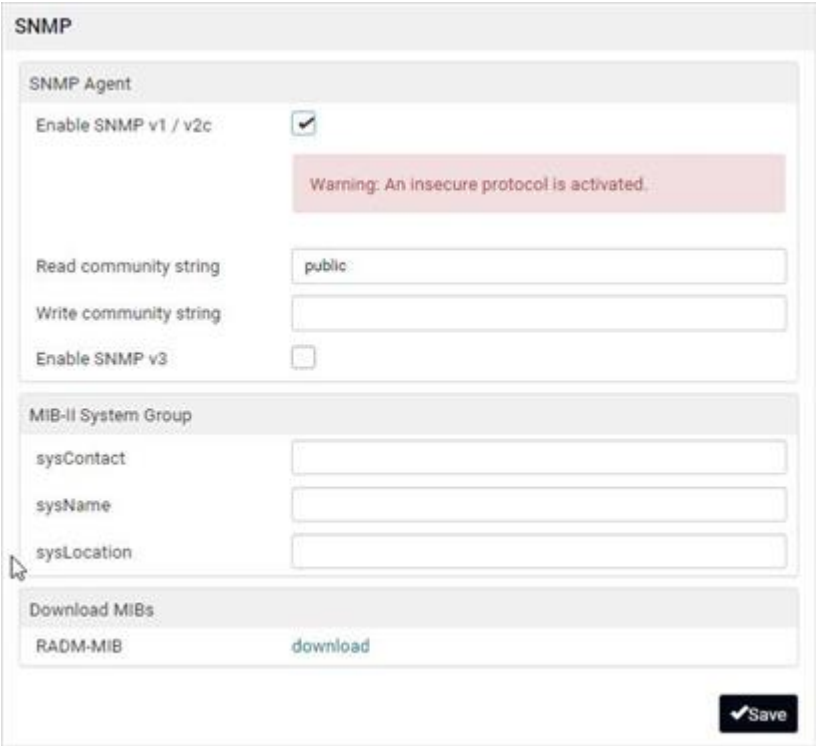
SNMP Settings

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. SNMPv2 provides for both traps and informs to be sent out over a network to gather information. The basic difference between traps and informs is that when the remote application receives an inform it sends back an acknowledgment, while traps are not acknowledged. In SNMPv3, there are further capabilities and restrictions on how the messages are handled. The traps and informs are configured on the Event Management page. See List of DKX3G2 SNMP Traps for a list of supported traps and informs.

You can enable or disable SNMP communication between an SNMP manager and the DKX3G2.

► *To configure SNMP Agent:*

1. Click Device Settings > Network Services > SNMP.
2. Enable or disable SNMP v1 / v2c and/or SNMP v3 by clicking the corresponding checkbox.
   a. The SNMP v1/v2c read-only access is enabled by default. The default 'Read community string' is "public".
   b. To enable read-write access, type the 'Write community string.' Usually the string is "private".
3. Enter the MIB-II system group information, if applicable.
   a. sysContact - the contact person in charge of the system
   b. sysName - the name assigned to the system
   c. sysLocation - the location of the system
4. Click the download link to get the SNMP RADM-MIB to use with your SNMP manager.
5. Click Save.



Note: If you uncheck SNMPv1/v2 c or SNMP v3 and save, the SNMP information is retained.

Caution: Factory defaults feature will remove the SNMP configuration and set the DKX3G2 to its original factory default.

SSH Settings

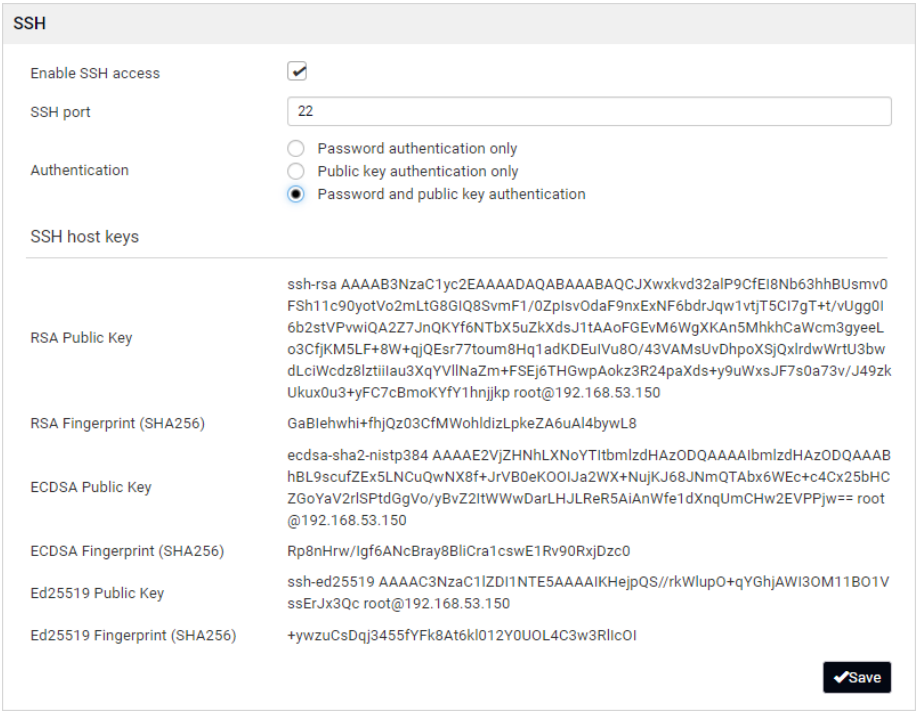
Enable or disable SSH access to the CLI, change the TCP port, or set a password or public key for login over SSH.

► *SSH settings:*

1. Click Device Settings > Network Services > SSH.
2. To enable or disable SSH access, select or deselect the checkbox.
3. To change the default port 22, type a port number.
4. Select one of the authentication methods.
   - Password authentication only: Enables password-based login only.
   - Public key authentication only: Enables public key-based login only.
   - Password and public key authentication: Enables both password and public key-based login, which allows either login authentication method to be used. This is the default setting.

   If public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connectin. See: Users and Groups

5. Click Save.



Note: The SSH host public key is generated at first boot or after factory reset.

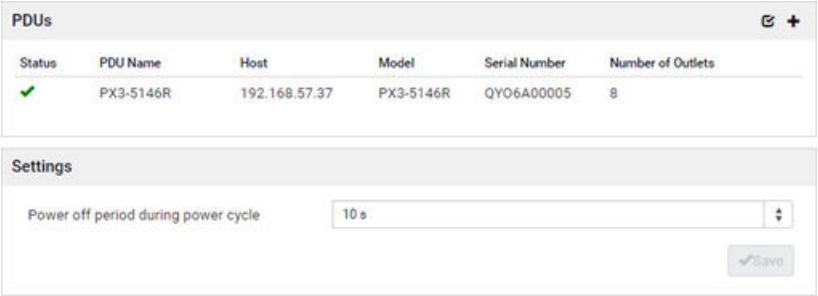
PDU Management

Power Distribution Units (PDUs), including Raritan PX2, PX3, PX4, and Server Technology PRO3X,PRO4X can be added to the DKX3G2 using SNMP. You can configure up to 8 PDUs in the DKX3G2 and get their current status. You can see all the added PDUs on the PDU Management page. The DKX3G2 checks the connection status of the configured PDU every 30 seconds. If it fails 10 times consecutively, the DKX3G2 will stop further checks. After adding PDUs, you can configure power associations to targets. See: Port Configuration: Power Association.

► *Added PDUs Information*

All the added PDUs will show the following information:

- Status
- PDU Name
- Host or IP
- Model
- Serial Number
- Number of Outlets



Note: Value of Power off period during power cycle applies to all the configured PDUs.

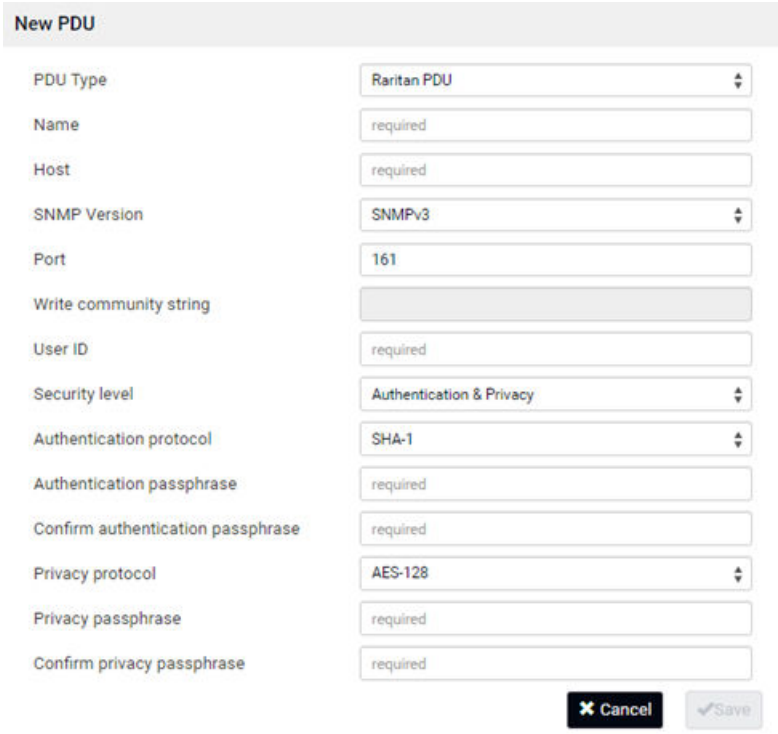
Adding PDUs

DKX3G2 supports PDUs using Simple Network Management Protocol (SNMP).

► *To add a PDU:*

1. Choose Device Settings > PDU Management and then click the add button .
2. On the New PDU page enter:
   - PDU Type: Select Raritan PDU or ServerTech PDU.
   - Name: Enter a PDU Name.
   - Host: Enter the hostname or the IP of the PDU.
   - SNMP Version: Select from the list: SNMP 1/2c or SNMP v3.

- Port: By default, 161 is the listening port.
- To enable an SNMP v1/v2 agent choose the SNMP Version as SNMP1/2c. This enables Write community string field. Choose from the following:
  - Enter the Write Community string.
- To enable an SNMP v3 agent choose the SNMPv3 and fill in the following information:
  - Enter the SNMP Manager "User" name in the UserID field. User ID may have 1-32 characters.
  - Select Security level: Select from the list:No Authentication & No Privacy, Authentication and Authentication & Privacy. If Authentication and or Privacy level are selected then you need to provide more information as follows.
  - Select MD5 or SHA from the Authentication Protocol drop-down list.
  - Enter the Authentication Passphrase in the field. Passphrase may have 8-64 characters. Authentication Passphrase should be different from Privacy Passphrase for best security practices.
  - Select, DES, or AES in the Privacy Protocol drop-down list.
  - Enter the Privacy Passphrase. Passphrase may have 8-64 characters. Authentication Passphrase should be different from Privacy Passphrase for best security practices.
  - Confirm the Passphrase.



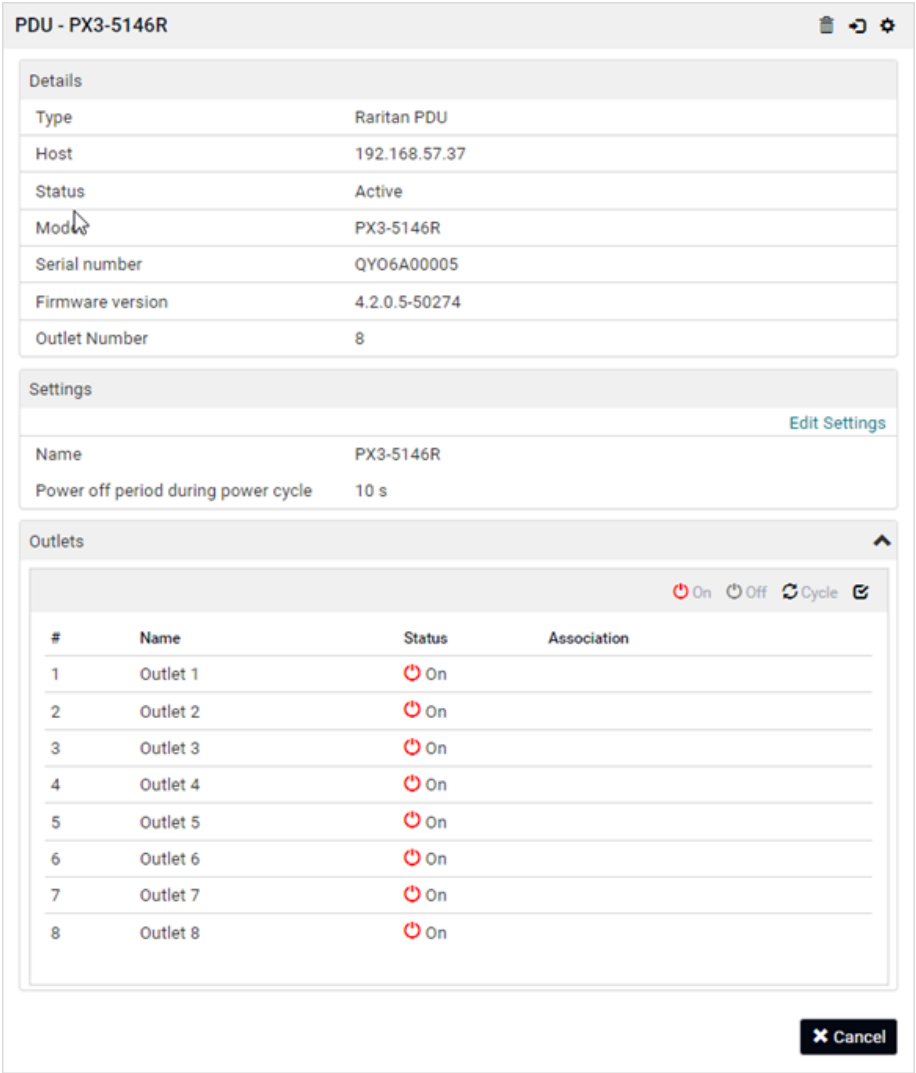
3. Click Save.
4. The PDU is added and appears in the PDU list on the PDU Management page.

PDU and Outlet Details

You can view the details of each configured PDU and its outlets.

► *To view PDU and outlet details:*

1. Choose Device Settings > PDU Management.
2. Click the PDU you want to view. Details, Settings and Outlets of the selected PDU display.
   - Details:
     - Type: Raritan PDU or ServerTech PDU
     - Host/IPaddress: Hostname or IP address of the PDU
     - Status: Active or inactive status of the PDU
     - Model: Model number of the PDU
     - Serial number: Serial number of the PDU
     - Firmware version: Firmware version of the PDU
     - Outlet Number: Total number of outlets of the PDU
   - Settings:
     - Name: Name of the PDU
     - Power off period during power cycle: Configured power off time period of the PDU during the power cycle
   - Outlets:
     - Outlet numbers: List of outlets
     - Name: Outlets names. To edit the name, click the outlet, then change the name on the Outlet Settings and click Save.
     - Status: Outlet status of on or off
     - Associations: Associations to KVM Ports or DSAM Serial Ports. If there is no association, the field is blank.



Note: PDU, outlet names, and power off period during power cycle can be customized. These are saved in the DKX3G2. However, when the DKX3G2 is managed by CC-SG, name updates and power association can only be done from CC-SG. Note that these updates are not synced to the PDUs.

Edit, Resume, and Delete PDUs

You can edit a PDU's configuration details, resume it's connectivity after a lapse, or delete a PDU from the DKX3G2.

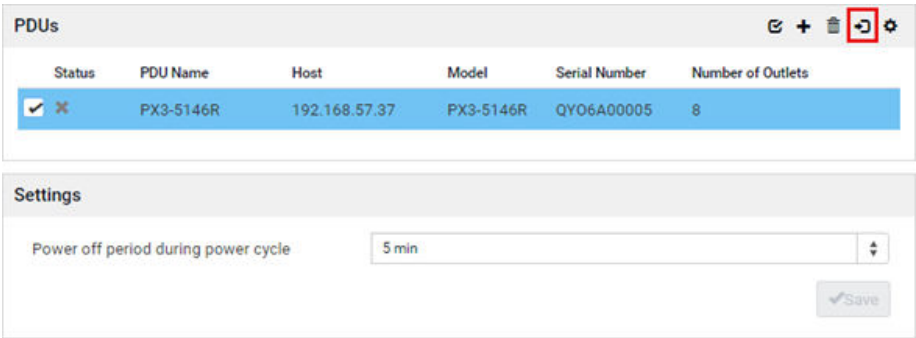
► *To Edit a PDU:*

1. Choose Device Settings > PDU Management.
2. Click the Select icon to enable the checkboxes in the PDUs list.
3. Click the Settings icon .
4. Update configuration information and click Save.

► *Resume a PDU:*

When the PDU stops communicating with the DKX3G2, the cross icon under Status appears. You can resume the PDU connection.

1. Choose Device Settings > PDU Management.
2. Click the Select icon to enable the checkboxes in the PDUs list.
3. Select the one, then click the resume icon .
4. Click Resume to confirm. Resume icon appears when the PDU drops communication with the DKX3G2.



The Status shows the green check icon when the connection resumes successfully.

► *To Delete a PDU:*

You can remove the added PDUs.

1. Choose Device Settings > PDU Management.
2. Click the Select icon to enable the checkboxes in the PDUs list.
3. Select the PDU and click the Trash icon .
4. Click Delete to confirm. The PDU is removed from the PDU list page.

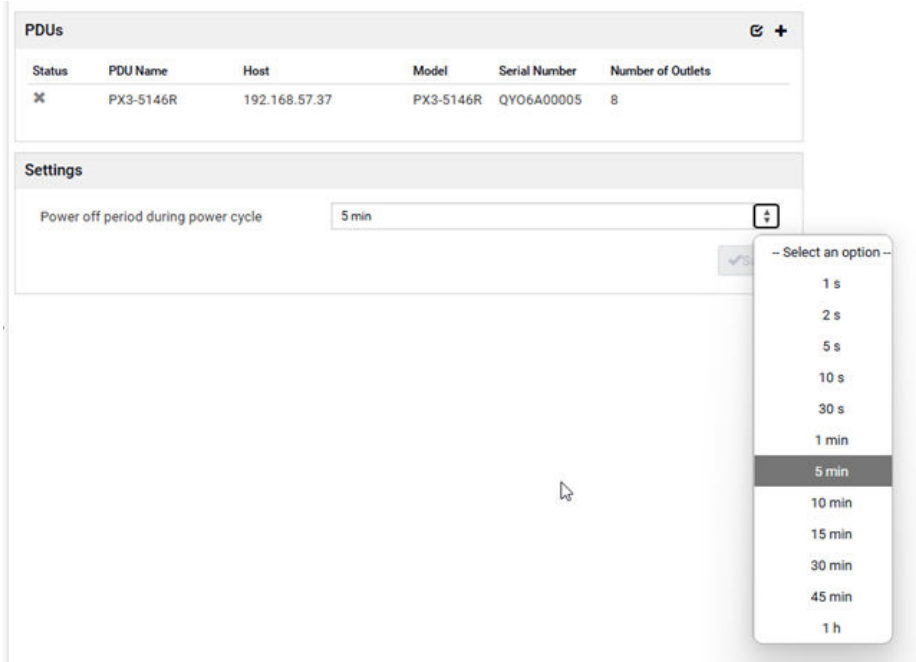
Settings for Power Cycling

The "Power off period during power cycle" settings controls how long the PDU outlet will remain powered down during a power cycle. By default, the delay before power is turned back on is 10 seconds.

► *To configure settings for power cycling:*

1. Click Device Settings > PDU Management.
2. In the Settings section, select a value for "Power off period during power cycle" from the list.
3. Click Save.

Note: Value selected for the power off period during power cycle will be applied to all PDUs.



Outlet Power Operations

In the Outlets section of the PDU detail page you can perform power operation on one or multiple outlets.

1. Click Device Settings >PDU Management.
2. Click the PDU.
3. The PDU details page displays.
4. Scroll down to the Outlets section.

► *Power On*

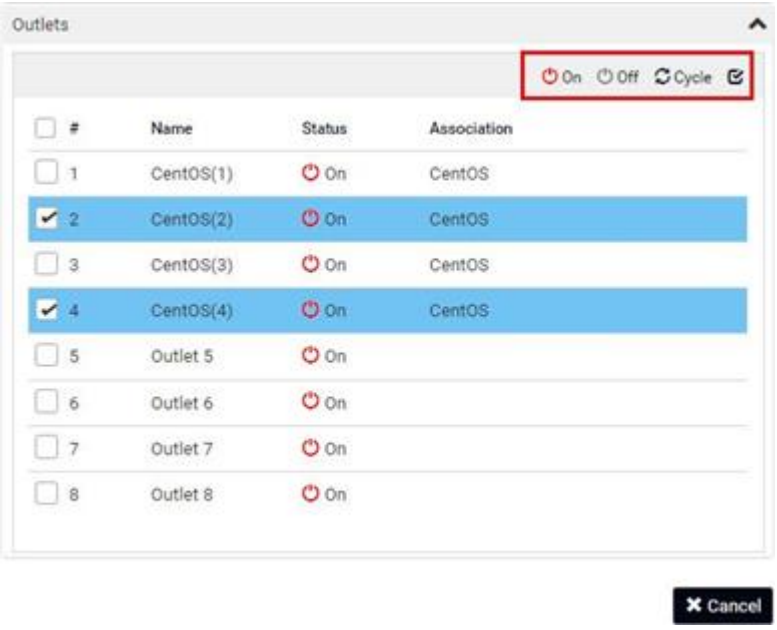
1. Click the Select icon to enable the checkboxes in the PDUs list.
2. Select one or multiple outlets.
3. Click On and then click Switch on to confirm.
4. All selected outlets turn on and show On status.

► *Power Off*

1. Click the Select icon to enable the checkboxes in the PDUs list.
2. Select one or multiple outlets.
3. Click Off and then click Switch off to confirm.
4. All selected outlets turn off and show Off Status.

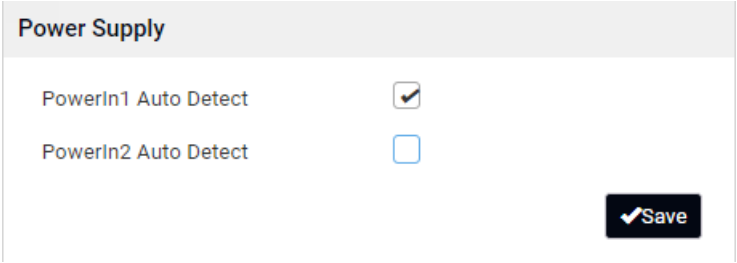
► *Power Cycle*

1. Click the Select icon to enable the checkboxes in the PDUs list.
2. Select one or multiple outlets.
3. Click Cycle and then click Power cycle to confirm.
4. All selected outlets turn off, remain off for the configured power cycle delay period, then turn back on. After completion, the outlets show "On" Status.



Power Supply

Connected power supplies can be set for auto detect. Once enabled status can be seen on the device information page as well as on the front panel.

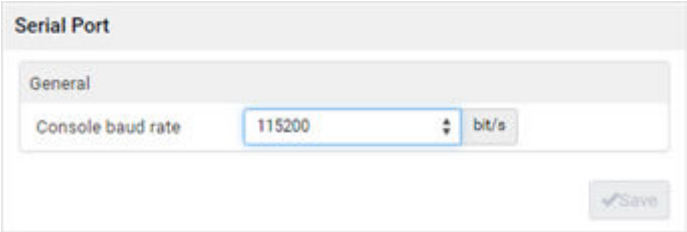


Serial Port

The Serial Port setting controls the baud rate of the DKX3G2 serial port. DKX3G2's serial port supports CLI serial console use only.

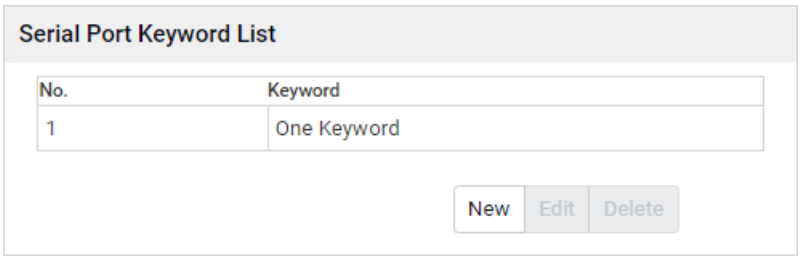
► *To configure the serial port:*

1. Click Device Settings > Serial Port.
2. Enter the Baud Rate and click Save.



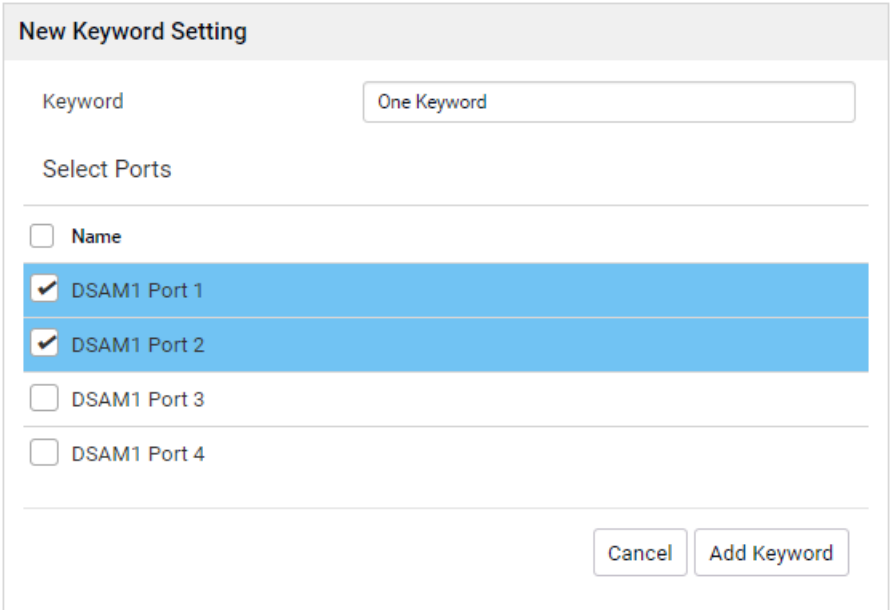
Serial Port Keyword List

A Keyword can be added to one or multiple serial ports. A Non admin User must have "device settings" permissions to add keywords.



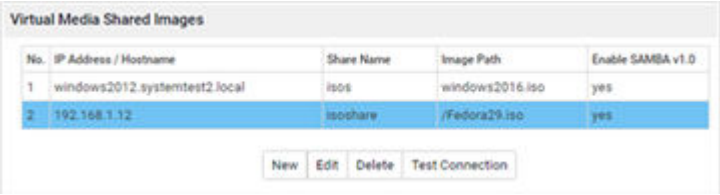
► *To configure serial port keywords:*

1. Choose Device Settings > Serial Port Keyword List. The Serial Port Keyword List page opens.
2. Click Add 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 Keyword to add them to the Selected box.



Virtual Media Shared Images

Configure Virtual Media Shared Images when using virtual media to access file server ISO images. ISO9660 format is the standard supported. However, other CD-ROM extensions may also work.



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

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

1. Click Device Settings > Virtual Media Shared Images.
2. Click New to add a shared image.
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. Up to 248 characters.
   - Share Name: Share name portion of the ISO image.
   - 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.
   - If required Select to Enable Samba 1.0 for older Samba version. When unchecked, Samba 3.0 is used.
4. Click Test Connection to verify.
5. Click Add Shared Image.

Security

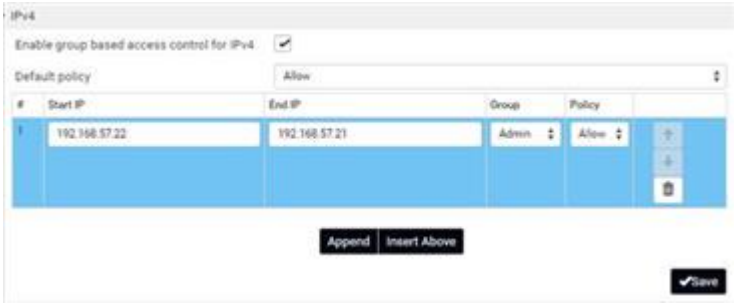
Group Based Access Control

Group based access control rules are similar to IP access control rules, except that they are applied to members of a user group. This enables granting/blocking access to the DKX3G2 from IP ranges based on usergroup membership.

The order of role-based access control rules is important, since the rules are executed in numerical order.

► *To create IPv4 or IPv6 group based access control rules:*

1. Choose Security > Group Based Access Control.
2. Select the Enable Group Based Access Control for IPv4 or scroll down to select the checkbox for IPv6.



3. Determine the default policy.
   - Accept: Accepts traffic when no matching rules are present.
   - Deny: Rejects any user's login attempt when no matching rules are present.
4. Create rules and put them in priority order.
   - Enter Start IP and End IP, Group the rule applies to, and Policy.
   - Click Append to add another rule. To add a rule above another, select a rule and click Insert Above.
   - To rearrange rules in order, click the arrow buttons on each rule.
   - To delete a rule, click the trashcan icon.
5. Click Save. Note that IPv4 and IPv6 rules are saved separately.

FIPS

For government and other high security environments, enabling FIPS 140-2 mode may be required. The DKX3G2 uses an embedded FIPS 140-2-validated cryptographic module running on a Linux® platform per FIPS 140-2 Implementation Guidance section G.5 guidelines. Once this mode is enabled, the private key used to generate the SSL certificates must be internally generated; it cannot be downloaded or exported.

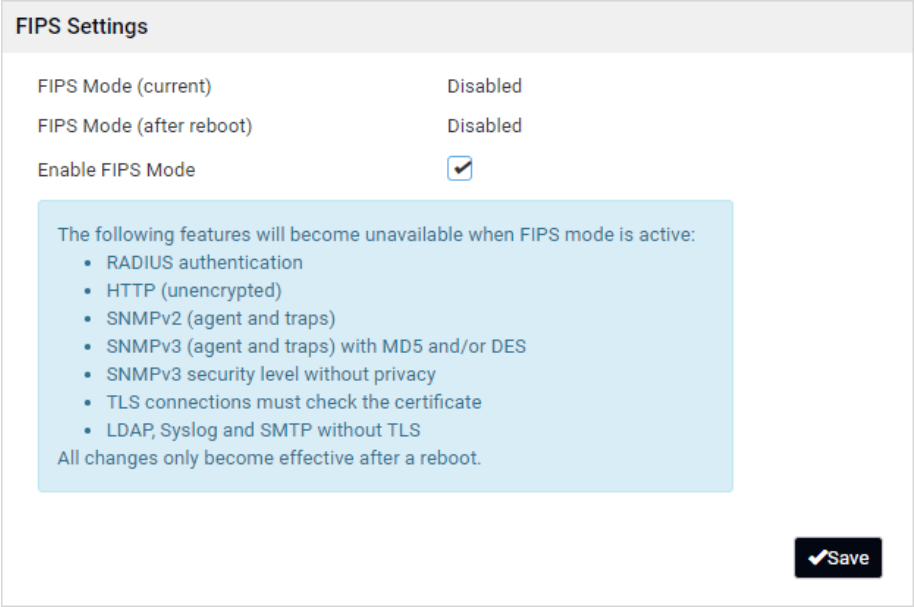
You will utilize FIPS 140-2 approved algorithms for external communications once in FIPS 140-2 mode. The FIPS cryptographic module is used for encryption of session traffic consisting of video, keyboard, mouse, virtual media and smart card data.

For additional security, you can also create a new Certificate Signing Request once FIPS mode is activated. This will be created using the required key ciphers. Upload the certificate after it is signed or create a self-signed certificate. The SSL Certificate status will update from 'Not FIPS Mode Compliant' to 'FIPS Mode Compliant'. When FIPS mode is activated, key files cannot be downloaded or uploaded. The most recently created CSR will be associated internally with the key file. Further, the SSL Certificate from the CA and its private key are not included in the full restore of the backed-up file. The key cannot be exported from DKX3G2.

Note that performance may be impacted once FIPS 140-2 mode is enabled.

► *To enable FIPS:*

1. Access the Security > FIPS page.
2. Select the check box "Enable FIPS Mode" to enable FIPS.
3. Reboot the DKX3G2.



FIPS 140-2 Support Requirements

The DKX3G2 supports the use of FIPS 140-2 approved encryption algorithms. This allows an SSL server and client to successfully negotiate the cipher suite used for the encrypted session when a client is configured for FIPS 140-2 only mode.

IP Access Control

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the DKX3G2, based on the IP address of the host sending or receiving the traffic. When creating rules, keep these principles in mind:

- Rule order is important.

  When traffic reaches or is sent from the DKX3G2, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored.
- Prefix length is required.

  When typing the IP address, you must specify it in the CIDR notation. That is, BOTH the address and the prefix length are included. For example, to specify a single address with the 24-bit prefix length, use this format:

  x.x.x.x/24

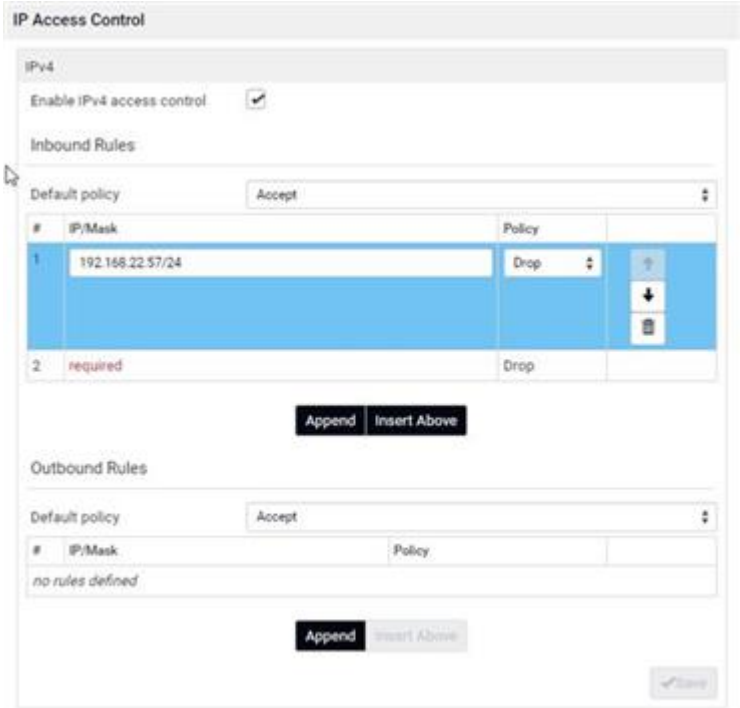
  /24 = the prefix length.

► *To create IPv4 or IPv6 IP access control rules:*

1. Choose Security > IP Access Control.
2. Select the Enable IP Access Control for IPv4 or scroll down to select the checkbox for IPv6.
3. Select the Default Policy:

- Accept: Accepts traffic from all addresses.
- Drop: Discards traffic from all addresses, without sending any failure notification to the source host.
- Reject: Discards traffic from all addresses, and an ICMP message is sent to the source host for failure notification.

4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.
   - Inbound rules control the data sent to the DKX3G2.
   - Outbound rules control the data sent from the DKX3G2.
5. Create rules and put them in priority order.
   - Enter IP address and mask and select the Policy.
   - Click Append to add another rule. To add a rule above another, select a rule and click Insert Above.
   - To rearrange rules in order, click the arrow buttons on each rule. The selected rule displays in blue.
   - To delete a rule, click the trashcan icon.



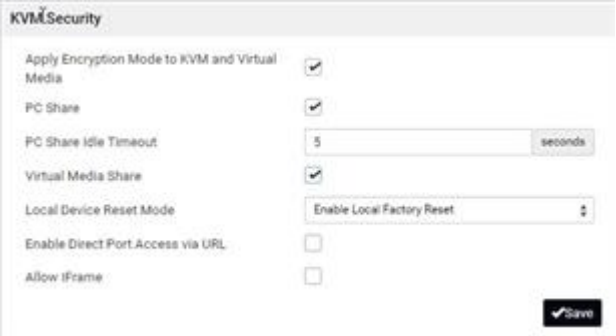
6. Click Save. Note that IPv4 and IPv6 rules are saved separately.

KVM Security

The KVM Security settings page includes options for encryption mode, virtual media, local ports, and other functions that affect the device locally.

► *To configure KVM Security settings:*

1. Click Security > KVM Security.



2. Select options as needed.

Field/setting	Description
Apply Encryption Mode to KVM and Virtual Media	Select this checkbox to use encryption for virtual media as well as KVM. Note: Only applies to AKC and VKCs target launches.
PC Share	Select PC Share to allow concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one DKX3G2 and concurrently view and control the same target server through the device. Note: PC Share mode cannot be disabled when Auto Scan is enabled. See: Auto Scan.
PC Share Idle Timeout	Set an idle time limit for users in PC Share mode. If a user has not moved the mouse or entered keyboard input and the timeout period expires, the user relinquishes control, and another user can access keyboard and mouse control of the target.
Virtual Media Share	This option is available only when PC-Share mode is enabled. When selected, Virtual Media Share permits the sharing of virtual media and audio among multiple users, that is, several users can access the same virtual media or audio session. The default is disabled.
Local Device Reset Mode	This option specifies which actions are taken when the hardware Reset button on the device is depressed. Choose one of the following options: • Enable Local Factory Reset (default): Returns the DKX3G2 device to the factory defaults. • Enable Local Admin Password Reset: Resets the local administrator password only. The password is reset to "raritan". • Disable All Local Resets: No reset action is taken.
Enable Direct Port Access via URL	When selected, users can access the target directly by entering login credentials for the DKX3G2 in a URL. See: Direct Port Access URL.
Allow IFrame	Enabling this option will allow WEB GUI to be embedded into iFrame, but it will decrease security level.

Direct Port Access URL

When Direct Port Access is enabled, you can access a target directly with a special URL that you can bookmark. This allows you to bypass logging into the DKX3G2 to connect to the target.

- Username and password are optional. If username and password are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.
- The port may be a port number or port name. If you are using a port name, the name must be unique or an error is reported. Port number is the number of the port the target is connected to.
- If the port is omitted altogether, an error is reported.
- Any special characters in the username, password, or port name must be passed in encoded URL codes.

► *Direct Port Access with VKCS:*

If you are using VKCS and direct port access, use one of the following syntaxes for standard ports.

• https://IPaddress/dpa.asp?username=username&password=password&port=1&client=vkcs
• https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=vkcs

► *Direct Port Access with AKC:*

If you are using AKC and direct port access, use one of the following syntaxes for standard ports.

• https://IPaddress/dpa.asp?username=username&password=password&port=1&client=akc
• https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=akc

► *Direct Port Access with HKC:*

If you are using HKC and direct port access, use one of the following syntaxes for standard ports.

• https://IPaddress/dpa.asp?username=username&password=password&port=1&client=hkc
• https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=hkc

Direct Port Access via SSH for DSAM

► *To Enable DSAM Direct Port Access*

This feature provides Direct Port Access (DPA) for DSAM ports via SSH. When Direct Port Access via SSH is enabled, you can configure a SSH port for each DSAM ports. The SSH port should be unique, and cannot conflict with the other DKX3G2 opened ports, such as SSH, HTTPS, Discovery. It is not necessary to configure all the SSH Ports for the available DSAM ports.

When enabled, all the configured SSH DPA ports will be opened; when disabled, all the SSH DPA ports will be closed. Changing the configured ports to empty or unplugging the DSAM will close all the ports. If you replug the same DSAM to the same DKX3G2, the configuration of SSH DPA ports will be auto-retrieved and will open all the configured ports.

Note: Connect one or two DSAM units to the DKX3G2.

---

1. Choose Security > KVM Security. The KVM Security page opens.
2. Scroll down to the Direct Port Access via SSH section and select Enable Direct Port Access via SSH checkbox.
3. Enter a unique SSH Port number for each DSAM port you want to configure.
4. Click Save.

► *To Access DSAM Ports*

You can also directly access DSAM ports using SSH session:

- ssh -l [user]:[DSAM Port Number] [KX4-101 IP/Hostname]

Note: Above command does not require SSH port setup for the DSAM ports.

- ssh -l [user] -p [SSH Port] [KX4-101 IP/Hostname]

Note: Above command requires SSH ports setup for each DSAM. See To Enable DSAM Direct Port Access

---

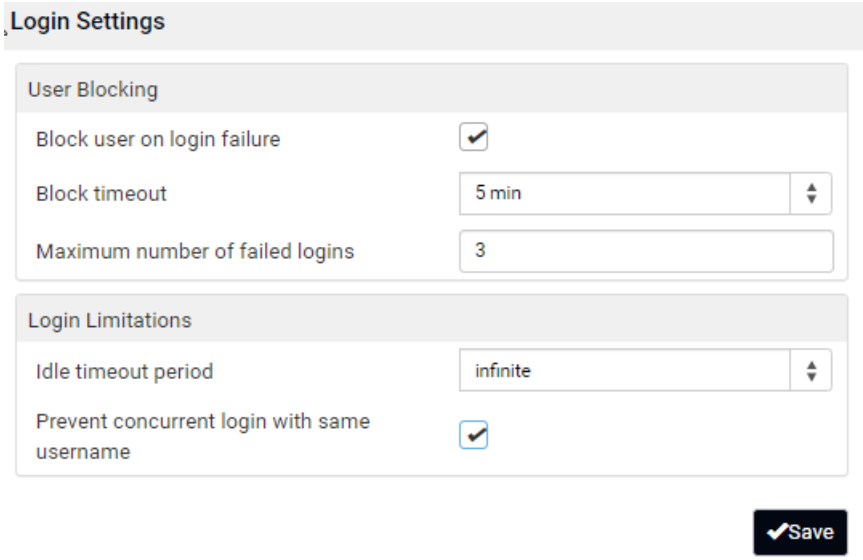
Login Settings

► *To enable User Blocking:*

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts. This option is enabled as default, with Timer Lockout values set to three Attempts and a Lockout Time of five minutes.

The three options are mutually exclusive:

Option	Description
Block user on login failure	When unchecked uers are not blocked regardless of the number of times they fail authentication.
Block Timeout	Default setting: Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled: • Attempts - The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10 and the default is 3 attempts. • Lockout Time - The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes and the default is 5 minutes. Note: Users in the role of Administrator are exempt from the timer lockout settings.
Maximum number of failed logins	This option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field: • Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Block user on login failure option is selected. The valid range is 3 - 10 and the default is 5 minutes



► *To set Login Limitations:*

Using login limitations, you can specify restrictions for single login, and the logging out of idle users.

Limitation	Description
Prevent concurrent login with same user name	When selected, only one login per user name is allowed at any time. When deselected, a given user name/password combination can be connected into the appliance from several client workstations simultaneously.
idle timeout period (1 min - infinite)	If there is no activity from the keyboard or mouse, all sessions and all resources are logged out based on the set time period. If there is an active virtual media or audio session in progress, the session does not timeout.

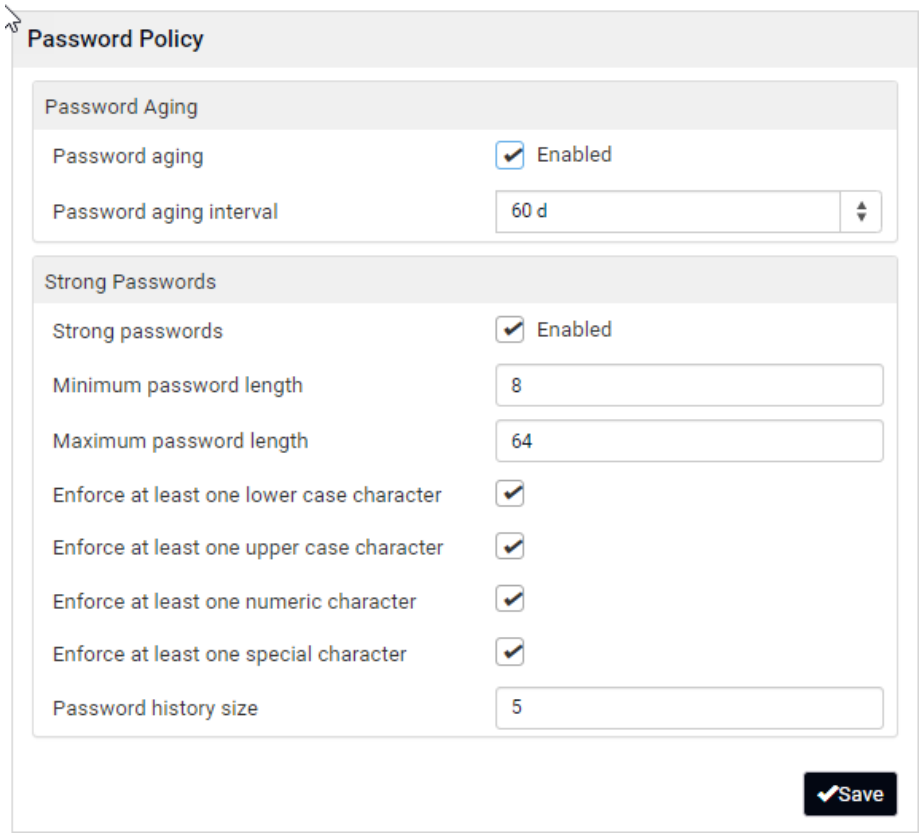
Note: During Port scan session Idle User Timeout settings are ignored.

Password Policy

The Password Policy page contains settings for password aging and strong passwords.

The default Password Policy is:

- Password Aging: Disabled
- Strong Passwords: Enabled



► *To configure a password policy:*

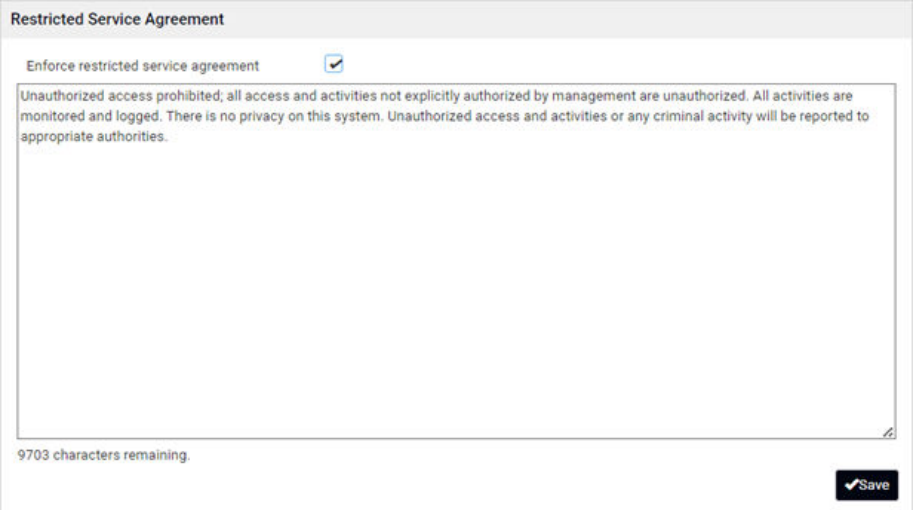
1. Click Security > Password Policy.
2. To enable Password Aging, which forces users to change their passwords at selected intervals:
   - Select the Enabled checkbox for Password Aging Interval.
   - Select a Password Aging Interval, from 7 days to 365 days.
3. To enable strong passwords and set their parameters:
   - Select the Enabled checkbox for Strong Passwords.
   - Set a Minimum and Maximum Password Length. Minimum is 8. Maximum is 64.
   - Select options to enforce at least one lower case, upper case, numeric, and/or special character.
   - Specify the Password History Size, which controls how frequently passwords can be reused. Maximum is 12.
4. Click Save.

Service Agreement

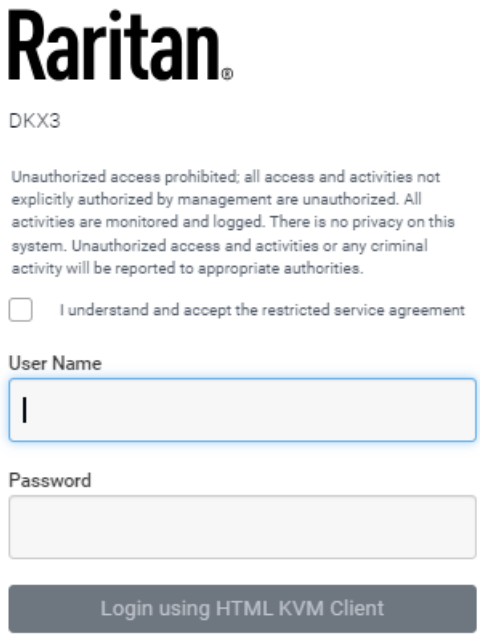
The Service Agreement page allows you to enable an agreement that appears on the login page of the DKX3G2. Users must select a checkbox on the agreement before logging in.

► *To configure the service agreement:*

1. Click Security > Service Agreement.



1. Select the Enforce Service Agreement checkbox.
2. Enter the agreement text in the field and click Save. The login page will present the service agreement. Users must select the checkbox before logging in.



TLS Certificate

DKX3G2 uses TLS 1.3 for any encrypted network traffic between itself and a connected client. When establishing a connection, DKX3G2 has to identify itself to a client using a cryptographic certificate. The DKX3G2 contains a default certificate that you should replace with your own.

DKX3G2 can generate a Certificate Signing Request (CSR) or a self-signed certificate using SHA-2.

The CA verifies the identity of the originator of the CSR. The CA then returns a certificate containing its signature to the originator. The certificate, bearing the signature of the well-known CA, is used to vouch for the identity of the presenter of the certificate.

Important: Make sure your DKX3G2 date/time is set correctly.

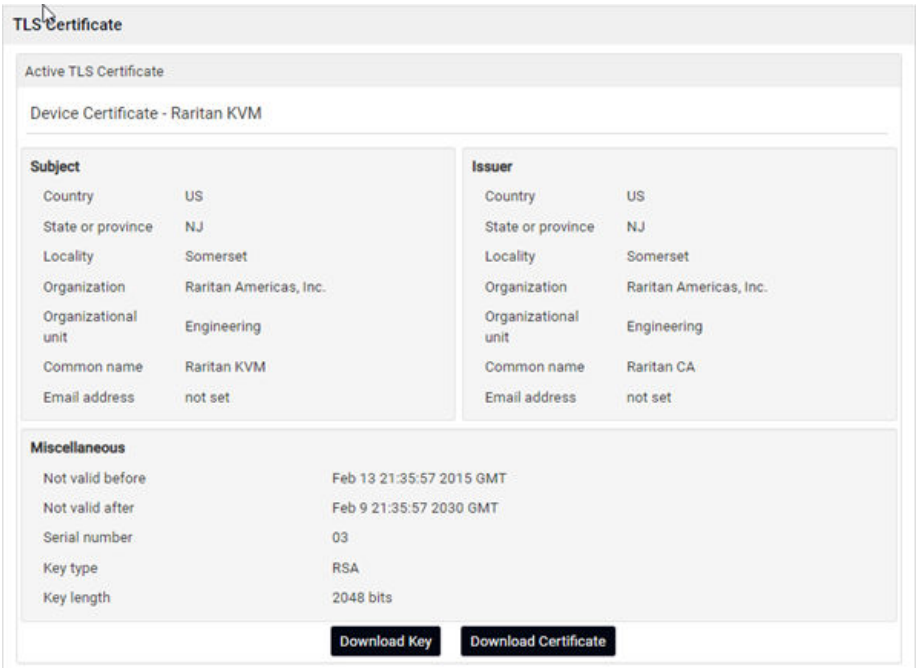
When a self-signed certificate is created, the DKX3G2 date and time are used to calculate the validity period. If the DKX3G2 date and time are not accurate, the certificate's valid date range may be incorrect, causing certificate validation to fail. See: Date and Time.

Note: The CSR must be generated on the DKX3G2.

Note: When upgrading firmware, the active certificate and CSR are not replaced.

► *To view and download the active certificate and key:*

1. Click Security > TLS Certificate. The active certificate details display.



2. Click Download Key and Download Certificate to get the active certificate files.

► *To create and install a new SSL certificate:*

1. Click Security > TLS Certificate. Scroll down to the New TLS Certificate section.
2. Complete the Subject fields:
   - Country (ISO code) - The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.
   - State/Province - The state or province where the organization is located.
   - Locality/City - The city where the organization is located.
   - Organization - The name of the organization to which the DKX3G2 belongs.
   - Organizational unit - This field is used for specifying to which department within an organization the DKX3G2 belongs.
   - Common name - The network name of the DKX3G2 once it is installed on your network (usually the fully qualified domain name). The common name is identical to the name used to access the DKX3G2 with a web browser, but without the prefix “http://”. In case the name given here and the actual network name differ, the browser displays a security warning when the DKX3G2 is accessed using HTTPS.
   - Email address - The email address of a contact person that is responsible for the DKX3G2 and its security.
3. Add up to 10 Subject Alternative Names (SAN) by clicking the Add Name button, then enter the hostname or IP in the field. SANs are the hostnames or IP addresses the certificate will be valid for.

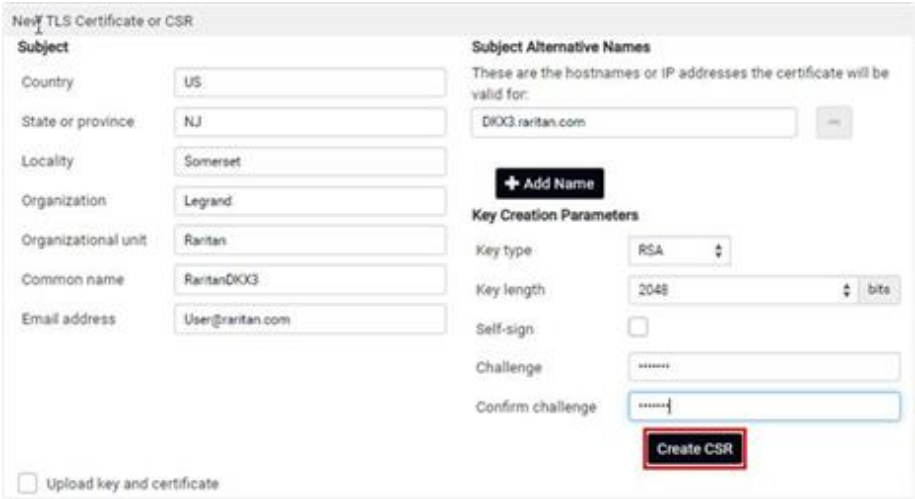
Note: It is highly recommended to use SubjectAlternativeName (SAN) and hostname in certificates. Using IP address as CN is no longer supported.

1. To generate self-signed certificate, do the following:
   a. In the Key Creation Parameters, select the Self-Sign checkbox . When you select this option, the a. Dominion KX IV–101 generates the certificate based on your entries, and acts as the signing certificate authority. The CSR does not need to be exported and used to generate a signed certificate.
   b. Select a key type of RSA or ECDSA, and enter the key length for RSA or elliptic curve for ECDSA.
   c. Set the Validity in Days, which controls how many days until this certificate expires. Ensure the DKX3G2 date and time are correct. If the date and time are not correct, the certificate's valid date range may not be calculated correctly.
   d. Click Create Self-Signed Certificate. This will generate the certificate based on your entries, and act as the signing certificate authority. The CSR does not need to be exported and used to generate a signed certificate.
   e. When the page refreshes, new buttons appear in the New TLS Certificate section, to allow you to install, download or delete the newly generated self-signed certificate and key.
   f. To start using the new certificate, click Install Key and Certificate.
   g. The page may refresh as the certificate loads.

2. To generate a CSR to send to the CA for certification:
   a. In the Key Creation Parameters, select a key type of RSA or ECDSA, and enter the key length for RSA or elliptic curve for ECDSA.
   b. Choose to enter an optional password in the Challenge and Confirm Challenge fields, which are not required to create a CSR.
   c. Click Create CSR.
   d. When the page refreshes, new buttons appear in the New TLS Certificate section, to allow you to download the CSR, download the key, or delete the CSR.
   e. Click the Download the Certificate Signing Request button to download the CSR. Click the Download Key button to download the file containing the private key.
   f. Send the CSR to a CA for certification. You will get the new certificate from the CA.

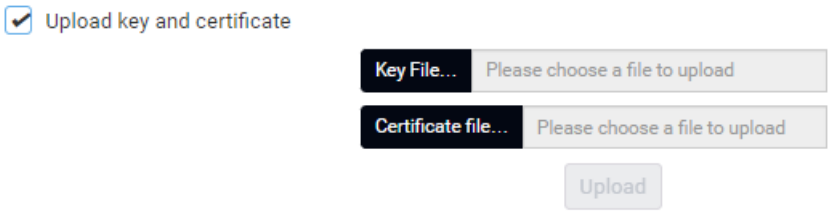
Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.

- Once you get the certificate from the CA, return to this page to upload it to the DKX3G2. After uploading, click Install to start using the new certificate. The page may refresh as the certificate loads.



► *To upload a key and certificate:*

1. To activate the upload fields, click Security > TLS Certificate, then scroll down to the New TLS Certificate section.
2. Select the Upload Key and Certificate checkbox. The Browse and upload controls appear.



Note: If the self signed certificate is expired, HKC client will work only after clearing the browser cache.

Maintenance

About

The About page provides information about your DKX3G2 device and the open source licenses under which this package has been released.

Third Party Licenses

This appendix contains third party licenses for software used by DKX3G2 that require including the license in documentation.

The table below lists all the packages having such modified third party programs, and the appropriate open source license under which that package has been released, including the GNU General Public License('GPL 3.0'), the 'GPL 2.0' , the GNU Lesser General Public License('LGPL 3.0'), the 'LGPL 2.1' and the GNU Library General Public License('LGPL 2.0').

The original and modified versions of the source code of the relevant programs are available at https://www.raritan.com/about/legal-statements/open-source-software-statement.

Package	Version	License
angular	13.3.6	Various Licenses
bootstrap	3.4.1	MIT
brotli	1.0.9	MIT
busybox	1.35.0	GPL 2.0
clish	0.7.3	BSD, GPL 2.0
conntrack-tools	1.4.6	GPL 2.0
dropbear	2020.81	BDS, MIT
e2fsprogs	1.46.5	GPL 2.0
edid-decode	2019-06-14	MIT
etherdump	2.10	GPL2.0
ethtool	5.16	GPL 2.0
gdb	8.0.1	GPL 2.0
iproute2	5.17.0	GPL 2.0
iptables	1.8.7	GPL2.0
iw	5.16	BSD
jquery	3.6.0	MIT
js-cookie	3.0.1	MIT
libaio	0.3.111	LGPL 2.1
libesmtp	1.0.6	LGPL 2.1
libmnl	1.0.4	LGPL 2.1
libnetfilter_conntrack	1.0.9	GPL 2.0

libnfnetlink	1.0.1	GPL 2.0
libnl	3.5.0	LGPL 2.1
libtirpc	1.3.2	BSD
libusb	1.0.24	LGPL 2.1
libxml2	2.9.14	MIT
linux	5.10.149	GPL 2.0
lua	5.3.5	MIT
net-snmp	5.9.3	BSD
ntpclient	2010.365	GPL 2.0
phytool	2	GPL 2.0
spectrum	1.7.1	MIT
strace	5.17	LGPL 2.1
sysvinit	2.84	GPL 2.0
term.js	0.0.6	MIT
text-encoding-js	0.5.3	MIT
u-boot	2017.07	GPL 2.0
uclibc-ng	1.0.40	LGPL 2.1
usbmuxd	1.0.8	GPL 2.0
util-linux-ng	2.18	BSD, GPL 2.0, PD
wpa_supplicant	2.10	BSD

In This Chapter

Licenses - Angular

@angular-devkit/build-angular

MIT

The MIT License

Copyright (c) 2017 Google, Inc.

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.

@angular-devkit/core

MIT

The MIT License

Copyright (c) 2017 Google, Inc.

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.

@angular/animations

MIT

@angular/cdk

MIT

The MIT License

@angular/common

MIT

@angular/core

MIT

@angular/forms

MIT

@angular/material

MIT

The MIT License

@angular/platform-browser

MIT

@angular/router

MIT

@babel/runtime

MIT

MIT License

Copyright (c) 2014-present Sebastian McKenzie and other contributors 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.

@ctrl/ngx-chartjs

MIT

MIT License

Copyright (c) Scott Cooper <scttcper@gmail.com>

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.

@ngx-translate/core

MIT

chart.js

MIT

The MIT License (MIT)

Copyright (c) 2018 Chart.js Contributors

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.

core-js

MIT

Copyright (c) 2014-2021 Denis Pushkarev

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.

regenerator-runtime

MIT

MIT License

Copyright (c) 2014-present, Facebook, Inc.

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.

rxjs

Apache-2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual,

worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made,

use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable

by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and

do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright (c) 2015-2018 Google, Inc., Netflix, Inc., Microsoft Corp. and contributors

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

tslib

0BSD

Copyright (c) Microsoft Corporation.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM 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.

zone.js

MIT

The MIT License

Copyright (c) 2010-2020 Google LLC. https://angular.io/license

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 - 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 - IW

Copyright (c) 2007, 2008 Johannes Berg

Copyright (c) 2007 Andy Lutomirski

Copyright (c) 2007 Mike Kershaw

Copyright (c) 2008-2009 Luis R. Rodriguez

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM 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.

Licenses - JSON-C

Copyright (c) 2009-2012 Eric Haszlakiewicz

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.

Copyright (c) 2004, 2005 Metaparadigm Pte Ltd

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 - LIBTIRPC

Copyright (c) Copyright (c) Bull S.A. 2005 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. 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.

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

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 - 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.

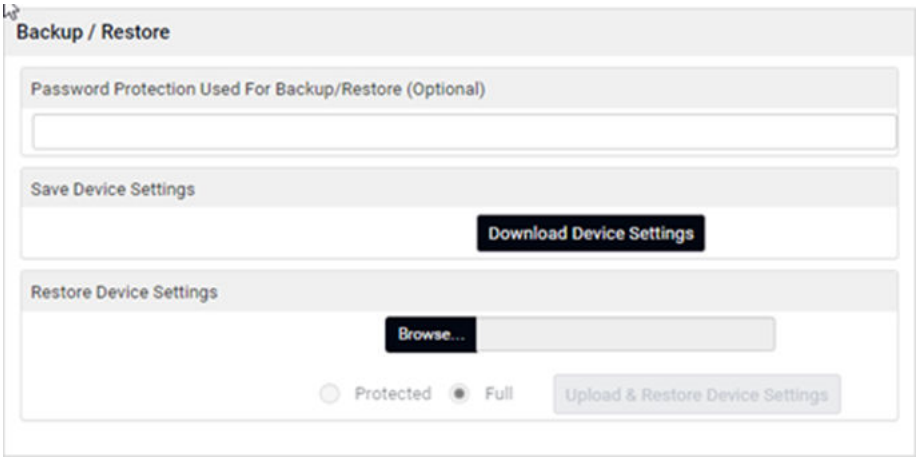
Backup and Restore

You must be a member of the admin group to download a backup file, and to restore a DKX3G2 with a backup file.

Backups can be encrypted by adding password protection. The password must be entered when the file is used to perform a restore.

► *To download the Device Settings backup file:*

1. Click Maintenance > Backup/Restore.
2. To password protect the backup file, enter a password in the Password Protection Used For Backup/ Restore (Optional) field.
3. Click Download Device Settings to automatically download the backup_settings.rfp file.



► *To restore the DKX3G2 using a backup file:*

1. Click Maintenance > Backup/Restore.
2. Click 

to select the backup file.
3. Select Protected or Full.
   - Protected: Restores all settings except for device specific settings: network information, names, preferred resolution.
   - Full: Restores everything.
4. If the file is password protected, enter the password in the Password Protection Used For Backup/ Restore (Optional) field.
5. Click Upload & Restore Device Settings to upload the file.
6. Wait until the DKX3G2 resets and the Login page re-appears, indicating that the restore is complete. Note: In a full restore, the IP address may have been changed. You must start a new browser session to login to the new IP address.

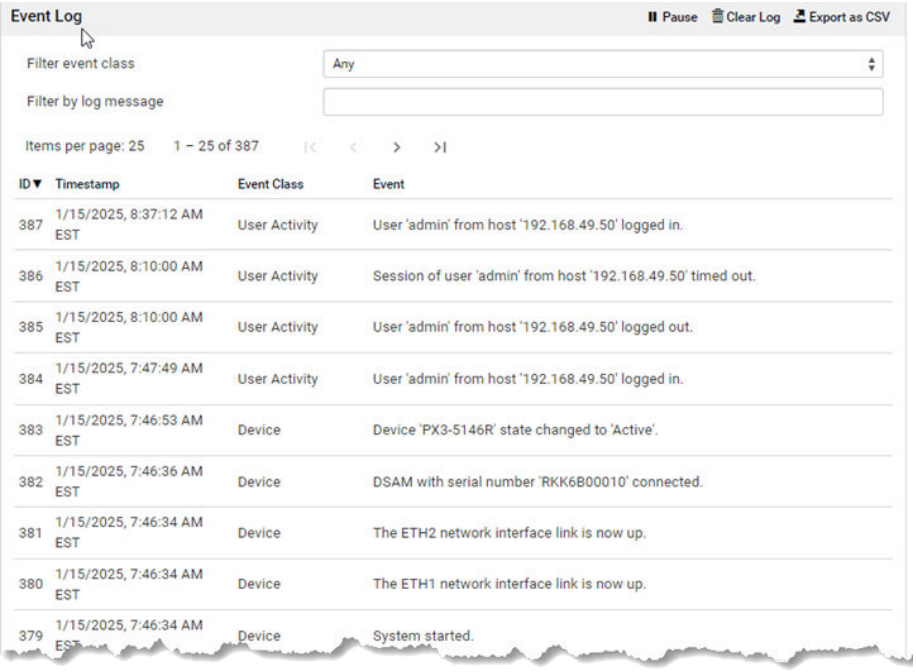
Event Log

The DKX3G2 captures certain system events and saves them in a local event log.

You can view over 2000 historical events that occurred on the DKX3G2 in the local event log. When the log size exceeds 384KB, each new entry overwrites the oldest one.

► *Event Classes:*

- Device
- KVM Port
- Outlet Port
- User Activity
- User Administration
- Serial Port



► *To display the event log:*

- Choose Maintenance > Event Log.
  Each event entry consists of:

- ID number of the event
- Timestamp of the event: The timestamp in the event log is automatically converted to your computer's time zone. To avoid time confusion, apply the DKX3G2 time zone settings to your computer or mobile device.
- Event class
- A description of the event
- All events are dynamically refreshed. You can control the flow by clicking 

or 

buttons.

► *To view by event category:*

- Select an option in the Filter Event Class field.

► *To view by log message:*

- You can filter log messages using specific characters of the messages.

► *To clear the local event log:*

1. Click the Clear Log trash icon  on the top-right corner.
2. Click Clear Log to confirm.

► *To export the log to CSV file:*

1. Click the Export as CSV icon  on the top right corner.
2. CSV file with event logs downloads to local folder.

Update Firmware

Use the Firmware Upgrade page to upgrade the firmware for your DKX3G2 and all attached CIMs. This page is available in the DKX3G2 Remote Console only.

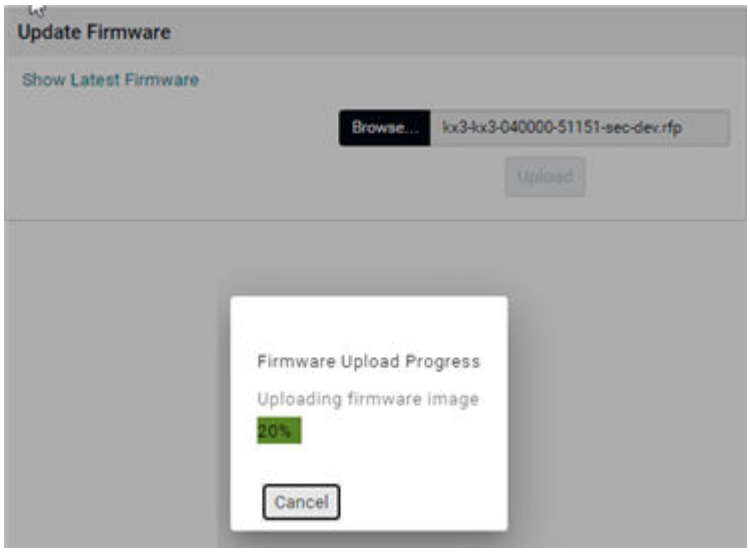
"Show Latest Firmware" link brings up Raritan's Support page: www.raritan.com/support where firmware files are available.

You must have the Maintenance privilege to update the DKX3G2 firmware.

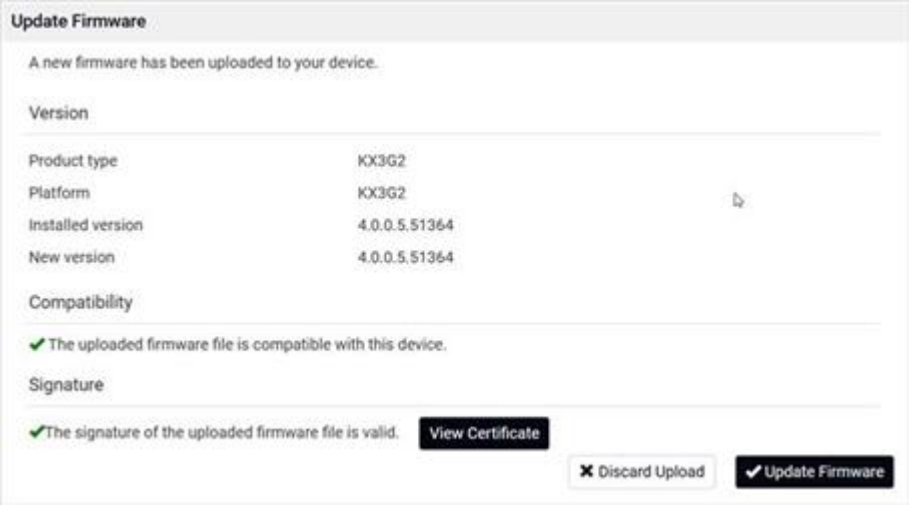
► *To update the firmware:*

1. Click Maintenance > Update Firmware.
2. Click Browse to select an appropriate firmware file, then click Upload. A progress bar appears to indicate the upload process.

Important: Do not turn off your DKX3G2 appliance or disconnect CIMs while the upgrade is in progress - doing so will likely result in damage to the appliance or CIMs.



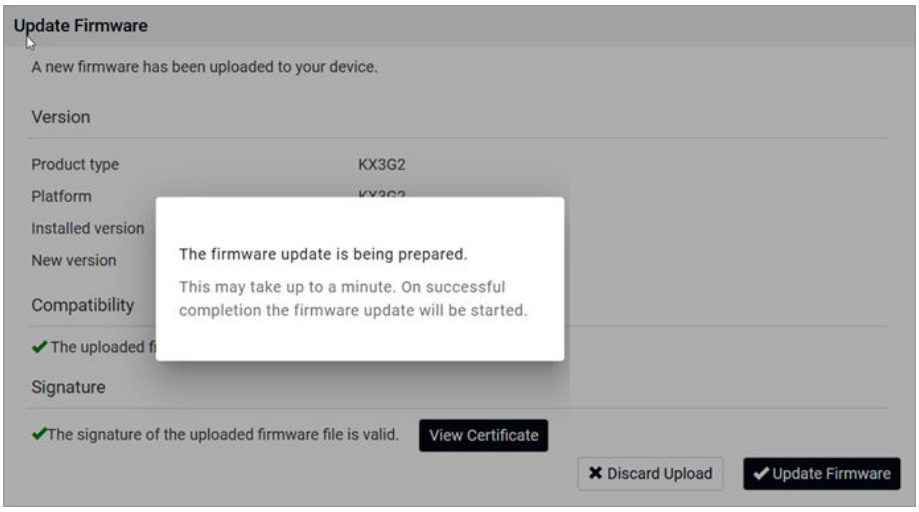
1. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.



- To cancel, click Discard Upload.
- To proceed with the update, click Update Firmware.

2. When the update begins, another progress bar appears.

Note:The status LED will be solid blue during the update and will change to solid green when update is complete.



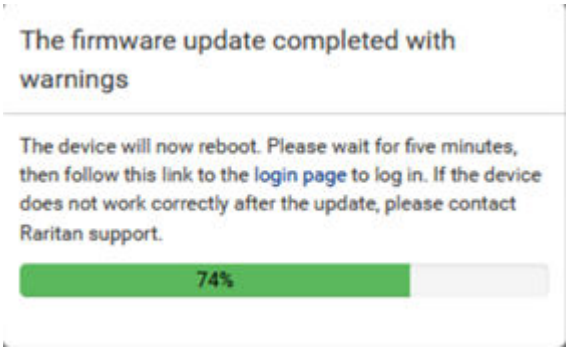
Note: No users can successfully log in during the update. Logged in users are forced to suspend operations.

1. When the update is complete, the DKX3G2 reboots, and the Login page re-appears. The update and reboot process should take around 5 minutes. If your device displays a "Loading" screen after update and reboot for longer, you can safely restart your browser and login to the DKX3G2 again to check the update results.

After Updating: The DKX3G2 MIB may have changed. If you are using an SNMP manager, you may need to re-download the MIB and make update. See: SNMP Settings.

► *The firmware update completed with warnings:*

The message, "The firmware update completed with warnings" may appear before reboot if you completed your update while an iOS device was connected to the USB port on the DKX3G2. This warning does not indicate any problems or that the update failed.



Firmware History

The firmware upgrade history is retained even after device reboot or firmware upgrade. The history is cleared in the event of a factory default reset.

► *To view the firmware update history:*

- Choose Maintenance > Firmware History.
  Each firmware update event consists of:
  - Update date and time
  - Previous firmware version
  - Update firmware version
  - Update result

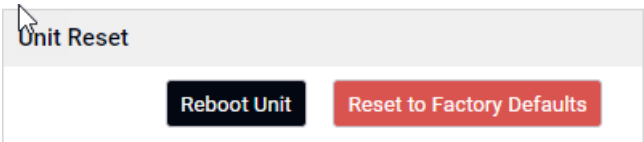
Firmware Update History

Timestamp ▼	Previous Version	Update Version	Status
1/15/2025, 10:27:50 AM EST	4.0.0.1.51020	4.0.0.1.51151	Successful
10/22/2024, 5:07:19 PM EDT	4.0.0.1.50883	4.0.0.1.50883	Successful
10/22/2024, 5:01:11 PM EDT	4.0.0.1.50880	4.0.0.1.50883	Successful
10/21/2024, 10:26:52 AM EDT	4.0.0.1.50880	4.0.0.1.50880	Successful
10/21/2024, 10:21:53 AM EDT	4.0.0.1.50865	4.0.0.1.50880	Successful
10/16/2024, 4:30:30 PM EDT	4.0.0.1.50865	4.0.0.1.50865	Successful
10/16/2024, 4:21:31 PM EDT	4.0.0.1.50844	4.0.0.1.50865	Successful
10/9/2024, 12:59:33 PM EDT	4.0.0.1.50844	4.0.0.1.50844	Successful
10/9/2024, 12:56:12 PM EDT	4.0.0.1.50802	4.0.0.1.50844	Successful
9/25/2024, 11:02:15 AM EDT	4.0.0.1.50719	4.0.0.1.50802	Successful
8/28/2024, 1:25:16 PM EDT	4.0.0.1.50716	4.0.0.1.50719	Successful
8/27/2024, 3:28:45 PM EDT	4.0.0.1.50695	4.0.0.1.50716	Successful

Unit Reset

The Unit Reset section has options to remotely reboot or reset to factory defaults.

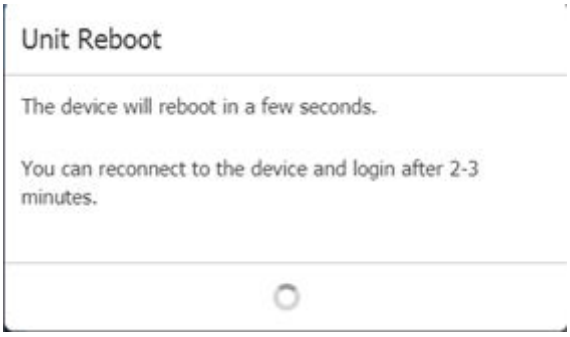
- Reboot Unit: Restarts the DKX3G2.
- Reset to Factory Defaults: Removes all customized settings and returns the DKX3G2 to the factory default settings. Requires admin privilege.



► *To reboot the device:*

1. Choose Maintenance > Unit Reset.
2. Click Reboot Unit.
3. A confirmation message appears. Click Reboot to proceed.

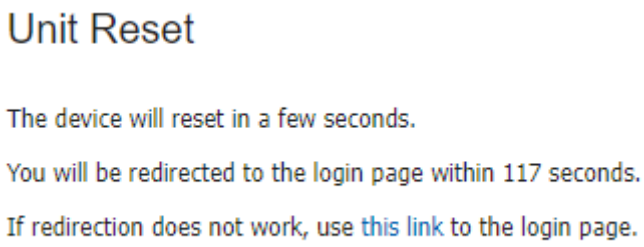
A countdown timer appears.



4. When the restart is complete, the login page opens.

► *To reset to factory defaults:*

1. Click Maintenance > Unit Reset.
2. Click Reset to Factory Defaults.
3. Reset to Factory Defaults screen appears for password verification.
4. Enter password and click Factory Reset.
5. A countdown timer appears. It takes a few seconds to complete.
6. When the reset is complete, proceed with initial configuration. See: Initial Configuration.



► *Other factory reset options:*

- Use the reset button on the DKX3G2 device. Press the reset button for 5 seconds. Device will reset and reboot.
- Perform the CLI command. See CLI: reset (on page 298)

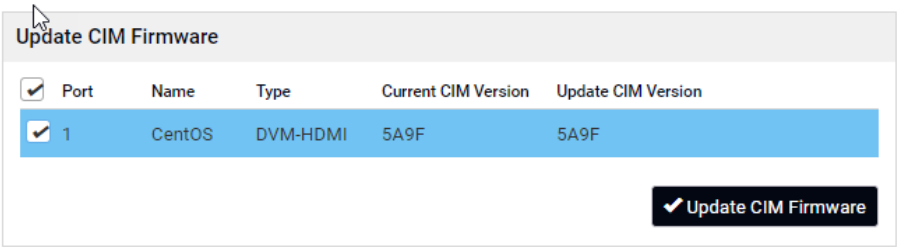
CIM Firmware Upgrade

► *To upgrade CIMs:*

1. Choose Maintenance > Update CIM Firmware. The CIM Upgrade from page opens.

The Port (number), Name, Type, Current CIM Version, and Current CIM Version are displayed for easy identification of the CIMs.

2. Check the Selected checkbox for each CIM you want to upgrade.
3. Click Update CIM Firmware. You are prompted to confirm the upgrade
4. Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes or less per CIM.
5. After the CIM upgrade is complete, the DKX3G2 will reboot.



Note: Message during CIM firmware upgrade: "The CIM firmware update is in progress. This may take some minutes. Please do not power off the device while the update is in progress! After a successful update, the device will be reboot automatically."

CIM Firmware History

The DKX3G2 provides information about upgrades performed.

► *To view the upgrade history:*

1. Choose Maintenance >CIM Firmware History. The CIM Firmware Update History page opens.
2. Information is provided about the DKX3G2's CIM upgrade(s):

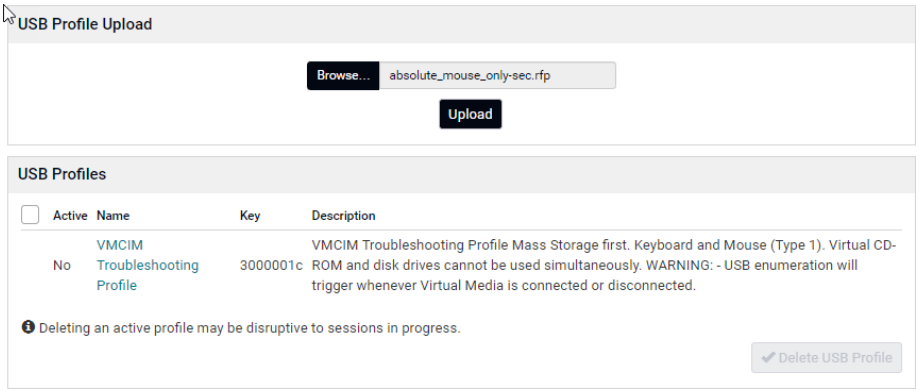
- Time stamp:
  - Date - Date of the upgrade
  - End Time - end time of the upgrade
- Port - The port where the CIM is connected
- Name of the port - The port name where the CIM is connected
- Type - The type of CIM
- Previous Version - Previous CIM firmware version
- Upgrade Version - Current CIM firmware version
- Status - The result of the upgrade (success or fail)

USB Profile Management

From the USB Profile Management page, you can upload custom profiles provided by technical support. These profiles are designed to address the needs of your target server's configuration, in the event that the set of standard profiles does not already address them. Technical support will provide the custom profile and work with you to verify the solution for your target server's specific needs.

► *To access the USB Profile Management page:*

- Choose Maintenance > USB Profile Management. The USB Profile Management page opens.



► *To upload a custom profile to your DKX3G2:*

1. Click Browse. A Choose File dialog appears.
2. Navigate to and select the appropriate custom profile file and click Open. The file selected is listed in the USB Profile File field.
3. Click Upload. The custom profile will be uploaded and displayed in the Profile table.

Note: If an error or warning is displayed during the upload process (for example. overwriting an existing custom profile), you may continue with the upload by clicking Upload or cancel it by clicking on Cancel.

► *To delete a custom profile to your DKX3G2:*

1. Check the box corresponding to the row of the table containing the custom profile to be deleted.
2. Click Delete. The custom profile will be deleted and removed from the Profile table.

Note: If you delete a custom profile from the system while it is still designated as an active profile you will terminate any virtual media sessions that were in place.

Diagnostics

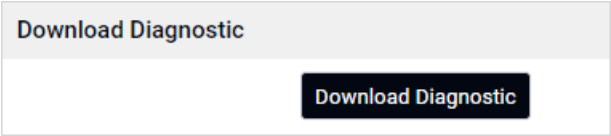
Download Diagnostics

Note: This page is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

Use this feature to download diagnostic information from the DKX3G2 to the client machine. This encrypted file is then sent to Raritan Technical Support. Only Raritan can interpret this file.

Note: This page is accessible only by users with administrative privileges.

1. Choose Diagnostics > DKX3G2 Diagnostics. The DKX3G2 Diagnostics page opens.
2. To create a diagnostics file to send to Raritan Technical Support, click Download Diagnostic.
3. Email this file as directed by Raritan Technical Support.



Network Diagnostics

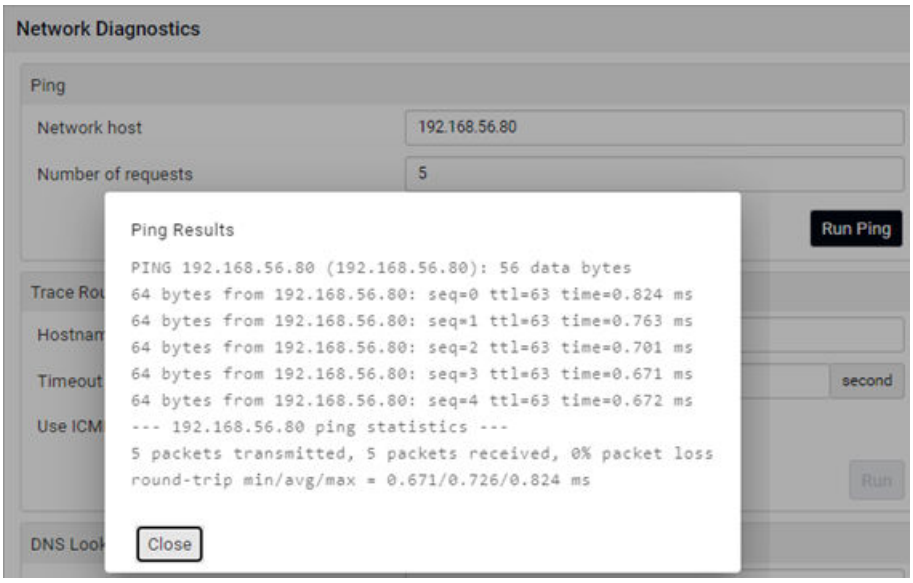
DKX3G2 provides the following tools to diagnose potential networking issues.

- Ping
- Trace Route: Find out the route over the network between two hosts or systems.
- List TCP Connections: Display a list of TCP connections.
- DNS Lookup:Display a list of DNS records for the domain in priority order.
- List TCP/UDP Listen Sockets: Display a list of TCP/UDP Listen Sockets.

  Choose Diagnostics > Network Diagnostics, and then perform any function below.

► *Ping:*

Enter the IP or hostname in the Network Host field, then set the of requests to send. Maximum is 20. This determines how many packets are sent for pinging the host. Click Run Ping to ping the host. The Ping results are then displayed.



► *Trace Route:*

1. Type values in the following fields.

Field/setting	Description
Hostname	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation. Maximum 900 seconds.
Use ICMP packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are displayed.

► *DNS Lookup:*

1. Type value in the following field.

Field/Setting	Description

Hostname	The IP address or name of the host whose DNS lookup you want to check.

2. Click Run. The DNS Lookup results are displayed.

► *List TCP Connections:*

1. Click the List TCP Connections title bar to show the list of active connections.

2. Click Refresh. The list will show latest connections.

► *List TCP/UDP Listen Sockets:*

1. Click the List TCP/UDP Listen Sockets title bar to show the list of active connections.

List TCP/UDP Listen Sockets

Refresh

#	Netid	State	Recv-Q	Send-Q	Local-Address:Port	Peer-Address:Port
1	udp	UNCONN	0	0	0.0.0.0:47157	0.0.0.0:*
2	udp	UNCONN	0	0	0.0.0.0:68	0.0.0.0:*
3	udp	UNCONN	0	0	0.0.0.0%eth1:5353	0.0.0.0:*
4	udp	UNCONN	0	0	0.0.0.0%eth0:5353	0.0.0.0:*
5	udp	UNCONN	0	0	0.0.0.0%eth1:5355	0.0.0.0:*
6	udp	UNCONN	0	0	0.0.0.0%eth0:5355	0.0.0.0:*
7	udp	UNCONN	0	0	*:53284	*:*
8	udp	UNCONN	0	0	*%eth1:5353	*:*
9	udp	UNCONN	0	0	*%eth0:5353	*:*
10	udp	UNCONN	0	0	*%eth1:5355	*:*
11	udp	UNCONN	0	0	*%eth0:5355	*:*
12	udp	UNCONN	0	0	*:5000	*:*
13	tcp	LISTEN	0	10	127.0.0.1:8181	0.0.0.0:*
14	tcp	LISTEN	0	10	*:5000	*:*
15	tcp	LISTEN	0	10	*:80	*:*
16	tcp	LISTEN	0	10	*:22	*:*
17	tcp	LISTEN	0	10	*:443	*:*

2. Click Refresh. The list will show latest connections.

Port Groups

The DKX3G2 supports the aggregation of multiple ports into a single port group. Port groups consist solely of ports configured as standard KVM ports.

A port may only be a member of a single group.

Ports that are available to be included in a port group are displayed in the Select Ports for Group > Available list.

Once a port is added to a port group, it is not available to add to another port group. Remove the port from its existing port group to use it in a new one.

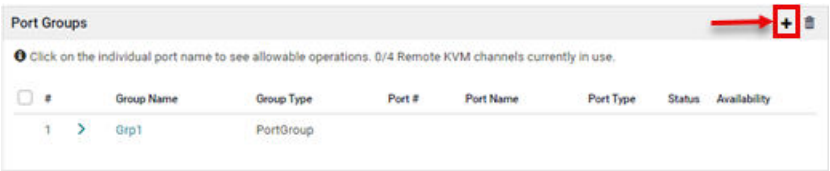
A maximum of 32 port groups can be created. The Add button is disabled once this limit is reached.

Port Groups are restored using the Backup and Restore option (see: Backup and Restore).

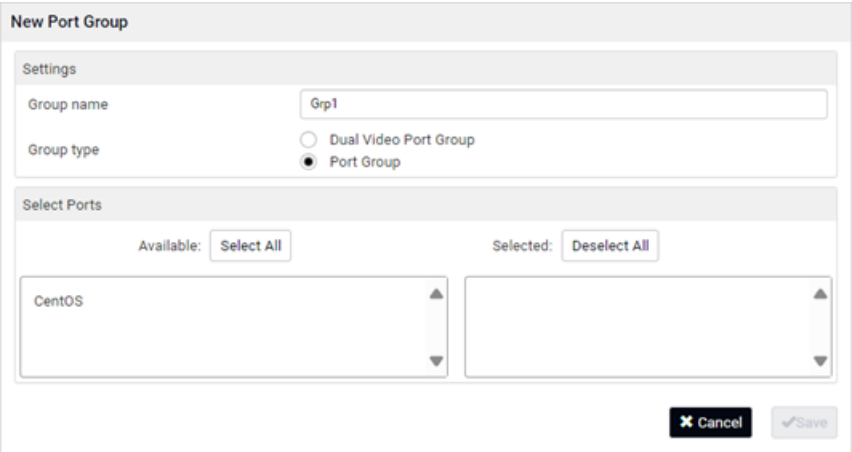
Create Port Groups

► *To create a port group:*

1. Select Port Groups. The Port Groups page opens. Any existing port groups are displayed.
2. Click Add. The page refreshes and displays all of the port group options available.



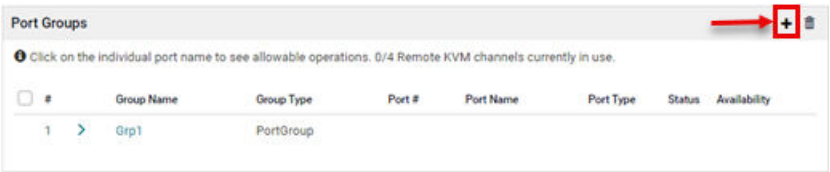
3. Select the Port Group radio button.
4. Enter Group name.
5. Select the ports to add to the group by clicking on them in the Available text box, to add it to the Selected text box.
6. Click OK to create the port group. The port group now appears on the Port Groups page.



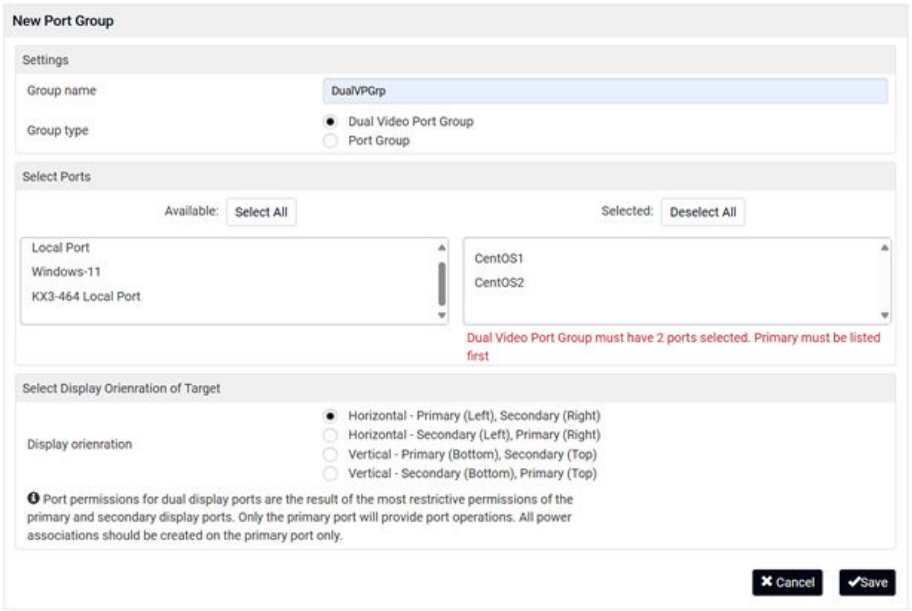
Create Dual Video Port Groups

► *To create a dual video port group:*

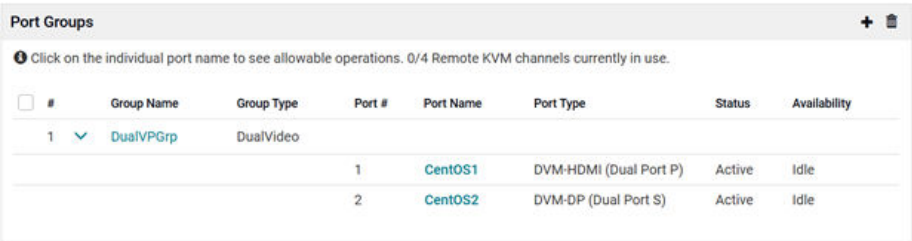
1. Select Device Settings > Port Groups. The Port Group page opens. Any existing port groups are displayed.
2. Click Add. The page refreshes and displays all of the port group options available.



3. Select the Dual Video Port Group radio button.
4. Enter Group name.
5. Select the two ports of the dual video group by clicking on them in the Available target section, to move to the Selected section.



6. Select Display orientation of the target.
7. Click Save.



Port Scan

► *To scan connected ports:*

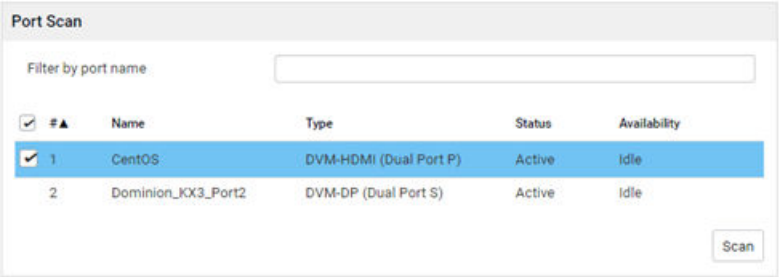
Use the port scanning feature to search for selected targets, and display them in a slide show view, allowing you to monitor up to 32 targets at one time. You can connect to targets or focus on a specific target as needed.

For dual video port groups, the primary port is included in a port scan, but the secondary port is not included.

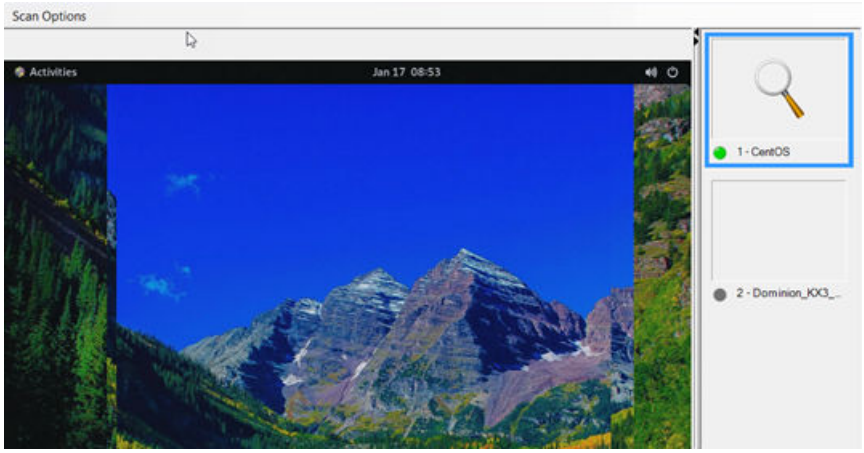
Note: The Scan Ports functionality is only available with the VKC and AKC clients.

---

1. Click the Port Scan->Port Scan page opens up.



2. Select one or multiple targets and click Scan.



Scanning Ports Slide Show

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.

Note: Scan settings for the Remote Console is configured in the KVM client.

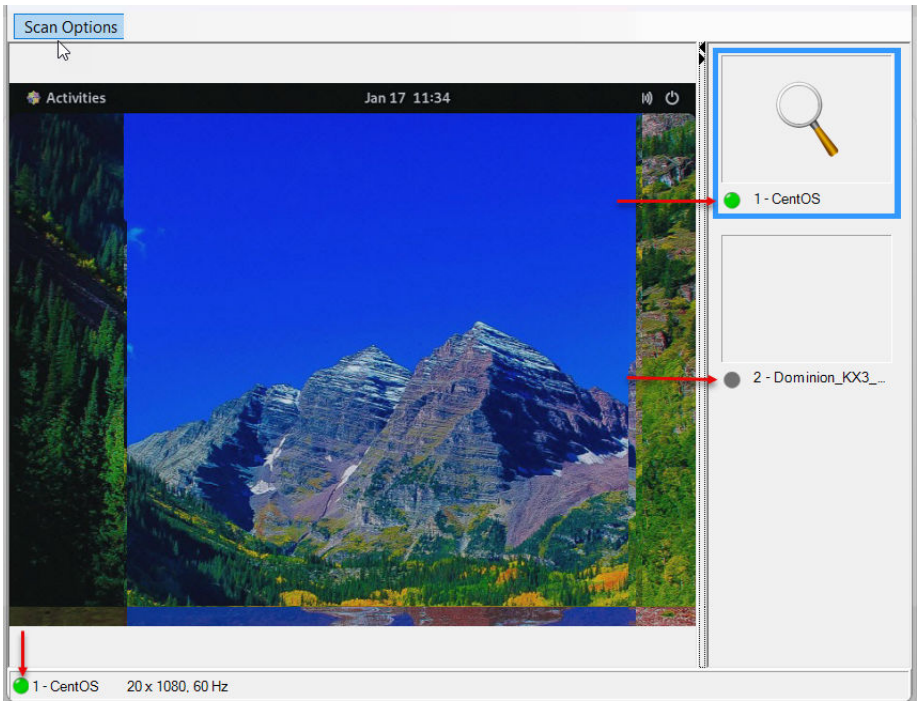
Target Status Indicators During Port Scanning

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:

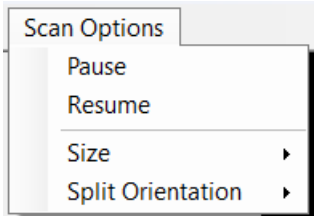
- Yellow - the target is down but connected.
- Green - the target is up/idle or up/connected
- Gray - the target is down but connected
- Red - the target is down/idle, busy, or otherwise not accessible
- 

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.

Dual Video Port Groups

Servers with dual video cards can be remotely accessed with an extended desktop configuration, which is available to remote users. This is done by creating dual port video groups. Extended desktop configurations allow you to view the target server desktop across two monitors vs. the standard single monitor view. Once a dual port video group is selected, all port channels in that group open simultaneously.

See: Dual Port Video Configuration Steps (on page 261).

Review the information in this section for important information regarding dual port video groups.

Recommendations for Dual Port Video

Set the target server's primary and secondary displays to the same video resolution in order to maintain mouse synchronization and minimize having to periodically resync.

The top display (vertical orientation) or left display (horizontal orientation) should be the designated primary display. This display will provide active menu selection for virtual media, audio, smart card and mouse operations.

To provide intuitive mouse movement and control, the following should have the same display orientation:

- Client PC's primary and secondary displays
- This device's dual video port group configuration
- Target server's primary and secondary displays

The use of single mouse mode is not recommended when displaying dual video ports in full screen mode on a single client monitor. This will require exiting single mouse mode in order to access and view the other display.

Dual Video Port Group Supported Mouse Modes

Target operating systems	Supported mouse modes	Comments
All Windows® operating systems	Absolute, Intelligent, Standard and Single Mouse Mode	Intelligent Mode works best provided "Enhanced Pointer Precision" is unticked on the target (Control Panel/Mouse/Pointer Options) and mouse speed is 50%. Standard Mode also works provided "Enhanced Pointer Precision" is unticked and mouse speed is 50%. Mouse does not sync correctly in Absolute Mouse Mode on latest Windows Operating Systems. You will have two mice, one for the client and one for the operating system. They do not sync together and allow for one continuous display across all monitors.

Target operating systems	Supported mouse modes	Comments
Linux®	Absolute, Intelligent, Standard and Single Mouse Mode	Absolute Mouse Mode works best.
Mac® operating system	Absolute, Intelligent, Standard and Single Mouse Mode	Single Mouse mode should be used as the mouse does not sync on any mode for Dual Video Port Apple Mac targets.

Note: 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.

CIMs Required for Dual Video Support

The following CIMs support the dual video port feature:

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2
- D2CIM-VUSB-USBC

See: Supported Computer Interface Module (CIMs) Specifications for CIM specifications.

If the original CIM attached to a primary or secondary video port is disconnected and replaced with another CIM, the port is removed from the dual port video group. If needed, re-add the port to the group.

Note: The CIM you use depends on your target server requirements.

Dual Port Video Group Usability Notes

Following are various functions that are affected when using the dual port video group feature.

- Client Launch Settings that are configured in the VKCS, and AKC clients via Tools > Options > Client Launch Settings will be applied to dual video port groups as follows:
  - Window Mode settings will be applied
  - Monitor settings will NOT be applied. Instead the Port Group Management configured 'Display Orientation' will be applied.
  - Other - Enable Single Mouse Cursor setting will be applied
  - Other - Enable Scale Video setting will be applied
  - Other - Pin Menu Toolbar setting will be applied
  - Cursor shape will be applied
  - Always Show toolbar will be applied
  - Always Show Status bar will be applied
- Dragging and moving items between windows on the primary and secondary target requires a release and press of the mouse button as the item is moved from one window to the other.
- On Linux® and Mac® target servers, when Caps Scroll, and Num Lock is turned on, the Caps Lock indicator in the status bar of the primary port window is displayed, but the indicator may not be displayed in the status bar of the secondary port window.

Permissions and Dual Video Port Group Access

Ideally, the permissions applied to each port in the port group should be the same. If they are not, the permissions of the port with the most restrictive permissions are applied to the port group.

For example, if VM Access Deny is applied to one port and VM Access Read-Write is applied to another port, VM Access Deny is applied to the port group.

If a user does not have the appropriate permissions to access a port that is part of a dual video port group, only the port that they do have permissions to access is displayed. If a user does not have permissions to access either port, access is denied.

A message indicating that the port is either not available or the user does not have permission to access the port is displayed when they try to access it.

Example Dual Port Video Group Configuration

The following is a general example.

Your configuration may vary in the type of CIMs used, the port you designate as the primary port, the ports you are connecting to and so on.

In this example, we are using:

- A target server with two video ports
- Target server video port 1 as the primary port, and target server video port 2 as the secondary port
- A DKX3G2-832 appliance
- A D2CIM-DVUSB-DP CIMs
- A target server and remote PC running AKC
- Intelligent mouse mode

An extended desktop view on the target server and remote client, so we are configuring the DKX3G2 to support a "Horizontal - Primary (Left), Secondary (Right)" display orientation.

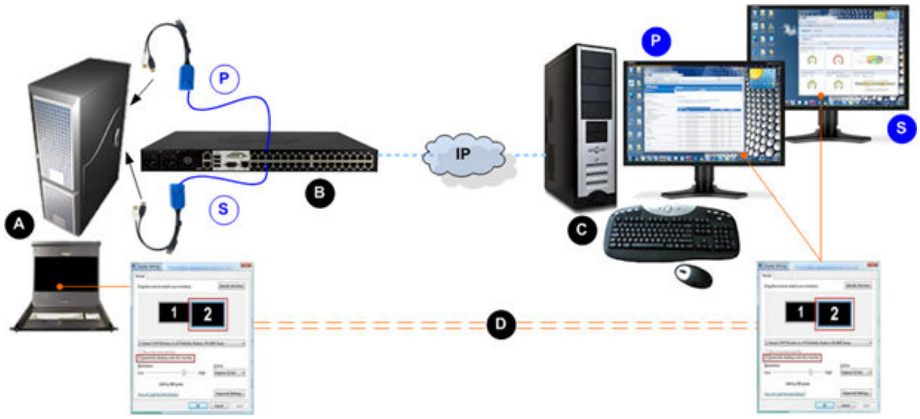


Diagram key	
A	Remote client - configure the dual port video group and display settings
B	DKX3G2

Diagram key	
P	Connection from the target's primary (first) video port to the DKX3G2
S	Connection from the target's secondary (second) video port to the DKX3G2
IP connection between the DKX3G2 and remote client	
C	Target server - configure the display settings and launch the dual port video group
D	Display settings are the same on the remote client and target server (recommended)
P	Horizontal - Primary (Left) - defined on the Port Group Management page in DKX3G2
S	Secondary (Right) - defined on the Port Group Management page in DKX3G2

Dual Port Video Configuration Steps

Step 1: Configure the Target Server Display

For information on display orientations and mouse modes, review the previous topics in this section.

Note: See your target server or operating system user documentation for exact steps on configuring display settings.

► *To configure target server display and mouse settings:*

1. At the target server, configure the target server display orientation for each video port to match the display orientation of your remote client.

For example, if you are using an extended desktop orientation moving from left-to-right across two monitors at the remote client, set the target server display orientation to the same.

2. Ensure that your target server's video has already been set to a supported resolution and refresh rate. See: Supported Target Server Video Resolutions (on page 311)

Step 2: Connect the Target Server to the DKX3G2

Dual port video groups can be created from existing port connections, or new port connections.

The steps provided here assume you are creating new connections.

If you are creating a dual port video group from existing connections, see Step 4: Create the Dual Video Port Group.

► *To connect the equipment:*

1. Install and power up your target server per the manufacturer's instructions if you have not already done so.
2. Attach each CIM's video connector to each of the target's video output ports, then connect the USB cables to available USB ports on the target.
3. Connect each CIM to the KVM switch using a CAT5/6 cable.
4. If you have not already done so:
   a. Connect to an AC power source using the provided power cable
   b. Connect to the network port and local port (if needed)
   c. Do the initial configurations.
5. Launch a supported web browser.
6. Enter the URL that corresponds to the client you want to use:
   - http://IP-ADDRESS/akc for the Active KVM Client from supported Microsoft .Net based environments.

Or

   - http://IP-ADDRESS/vkcs for the standalone Java-based Virtual KVM Client for Chrome, Firefox, and Edge browsers.

Or

   - http://IP-ADDRESS/hkc for the HTML KVM Client.

IP-ADDRESS is the IP address assigned to your DKX3G2

You can also use HTTPS, or the DNS name of the DKX3G2 assigned by your administrator (if applicable).

You are always redirected to the IP address from HTTP to HTTPS.

7. Enter your username and password, then click Login.
8. Accept the user agreement (if applicable).
9. If security warnings appear, accept and/or allow access.

Step 3: Configure the Mouse Mode and Ports

Once you have connected the target server through the target server video ports, the connection is detected, and the ports display on the Port Configuration page.

After the ports are configured, they can be grouped in a dual video port group.

Note: Existing ports do not have to be configured if you have already done so when creating dual port video groups. See: Create Dual Video Port Groups (on page 251)

Configure the target server mouse mode after you connect to the target. See: Dual Video Port Group Supported Mouse Modes.

Step 4: Create the Dual Video Port Group

See: Create Port Groups (on page 251)

Step 5: Launch a Dual Port Video Group

Once you have created the dual video port group, it is available on the Port Access page.

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.

Session timeouts that are configured on the DKX3G2 are applied to both ports of a dual video group.

► *To launch a dual port group:*

- On the Port Access page, click on the primary port name, then click Connect.

Both connections are launched at once and displayed in two different windows.

Once the windows are displayed, they can be moved based on the display setup you are using. For example, if you are using extended desktop mode, the port windows can be moved between monitors.

Client Navigation when Using Dual Video Port Groups

When using full screen mode in the clients, switch between ports by:

- Virtual KVM Client (VKC)
  - Pressing Alt+Tab
  - For Mac® clients, pressing F3, then selecting the port display
- Active KVM Client (AKC)
  - Clicking your mouse outside the display window, then pressing Alt+Tab
- HKC
  - See: HTML KVM Client (HKC).

Direct Port Access and Dual Port Video Groups

Direct Port Access allows users to bypass having to use the DKX3G2's Login dialog and Port Access page.

This feature also provides the ability to enter a username and password directly to proceed to the target, if the username and password is not contained in the URL.

If you are accessing a target that is part of a dual port video group, direct port access uses the primary port to launch both the primary and secondary ports.

Direct port connections to the secondary port are denied, and usual permission rules apply.

For information on the dual port video group feature, see Creating a Dual Video Port Group.

For information on direct port access, see: Enabling Direct Port Access via URL.

Dual Port Video Groups Displayed on the Ports Page

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

For dual video port groups, the primary port is included in a port scan, but the secondary port is not included.

See: Port Scan (on page 253) for information on performing scans.

Local Port Console Interface

The DKX3G2 provides at-the-rack access and administration via its local port. Access to DKX3G2 features are provided via the Local Console.

The majority of administrative functions are performed from the DKX3G2 Remote Console whereas on Local port you can only configure network settings.

Device Information tab provides DKX3G2 information, network information, CIM details and Open Source license notification.

Note: The local port can be configured from the Remote Console see:Local Port (on page 175)

Foreign KBs are not supported at the local port

Local Port User Authentication

Set the authentication mode via DKX3G2 Remote Console.See: Select the Local User Authentication (on page 177). In order to use the DKX3G2 Local Console, you must first authenticate with a valid username and password.

The DKX3G2 provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port.

In either case, the DKX3G2 allows access only to those servers to which a user has access permissions. See User Management for additional information on specifying server access and security settings.

If your DKX3G2 has been configured for external authentication services (LDAP/LDAPS, RADIUS, or Active Directory), authentication attempts at the Local Console also are authenticated against the external authentication service.

Note: You can also specify no authentication for Local Console access; this option is recommended only for secure environments.

1. To use the DKX3G2 Local Console:
2. Connect a keyboard, mouse, and video display to the local ports at the back of the DKX3G2.
3. Start the DKX3G2. The DKX3G2 Local Console interface displays.

Simultaneous Users

The DKX3G2 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 DKX3G2, you can still simultaneously access your servers from the rack via the Local Console.

Accessing a Target Server

► *To access a target server:*

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

Select the Local Port Hotkey

Because the DKX3G2 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.

The Local Port hot key allows you to rapidly access the DKX3G2 Local Console user interface when a target device is currently being viewed.

See: Select the Local Port Hotkey (on page 176) to set the hot key. The default is to Double Click Scroll Lock.

Select the Local Port Connect Key

See: Select the Local Port Connect Key (on page 177) to setup local port connect key. Use a connect key sequence to connect to a target and switch to another target without returning to the GUI. See: Connect and Hot Key Examples (on page 177). Then use the hot key to disconnect and return to the local port GUI.

Local Console Video Resolution Behavior

By default, monitors are typically set to the highest resolution they support. Once a monitor is connected to the DKX3G2 Local Console, DKX3G2 detects the monitor's native resolution. As long as the native resolution is supported by the Local Console, DKX3G2 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, DKX3G2 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 DKX3G2 Local Console. DKX3G2 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, DKX3G2 uses the resolution of 1600x1200@60Hz.

See: Local Port Supported Resolutions by HDMI Interface (on page 313) for the full list of Local Console video resolutions supported by HDMI interface.

Dominion User Station

To use a standalone appliance for remote access to DKX3G2 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

The Dominion User Station is designed to access servers and computer devices connected to DKX3G2's from your LAN/WAN networks. ALL DKX3G2 models are supported. DKX3G2 Release 4.0.0 and above is required.

User Station Photo and Features

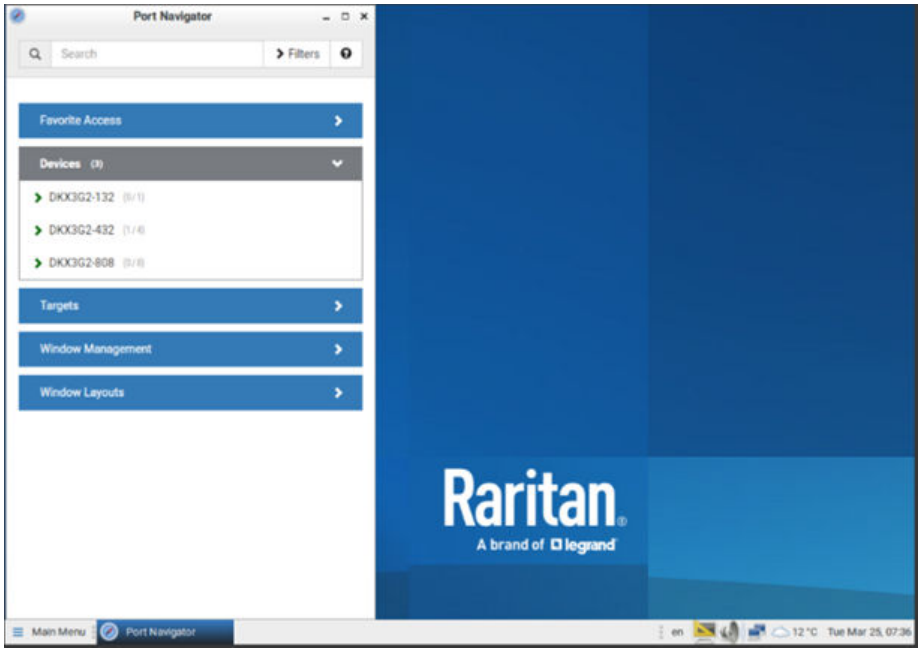
- Supports up to 4 monitors
- Three 1080p streaming video sessions at 30 FPS
- Supports VGA, DVI, HDMI and DisplayPort video
- Favorites and hot-key switching
- Access hundreds of servers
- Dual Gigabit Ethernet ports
- Self-contained, low maintenance appliance
- Desktop, rack and VESA mountable

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 DKX3G2's data. See: Logging In to DKX3G2.
4. The added DKX3G2's are displayed in the Port Navigator window.



5. Click a DKX3G2 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.

Command Line Interface (CLI)

In This Chapter

CLI Overview

The Command Line Interface (CLI) can be used to configure the DKX3G2 network interface and perform diagnostic functions, provided you have the appropriate permissions to do so.

There is a limited set of CLI commands. See: CLI Commands for a list of all the commands, definitions and links to examples.

Accessing the DKX3G2 Using CLI

Access the DKX3G2 by using one of the following methods:

- SSH (Secure Shell) via IP connection or via connecting at the local serial port

A number of SSH clients are available and can be obtained from the following locations:

- Putty - http://www.chiark.greenend.org.uk/~sgtatham/putty/
- SSH Client from ssh.com - www.ssh.com
- Applet SSH Client - www.netspace.org/ssh
- OpenSSH Client - www.openssh.org

SSH Connection to the DKX3G2

Use any SSH client that supports SSHv2 to connect to the DKX3G2. You must enable SSH access from the Devices Services page.

Note: For security reasons, SSH V1 connections are not supported by the DKX3G2.

SSH Access from a Windows PC

► *To open an SSH session from a Windows® PC:*

1. Launch the SSH client software.
2. Enter the IP address of the DKX3G2 server. For example, 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click Open.

The `login as:` prompt appears.

See: Logging In (on page 270).

SSH Access from a UNIX/Linux Workstation

► *To open an SSH session from a UNIX®/Linux® workstation:*

1. Log in as the user `admin`, enter the following command:

```
ssh -l admin <IP address>
```

Enter your password when the `Password` prompt appears.

See: Logging In (on page 270).

Logging In

► *To log in, enter the user name admin as shown:*

1. Log in as `admin`
2. The Password prompt appears. Enter the default password: *raritan*

The welcome message displays. You are now logged on as an administrator.

After reviewing the following Navigation of the CLI section, perform the Initial Configuration tasks.

Navigating the CLI

Before using the CLI, it is important to understand CLI navigation and syntax.

There are also some keystroke combinations that simplify CLI use.

Completion of Commands

The CLI supports the completion of partially-entered commands.

After entering the first few characters of an entry, press the Tab key.

- If the characters form a unique match, the CLI will complete the entry.
- If no match is found, the CLI displays the valid entries for that level.
- If multiple matches are found, the CLI displays all valid entries.

Enter additional text to make the entry unique and press the Tab key to complete the entry.

CLI Syntax-Tips and Shortcuts

Tips

- Commands are listed in alphabetical order.
- Commands are not case sensitive.
- Parameter names are a single word without an underscore.
- Commands without arguments default to show current settings for the command.
- Typing a question mark (`?`) after a command produces help for that command.
- A slash symbol ([/]) indicates a choice within an optional or required set of keywords or arguments.

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 to execute the command.
- Press Tab to complete a command. For example,#config:# `port > p and tab` The system then displays the config:# `port >parity`.

Initial Configuration Using CLI

Note: These steps, which use the CLI, are optional. The same configuration can be done via the Remote or Local Console.

DKX3G2 devices come from the factory with default factory settings. When you first power up and connect to the device, you must set the following basic parameters so the device can be accessed securely from the network:

1. Reset the administrator password. All DKX3G2 devices are shipped with the same default password. To avoid security breaches you must change the admin password from raritan to a custom password for the administrators who will manage the DKX3G2 device.
2. Assign the IP address, subnet mask, and gateway IP address to allow remote access.

Setting Parameters

To set parameters, you must be logged on with administrative privileges.

Setting Network Parameters

Network parameters are configured using the interface command.

IPV4:

```
config:# network ipv4 interface <interface> [enabled <enabled>]
[configMethod <configMethod>] [preferredHostName <prefHostname>]
[address <addrCidr>] [gateway <gateway>]

IPV6:

config:# network ipv6 interface <interface> [enabled <enabled>]
[configMethod <configMethod>] [preferredHostName <prefHostname>]
[address <addrCidr>] [gateway <gateway>]
```

When the command is accepted, the device automatically drops the connection. You must reconnect to the device using the new IP address and the user name and password you created in the resetting factory default password section.

Important: If the password is forgotten, the DKX3G2 will need to be reset to the factory default from the Reset button on the back of the DKX3G2. The initial configuration tasks will need to be performed again if this is done.

The DKX3G2 can now has be accessed remotely via SSH or the GUI using the new IP address. The administrator needs to configure the users and groups, services, security, and serial ports to which the serial targets are attached to the DKX3G2.

CLI Prompts

The Command Line Interface prompt indicates the current command level.

The root portion of the prompt is the login name.

The root prompt is "#" or ">". It is the root portion of a command when you establish a direct admin serial port connection via a terminal emulation application.

```
#
```

CLI Commands

► *To see the available commands:*

- Login and type ?: #?

Command	Description
check	Check services
clear	Clear logs
config	Enter configuration view
connect	Connect to a port. (Only when DSAM is attached.)
diag	Change to diagnostics sub menu.

Command	Description
exit	Exit CLI session
reset	Reset
show	Shows various device information

CLI: check

check

check ntp

CLI: clear

clear

clear eventlog

Do you really want to clear the event log? [y/n]

CLI: config

► *To see available config commands:*

- # config?

Command	Description
apply	Save changed settings and leave config mode
authentication	Configure authentication settings
autoscan	Configure auto scan settings
cancel	Save changed settings and leave config mode
check	Check services
device	Configure Device
group	Configure user groups
keyset	Configure keyset settings
keyword	Configure keywords for DSAM serial ports
localport	Configure local port settings
network	Configure network settings
password	Change password of currently logged in user

Command	Description
pdu	Configure PDU settings
port	Configure DSAM serial port settings
security	Configure security settings
serial	Configure serial port settings
time	Configure date/time settings
user	Configure users
vmshare	Configure virtual media shared image settings

CLI: config authentication

authentication

config # authentication

Available commands:

- ldap Configure LDAP server settings
- radius Configure Radius server settings
- type Configure authentication type (local/ldap/radius)

► *LDAP:*

add Add a new LDAP server

addClone Add a new LDAP server, cloning another server

delete Delete LDAP server

modify Modify an existing LDAP server

config # authentication ldap add

authentication ldap add <host> <port> < type> <security> <bindtype> <basedn> <loginnameattr> <userentryclass> [userSearchSubfilter <usersearchfilter>] [groupInfoInUserEntry<Group membership info>] [groupMemberAttribute <Group member attribute] [groupEntryObjectClass <Group entry class>] [groupSearchSubfilter <Group search subfilter>] [adDomain <addomain>] [verifyServerCertificate <certverify>] [allowExpiredCertificate <allowexpiredcert>] [bindDN <binddn>]

Add a new LDAP server

host IP address/host name

port Port number (0..4294967295)

type LDAP server type (openldap/activeDirectory)

security Security type (none/startTls/tls)

bindtype Bind type (anonymousBind/authenticatedBind)

basedn Base DN for search

loginnameattr Login name attribute

userentryclass User entry object class

userSearchSubfilter User search subfilter

groupInfoInUserEntry Group membership info in user entry (true/false)

groupMemberAttribute Group member attribute

groupEntryObjectClass Group entry object class

groupSearchSubfilter Group search subfilter

adDomain Active directory domain

verifyServerCertificate Enable validation of LDAP server certificate (true/false)

allowExpiredCertificate Allow expired and not yet valid server certificates (true/false)

bindDN Bind DN

config # authentication ldap addClone

authentication ldap addClone <index> <host>

Add a new LDAP server, cloning another server

index Source server index

host IP address/host name

- config # authentication ldap delete

authentication ldap delete <index>

Delete LDAP server

index Server index

config # authentication ldap modify

authentication ldap modify <index> [host <host>] [port <port>] [serverType <Server type>] [securityType <security>] [bindType <bindtype>] [searchBaseDN <basedn>] [loginNameAttribute <loginnameattr>] [userEntryObjectClass <userentryclass>] [userSearchSubfilter <usersearchfilter>] [groupInfoInUserEntry<Group membership info>] [groupMemberAttribute <Group member attribute] [groupEntryObjectClass <Group entry class>] [groupSearchSubfilter <Group search subfilter>] [adDomain <addomain>] [verifyServerCertificate <certverify>] [certificate] [allowExpiredCertificate <allowexpiredcert>] [bindDN <binddn>] [bindPassword] [sortPosition <position>]

Modify an existing LDAP server

index Index

host IP address/host name

port Port number (0..4294967295)

serverType LDAP server type (openldap/activeDirectory)

securityType Security type (none/startTls/tls)

bindType Bind type (anonymousBind/authenticatedBind)

searchBaseDN Base DN for search

loginNameAttribute Login name attribute

userEntryObjectClass User entry object class

userSearchSubfilter User search subfilter

groupInfoInUserEntry Group membership info in user entry (true/false)

groupMemberAttribute Group member attribute

groupEntryObjectClass Group entry object class

groupSearchSubfilter Group search subfilter

adDomain Active directory domain

verifyServerCertificate Enable validation of LDAP server certificate (true/false)

certificate Certificate CA chain

allowExpiredCertificate Allow expired and not yet valid server certificates (true/false)

bindDN Bind DN

bindPassword Bind password

sortPosition New position in server list

► *RADIUS:*

config # authentication radius

Available commands:

- add

Add a new Radius server

authentication radius add <host> <authport> <acctport> <timeout> <retries> [disableAcct <disableacct>]

host IP address/host name

type Authentication type (pap/chap/msChapV2)

authport Authentication port number (0..4294967295)

acctport Accounting port number (0..4294967295)

timeout Timeout (1..60)

retries Number of retries (0..5)

- delete

Delete Radius server

index Server index

- modify

Modify an existing Radius server

config:# authentication radius modify

authentication radius modify <index> [host <host>] [authType] [authPort <authport>] [accountPort <acctport>] [timeout <timeout>] [retries <retries>] [secret] [sortPosition <position>]

index Index

host IP address/host name

authType Authentication type (pap/chap/msChapV2)

authPort Authentication port number (0..4294967295)

accountPort Accounting port number (0..4294967295)

timeout Timeout (1..60)

retries Number of retries (0..5)

secret Shared secret

sortPosition New position in server list

► *TYPE:*

config # authentication type

authentication type [useLocalIfRemoteUnavailable <localfallback>]

Configure authentication type

type Authentication type (local/ldap/radius)

useLocalIfRemoteUnavailable Use local authentication if remote authentication is unavailable (true/false)

CLI: config autoscan

autoscan

config # autoscan

Available commands:

autoscan [enable <enable>] [scale <scale>] [interval <interval>] [host <host>] [dir <dir>] [maxfiles <maxfiles>]

enable Enable/Disable auto scan (enable/disable)

scale Setup scan scale (1..100)

interval Setup scan interval(seconds) (10..86400)

host Setup NFS server IP address/host name

dir Setup NFS server directory

maxfiles Setup maximum number of stored snapshot image files(The snapshot image file will be overwritten at interval time if maximum number of image files is 0.) (0..128)

CLI: config device

device

config:# device name

device [name <name>]

Configure Device

name Device name

For example, to name device "KX3newname", at config menu type "device name KX3newname", then type "apply" to save.

CLI: config group

group

config:# group create

group create [name <name>] [privileges <privs>] [restrictions <restricts>]

Create a new group

name Group name

privileges Group privileges (one or more (separated by '/') of changePassword/deviceAccessUnderCcsg/deviceSettings/maintenance/pcShare/portControl:<port#>/portViewOnly:<port#>/portVmROnly:<port#>/portVmRW:<port#>/securitySettings/userManagement)

Note: DKX3G2 has multiple ports, so portControl will list all the ports.

---

restrictions Group restrictions (hideClientToolbar)

config:# group delete [name <name>]

Delete group

name Group name (Admin)

config:# group modify [name <name>] [description <desc>] [addPrivileges <addprivs>] [removePrivileges <removeprivs>]

Edit a group

name Group name (Admin)

description Group description

addPrivileges Add group privileges (one or more (separated by '/') of changePassword/deviceAccessUnderCcsg/deviceSettings/maintenance/pcShare/portControl:<port#>/portViewOnly:<port#>/portVmROnly:<port#>/portVmRW:<port#>/securitySettings/userManagement)

removePrivileges Remove group privileges (one or more (separated by '/') of changePassword/deviceAccessUnderCcsg/deviceSettings/maintenance/pcShare/portControl:<port#>/portViewOnly:<port#>/portVmROnly:<port#>/portVmRW:<port#>/securitySettings/userManagement)

CLI: config keyset

keyset

config # keyset

Available commands:

keyset <command> [arguments...]

Available commands:

- add Add a new keyset
- delete Delete a keyset
- modify Modify a keyset

config:# keyset add

keyset add [name <name>] [keyboardType <keyboardType>] [keys]

Add a new keyset

name Keyset name

keyboardType keyboard type (US/US-International/Danish/German-CH/German/UK/Spanish/Belgian/French-CH/French/Hungarian/Italian/Japanese/Korean/Norwegian/Portuguese/Slovenian/Swedish)

keys add keys

config:# keyset delete

keyset delete <name>

Delete a keyset

name keyset name (Num Lock)

config:# keyset modify

keyset modify <name> [newname <newname>] [keyboardType <keyboardType>] [addkeys] [removekeys]

Modify a keyset

name keyset name (Num Lock)

newname keyset new name

keyboardType keyboard type (US/US-International/Danish/German-CH/German/UK/Spanish/Belgian/French-CH/French/Hungarian/Italian/Japanese/Korean/Norwegian/Portuguese/Slovenian/Swedish)

addkeys Add keys

removekeys Remove keys

CLI: config keyword

keyword

config:# keyword add

keyword add [key <key>] [port <port>]

Add a new keyword

key Keyword

port Port index (1.1,1.2,...,4.4)

config:# keyword delete

keyword delete [key <key>]

Delete a keyword

key Keyword

config:# keyword modify

keyword modify [key <key>] [port <port>]

Edit a keyword

key Keyword

port Port index (1.1,1.2...,4.4)

CLI: config localport

config: localport [enable <enable>] [hotkey <hotkey>] [connectkey <connectkey>] [authMode <authMode>] [ignoreCC <ignoreCC>]

Configure local port settings

enable Enable/Disable local port (enable/disable)

hotkey Setup hotkey (Scroll-Lock/Num-Lock/Caps-Lock/Left-Alt/Left-Shift/Left-Ctrl)

connectkey Setup connectkey (Disabled/Left-Alt/Left-Shift/Left-Ctrl)

authMode Setup authMode (Local-LDAP-RADIUS/None)

ignoreCC Ignore CC Managed Mode On Local Port (enable/disable)

CLI: config network

► *To see Network commands*

- `config # network`.

Command	Description
dns	Display DNS information
ethernet	Configure ethernet interface
ethernetfailover	Enable or disable automatic failover
ipv4	IPv4 settings
ipv6	IPv6 settings.
services	Configure network service settings

config:# network dns [firstServer <server1>] [secondServer <server2>] [searchSuffixes <searchSuffixes>] [resolverPreference <resolverPreference>]

Configure DNS settings

firstServer First DNS server

secondServer Second DNS server

searchSuffixes Search suffixes

resolverPreference DNS resolver preference (preferV4/preferV6)

config:# network ethernet [speed <speed>] [duplexMode <duplexMode>] [authMethod <authType>]

[eapIdentity <eapIdentity>] [eapPassword] [eapClientPrivateKey] [eapClientCertificate]

[eapOuterAuthentication <eapOuterAuthMethod>] [eapInnerAuthentication <eapInnerAuthMethod>]

[eapCACertificate] [enableCertVerification <enableCertVerification>] [allowOffTimeRangeCerts <allowOffTimeRangeCerts>]

[allowConnectionWithIncorrectClock <allowConnectionWithIncorrectClock>] [eapAuthServerName <eapAuthServerName>]

Configure ethernet interface

speed Speed (1000Mbps/100Mbps/10Mbps/auto)

duplexMode Duplex mode (half/full/auto)

authMethod Authentication method (NONE/EAP)

eapIdentity EAP identity

eapPassword EAP password

eapClientPrivateKey Set EAP client private key

eapClientCertificate Set EAP client certificate

eapOuterAuthentication Outer EAP authentication method (PEAP/TLS)

eapInnerAuthentication Inner EAP authentication method (MSCHAPv2/TLS)

eapCACertificate Set EAP CA certificate

enableCertVerification Enable Verification of TLS Certificate Chain (true/false)

allowOffTimeRangeCerts Allow expired and not yet valid TLS certificates (true/false)

allowConnectionWithIncorrectClock Allows a connection when a TLS certificate is not yet valid because the system time is before the firmware build time. (true/false)

eapAuthServerName EAP RADIUS authentication server name

config:# network ipv4 gateway

network ipv4 gateway <gateway>

Configure default IPv4 gateway

gateway Default IPv4 gateway

config:# network ipv4 interface [enabled <enabled>] [configMethod <configMethod>] [preferredHostName <prefHostname>] [address <addrCidr>]

Configure interface IPv4 settings

enabled Enable/disable IPv4 protocol (true/false)

configMethod IPv4 Configuration method (dhcp/static)

preferredHostName Preferred host name

address IPv4 address/prefix-len

config:# network ipv6 gateway

network ipv6 gateway <gateway>

Configure default IPv6 gateway

gateway Default IPv6 gateway

config:# network ipv6 interface [enabled <enabled>] [configMethod <configMethod>] [preferredHostName <prefHostname>] [address <addrCidr>]

Configure interface IPv6 settings

enabled Enable/disable IPv6 protocol (true/false)

configMethod IPv6 Configuration method (automatic/static)

preferredHostName Preferred host name

address IPv6 address/prefix-len

config:# network services discovery

network services discovery [port <port>]

Configure Discovery Port

port RDM discovery port (1..65535)

config:# network services http [enabled <enabled>] [port <port>] [enforceHttps <enforcehttps>]

Configure HTTP access

enabled Enable/disable HTTP access (true/false)

port HTTP access TCP port (1..65535)

enforceHttps Enable HTTPS enforcement for web access (true/false)

config:# network services https [enabled <enabled>] [port <port>]

Configure HTTPS access

enabled Enable/disable HTTPS access (true/false)

port HTTPS access TCP port (1..65535)

config:# network services snmp [v1/v2c <v12enabled>] [v3 <v3enabled>] [readCommunity <readcommunity>] [writeCommunity <writecommunity>] [sysContact <syscontact>] [sysName <sysname>] [sysLocation <syslocation>]

Configure SNMP settings

v1/v2c Enable SNMP v1/v2c access (enable/disable)

v3 Enable SNMP v3 access (enable/disable)

readCommunity SNMP read community string

writeCommunity SNMP write community string

sysContact MIB-II sysContact

sysName MIB-II sysName

sysLocation MIB-II sysLocation

config:# network services ssh [enabled <enabled>] [port <port>] [authentication <authmode>]

Configure SSH access

enabled Enable/disable SSH access (true/false)

port SSH access TCP port (1..65535)

authentication Authentication type (passwordOnly/publicKeyOnly/passwordOrPublicKey)

CLI: config password

config:# password

Then press Enter key. System will prompt for current password, new password, and confirm new password.

config:# apply

The password is changed if confirm password is correct.

CLI: config pdu

pdu

config:# pdu

pdu <command> [arguments...]

Available commands:

- add Add a new pdu
- cycledelay Set power cycle delay
- delete Delete a pdu
- modify Modify a pdu
- outlet Set pdu outlet name
- resume Resume a pdu

config:# pdu add

pdu add [type] [name <name>] [host <host>] [snmpVersion <snmpVersion>] [port <port>] [community <community>] [userId <userId>] [secLevel <secLevel>] [authProto <authProto>] [authPass <authPass>] [privProto <privProto>] [privPass <privPass>]

Add a new pdu

type PDU type (raritan/serverTech)

name PDU name

host Ip Address/host name

snmpVersion SNMP Version (v2/v3)

port SNMP port (1..65535)

community SNMP write community

userId User Id

secLevel SNMPv3 security level (NoAuthNoPriv/AuthNoPriv/AuthPriv)

authProto Authentication protocol (MD5/SHA)

authPass Authentication pass phrase

privProto Privacy protocol (DES/AES)

privPass Privacy pass phrase

config:# pdu cycledelay

pdu cycledelay <cycledelay>

Set power cycle delay

cycledelay Power cycle delay (1..3600)

config:# pdu delete

pdu delete <name>

Delete a pdu

name PDU name (PX2-2166R/PX3-5146R/ServerTech-PRO3X)

config:# pdu modify

pdu modify <name> [type] [newname <newname>] [snmpVersion <snmpVersion>] [port <port>] [community <community>] [userId <userId>] [secLevel <secLevel>] [authProto <authProto>] [authPass <authPass>] [privProto <privProto>] [privPass <privPass>]

Modify a pdu

name PDU name (PX2-2166R/PX3-5146R/ServerTech-PRO3X)

type PDU type (raritan/serverTech)

newname PDU name

snmpVersion SNMP Version (v2/v3)

port SNMP port (1..65535)

community SNMP write community

userId User Id

secLevel SNMPv3 security level (NoAuthNoPriv/AuthNoPriv/AuthPriv)

authProto Authentication protocol (MD5/SHA)

authPass Authentication pass phrase

privProto Privacy protocol (DES/AES)

privPass Privacy pass phrase

config:# pdu outlet

pdu outlet [pduname <pduname>] [outletlabel <outletlabel>] [outletname <outletname>]

Set pdu outlet name

pduname PDU name (PX2-2166R/PX3-5146R/ServerTech-PRO3X)

outletlabel Outlet label
(1/10/11/12/13/14/15/16/17/18/19/2/20/21/22/23/24/25/26/27/28/29/3/30/31/32/33/34/35/36/4/5/6/7/8/9)

outletname Outlet name

config:# pdu resume

pdu resume <name>

Resume a pdu

name PDU name (PX2-2166R/PX3-5146R/ServerTech-PRO3X)

CLI: config port

port: Configure DSAM serial port settings:

config:# port

port [index <index>] [name <name>] [emulation <emulation>] [encoding <encoding>] [eqtype <eqtype>] [bps <bps>] [parity <parity>] [flowcontrol <flowcontrol>] [stopbits <stopbits>] [multiwrite <multiwrite>] [escapemode <escapemode>] [escapechar <escapechar>] [chardelay <chardelay>] [linedelay <linedelay>] [sendbreak <sendbreak>] [suppress <suppress>] [alwaysactive <alwaysactive>] [exitcommand <exitcommand>]

Configure DSAM serial port settings

index Port index (1.1, 1.2 ... 4.4)

name Port name

emulation Target emulation type (VT100/VT220/VT320/ANSI)

encoding Target Encoding type (Default/ISO-8859/ISO-8859-15/UTF-8/Shift-JIS/EUC-JP/EUC-KR/8BIT-ASCII)

eqtype Equipment type (DTE/DCE/AUTO)

bps Port speed (bit rate) in bits-per-second (1200/1800/2400/4800/9600/19200/38400/57600/115200/230400)

parity Port Parity (odd/even/none)

flowcontrol Port flowcontrol type (none/hw/sw)

stopbits Number of bits used to signal the end of a character (1/2)

multiwrite Port set in multiple writer mode (true/false)

escapemode Use Ctrl-key (escapemode=control)OR single key (escapemode=none) as escape sequence (control/none)

escapechar Escape character

chardelay Delay inserted between characters (0-9999 msec)

linedelay Delay inserted between lines (0-9999 msec)

sendbreak Duration of sendbreak signal in ms

suppress Suppress messages when connecting to this target (true/false)

alwaysactive Port active if no users are connected (true/false)

exitcommand Execute exit string when port session closes

CLI: config security

config:# security fips

security fips [enabled <enabled>]

Configure FIPS mode

enabled Enable/disable FIPS mode on next reboot (true/false)

config:# security groupBasedAccessControl ipv4

security groupBasedAccessControl ipv4 [enabled <enable>] [defaultPolicy <defpolicy>]

Configure group based access control settings for IPv4

enabled Enable group based access control (true/false)

defaultPolicy Default policy (allow/deny)

config:# security groupBasedAccessControl ipv6 [enabled <enable>] [defaultPolicy <defpolicy>]

Configure group based access control settings for IPv6

enabled Enable group based access control (true/false)

defaultPolicy Default policy (allow/deny)

config:# security ipAccessControl ipv4

security ipAccessControl ipv4 [enabled <enable>] [defaultPolicyIn <defpolicyin>] [defaultPolicyOut <defpolicyout>]

Configure IPv4 access control settings

enabled Enable IP access control (true/false)

defaultPolicyIn Default policy for inbound traffic (accept/drop/reject)

defaultPolicyOut Default policy for outbound traffic (accept/drop/reject)

config:# security ipAccessControl ipv6 [enabled <enable>] [defaultPolicyIn <defpolicyin>] [defaultPolicyOut <defpolicyout>]

Configure IPv6 access control settings

enabled Enable IP access control (true/false)

defaultPolicyIn Default policy for inbound traffic (accept/drop/reject)

defaultPolicyOut Default policy for outbound traffic (accept/drop/reject)

config:# security kvmSecurity

security kvmSecurity [encryption <encryption>] [pcshare <pcshare>] [pcshareIdletimeout <pcshareIdletimeout>] [vmshare <vmshare>] [disableLPOutput <disableLPOutput>] [localdeviceReset <localdeviceReset>] [dpaUrl <dpaUrl>] [iframe <iframe>]

Configure KVM security settings

encryption Enable encryption mode to KVM and VM (enable/disable)

pcshare Enable PC share mode (enable/disable)

pcshareIdletimeout Set pc share idle timeout (in seconds) (1..600)

vmshare Enable VM share mode (enable/disable)

disableLPOutput Disable local port output (enable/disable)

localdeviceReset Set local device reset mode (factoryReset/adminPwReset/disableReset)

dpaUrl Enable direct port access via url (enable/disable)

iframe Allow IFrame (enable/disable)

config:# security loginLimits [singleLogin <singlelogin>] [passwordAging <pwaging>] [passwordAgingInterval <pwaginginterval>] [idleTimeout <idletimeout>]

Configure login limitations

singleLogin Prevent concurrent user login (enable/disable)

passwordAging Enable password aging (enable/disable)

passwordAgingInterval Set password aging interval (in days) (7..365)

idleTimeout Set user idle timeout (in minutes) (1..1440 or infinite)

config:# security restrictedServiceAgreement [enabled <enabled>] [bannerContent]

Configure the Restricted Service Agreement banner

enabled Enable Restricted Service Agreement enforcement (true/false)

bannerContent The Restricted Service Agreement banner

config:# security strongPasswords [enabled <enable>] [minimumLength <minlength>] [maximumLength <maxlength>] [enforceAtLeastOneLowerCaseCharacter <forcelower>] [enforceAtLeastOneUpperCaseCharacter <forceupper>] [enforceAtLeastOneNumericCharacter <forcenumeric>] [enforceAtLeastOneSpecialCharacter <forcespecial>] [passwordHistoryDepth <historydepth>]

Configure strong password requirements

enabled Enable strong passwords (true/false)

minimumLength Minimum password length (8..32)

maximumLength Maximum password length (16..64)

enforceAtLeastOneLowerCaseCharacter Enforce at least one lower case character (enable/disable)

enforceAtLeastOneUpperCaseCharacter Enforce at least one upper case character (enable/disable)

enforceAtLeastOneNumericCharacter Enforce at least one numeric character (enable/disable)

enforceAtLeastOneSpecialCharacter Enforce at least one special character (enable/disable)

passwordHistoryDepth Password history depth (1..12)

config:# security userBlocking [maximumNumberOfFailedLogins <maxfails>] [blockTime <blocktime>]

Configure user blocking

maximumNumberOfFailedLogins Set maximum number of failed logins before blocking a user (3..10 or unlimited)

blockTime Set user block time (in minutes) (1..1440 or infinite)

config:# security sshdpa [enabled <enabled>]

Configure SSH DPA

enabled Enable/disable SSH DPA (true/false)

config:# security sshdpaport [id <id>] [port <port>]

Configure SSH DPA Ports

id Port id (1.1, 1.2 ... 4.4)

port SSH DPA port (0..65535)

CLI: config serial

config:# serial [consoleBaudRate <consolebps>]

Configure serial port settings

consoleBaudRate Serial console baud rate (1200/2400/4800/9600/19200/38400/57600/115200)

CLI: config time

config:# time [method <method>] [zone] [autoDST <autodst>]

Configure date/time settings

method Time setup method (manual/ntp)

zone Select time zone

autoDST Automatic daylight saving time adjustment (enable/disable)

CLI: config user

config:# user create

user create [name <name>] [enabled <enabled>] [groups <groups>]

Create a new user

name User name

enabled User enabled state (true/false)

groups Groups (comma separated list of group names) (Admin)

- If user wants to create a new user "cccc" into groups "aaa" and "bbb bbb", you must use quotes around the group names, because spaces in the group names cannot be accepted. Example command:
  - user create name cccc enabled true groups "aaa/bbb bbb"

config:# user delete [name <name>]

Delete user

name User name (admin)

config:# user modify [name <name>] [newName <newname>] [password] [password] [fullName <fullname>] [telephoneNumber <telephone>] [eMailAddress Info@Acme.com] [enabled <enabled>] [forcePasswordChangeOnNextLogin <forcepwchange>] [snmpV3Access <snmpv3>] [securityLevel <seclevel>] [userPasswordAsAuthenticationPassphrase <pwasauthpass>] [authenticationPassPhrase] [useAuthenticationPassPhraseAsPrivacyPassPhrase <authpassasprivpass>] [privacyPassPhrase] [authenticationProtocol <authproto>] [privacyProtocol <privproto>] [groups <groups>] [sshPublicKey]

Create or edit user

name User name (admin)

newName New name

password Account password

fullName Full name

telephoneNumber Telephone number

eMailAddress E-mail address

enabled User enabled state (true/false)

forcePasswordChangeOnNextLogin Select whether the user needs to change his password on next login (true/false)

snmpV3Access Enable/disable SNMPv3 access (enable/disable)

securityLevel SNMPv3 security level (noAuthNoPriv/authNoPriv/authPriv)

userPasswordAsAuthenticationPassphrase Use password as SNMPv3 authentication passphrase (true/false)

authenticationPassPhrase Authentication pass phrase

useAuthenticationPassPhraseAsPrivacyPassPhrase Use authentication pass phrase as privacy pass phrase (true/false)

privacyPassPhrase Privacy pass phrase

authenticationProtocol Authentication protocol (MD5/SHA-1)

privacyProtocol Privacy protocol (DES/AES-128)

groups Groups (Comma separated list of group names) (Admin)

sshPublicKey Set SSH public key

config:# user modify

user modify [name <name>] [newName <newname>] [password] [fullName <fullname>] [telephoneNumber <telephone>] [eMailAddress Info@Acme.com] [enabled <enabled>] [forcePasswordChangeOnNextLogin <forcepwchange>] [snmpV3Access <snmpv3>] [securityLevel <seclevel>] [userPasswordAsAuthenticationPassphrase <pwasauthpass>] [authenticationPassPhrase] [useAuthenticationPassPhraseAsPrivacyPassPhrase <authpassasprivpass>] [privacyPassPhrase] [authenticationProtocol <authproto>] [privacyProtocol <privproto>] [groups <groups>] [sshPublicKey]

Create or edit user

name User name (admin/admin1/all-permissions/device/general/no-power/terminal/user/user1)

newName New user name

password Account password

fullName Full name

telephoneNumber Telephone number

eMailAddress E-mail address

enabled User enabled state (true/false)

forcePasswordChangeOnNextLogin Select whether the user needs to change his password on next login (true/false)

snmpV3Access Enable/disable SNMPv3 access (enable/disable)

securityLevel SNMPv3 security level (noAuthNoPriv/authNoPriv/authPriv)

userPasswordAsAuthenticationPassphrase Use password as SNMPv3 authentication passphrase (true/false)

authenticationPassPhrase Authentication pass phrase

useAuthenticationPassPhraseAsPrivacyPassPhrase Use authentication pass phrase as privacy pass phrase (true/false)

privacyPassPhrase Privacy pass phrase

authenticationProtocol Authentication protocol (MD5/SHA-1)

privacyProtocol Privacy protocol (DES/AES-128)

groups Groups (Comma separated list of group names) (one or more (separated by '/') of Admin/Administrators/All Permissions/Device Settings/General/No Power Control Permission/Regular User/Terminal Block/Test/User Management/newgroup/radius)

sshPublicKey Set SSH public key

CLI: config vmshare

vmshare

config:# vmshare

vmshare <command> [arguments...]

Available commands:

- add Add a new shared image
- delete Delete a shared image
- modify Edit shared image

config:# vmshare add

vmshare add [host <host>] [name <name>] [path <path>] [enableSamba <enableSamba>]

Add a new shared image

host IP address/host name

name Share name

path Image path

enableSamba Enable/Disable SAMBA v1.0 (enable/disable)

config:# vmshare delete

vmshare delete <index>

Delete a shared image

index shared image index

config:# vmshare modify

vmshare modify <index> [host <host>] [name <name>] [path <path>] [enableSamba <enableSamba>]

Edit shared image

index shared image index

host IP address/host name

name Share name

path Image path

enableSamba Enable/Disable SAMBA v1.0 (enable/disable)

CLI: connect

```
connect <port index> (1.1/1.2…/2.4)
```

After connecting to a port, following are the available commands:

clearhistory Clear history buffer for this port

clientlist Display all users on the port

close Close this target connection

gethistory Display the history buffer for this port

getwrite Get write access for the port

powercycle Power Cycle of this port

poweroff Power Off of this port

poweron Power On of this port

powerstatus Query Power status of this port

resetport Reset port

return Return to the target session

sendbreak Send a break to the connected target

writelock Lock write access to this port

writeunlock Unlock write access to this port

CLI: diag

diag

diag:#

Available commands:

exit Leave diagnostic mode

netstat Netstat

nslookup DNS lookup

ping Ping

traceroute Trace route

diag:# netstat

netstat <mode>

Netstat

diag:# netstat connections

TCP Connections.

State Recv-Q Send-Q Local-Address:Port Peer-Address:Port

ESTAB 0 0 [::ffff:192.168.59.146]:443 [::ffff:192.168.62.56]:57858

ESTAB 0 0 [::ffff:192.168.59.146]:443 [::ffff:192.168.62.56]:57857

diag:# netstat ports

List TCP/UDP Listen Sockets

Netid State Recv-Q Send-Q Local-Address:Port Peer-Address:Port

udp UNCONN 0 0 0.0.0.0%eth0:5353 0.0.0.0:*

udp UNCONN 0 0 0.0.0.0%eth0:5355 0.0.0.0:*

udp UNCONN 0 0 *:55213 *:*

tcp LISTEN 0 10 127.0.0.1:8181 0.0.0.0:*

tcp LISTEN 0 10 *:80 *:*

tcp LISTEN 0 10 *:2130 *:*

mode Specify the netstat mode (ports/connections)

diag:# nslookup <host>

Name server query

host Host name or IP address to query DNS information for

diag:# ping <dest> [count <num_echos>] [size <packet_size>] [timeout <timeout>]

Ping

dest Target host name or IP address

count Specify the number of echo requests to be sent (1..20) [5]

diag:# traceroute <dest> [useICMP]

Trace route

dest Target host name or IP address

useICMP Use ICMP packets instead of UDP packets

timeout Maximum amount of time (in s) until traceroute will be terminated (1..900)

diag:# nslookup

nslookup <host>of device

DNS lookup

host Host name to lookup

diag:# nslookup <IP address>of device

NOTE: This may take up to 30 seconds if a DNS server is unreachable!

DNS search suffixes:

raritan.com.

DNS resolver preference: IPv6 address

Results from DNS server <IP address>:

<IP address>of device.

Results from DNS server <IP address>:

<IP address> of device.

CLI: exit

exit

exit

CLI: reset

reset

reset

reset <command> [arguments...]

► *Available commands:*

factorydefaults	***Reset device to factory defaults***
unit	***Reset and reboot device***

reset factorydefaults

reset factorydefaults /y ...

Reset device to factory defaults

/y ... Assume 'yes' as answer to questions

reset unit /y ...

Reset and reboot device

/y ... Assume 'yes' as answer to questions

CLI: show

► *To see available show commands*

show?

show <command> [arguments...]

► *Available commands:*

authentication	***Shows info about authentication settings***
autoscan	***Shows auto scan information***
connectedusers	***Shows connected user information***
device	***Shows Device info. Shows DSAM info if connected***
eventlog	***Shows event log***
groups	***Shows group information***
history	***Shows session command history***
keyset	***Shows keyset settings***
keyword	***Shows configured serial port keywords***
kvmport	***Shows kvm ports***
localport	***Show local port settings***
network	***Shows all network information***
pdu	***Shows PDU information***
port	***Shows DSAM serial port parameters***
security	***Shows security settings***
serial	***Shows serial port parameters***
time	***Shows date/time information***
user	***Shows user information***
vmshare	***Shows information about auto virtual media shared images***

```
# show authentication

Authentication type: Local

# show autoscan

Enable Auto Scan: Disabled

Scan Scale(%): 100

Scan Interval(seconds): 10

NFS Server IP Address/Hostname: 192.168.62.30

NFS Server Directory: /nfs/autoscan

Max number of stored image files: 0

Auto Scan NFS Status: Inactive

Configured LDAP servers:

# IP address Server type

No servers are currently configured.
```

Configured Radius servers:

IP address Authentication type Ports (auth./acc.)

No servers are currently configured.

show connectedusers

User Name IP Address Client Type Idle Time

admin 192.168.55.11 CLI (SSH) 0m

show device

Device 'KX4101_5989'

Product: KX4

Model: DKX4-101

Firmware Version: 4.2.0.5.48758

Hardware ID: 2

Serial Number: 1IT8C00002

Internal Temperature Current Value: 40.6 C / 105.1 F

Internal Temperature Maximum Value: 46.1 C / 115.0 F

show eventLog

Event Time Event Class Event Message

2019-03-01 09:17:34 EST User Activity User 'admin' from host '192.168.32.187' logged out.

2019-03-01 09:17:34 EST User Activity Session of user 'admin' from host '192.168.32.187' timed out.

2019-03-01 09:44:54 EST User Activity User 'admin' from host '192.168.32.206' logged in.

2019-03-01 09:55:00 EST User Activity User 'admin' from host '192.168.32.206' logged out.

2019-03-01 09:55:00 EST User Activity Session of user 'admin' from host '192.168.32.206' timed out.

2019-03-01 16:03:52 EST User Activity Authentication failed for user 'admin' from host '192.168.32.187'.

2019-03-01 16:03:56 EST User Activity User 'admin' from host '192.168.32.187' logged in.

2019-03-01 16:15:00 EST User Activity User 'admin' from host '192.168.32.187' logged out.

2019-03-01 16:15:00 EST User Activity Session of user 'admin' from host '192.168.32.187' timed out.

2019-03-04 06:32:19 EST User Activity User 'admin' from host '192.168.32.184' logged in.

2019-03-04 06:33:17 EST Device Firmware upgrade started from version '4.0.0.1.45553' to version '4.0.0.1.45557' by user 'admin' from host '192.168.32.184'.

2019-03-04 06:35:52 EST Device The ETHERNET network interface link is now up.

2019-03-04 06:35:54 EST Device Firmware upgraded successfully from version '4.0.0.1.45553' to version '4.0.0.1.45557' by user 'admin' from host '192.168.32.184'.

2019-03-04 06:35:54 EST Device System started.

2019-03-04 06:36:34 EST User Activity Authentication failed for user 'admin' from host '192.168.32.184'.

2019-03-04 06:36:39 EST User Activity User 'admin' from host '192.168.32.184' logged in.

2019-03-04 06:45:00 EST User Activity User 'admin' from host '192.168.32.184' logged out.

2019-03-04 06:45:00 EST User Activity Session of user 'admin' from host '192.168.32.184' timed out.

2019-03-06 07:43:24 EST User Activity User 'admin' from host '192.168.55.11' logged in.

2019-03-06 07:55:10 EST User Activity User 'admin' from host '192.168.55.11' logged out.

2019-03-06 07:55:10 EST User Activity Session of user 'admin' from host '192.168.55.11' timed out.

2019-03-07 09:39:44 EST User Activity User 'admin' from host '192.168.55.11' logged in.

2019-03-07 09:53:22 EST User Activity User 'admin' from host '192.168.55.11' logged out.

2019-03-07 09:53:22 EST User Activity Session of user 'admin' from host '192.168.55.11' timed out.

2019-03-11 13:14:34 EDT User Activity User 'admin' from host '192.168.55.11' logged in.

2019-03-11 13:16:39 EDT User Activity User 'admin' from host '192.168.55.11' logged in.

2019-03-11 13:24:46 EDT User Activity User 'admin' from host '192.168.55.11' logged out.

2019-03-11 13:24:46 EDT User Activity Session of user 'admin' from host '192.168.55.11' timed out.

2019-03-11 13:29:13 EDT User Activity User 'admin' from host '192.168.55.11' logged out.

2019-03-11 13:30:32 EDT User Activity User 'admin' from host '192.168.55.11' logged in.

show groups

Group 'Admin':

Description: System defined administrator group including all privileges.

Privileges: adminPrivilege

show history

1 show vmshare

2 config

3 cancel

4 show history

#show keyset

Keyset name: US-International-block-left-ctrl

Keyboard type: English (US/Intl)

Key: Left Ctrl

show keyword

Keyword: Example

Port: 1.1

show kvmport

KVM Ports:

Port Name CIM Type Status Availability

---

1 CentOS DVM-HDMI Active Idle

2 Dominion_KX3_Port2 DVM-DP Active Idle

3 Local Port DVM-HDMI Active Idle

4 Windows-11 DVM-DP Active Idle

5 KX3-464 Local Port DVM-DVI Active Idle

6 Dominion_KX3_Port6 Not Available Inactive Idle

show localport

Enable Local Port: Enabled

Keyboard Type: US

Hotkey: Caps-Lock

Connectkey: Left-Alt

Auth Mode: Local-LDAP-RADIUS

Ignore CC Managed Mode On Local Port: Disabled

show network

DNS resolver

Servers: 192.168.50.115

192.168.50.116

Search suffix: raritan.com.

Resolver preference: Prefer IPv6 addresses

Routing

IPv4

Default gateway: 192.168.50.126

Static routes: None

IPv6

Default gateway: None

Static routes: None

Interface 'ETHERNET'

Link

Configured speed: Automatic

Configured duplex: Automatic

Link state: Autonegotiation On, 1 Gbit/s, Full Duplex, Link OK

Authentication: EAP (Current status:Pending)

EAP outer auth: PEAP

EAP inner auth: MSCHAPv2

EAP identity: radtest

Auth server certificate

Verification: Enabled

CA certificate: Example Certificate Authority

Auth server : Not set

MAC address: 00:0d:5d:00:02:d5

MTU: 1500

IPv4

Config method: DHCP

Address: 192.168.50.35/24

Preferred hostname: Not configured

DHCP server: 192.168.50.115

IPv6

Disabled

#show pdu

PDU name: PX3-5146R

Host: 192.168.57.37

Model: PX3-5146R

Serial number: QYO6A00005

Outlets: 8

Status: Active

#show port

Port number: 1.1

Port Name: KX4-101 at 192.168.62.217

Port Status: active Available

Emulation: VT100

Encoding: Default

Equipment Type: AUTO

BPS: 115200

Parity/Bits: None

Flow Control: None

Stop Bits: 1

Multiple Writers: false

Escape Mode: true

Escape Character:]

Char Delay: 0

Line Delay: 0

Send Break: 300

Suppress Messages: false

Always Active: true

Exit Command:

show security

IPv4 access control: Disabled

IPv6 access control: Disabled

Group based access control for IPv4: Disabled

Group based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login: No

Strong passwords: Disabled

Restricted Service Agreement: disabled

KVM Security:

Encryption to KVM and virtual media: Enabled

PC share: Enabled

PC share idle timeout: 5 seconds

Virtual media share: Enabled

Disable local port output: Disabled

Local device reset mode: Local Factory Reset

Enable direct port access via URL: Enabled

Allow IFrame: Disabled

SSH DPA: Disabled

show serial

Configured baud rate: 9600 bit/s

Device detection type: Force console

Detected device: Console

show time

Device Time: 2019-03-11 13:50:26 EDT

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Setup Method: NTP synchronized

show user

User 'admin':

Enabled: Yes

Groups: Admin

SNMP v3 Access: Disabled

#show security details

IPv4 access control: Disabled

IPv6 access control: Disabled

Group based access control for IPv4: Disabled

Group based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login: No

Maximum number of failed logins: 3

User block time: 5 minutes

User idle timeout: 20 minutes

Strong passwords: Enabled

Allowed password length: 8 - 64 characters

Enforce at least one lower case character: Yes

Enforce at least one upper case character: Yes

Enforce at least one numeric character: Yes

Enforce at least one special character: Yes

Password history depth: 5

Restricted Service Agreement: disabled

Restricted Service Agreement Banner Content:

Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

SSH DPA: Disabled

SSH DPA port settings:

Port Id: 2.1 SSH Port: 2225

Port Id: 2.2 SSH Port: 0

Port Id: 2.3 SSH Port: 0

Port Id: 2.4 SSH Port: 0

#show vmshare

Virtual Media Shared Image #1

IP Address/Hostname: 192.168.62.30

Share Name: share

Image Path: /Fedora-Workstation-Live-x86_64-34-1.2.iso

Enable SAMBA v1.0: Disabled

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).

Appendix A Appendix

In This Chapter

LDAP and Radius Configuration

To configure LDAP or Radius authentication, four main steps are required:

a. Determine user accounts and roles (groups) intended for the device
b. Create user groups for the device on the LDAP or Radius server
c. Configure LDAP or Radius authentication on the device
d. Configure roles on the device

Specifications

Hardware-specs

Dimensions and Physical Specifications

Dominion DKX3G2 model	Description	Power & heat dissipation	Dimensions (WxDxH)	Gross Weight	Net Weight	Operating temp	Humidity	Power Consumption
DKX3G2-108	8 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'' or 439x334x44mm	7.24 kg	4.48 kg	0º - 45º C or 32º - 113º F	0-85 % RH	55W
DKX3G2-116	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'' or 439x334x44mm	7.24 kg	4.48 kg	0º - 45º C or 32º - 113º F	0-85 % RH	55W

DKX3G2-132	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'' or 439x334x44mm	7.24 kg	4.48 kg	0º - 45º C or 32º - 113º F	0-85 % RH	55W
DKX3G2-216	16 server ports 2 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'' or 439x334x44mm	7.24 kg	4.48 kg	0º - 45º C or 32º - 113º F	0-85 % RH	55W
DKX3G2-232	32 server ports 2 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'' or 439x334x44mm	7.24 kg	4.48 kg	0º - 45º C or 32º - 113º F	0-85 % RH	55W
DKX3G2-416	• 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'' or 439x334x44mm	7.27 kg	4.52 kg	0º - 45º C or 32º - 113º F	0-85 % RH	57W
DKX3G2-432	• 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'' or 439x334x44mm	7.27 kg	4.52 kg	0º - 45º C or 32º - 113º F	0-85 % RH	57W
DKX3G2-464	• 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 13.15'' x 1.73'' or 439x334x44mm	9.20 kg	5.89 kg	0º - 45º C or 32º - 113º F	0-85 % RH	74W

DKX3G2-808	• 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'' or 439x334x44mm	7.34 kg	4.66 kg	0º - 45º C or 32º - 113º F	0-85 % RH	61W
DKX3G2-816	• 16 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'' or 439x334x44mm	7.34 kg	4.66 kg	0º - 45º C or 32º - 113º F	0-85 % RH	61W
DKX3G2-832	• 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'' or 439x334x44mm	7.34 kg	4.66 kg	0º - 45º C or 32º - 113º F	0-85 % RH	61W
DKX3G2-864	• 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 13.15'' x 1.73'' or 439x334x44mm	10.67 kg	6.17 kg	0º - 45º C or 32º - 113º F	0-85 % RH	78W

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.

Local Port Supported Resolutions by HDMI Interface

The local port supports video resolutions up to 1920x1200 pixels. See:Supported Target Server Video Resolutions (on page 311) for the detail list.

Note: The local port and remote console support the same resolutions.

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 311) for the video resolutions supported by the DKX3G2.

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 	• 1.7" x 3.5" x 0.8" • 43 x 90 x 19mm	• 0.25lb • 0.11kg
D2CIM-VUSB	USB CIM for: • OS virtual media • Absolute Mouse Synchronization • No audio or Audio or Smartcard 	• 1.3" x 3.0" x 0.6" • 33 x 76 x 15mm	• 0.20lb • 0.09kg
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 	• 1.7" x 3.5" x 0.8" • 43 x 90 x 19mm	• 0.25lb • 0.11kg

CIM model	Description	Dimensions (WxDxH)	Weight
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 	• 1.7" x 3.5" x 0.8" • 43 x 90 x 19mm	• 0.25lb • 0.11kg
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 	• 1.7" x 3.5" x 0.8" • 43 x 90 x 19mm	• 0.25lb • 0.11kg
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 	• 1.7" x 3.5" x 0.8" • 43 x 90 x 19mm	• 0.25lb • 0.11kg

CIM model	Description	Dimensions (WxDxH)	Weight
DCIM-PS2	CIM for PS2 	• 1.3" x 3.0" x 0.6" • 33 x 76 x 15mm	• 0.20lb • 0.09kg
DCIM-USBG2	CIM for USB and Sun USB 	• 1.3" x 3.0" x 0.6" • 33 x 76 x 15mm	• 0.20lb • 0.09kg

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 DKX3G2 for Mac, see: Digital CIM Established and Standard Modes (on page 317)

Digital CIM Timing Modes

Following are the default timing modes that are used when the DKX3G2 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 DKX3G2.

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

DKX3G2 network speed setting							
Network switch port setting		**Auto**	**1000/Full**	**100/Full**	**100/Half**	**10/Full**	**10/Half**
	Auto	Highest Available Speed	1000/Full	DKX3G2: 100/Full Switch: 100/Half	100/Half	DKX3G2: 10/Full Switch: 10/Half	10/Half
	1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
	100/Full	DKX3G2: 100/Half Switch: 100/Full	DKX3G2: 100/Half Switch: 100/Full	100/Full	DKX3G2: 100/Half Switch: 100/Full	No Communication	No Communication
	100/Half	100/Half	100/Half	DKX3G2: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/Full	DKX3G2: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	DKX3G2: 10/Half Switch: 10/Full
	10/Half	10/Half	No Communication	No Communication	No Communication	DKX3G2: 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 DKX3G2 behavior deviates from expected behavior

Note: For reliable network communication, configure the DKX3G2 and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure the DKX3G2 and LAN Switch to Autodetect (recommended), or set both to a fixed speed/duplex such as 100MB/s/Full.

Smart Card Minimum Requirements

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.

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 DKX3G2 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
Rocky Linux 9	pcsc-lite 1.9.4-e|9
Fedora® Core 39	pcsc-lite-2.0.1-1.fc39

- Create a Java® Library Link

  A soft link must be created to the libpcsclite. 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
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 under each of the selected formats.

Audio format	Network bandwidth requirement
44.1 KHz, 16bit stereo	176 KB/s
44.1 KHz, 16bit mono	88.2 KB/s
22.05 KHz, 16bit stereo	88.2 KB/s
22.05 KHz, 16bit mono	44.1 KB/s
11.025 KHz, 16bit stereo	44.1 KB/s
11.025 KHz, 16bit mono	22.05 KB/s

- In practice, the bandwidth used when an audio device connects to a target is higher due to the keyboard and video data consumed when opening and using an audio application on the target.
- A general recommendation is to have at least a 1.5MB connection before running 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

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)

DKX3G2 Supported Keyboard Languages

The DKX3G2 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 DKX3G2 Local Console functions. For more information about non-US keyboards, see Informational Notes (on page 328).

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

Language	Regions	Keyboard layout
French	France	French (AZERTY) layout keyboard.
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 BIOS Keystroke Commands

Use the following Mac keystroke commands when controlling the EFI (Extensible Firmware Interface), which is Mac's version of a BIOS.

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

Keystroke	Description	Virtual Media CIM	Dual Virtual Media CIM	Mac Lion Server HDMI CIM
Press Eject, F12, or hold the mouse button	Ejects any removable media, such as an optical disc	Yes	Yes	
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 DKX3G2. 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:*

Oracle Java™ Runtime Environment (JRE) version 8 is supported up to 1.8.0_351 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.

► *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 DKX3G2 when used with CC-SG. Check the CC-SG Release Notes and Compatibility Matrix.

Operating Systems	Browsers	Java
Windows 11	Windows Edge Chrome Firefox	Java 1.8 or later for VKC Java 1.8.0_151 or later for VKCs
openSUSE® 15	Firefox	
Fedora® 40	Firefox	
Red Hat 7.5	Firefox	
Mac 15.2	Safari Chrome Firefox	

JRE Requirements and Browser Considerations for Mac

Java Runtime Environment Requirements for Mac

Install Java Runtime Environment 8 (JRE)® on PCs and Macs® when using the Virtual KVM Client (VKC) to access target devices via DKX3G2.

This ensures in order to provide high performance, KVM-over-IP video processing when remotely accessing target devices/PCs/Macs.

The latest version of JRE for Mac can be downloaded from the Oracle Support website.

Browser Considerations for Mac

Java may be disabled by default in certain browsers. Enable Java and accept all security warnings in order to use DKX3G2.

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.

BSMI Certification

BSMI Certification is needed for DKX3G2.

Informational Notes

Overview

This section includes important notes on DKX3G2 usage. Future updates will be documented and available online through the Help link in the DKX3G2 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

Disable Java Caching and Clear the Java Cache

It is highly recommended that you disable Java caching in Microsoft Windows®, and clear the Java™ cache.

► *To disable Java caching and clear the cache:*

1. From the Windows Start menu, click Control Panel.
2. Double-click on the Java icon to launch it. The Java Control Panel dialog appears.
3. To disable Java caching:
   a. From the General tab, click the Settings button. The Temporary Files Settings dialog appears.
   b. Click the View Applets button. The Java Applet Cache Viewer opens.
   c. Deselect the Enable Caching checkbox if it is already checked.
   d. Click OK.
4. To clear the Java cache:
   a. From the Temporary Files Settings dialog, click the Delete Files button. The Delete Temporary Files dialog appears.
   b. Select the temporary files that you want to delete.
   c. Click OK.

Java Not Loading Properly on Mac

If you are using a Mac® and see the following message when connecting to a device from the DKX3G2 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: http://www.java.com/en/download/testjava.jsp

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 DKX3G2 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 DKX3G2 in a dual stack configuration, it is important you configured the domain system (DNS) correctly in the DKX3G2 in order to avoid delays when logging in.

See: Tips for Adding a Web Browser Interface for information on configuring your DNS in DKX3G2.

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 DKX3G2:

- 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.

Virtual Media Notes

Virtual Media via VKC and AKC in a Windows Environment

When Virtual Media is enabled, access to fixed drives and fixed drive partitions will not be accessible with a Standard Windows user. To access those drives, a Windows Administrator user must be used. This is because Windows User Access Control (UAC) provides the lowest level of rights and privileges a user needs for an application.

Both features affect the types of virtual media that can be accessed in VKC, VKCS, and AKC. See your Microsoft® help for additional information on these features and how to use them.

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

Client	Administrator	Standard User
AKC and VKC	Access to: • Fixed drives and fixed drive partitions • Removable drives • CD/DVD drives • ISO images • Remote ISO images	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 switch from the Generic USB profile to one that uses Full Speed for Virtual Media. For example where a target has problems with High Speed USB connections or when the target is experiencing USBprotocol errors caused by signal degradation due to additional connectors and cables.

USB Port and Profile Notes

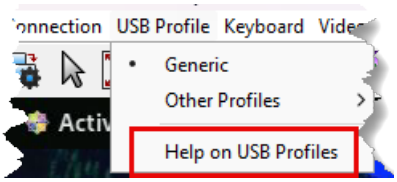
VM-CIMs and DL360 USB Ports

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.

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 DKX3G2, 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 DKX3G2.

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.

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

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

When using Firefox® to connect to a DKX3G2 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 DKX3G2

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 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.

General Frequently Asked Questions

General FAQs

Question	Answer
What is <ProdcutName>?	<ProdcutName> 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. <ProdcutName> is completely hardware- and OS-independent; users can troubleshoot and reconfigure servers even when servers are down. At the rack, <ProdcutName> provides the same functionality, convenience, and space and cost savings as traditional analog KVM switches. However, <ProdcutName> 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 DKX3G2 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 <ProdcutName> 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 <ProdcutName> differ from remote control software?	When using <ProdcutName> 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 <ProdcutName> is not a software but a hardware solution, it's much more powerful: Hardware- and OS-independent – <ProdcutName> can be used to manage servers running many popular OSs, including Intel®, PowerPC running Windows, Linux, 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 <ProdcutName>. 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, <ProdcutName> still works flawlessly to enable these configurations to be made.
Can the <ProdcutName> be rack mounted?	Yes. The <ProdcutName> ships standard with 19" rack mount brackets. It can also be reverse rack mounted so the server ports face forward.
How large is the <ProdcutName>?	<ProdcutName> 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 <ProdcutName>?	<ProdcutName> 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 DKX3G2-116, up to eight remote users can access and control a single target server. For two-channel appliances, like the DKX3G2-216, 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.
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.

Question	Answer
In order to access <ProdcutName> from a client, what hardware, software or network configuration is required?	Because <ProdcutName> is completely Web-accessible, it doesn't require customers to install proprietary software on clients used for access. <ProdcutName> can be accessed through major Web browsers, including: Edge® and Firefox®. <ProdcutName> can be accessed on Windows®, Linux® and Mac® desktops, via Raritan's Windows Client, and the Java™-based Virtual KVM Client™. <ProdcutName> administrators can also perform remote management (set passwords and security, rename servers, change IP address, etc.) using a convenient browser-based interface.
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)
Do you have a non-Windows KVM Client?	Yes. The Virtual KVM Client (VKC) and HTML KVM Client (HKC) allows non-Windows users to connect to target servers in the data center. See: Virtual KVM Client (on page 42) and HTML KVM Client (HKC)
Do your KVM Clients have multi-language support?	Yes. The <ProdcutName>'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 <ProdcutName> 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.

Universal Virtual Media

Question	Answer
Which <ProdcutName> models support virtual media?	All <ProdcutName> models support virtual media. It is available stand-alone and through CommandCenter® Secure Gateway, Raritan's centralized management appliance.

Question	Answer
Which types of virtual media does the <ProdcutName> support?	<ProdcutName> supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives and ISO images.
What is required for virtual media?	A <ProdcutName> 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 by enabling the KVM Security setting "Apply Encryption Mode to KVM and Virtual Media", which will utilize 256-bit AES or 128-bit AES encryption, depending on the target or client capabilities.
Does virtual media really support audio?	Yes. Audio playback and recording to a server connected to the <ProdcutName> 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.

Question	Answer
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?	<ProdcutName> 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 <ProdcutName> 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 <ProdcutName> 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. 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 <ProdcutName> 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 DKX3G2 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 DKX3G2?	Use the "Network" 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 DKX3G2?	The DKX3G2 can access external servers via their IPv6 addresses, for example, an SNMP manager, syslog server or LDAP server. Using the DKX3G2's dual-stack architecture, these external servers can be accessed via: (1) an IPv4 address, (2) IPv6 address or (3) hostname. So, the DKX3G2 supports the mixed IPv4/IPv6 environment many customers will have.
What if my network doesn't support IPv6?	The DKX3G2'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 DKX3G2 user guide describes the DKX3G2's support for IPv6.

Servers

Question	Answer
Does <ProdcutName> 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), <ProdcutName> is designed to be completely independent from any external server.
What should I do to prepare a server for connection to <ProdcutName>?	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 <ProdcutName>'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 <ProdcutName> box?	The following is included: (1) <ProdcutName> 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 <ProdcutName>?	Each server that connects to <ProdcutName> 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?	<ProdcutName> 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 <ProdcutName>.
Which types of servers and PCs can be connected to <ProdcutName>?	<ProdcutName> 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 <ProdcutName>?	Servers that connect to the <ProdcutName> require a Dominion CIM, which connects directly to the keyboard, video and mouse ports of the server. Then, connect each CIM to <ProdcutName> using standard UTP (unshielded twisted pair) cable such as Cat5, Cat5e or Cat6.
How far can my servers be from <ProdcutName>?	In general, servers can be up to 150 feet (45 m) away from <ProdcutName>, depending on the type of server. (See: Target Server Video Resolution - Supported Connection Distances and Refresh Rates (on page 313)) 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 <ProdcutName> 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 many 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 <ProdcutName>?	Servers connected to <ProdcutName> do not require any software agents to be installed because <ProdcutName> connects directly via hardware to the servers' keyboard, video and mouse ports.
How many servers can be connected to each <ProdcutName> appliance?	<ProdcutName> 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 <ProdcutName> and reconnect it to another <ProdcutName> appliance, or connect it to a different port on the same <ProdcutName> appliance?	<ProdcutName> 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

Question	Answer
Can I access my servers directly from the rack?	Yes. At the rack, <ProdcutName> 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.
When I am using the local port, do I prevent other users from accessing servers remotely?	No. The <ProdcutName> 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 <ProdcutName> has USB keyboard and mouse ports on the local port. <ProdcutName> switches do not have PS/2 local ports. Customers with PS/2 keyboards and mice should utilize a PS/2 to USB adapter.
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.

Question	Answer
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 <ProdcutName> 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, <ProdcutName> fails over to its own internal authentication database. <ProdcutName> has its own stand-alone authentication, enabling instant, out-of-the-box installation.

Dual Power Supplies

Question	Answer
Does <ProdcutName> have a dual power option?	Yes. All <ProdcutName> 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.
Does the power supply used by <ProdcutName> automatically detect voltage settings?	Yes. <ProdcutName>'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 <ProdcutName> 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 <ProdcutName> offer?	Raritan's intelligent PDUs can be connected to the <ProdcutName> 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 <ProdcutName> 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 <ProdcutName> as these power strips do not provide outlet-level switching.
How many PDUs can be connected to a <ProdcutName>?	Up to eight PDUs can be connected to a <ProdcutName> appliance.
How do I connect the PDU to the <ProdcutName>?	DKX3G2 manages PDU via SNMP.

Question	Answer
Does <ProdcutName> support servers with multiple power supplies?	Yes. <ProdcutName> 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 <ProdcutName> display statistics and measurements from the PDU?	No. Only generic PDU information such as PDU model, serial number, firmware version and ip address is displayed.
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 <ProdcutName>'s Ethernet interfaces?	<ProdcutName> 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. <ProdcutName> 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 <ProdcutName>, servers can be configured and managed at the BIOS level wirelessly.
Does the <ProdcutName> offer dual gigabit Ethernet ports to provide redundant failover or load balancing?	Yes. <ProdcutName> 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, <ProdcutName> 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 <ProdcutName> with a VPN?	Yes. <ProdcutName> 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 <ProdcutName>?	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. <ProdcutName>'s TCP ports are configurable by the administrator.

Question	Answer
Can the <ProdcutName> use DHCP?	DHCP addressing can be used; however, Raritan recommends fixed addressing since the <ProdcutName> is an infrastructure appliance and can be accessed and administered more effectively with a fixed IP address.
I'm having problems connecting to the <ProdcutName> over my IP network. What could be the problem?	The <ProdcutName> 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 <ProdcutName> 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 <ProdcutName> is the same as another appliance, network connectivity may be inconsistent. • Port 5000 conflicts. If another appliance is using port 5000, the <ProdcutName> default port must be changed (or the other appliance must be changed). • When changing the IP address of a <ProdcutName>, or swapping in a new <ProdcutName>, sufficient time must be allowed for its IP and Mac® addresses to be known throughout the Layer 2 and Layer 3 networks.

•

Security

Question	Answer
Is the <ProdcutName> FIPS 140-2 Certified?	The <ProdcutName> uses an embedded FIPS 140-2 validated cryptographic module running on a Linux platform per FIPS 140-2 implementation guidelines. This cryptographic module is used for encryption of KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.
What kind of encryption does <ProdcutName> use?	<ProdcutName> 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 <ProdcutName> that is not completely secured by encryption.
Does <ProdcutName> support AES encryption as recommended by the U.S. government's NIST and FIPS standards?	Yes. The <ProdcutName> 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 <ProdcutName> allow encryption of video data? Or does it only encrypt keyboard and mouse data?	Unlike competing solutions, which only encrypt keyboard and mouse data, <ProdcutName> does not compromise security – it allows encryption of keyboard, mouse, video and virtual media data.

Question	Answer
How does <ProdcutName> integrate with external authentication servers such as Active Directory, RADIUS or LDAP?	Through a very simple configuration, <ProdcutName> can be set to forward all authentication requests to an external server such as LDAP, Active Directory or RADIUS. For each authenticated user, <ProdcutName> receives from the authentication server the user group to which that user belongs. <ProdcutName> 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 <ProdcutName>'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.
Does <ProdcutName> support strong passwords?	Yes. The <ProdcutName> 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 Dominion KX IIKX IIII?	Yes. Customers can upload self-signed or certificate authority-provided digital certificates to the <ProdcutName> 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 <ProdcutName> allows the administrator to configure alternate port numbers.

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.
Does <ProdcutName> support Paragon Dual CIMs?	No

Smart Cards and CAC Authentication

Question	Answer
Does <ProdcutName> support smart card and CAC authentication?	Yes. Smart cards and DoD common access cards (CAC) authentication to target servers is supported.

Question	Answer
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 <ProdcutName> models are supported. The <ProdcutName>-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 and D2CIM-DVUSB-DP 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 <ProdcutName>.

Manageability

Question	Answer
Can <ProdcutName> be remotely managed and configured via Web browser?	Yes. <ProdcutName> 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 <ProdcutName>'s IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and <ProdcutName>'s default IP address, you can even configure the initial settings via Web browser.)
Can I back up and restore <ProdcutName>'s configuration?	Yes. <ProdcutName>'s appliance and user configurations can be completely backed up for later restoration in the event of a catastrophe. <ProdcutName>'s backup and restore functionality can be used remotely over the network, or through your Web browser.
What auditing or logging does <ProdcutName> offer?	For complete accountability, <ProdcutName> 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 <ProdcutName> integrate with syslog?	Yes. In addition to <ProdcutName>'s own internal logging capabilities, <ProdcutName> can send all logged events to a centralized syslog server.

Question	Answer
Can <ProdcutName> integrate with SNMP?	Yes. In addition to <ProdcutName>'s own internal logging capabilities, <ProdcutName> 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 <ProdcutName>'s internal clock be synchronized with a timeserver?	Yes. <ProdcutName> 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 DKX3G2 user interface, and at raritan.com with the documentation. Online help includes DKX3G2 user guide and end user information on using the Remote Console, Virtual KVM Client (VKC) Active KVM Client (AKC) and Local Console, as well DKX3G2 specifications, informational notes, connecting DKX3G2 to the T1700G2-LED, and so on.
Where do I find documentation on the <ProdcutName>?	The documentation is available at raritan.com. The documentation is listed by firmware release.
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.

Question	Answer
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 DKX3G2?	The <ProdcutName> comes with a standard two-year warranty, which can be extended to 5 years of warranty coverage.

Miscellaneous

Question	Answer
What is <ProdcutName>'s default IP address?	DHCP
What is <ProdcutName>'s default username and password?	The <ProdcutName>'s default username and password are admin/raritan. However, for the highest level of security, the <ProdcutName> forces the administrator to change the <ProdcutName> default administrative username and password when the appliance is first booted up. Username is not case sensitive.
I changed and subsequently forgot <ProdcutName>'s administrative password; can you retrieve it for me?	<ProdcutName> 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.
Will my existing KX III CIMs work with <ProdcutName> switches?	Yes. Existing KX III CIMs will work with the <ProdcutName> switch. 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.