KX4-101 User Guide

KX4101-0H-v4.5.0-E
June 2025
Release 4.5.0

FCC Information

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

VCCI Information (Japan)

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

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

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

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

Contents

Installation and Initial Configuration

In This Chapter

Supported Browsers

- Chrome
- Edge
- Firefox
- Safari

See the Release Notes for more details on versions and compatibility.

Minimum Client and System Recommendations

Minimum client requirements vary somewhat depending on what client you want to use, and what kind of video you plan to stream.

► *Network Speed Recommendation:*

- A fast network like Gigabit Ethernet or WiFi 802.11ac

► *Standalone Virtual KVM Client (VKCS) and Active KVM Client (AKC)*

- CPU:
  - For FullHD video: a modern and fast dual core CPU, such as Intel Core i3 4xxx or newer, or a quad core CPU. If you plan to run more than one KVM session, a quad core CPU is recommended.
  - For 4K video: a modern and fast quad core CPU, such as Intel Core i5 4xxx or newer. If you plan to run more than one 4K stream, a CPU with 6 or more cores is recommended, such as Intel Core i5/i7 8xxx.
- 8GB RAM
- Graphics Card: a modern OpenGL capable graphics card, such as GeForce or Radeon. At least 1GB.

► *HTML KVM Client (HKC):*

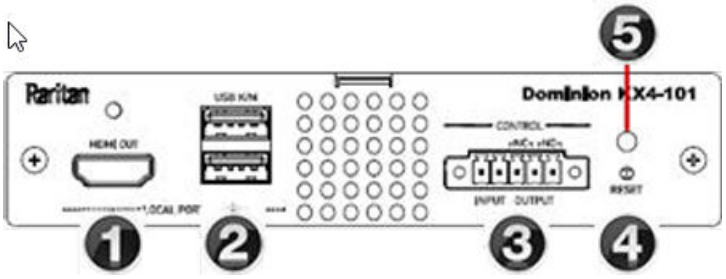
4K video not recommended on HKC.

- CPU: a modern and fast dual core CPU
- 8GB RAM
- OpenGL capable graphic card

Package Contents

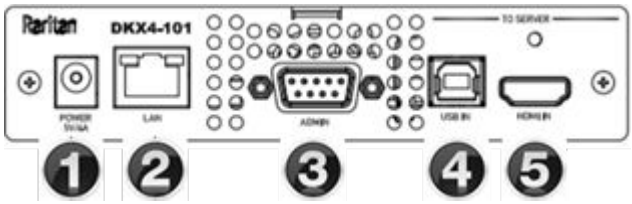
- 1 Dominion KX IV–101
- 1 power cord
- 1 HDMI cable
- 1 USB-B to USB-A cable
- 1 mounting bracket kit

Front View



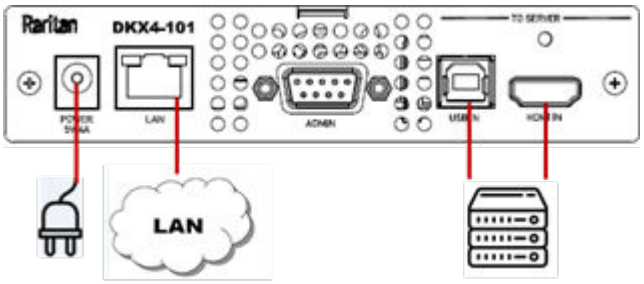
1. Local Port HDMI Out to local port monitor
2. Local Port USB
3. Input/Output
4. Reset
5. Power Status LED:
   - Green ON: Power on
   - Green BLINKING: Remote target connection

Rear View



1. Power-5V/4A from power adapter
2. RJ-45 LAN Network Port with 2 LEDs for network speed and activity:
   - Amber OFF/Green OFF: Link Inactive
   - Amber ON/Green OFF: 1000 MBps Link/No Activity
   - Amber BLINKING/Green OFF: 1000 MBps Link/Activity(RX, TX)
   - Amber OFF/Green ON: 100 MBps Link/No Activity
   - Amber OFF/Green BLINKING: 100 MBps Link/Activity(RX, TX)
   - Amber ON/Green ON: 10 MBps Link/No Activity
   - Amber BLINKING/Green BLINKING: 10 MBps Link/Activity(RX, TX)
3. Serial Admin Port
4. USB In from target server
5. HDMI In from target server

Connecting the Equipment



Connect the Dominion KX IV–101 to the network:

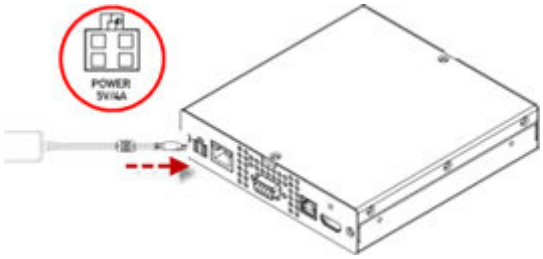
- Connect the Dominion KX IV–101 to the network using the LAN port.

Connect your target server:

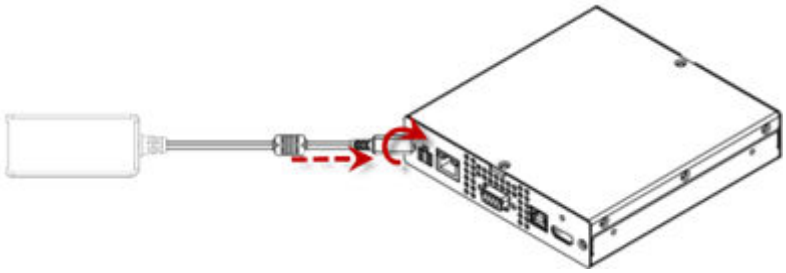
- Connect the target server with an HDMI cable to the Dominion KX IV–101 HDMI IN port. If the target server video is not HDMI, purchase a Raritan cable- or video-adapter.
- Connect the target server to the Dominion KX IV–101 USB IN port using the included USB cable.

Connect the power adapter:

- Newer models include a power adapter with a 4-pin connector. Push the adapter in to lock.



- Some of the original models include twist-to-lock adapters, as shown in the image below. These are marked with an arrow. Connect with the arrow facing up. Push in firmly and twist clockwise to lock. Check to ensure it is locked.



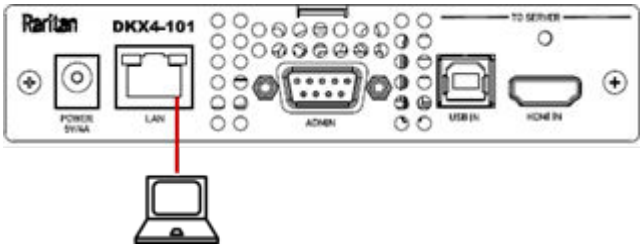
Power on all devices.

Initial Configuration

Default login: admin/raritan

Option 1: Connect a PC to the LAN Port

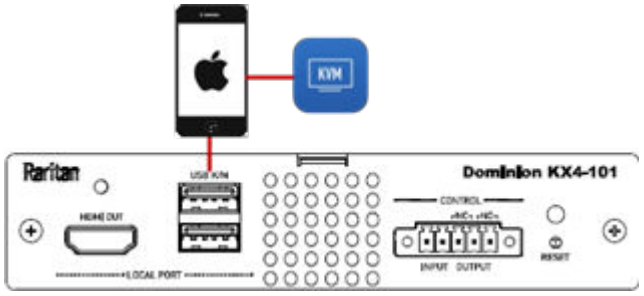
Re-connect the Dominion KX IV–101 to the LAN after initial configuration.



- Disable the wireless interface of the PC, and make sure the PC is set to DHCP.
- Connect a network cable between the PC and Dominion KX IV–101 LAN port.
- Open a browser. Enter the URL "https://kvm.local". The login page appears.
- Follow the prompts to change the default password.

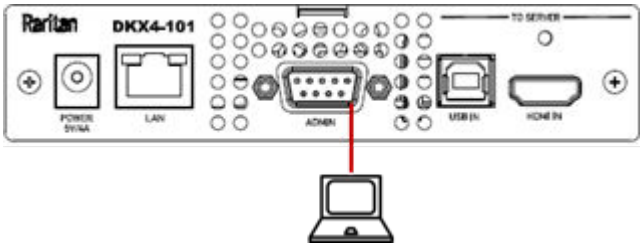
Option 2: Connect an iOS device at the Local Port

Required App: Raritan KVM by Raritan: https://itunes.apple.com/us/app/raritan-kvm/id1455817539?mt=8



- Launch the Raritan KVM app on an iOS device.
- Connect the iOS device with the Raritan KVM app to the Dominion KX IV–101 USB port.
- Wait until the app detects the connected Dominion KX IV–101.
- Follow the prompts to change the default password.

Option 3: Serial configuration



- Connect a DB9 serial cable or USB-Serial adapter between the PC and the Dominion KX IV–101 serial Admin port.
- Serial console configuration: (default) 115200bps/None/8bits/1stop
- To find the default DHCP IP address, use the "show" command to "show network".
- For help with all commands, see CLI Commands (on page 219).

Next Steps

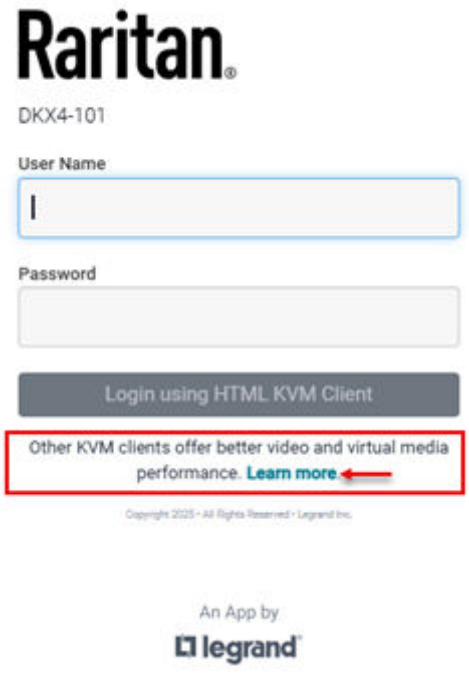
- Configure network settings: See Network (on page 161)
- Configure time settings: See Date and Time (on page 152)
- Install certificates: See TLS Certificate (on page 195)
- Configure users: See User Management (on page 121)
- Configure port settings: Port Configuration: KVM Port Settings - General, Video, Audio, Mouse (on page 18)

KVM Client Options

Dominion KX IV–101 offers a selection of KVM clients. Upon launching the Dominion KX IV–101 IP address in a supported browser, the login page appears.

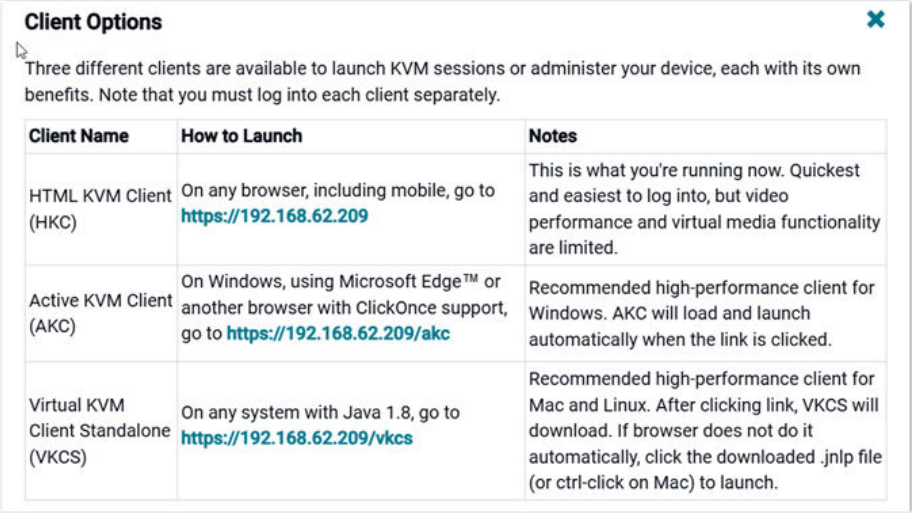
The HTML KVM Client (HKC) is loaded by default.

- Click the Learn more link in the login page to view other KVM client options.



- The Learn more link launches a client options dialog. Click the provided links to launch a different client.

- https://<IP address> launches HKC
- https://<IP address>/akc launches AKC
- https://<IP address>/vkcs launches VKC



When a different client is selected, Dominion KX IV–101 automatically checks your system to make sure it meets the requirements of the client. If your system is ready, the selected client loads. If your system needs to meet additional requirements, another message displays with details.

Note: For AKC and VKCS, your browser may display a "This site is not secure" warning message until you have installed valid certificates. Click to accept the warnings and go to the site. See TLS Certificate for help installing certificates that prevent these warnings.

For more details and instructions for using all clients, see KVM Clients (on page 55).

Port Access and Configuration

In This Chapter

Port Access

Click Port Access to view the port preview and connect to the target.

► *Port Preview:*

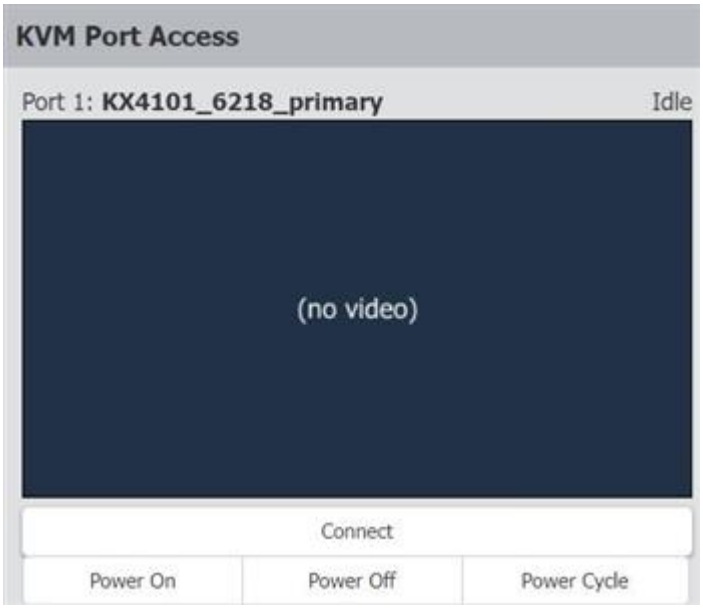
- The preview image refreshes every 5 seconds.
- Your ability to see the preview depends on your privileges. If you do not have sufficient privileges, a message displays with details.

► *Connect to the target:*

- Click the Connect button to open a connection to the target server.
- For help with using the KVM clients, see KVM Clients (on page 55).

► *Control power to the target:*

- You will see power control options only if you have associated one or more PDUs to the target, and have permission to do power functions.
- Click the Power On, Power Off or Power Cycle to control power to the target. Power association must be setup first. See Port Configuration: Power Association (on page 28)

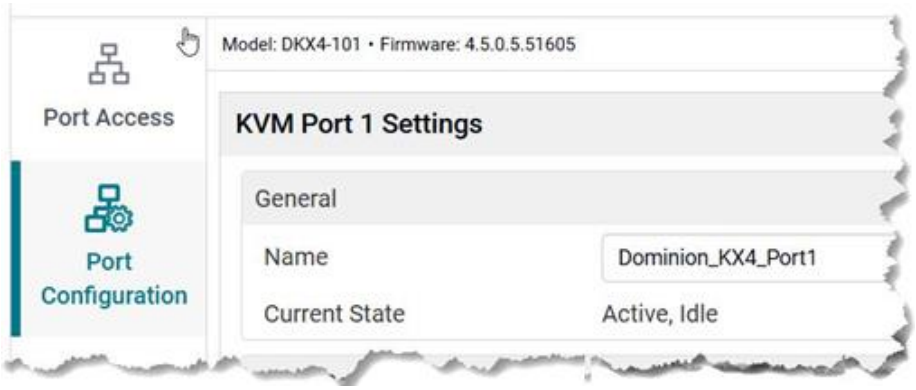


Port Configuration: KVM Port Settings - General, Video, Audio, Mouse

The Port Configuration page contains all port settings for the KVM port name and video resolution, as well as USB port and audio settings.

► *To access all port configuration:*

- Click Port Configuration.



► *KVM Port Settings:*

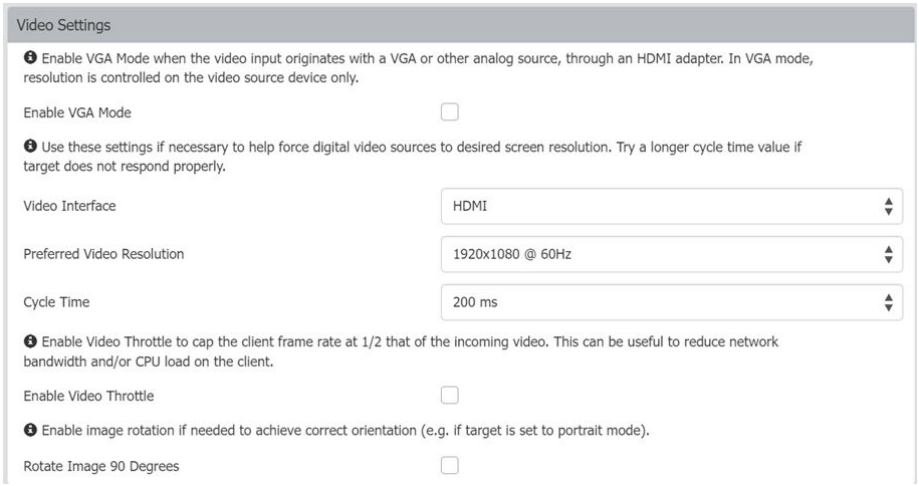
General Settings:

- To rename the KVM port: enter a new name and click Save.
- View the Current Port Status:

- Active, Idle
- Active, Busy: Connected, but PC Share is disabled. See KVM Security (on page 187).
- Active, Connected: Connected, and PC Share is enabled.

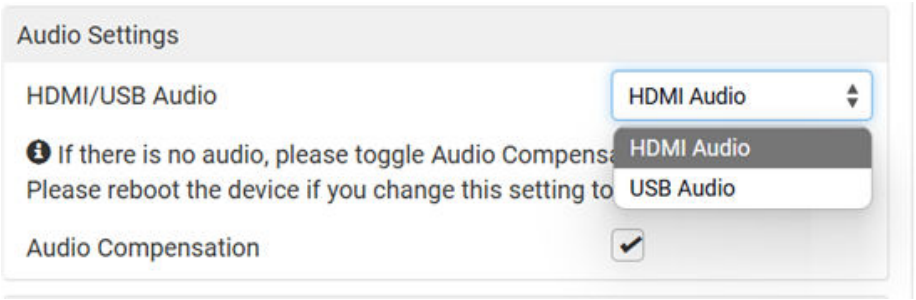
Video Settings:

- Select Enable VGA Mode if the video input originates with a VGA or other analog source, through an HDMI adapter. In VGA mode, resolution is controlled on the video source device only.
- Set the Video Interface to HDMI or DVI (no audio).
- Select the Preferred Video Resolution: Important! The KX IV uses an "EDID" data structure to tell the target server what video resolution is wanted. 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 20) for a list of all supported resolutions.
  - If you have a specific EDID to load, see Port Configuration: Custom EDIDs (on page 29).
- Set a longer Cycle Time if your target video is not responding properly to changes in preferred video resolution. Default is 200ms. A longer Cycle Time may allow your target to respond accurately to a new preferred video resolution.
- Select Enable Video Throttle to cap the client frame rate at half the frame rate of the incoming video. This can be useful to reduce network bandwidth and CPU load on the client.
- Select Rotate Image 90 Degrees and change the target's display orientation to obtain the proper video orientation between landscape and portrait modes.



Audio Settings

- Select either HDMI Audio or USB Audio for Audio Settings. By default HDMI Audio is selected. You need to reboot the device when the audio compensation is disabled or enabled.

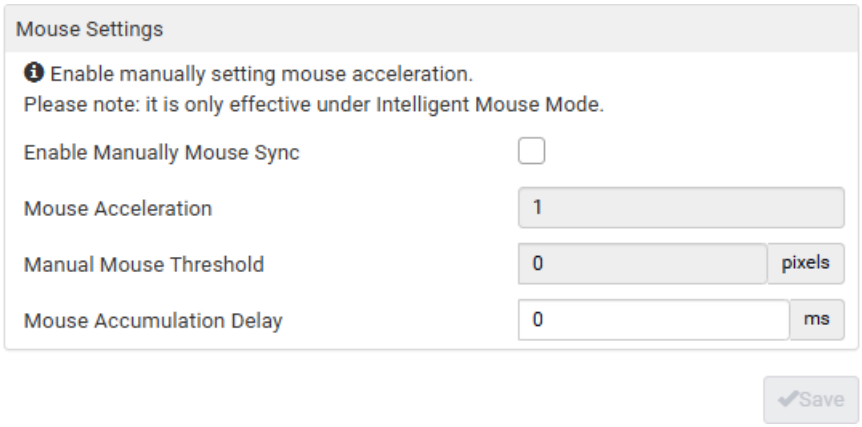


- Click Save to apply all settings.

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 EDID is listed with the preferred video resolutions it can offer. The server will generally choose the largest resolution and refresh rate that it can support.

► *1024x768@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz

► *1152x864@60Hz*

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz

► *1280x720@60Hz*

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz
- 1280x720@60Hz

► *1280x960@60Hz*

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz

► *1280x1024@60Hz*

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz
- 1280x1024@60Hz, @75Hz

► *1360x768@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz
- 1280x1024@60Hz
- 1360x768@60Hz

► *1440x900@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x960@60Hz
- 1280x1024@60Hz
- 1440x900@60Hz

► *1400x1050@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1400x1050@60Hz

► *1600x900@60Hz*

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz, @85Hz
- 1600x900@60Hz

► *1600x1200@60Hz*

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz, @85Hz
- 1280x1024@75Hz
- 1600x1200@60Hz

► *1680x1050@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1680x1050@60Hz

► *1920x1080@60Hz (148.5MHz clock)*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz

► *1920x1200@60Hz (Reduced Blanking 154MHz clock)*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz

- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x1200@60Hz

► *1920x2160@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x2160@60Hz

► *2560x1440@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz

- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@30Hz
- 2560x1440@60Hz

► *2560x1600@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@30Hz
- 2560x1600@60Hz

► *3840x1080@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz

- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@30Hz, @60Hz
- 2560x1440@60Hz
- 2560x1600@60Hz
- 3840x1080@60Hz

► *3840x1200@60Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@30Hz, @60Hz
- 2560x1440@60Hz
- 3840x1200@60Hz

► *3840x1600@30Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz

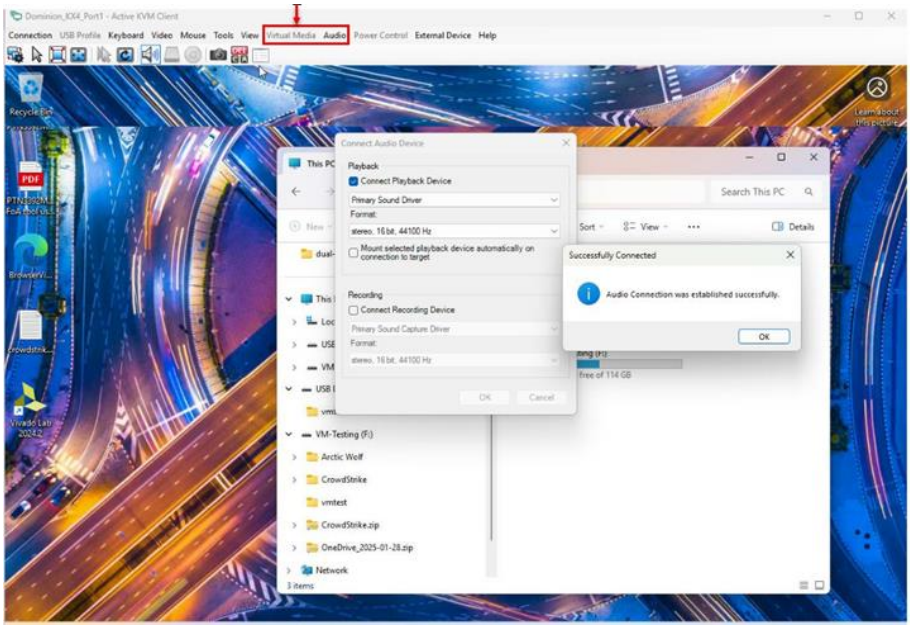
- 1280x720@60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x1200@60Hz
- 2560x1080@60Hz
- 2560x1440@60Hz
- 3840x1600@30Hz

► *3840x2160@30Hz*

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@60Hz
- 2560x1440@60Hz
- 2560x1600@60Hz
- 3440x1440@50Hz
- 3840x2160@24Hz, @25Hz, @30Hz
- 4096x2160@30HZ

USB Audio Restrictions on KVM Clients

Virtual Media option will be disabled if USB Audio is connected. USB recording is available in VKCs and AKC and only one recoding session is allowed.



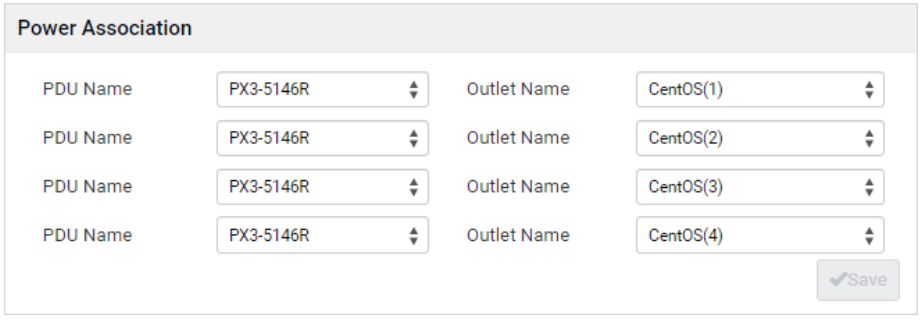
Port Configuration: Power Association

Port association can be done once a power strip is added to the Dominion KX IV–101. See Adding PDUs (on page 171). 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 Dominion KX IV–101.

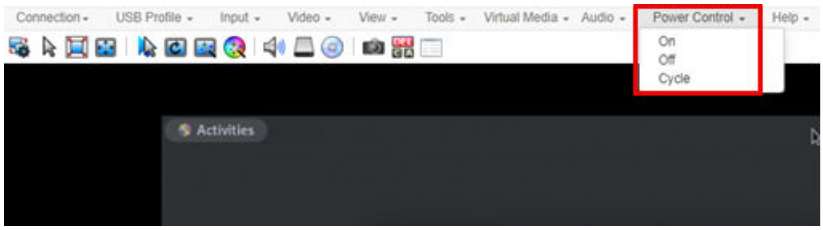
► *To configure Power Associations:*

1. Select Port Configuration then scroll down to Power Association.
2. In the PDU Name fields, select from the drop down list of configured PDUs.
3. In the Outlet Name fields, select the outlet from each PDU you want to associate with this target.
4. Leave extra fields blank or select none.
5. Click Save.



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

Raritan
A brand of legrand



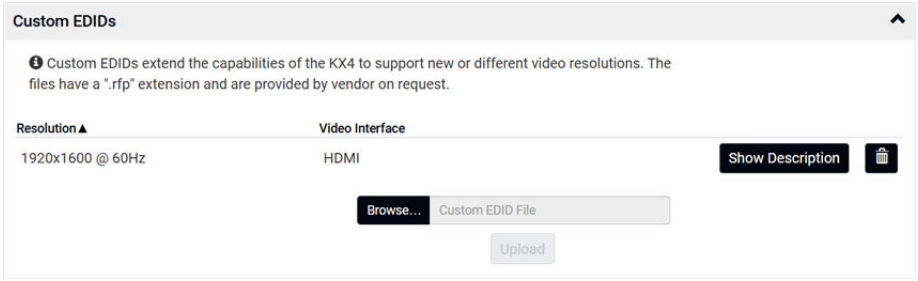
Port Configuration: Custom EDIDs

A custom EDID can be loaded to allow the Dominion KX IV–101 to support a new or different video resolution, or to specify a custom version of standard supported resolution. Only one custom EDID per resolution can be added. The files have a ".rfp" extension and are provided by the vendor on request.

You can upload up to 20 custom EDIDs with a maximum of 10 custom HDMI EDIDs and 10 custom DVI EDIDs. Custom EDIDs are not included in backups.

► *To upload a custom EDID:*

1. Click Port Configuration, then scroll down to Custom EDIDs.
2. Click Browse to find and select the .rfp EDID file.
3. Click Upload. Repeat these steps to add more files.
4. Once EDIDs are uploaded, they display in a list sorted by resolution.
   - Click Show Description to view the details.
   - Click the Delete icon to remove a file.



Port Configuration: Local Port Monitor EDID

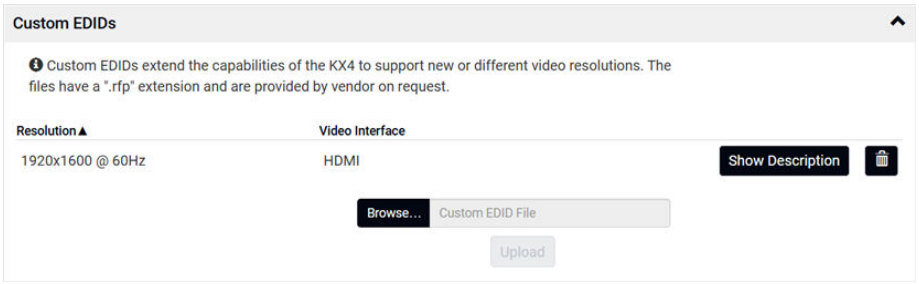
If a Local Port Monitor is attached to Dominion KX IV–101, a Local Port Monitor EDID section appears on the Port Configuration page and the monitor's EDID is included in the Preferred Video Resolution. You can use the Local Port Monitor's EDID by selecting it as the Preferred Video Resolution.

If the Local Port Monitor is removed while it's EDID was in use as the preferred video resolution, the preferred video resolution will revert back to the default 1920x1080@60Hz standard EDID.

If a new monitor is attached, it will overwrite the old Local Port Monitor EDID.

► *To view Local Port Monitor EDID:*

1. Click Port Configuration, then scroll down to Custom EDIDs.
2. Expand to see the EDID of the currently attached local port monitor.
   - Click Show Description to view the details.



Port Configuration: USB Connection Settings

USB Connection Settings are disabled when the port is connected. All users must be disconnected from the KVM target to change the USB port settings.

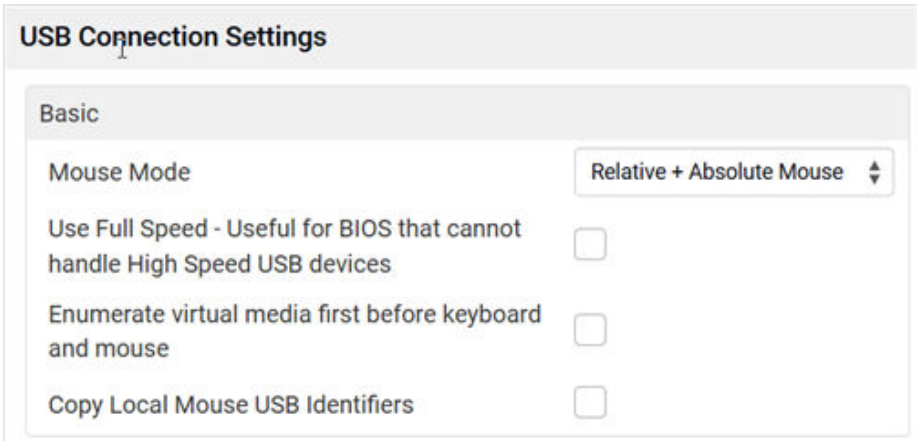
► *To define USB connections for the target server:*

- Click Port Configuration, then scroll down to USB Connection Settings.
- Select the USB connection settings you will be using:
  - Mouse Mode: Relative, Absolute and Relative +Absolute options are supported. Select Relative if the target does not support absolute mouse mode. When a local mouse is connected to and configured on the KVM, the KVM introduces a mouse via the USB interface. The available options displayed on KVM targets depend on the 'Mouse Mode on USB Connection' settings which will work on remote or local KVM connections.

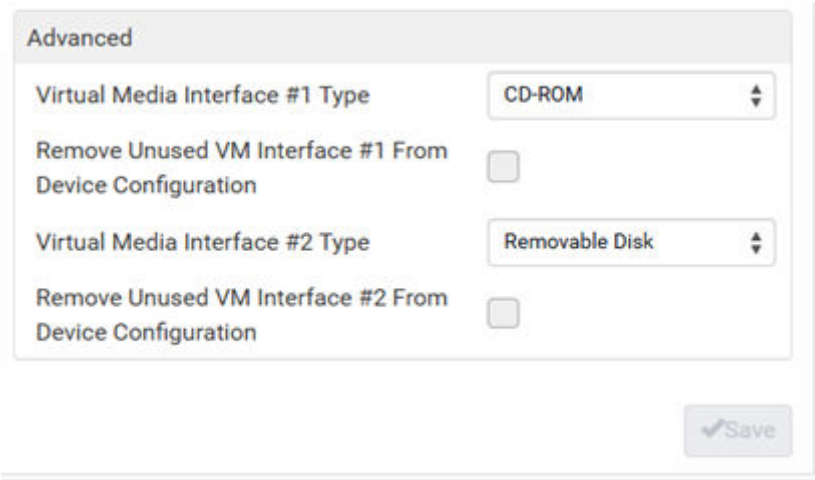
    Relative Mouse : Mouse option in KVM client will allow both intelligent and standard mouse.

    Absolute mouse: Mouse option in KVM client will only allow absolute mouse.

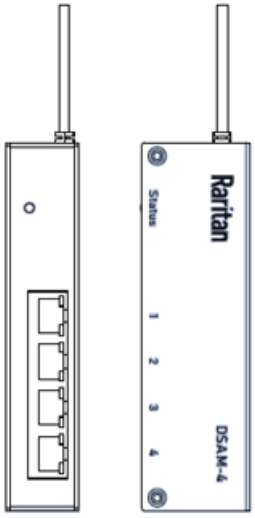
    Relative mouse + Absolute mouse: Mouse option in KVM client will allow all mouse modes (absolute, intelligent, standard).
  - Use Full Speed - Useful for BIOS that cannot accommodate High Speed USB devices: Clear the checkbox to allow negotiation to the target's highest USB speed capability.
  - Enumerate virtual media first before keyboard and mouse: Useful to resolve issues when a target cannot detect USB mass storage at the BIOS.
  - Copy Local Mouse USB Identifiers: When enabled, this allows the USB descriptor for the mouse, to match the mouse that is plugged into the local port.
- Click Save.



- Set Advanced Options as needed:
  - Virtual Media Interface Types: Both interfaces cannot be set to CDROM or Removable Disk.
    - Disabled
    - CDROM
    - Removable Disk
    - Auto - can function as either CDROM or Removable Drive but not both at the same time
  - Remove Unused VM Interface From Device Configuration: Select this option to remove the drive when VM is disconnected. Clear this option to allow empty drives.
- Click Save.



Serial Access With Dominion Serial Access Module



Connecting a Dominion KX IV–101 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 Dominion KX IV–101.

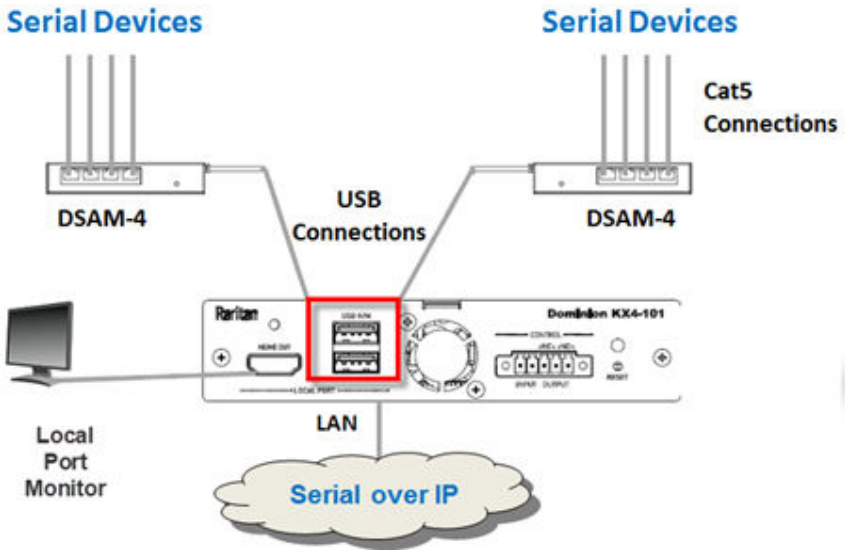
Connect a maximum of 2 DSAM modules to the Dominion KX IV–101 using USB cables. DSAM can be mounted in a 0U configuration.

In This Chapter

Connect DSAM

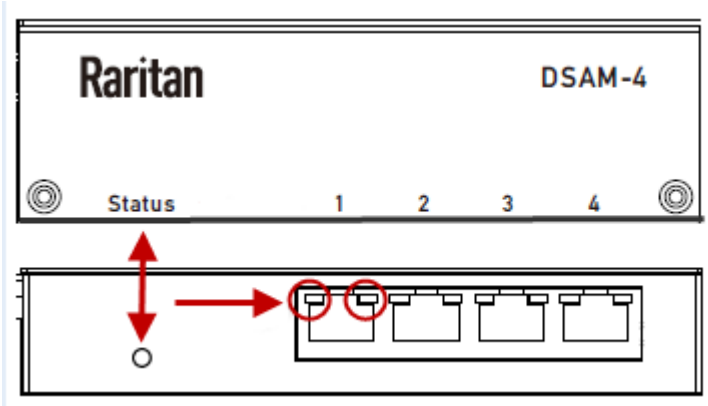
► *To connect DSAM to Dominion KX IV–101:*

- Connect the DSAM unit's USB cable to either of the USB K/M ports on the front of the Dominion KX IV–101.
- Connect the serial devices to the serial ports on the DSAM unit.
- When 2 DSAM units are connected, a local keyboard and mouse cannot be connected.
- When only 1 DSAM unit is connected, a combined keyboard/mouse can be connected to the available USB port.



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 Dominion KX IV–101.
- Blue LED - Slow blink: DSAM controlled by Dominion KX IV–101.
- Blue LED - Fast blink: Firmware upgrade in progress.

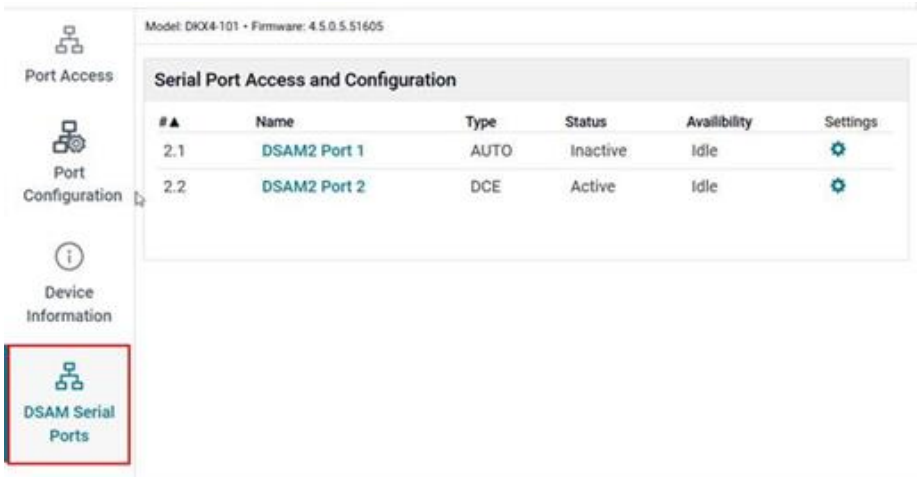
► *Port LEDs:*

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 Dominion KX IV–101, a DSAM Serial Ports page is available.



► *To view DSAM serial ports:*

Click DSAM Serial Ports. You can access and configure serial ports from this page.

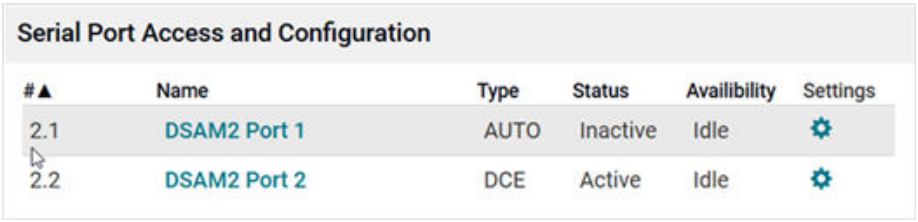
- Ports are listed by physical USB position on the DSAM unit.
- # column indicates which Dominion KX IV–101 USB port DSAM is plugged into.
- Type column indicates port's DTE/DCE setting.
- Status and Availability columns show current activity.

Configure DSAM Serial Ports

You can rename serial ports and configure their settings.

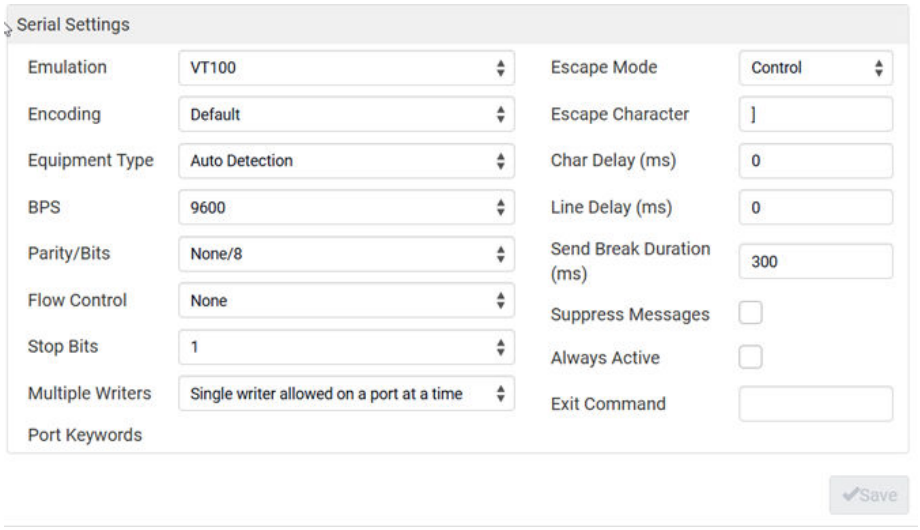
► *To configure DSAM serial ports:*

1. Click DSAM Serial Ports, then click the gear icon for the port you want to configure to open the settings.



2. In the General section:

   - Enter a Name for the port.
   - Check the Current State of the port. Status and Availability are listed.
3. In the Serial Settings section, check or change the following settings:



4. Emulation: Select the terminal emulation mode used to match the serial targets connected to the ports.
   - VT100
   - VT220
   - VT320
   - ANSI
5. Encoding: Select a specific character encoding for this port if needed. Encoding overrides the global setting for the port to whatever value you set.
   - DEFAULT
   - 8-BIT ASCII
   - ISO-8859-1
   - ISO-8859-15
   - UTF-8
   - Shift-JIS
   - EUC-JP
   - EUC-KR
6. Equipment Type: Indicate whether you want the Dominion KX IV–101 to automatically detect a physical connection to the target.
   - Default is Auto Detection.
   - Force DTE causes Dominion KX IV–101 to act as a piece of data terminal detection equipment to detect targets connected to it.
   - Force DCE causes Dominion KX IV–101 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. Dominion KX IV–101 does not support autodetection of both DCE and DTE on the same port.

---

7. Bits Per Second (BPS): Select a value.
   - BPS options: 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
8. Parity/Bits: Select a value.
9. Flow Control: Select a value.
10. Stop Bits: Select a value.
11. Multiple Writers: Select an option to allow single or multiple writers on a port at one time.
12. Port Keywords: When configured, port keywords appear here. Go to Device Settings > Serial Port Keyword List to add port keywords.
13. Escape Mode: The escape sequence affects only the CLI. When entering escape mode, the user is given a menu of commands that can be performed (for example, gethistory, view commands, and so on), a command to return to the port session, and a command to exit the port connection. Default is Control.
    - None
    - Control
14. Escape Character: The default for the Dominion KX IV–101 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.

---

15. Char Delay: To specify the delay between when individual characters are sent via the port, enter the time in milliseconds.
16. Line Delay: To specify the delay between when lines of text are sent via the port, enter it in the field.
17. Send Break Duration: Entering the send break time in milliseconds. Range is from 0ms - 1000ms.
18. Always Active: Select the checkbox 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 .

---

19. Exit Command: Type a command, such as `logout`, to be sent to your system when a user with write permission disconnects from the port. This ensures that the user's session on the target machine is closed, but it is not imperative to have an Exit command configured on a port.
20. Click Save.

Serial Port Keyword List

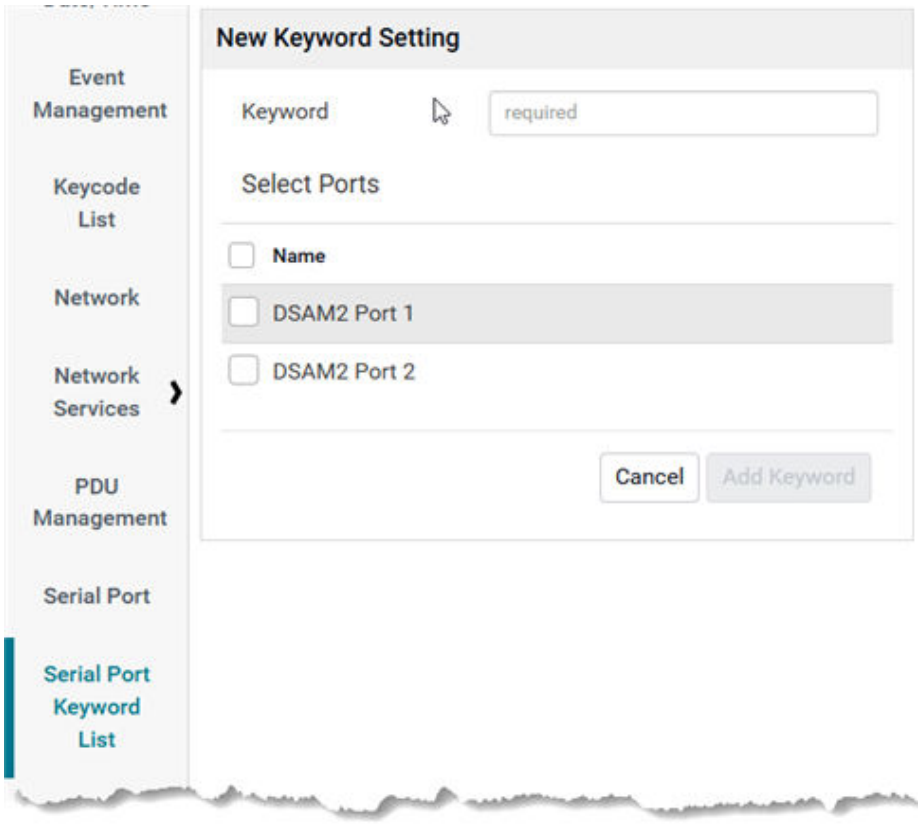
Port keywords work as a filter. If a keyword is detected, message are sent to:

- Event Log
- SNMP
- SMTP
- Syslog

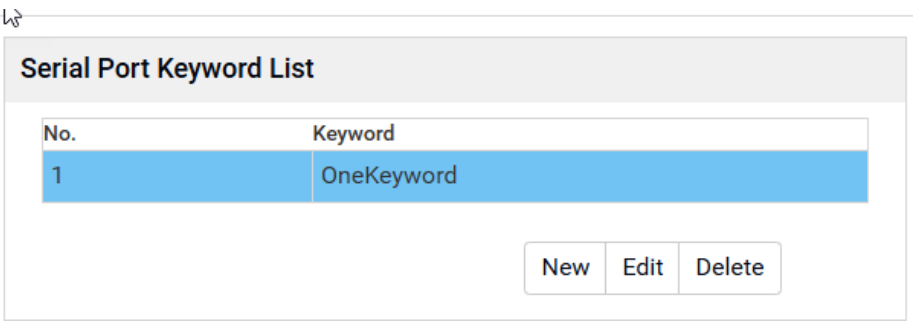
This feature is useful for notifying administrators if a particular event occurs on a port. For keywords to trigger when no users are connected to a port, "Always Active" must be selected in the port settings. (See Configure DSAM Serial Ports (on page 35).) You can also view the list of existing port keywords on the serial port settings page.

► *To configure serial port keywords:*

1. Click Device Settings > Serial Port Keywords. The Serial Port Keyword List page opens.
2. Click New. The New Keyword Settings page opens.
3. Enter a keyword in the Keyword field, then select the ports you want to associate with that keyword. For all ports, select the top checkbox.



4. Click Add Keyword. The Serial Port Keyword List appears.



- To edit or delete a keyword, select it to highlight blue, then click Edit or Delete.

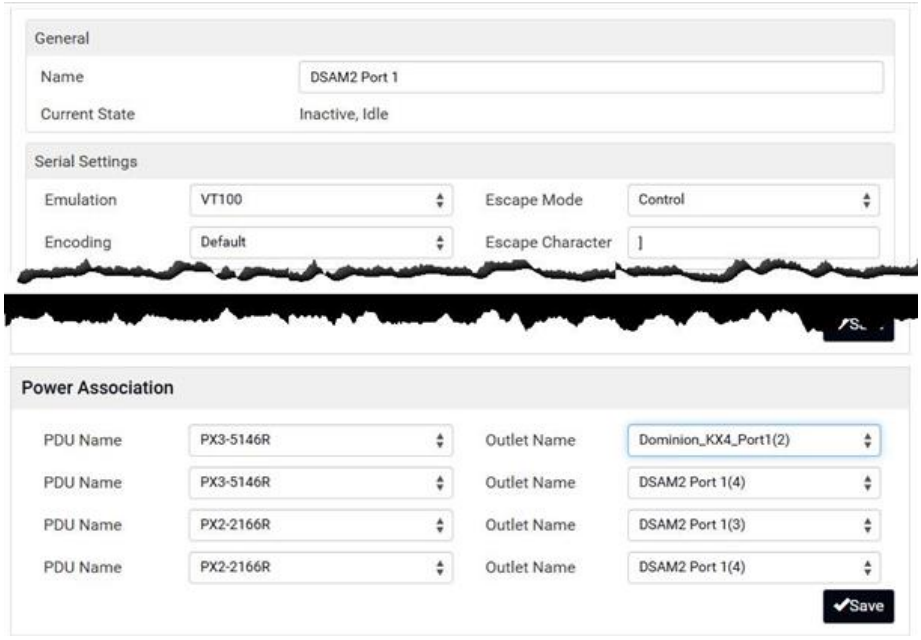
Power Association and Operation from DSAM Serial Ports

You can perform power operations from DSAM serial ports just like KVM ports. Serial port association can be done once a power strip is added to the Dominion KX IV–101. See Adding PDUs (on page 171). You can configure up to four power associations on each serial port. The outlets may be on the same or different PDUs.

Note: DSAM Serial Ports menu will become available when DSAM is connected to the Dominion KX IV–101.

► *To configure power association to DSAM serial ports:*

1. Click DSAM Serial Ports >click the Settings icon to open configuration for the port.
2. Scroll down to the Power Association section.



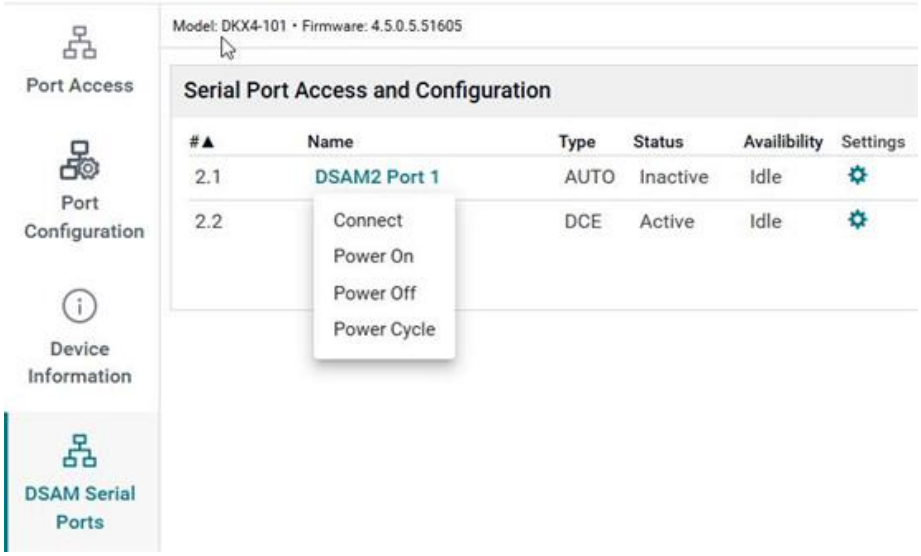
3. In the PDU Name fields, select from the drop down list of configured PDUs.
4. In the Outlet Name fields, select the outlet from each PDU you want to associate with this serial port.
5. Click Save.

Note: Power association will be grayed out if no PDU is added to the Dominion KX IV–101.

► *To perform power operation from DSAM serial ports:*

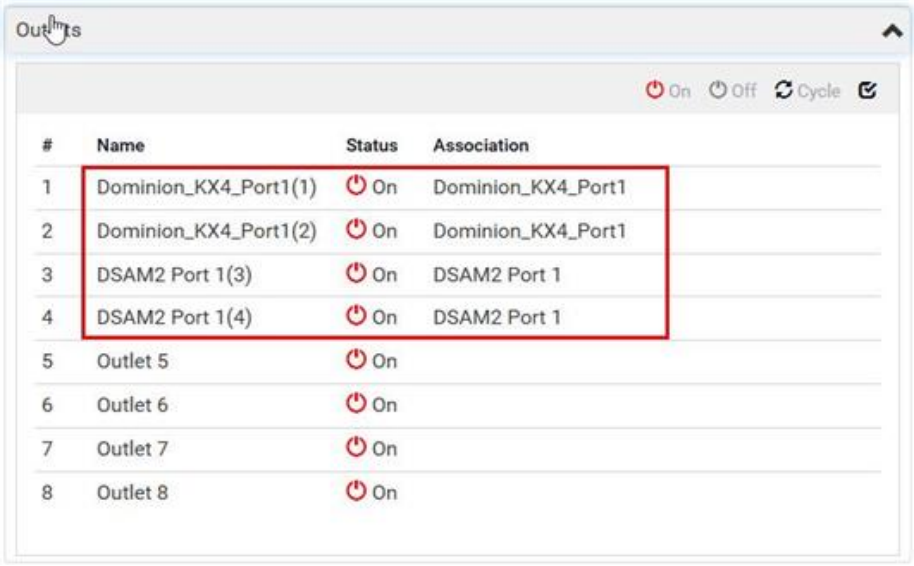
Power operations are done from the Serial Port Access and Configuration page.

1. Select DSAM Serial Ports.
2. On the Serial Port Access and Configuration page, click one of the associated DSAM Ports.
3. Click Power On or Power Off or Power Cycle.



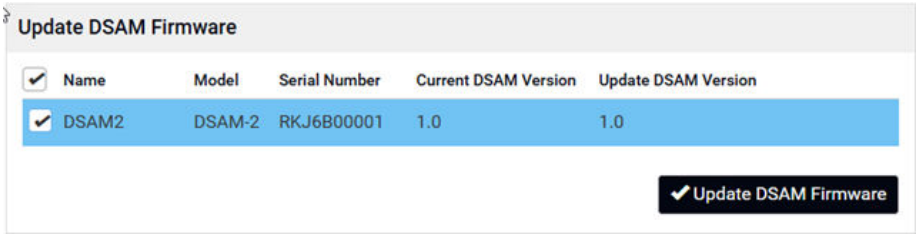
► *To check the outlet status:*

1. Click Device Settings > PDU Management, then click the PDU whose outlets you want to check.
2. Scroll down to the Outlets to see the status.



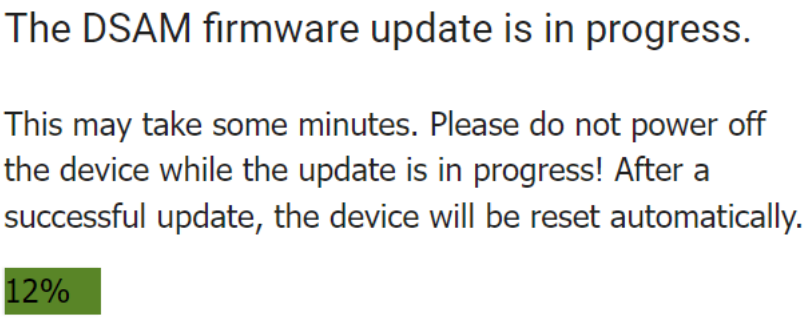
Update DSAM Firmware

DSAM firmware is upgraded automatically during Dominion KX IV–101 device firmware upgrades if a new DSAM version is detected in the device firmware. You can also upgrade your DSAM firmware manually.



► *To update 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 Firmware, then click OK to confirm. A progress message appears.



4. When firmware upgrade completes, a success message appears.

Supported CLI Commands

- show
  - `show device`
    If DSAMs is attached in KX4-101, show device will include DSAM device information
  - `show keyword`
    Shows all configured keywords
  - `show port`
    Shows DSAM serial port parameters
- connect:
  Connect to a DSAM serial port
  - `connect <port index> (1.1/1.2…/2.4)`
    During connecting to target, using the escape key sequence, the following target port CLI command can be reached:
  - `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
- `resetport`
  Reset of this 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
- `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

- config
- keyword
  - `keyword add [key <key>] [port <port>]`
    Add a keyword
  - `keyword delete [key <key>]`
    Delete a keyword
  - `keyword modify [key <key>] [port <port>`
    Edit a keyword
- port
  Configure DSAM serial port settings
  - `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>]
```

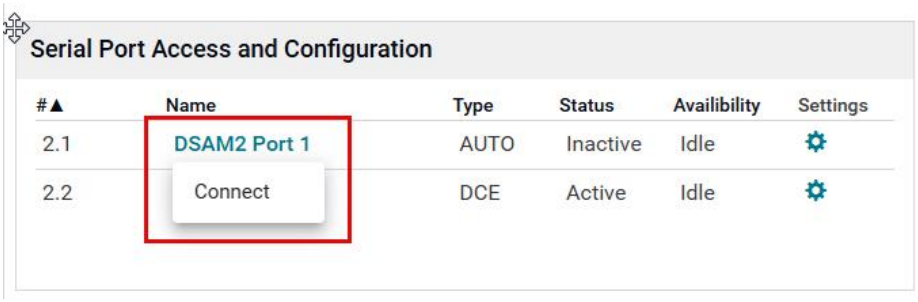
Supported Escape Key Characters

The default escape key is CTRL]

The following characters are supported for customized escape keys.

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

Connect to DSAM Serial Targets in the Web Interface



► *To connect to DSAM serial targets in the web interface:*

1. Click DSAM Serial Ports to view the list of ports.
2. Click the port you want to connect to, then click the pop-up Connect button.

HSC launches in a new window.

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 Targets via SSH

See Supported CLI Commands (on page 42).

► *To connect to DSAM serial targets via SSH:*

1. Make sure that SSH Access is enabled in Device Settings > Network Services > SSH.
2. Launch SSH client in client PC to connect to Dominion KX IV–101.
3. After login, user will enter CLI interface.
4. Type command "`connect <serial port number>`".

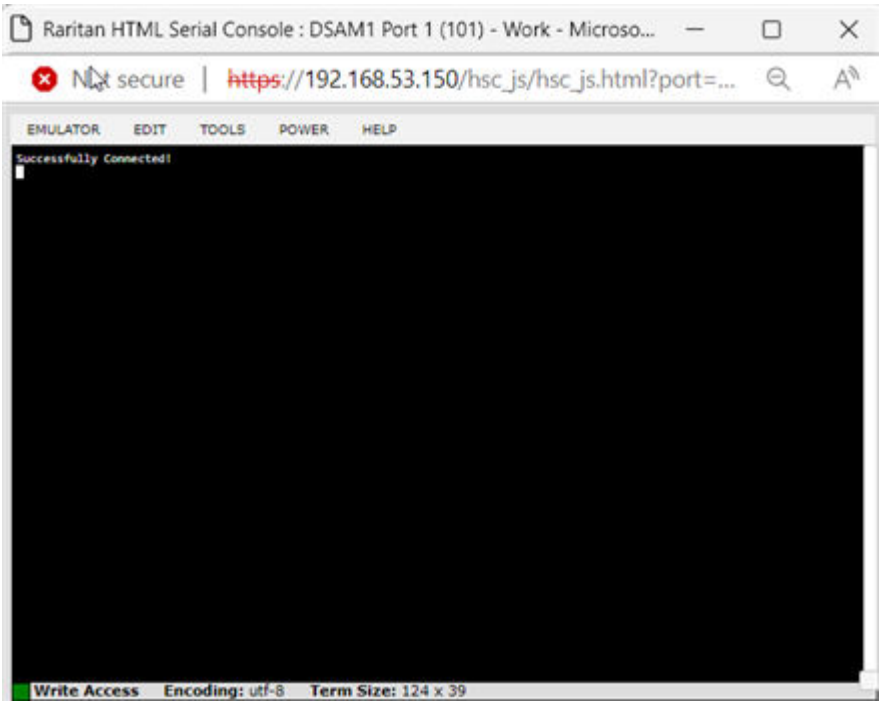
Example: `connect 1.4`

---

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 "close", then enter main CLI interface.

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.



Emulator

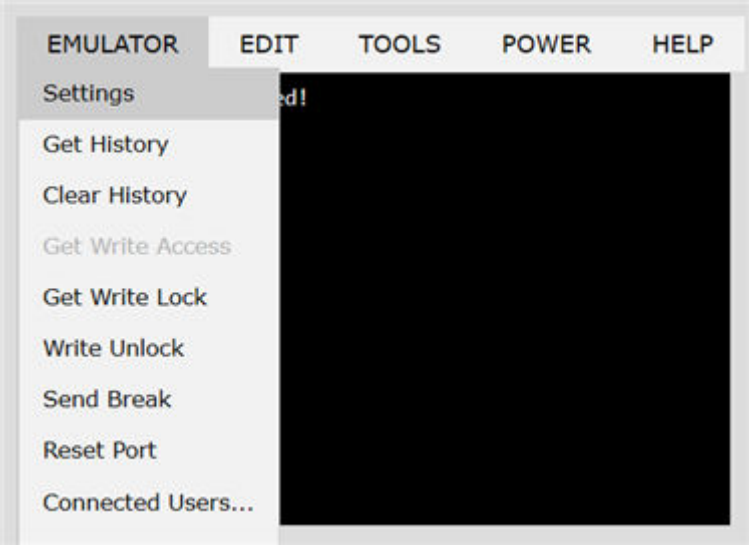
IMPORTANT: HSC sessions are affected by the Dominion KX IV–101 Idle Timeout.

If you have not changed the Dominion KX IV–101 Idle Timeout setting from the default, your session could be closed automatically if it exceeds the Idle Timeout period.

Change the default Idle Timeout setting and then launch the HSC. See Login Limitations for details on changing the Idle Timeout setting.

Access Emulator Options

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



Settings

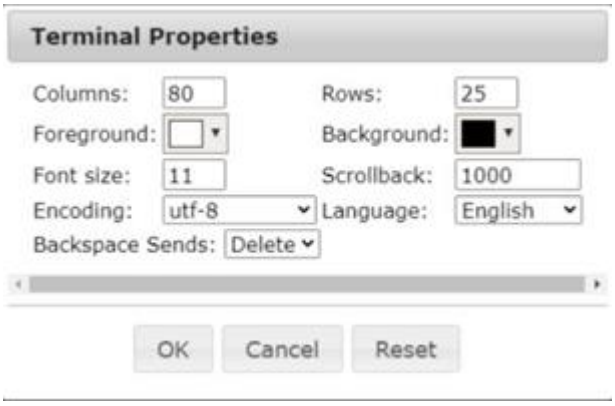
Note:

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

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

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

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



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

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

Get History

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

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

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

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

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

Clear History

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

Get Write Access

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

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

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

Get Write Lock

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

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

Write Unlock

To get Write Unlock, choose Emulator > Write Unlock.

Send Break

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

Only users with Write Access privileges can send a break.

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

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

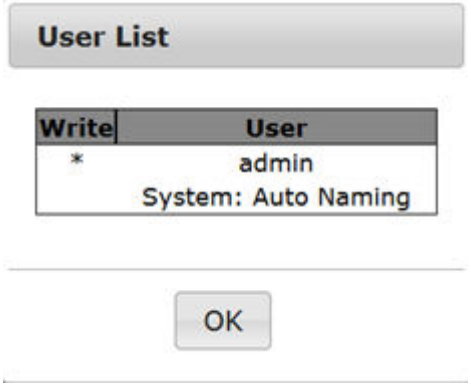
Reset Port

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

Connected Users

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

1. Choose Emulator > Connected Users.



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

Exit

1. Choose Emulator > Exit to close the HSC.

Copy and Paste and Copy All

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

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

If you need to paste a large amount of data, it is better to save the data in a file and use the Send a Text File function. Pasting a large amount of data in a browser windows can cause the browser to hang as it processes the data. See Send Text File (on page 50).

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

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

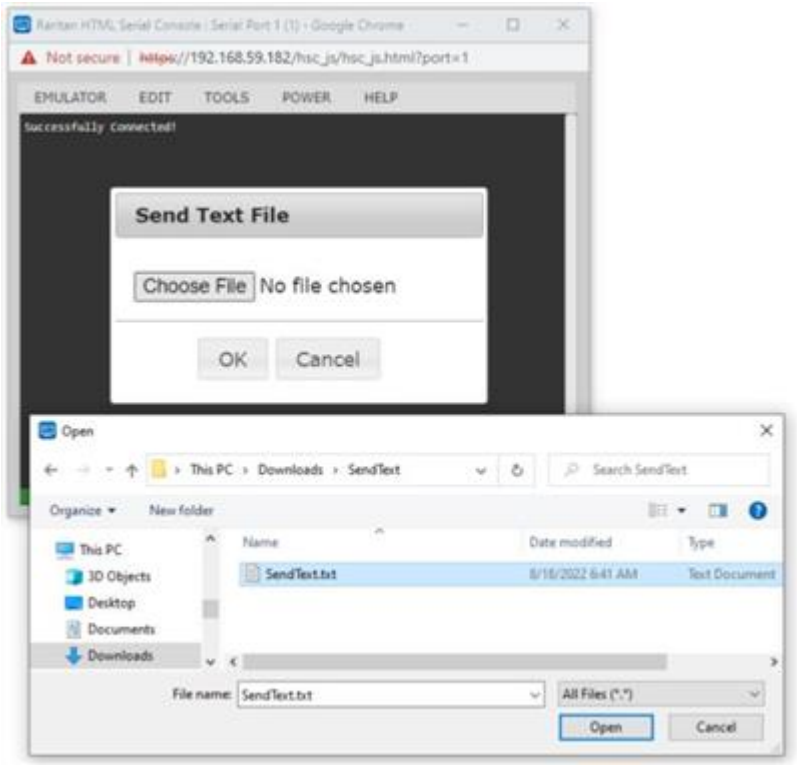
Do not use the Delete option that appears in the right-click menu of IE and some versions of Firefox. This Delete option will remove display lines entirely from the emulator window.

► *Browser-specific behaviors*

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

Send Text File

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



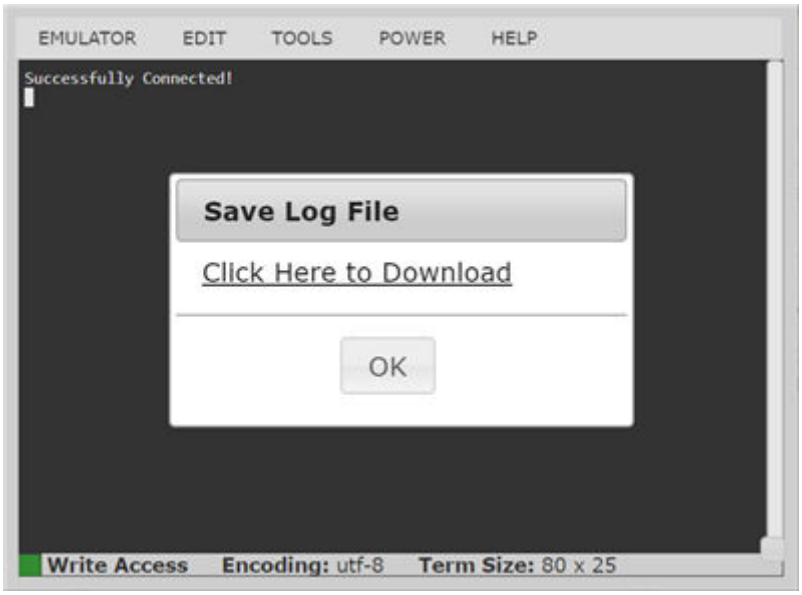
► *Note, if you are using a Mac® and/or Safari®, do the following in order to use this feature:*

1. In Safari, select Preferences.
2. Under the Security tab, select "Manage Website Settings"
3. Click on the Dominion KX IV–101 website.
4. Select "Run in unsafe mode" from the drop-down box.
5. Restart Safari.

Tools: Start and Stop Logging

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

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



Power

Note: You must have permission to manage the target's power, and the target must have configured power associations. If you only have Access permission and not Power Control, power actions will be denied.

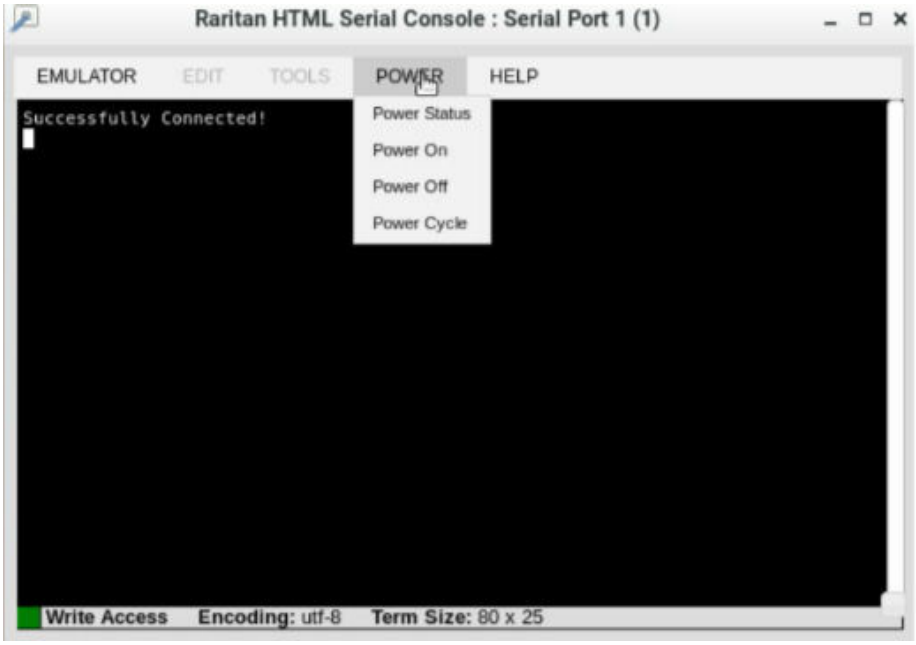
► *To view power status:*

- Choose Power > Power Status to view the status of the outlet the target is plugged into.
  - The Notification dialog shows the status of the outlet as ON or OFF.

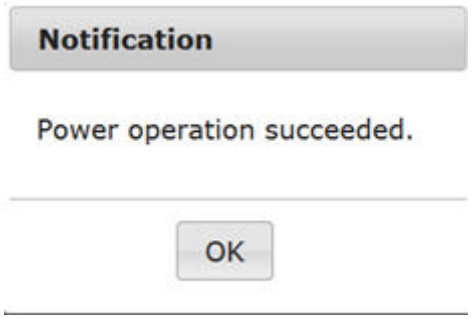
- Status may also show no associated outlet, or no power permission to the port.

► *To perform power operations:*

- Choose an option from the Power menu to control the serial target's power.
  - Power On
  - Power Off
  - Power Cycle



- Click OK in the success message.



Browser Tips for HSC

Some browsers have limitations that affect HSC.

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

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

Virtual KVM Client (VKCS) Help

To launch VKCS, enter https://<KX4-101 IP address>/vkcs in a browser.

Java Requirements

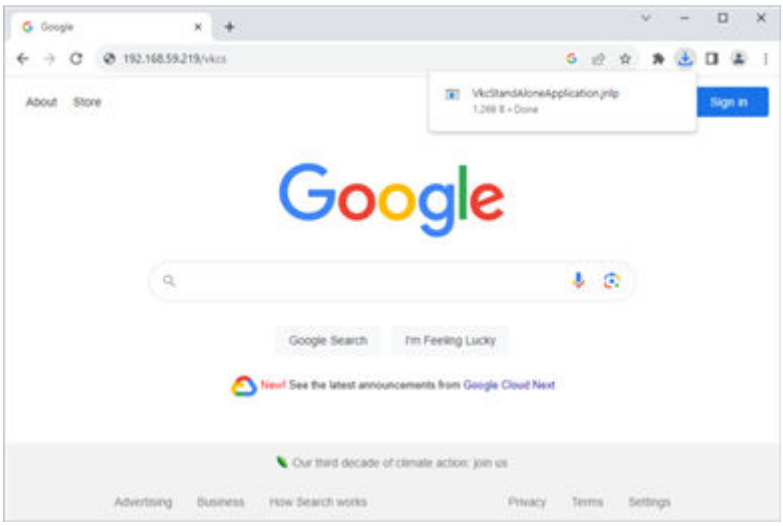
- A supported Java version is required. Check the release notes for latest supported version.
- If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

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

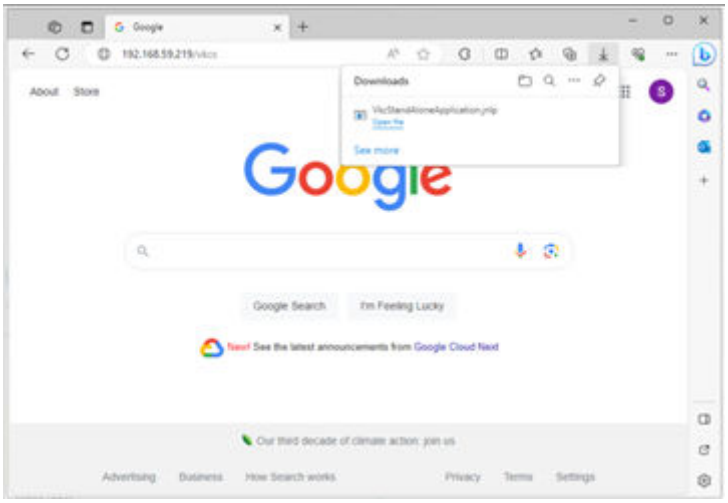
► *VKCS Launching:*

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'.

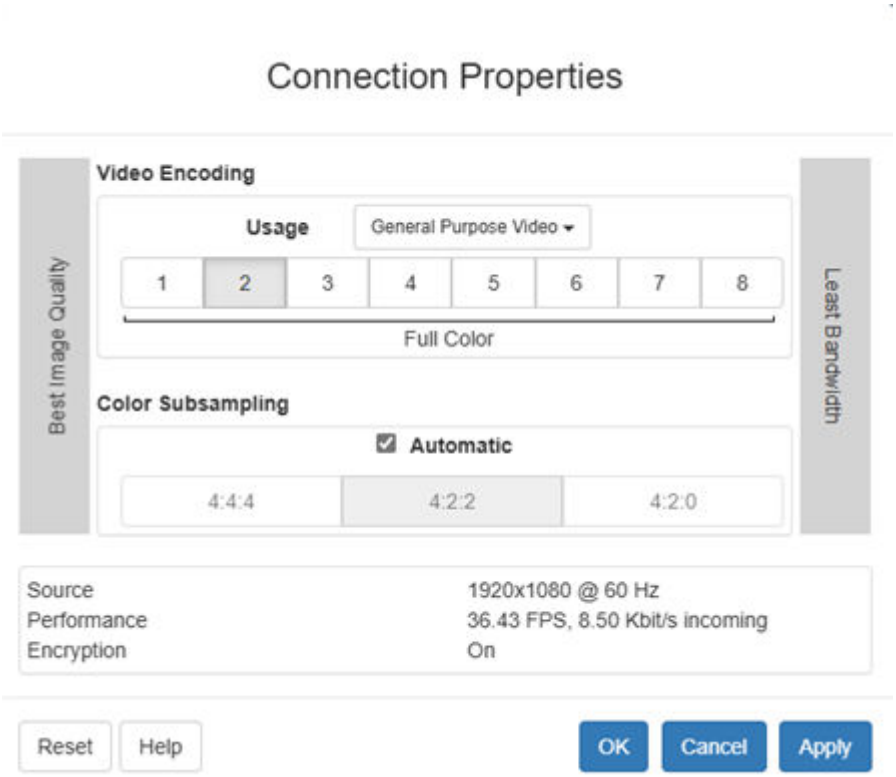
      Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

   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*

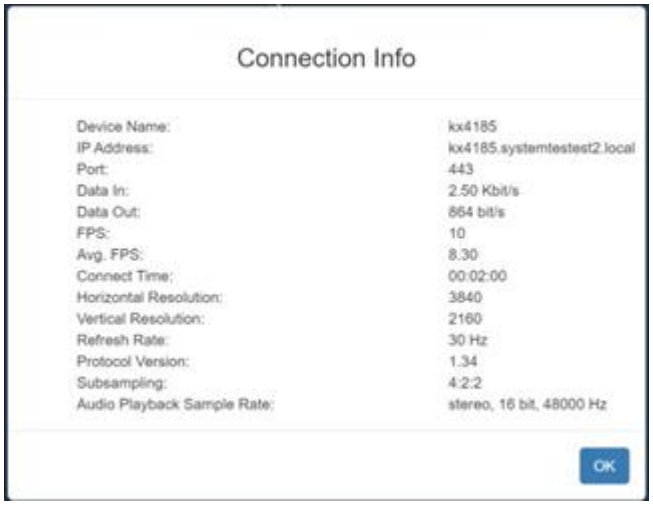
Current status includes real-time video performance statistics. As you change settings in the dialog, you can immediately see the effects on performance.

- 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 57).

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



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

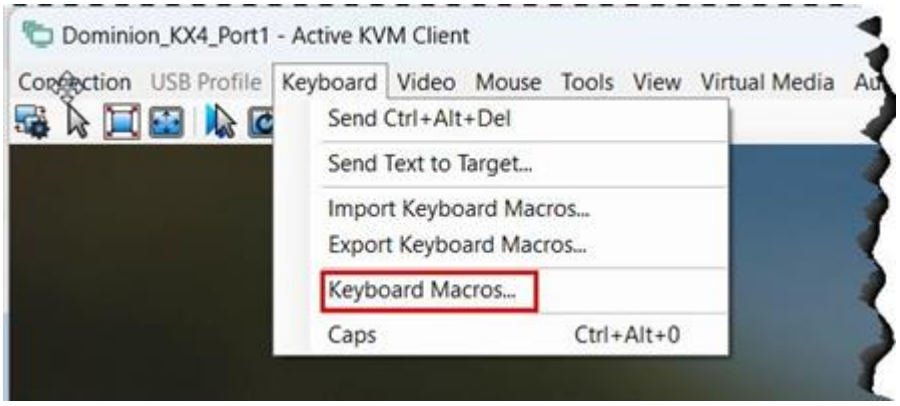
6. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
   a. To remove a step in the sequence, select it and click Remove.
   b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.
7. Click 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.

Construct Macro From Text

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

► *To add text to a macro:*

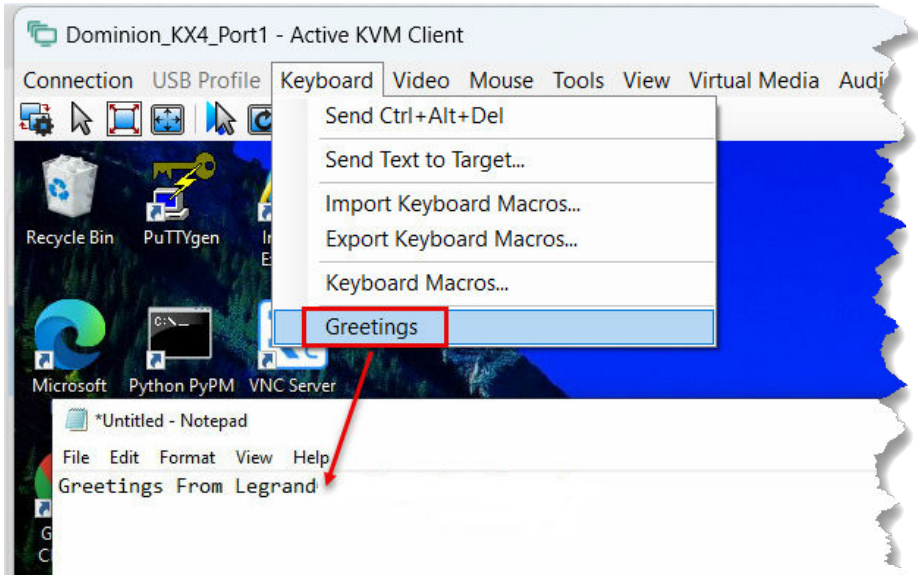
1. Choose Keboard > Keyboard Macros.



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

► *To use macros with text:*

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



Importing and Exporting Macros

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

Import Macros

► *To import macros:*

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

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

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

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

Export Macros

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

2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.
3. Click OK. An "Export Keyboard Macros to" dialog is displayed. Locate and select the macro file. By default, the macro exists on your desktop.
4. Select the folder to save the macro file to, enter a name for the file and click Save. If the macro already exists, you receive an alert message.
5. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.

Video

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.

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 Dominion KX IV–101 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).

Dual Mouse Modes

Absolute Mouse Synchronization

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

This 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.

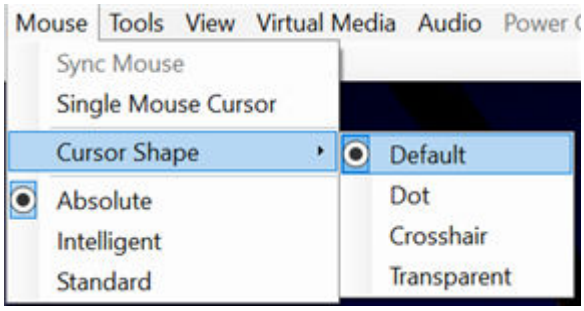
Note: This option is available only in Standard and Intelligent mouse modes.

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 (on page 70).

► *To change the cursor shape:*

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



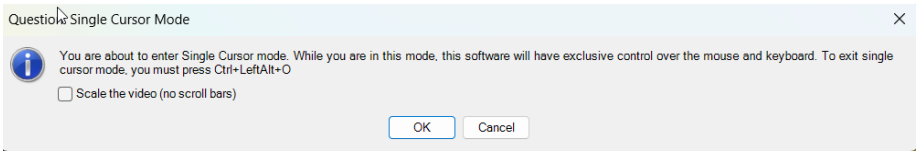
Single Mouse Mode

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

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

► *To enter single mouse mode, do one the following:*

- Choose Mouse > Single Mouse Cursor.
- Click the Single/Double Mouse Cursor button in the toolbar.



► *To exit single mouse mode:*

1. Press Ctrl+LeftAlt+O on your keyboard to exit single mouse mode.

Tool Options

General Settings

► *To set the tools options:*

1. Click Tools > Options. The Options dialog appears.
2. OpenGL rendering of scaled KVM images is enabled by default. If there are performance issues, select the Disable Hardware Accelerated Rendering checkbox to disable. Only available in AKC.
3. Select the Enable Logging checkbox only if directed to by Technical Support.

This option creates a log file in your home directory.

4. Choose the Keyboard Type from the drop-down list (if necessary).

The options include:

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

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

---

5. Select Adjust Full Screen Window Size to Target Resolution Instead of Client Resolution if you prefer. Option not available for Linux clients. See Adjust Full Screen Window Size to Target Resolution (on page 70) for details and examples.
6. 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.
7. Select Disable Menu in Full Screen to hide the menu options in Full screen mode if you do not want to see it.

- 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.

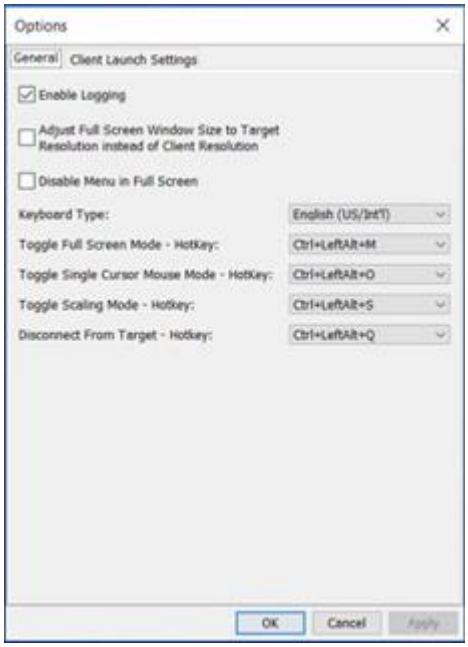
    Enable this hotkey to allow users to quickly disconnect from the target.

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

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

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

1. Click OK.



Keyboard Limitations

Turkish Keyboards

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

Slovenian Keyboards

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

Language Configuration on Linux

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

Language	Configuration method
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 (on page 67) for instructions on enabling the setting.

► *Example:*

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

1	2	3	4
5	6	7	8

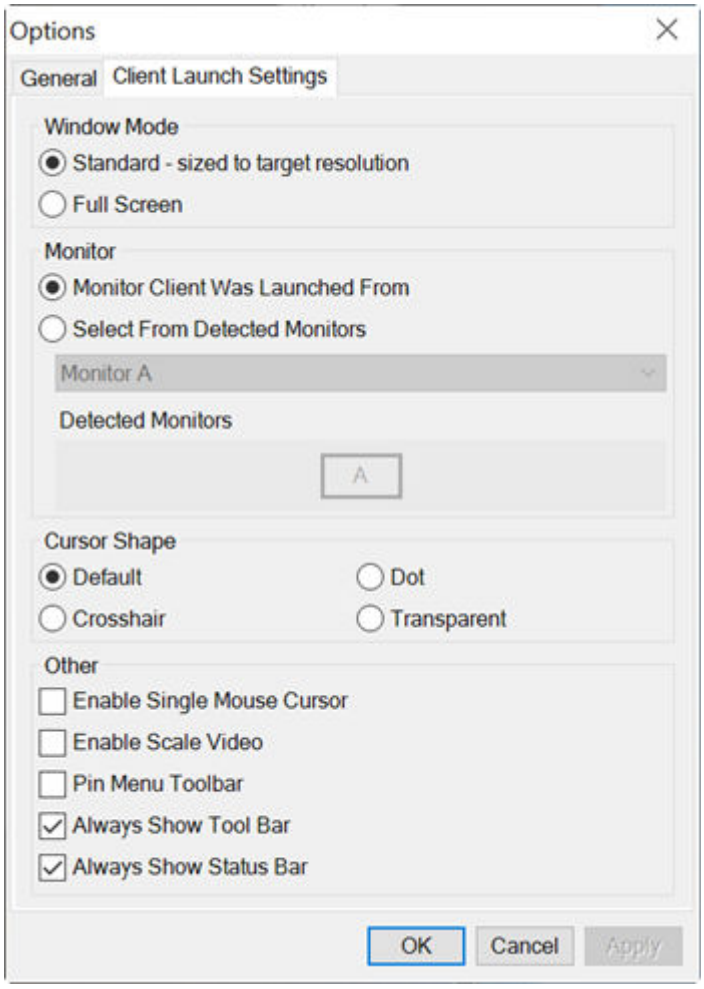
A KVM session is launched on monitor 6 with a the target resolution of 3840 x 1080. The client window opens on monitor 6 and 7 in native resolution and covers both monitors by 100%.

Client Launch Settings

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

► *To configure client launch settings:*

1. Click Tools > Options. The Options dialog appears.
2. Click on the Client Launch Settings tab.
   - To configure the target window settings:
     - Select 'Standard - sized to target Resolution' to open the window using the target's current resolution. If the target resolution is greater than the client resolution, the target window covers as much screen area as possible and scroll bars are added (if needed).
     - Select 'Full Screen' to open the target window in full screen mode.
   - To configure the monitor on which the target viewer is launched:
     - Select 'Monitor Client Was Launched From' if you want the target viewer to be launched using the same display as the application that is being used on the client (for example, a web browser or applet).
     - Use 'Select From Detected Monitors' to select from a list of monitors that are currently detected by the application. If a previously selected monitor is no longer detected, 'Currently Selected Monitor Not Detected' is displayed.
   - To configure cursor shape:
     - Select Default arrow, Dot, Crosshair, or Transparent to set the cursor shape for all sessions. Use the Mouse menu to change the cursor shape during a session.
   - To configure additional launch settings:
     - Select 'Enable Single Cursor Mode' to enable single mouse mode as the default mouse mode when the server is accessed.
     - Select 'Enable Scale Video' to automatically scale the display on the target server when it is accessed.
     - Select 'Pin Menu Toolbar' if you want the toolbar to remain visible on the target when it is in Full Screen mode. By default, while the target is in Full Screen mode, the menu is only visible when you hover your mouse along the top of the screen.
     - Always Show Tool Bar 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.



Collecting a Diagnostic Snapshot of the Target

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

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

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

The following files are included in the zip file:

- screenshot_image.png

  This is a screenshot of the target that captures a picture of the issue you are experiencing. This feature operates like the "Screenshot from Target" feature.
- raw_video_image.png:

  A snapshot image created from raw video data. Please note that client's postprocessing is applied, just as if it were a "regular" screen update.
- raw_video_ycbcr420.bin:

Binary file of the raw snapshot.

- raw_video_ycbcr420.txt:

  Text file containing data used to help diagnose issues.

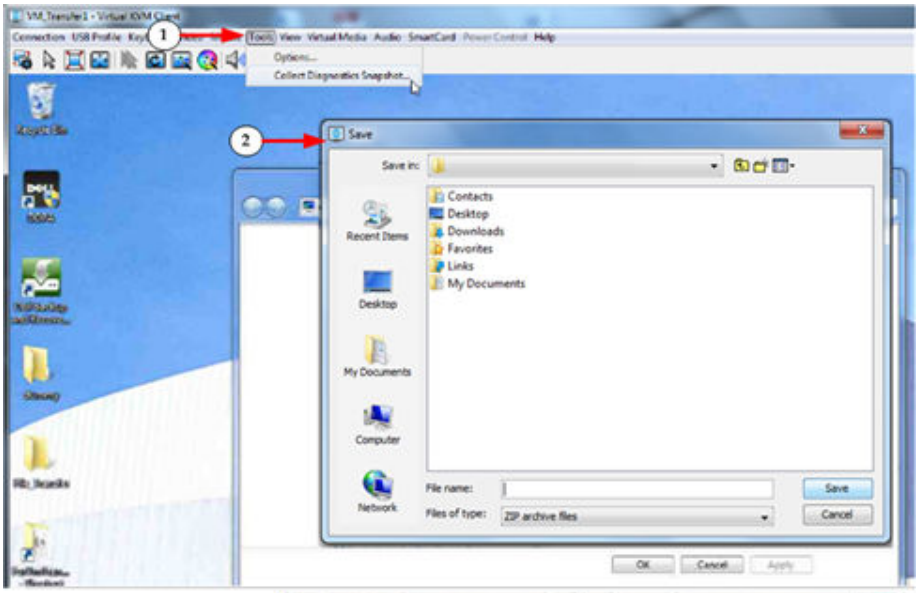
- Log.txt file:

  These are the client logs.

  Note that the logs are included even if you have not enabled information to be captured in them. VKC uses internal memory to capture the information in this case.

Collect a Diagnostic Snapshot

To capture a diagnostic snapshot:



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

2	You are prompted to save the zip file containing the diagnostic files.
3	The zip file containing the diagnostic files is saved.

View Options

View Toolbar

You can 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 (on page 67).

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

If you want the menu bar to remain visible while in Full Screen mode, enable the Pin Menu Toolbar option from the Tool Options dialog. See Tool Options (on page 67).

► *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.

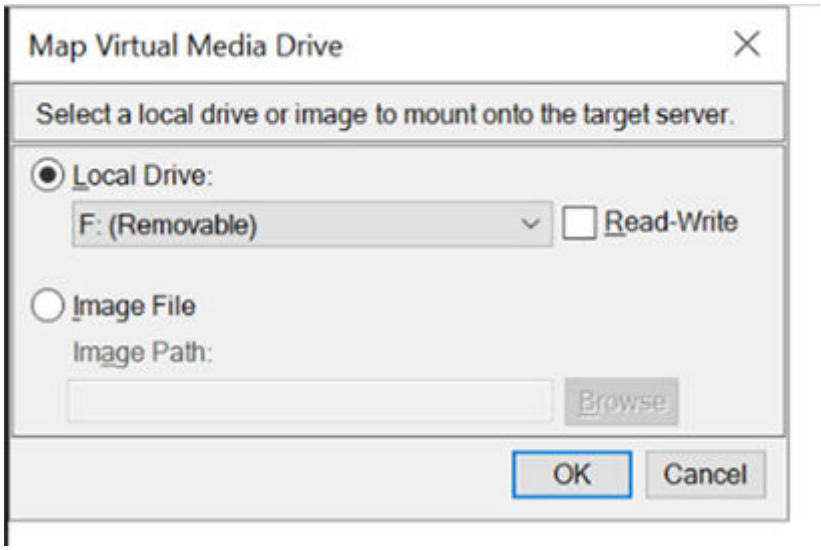
Virtual Media

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

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

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.

Digital Audio

The Dominion KX IV–101 supports audio playback over HDMI and USB as well as audio capture over USB Audio.

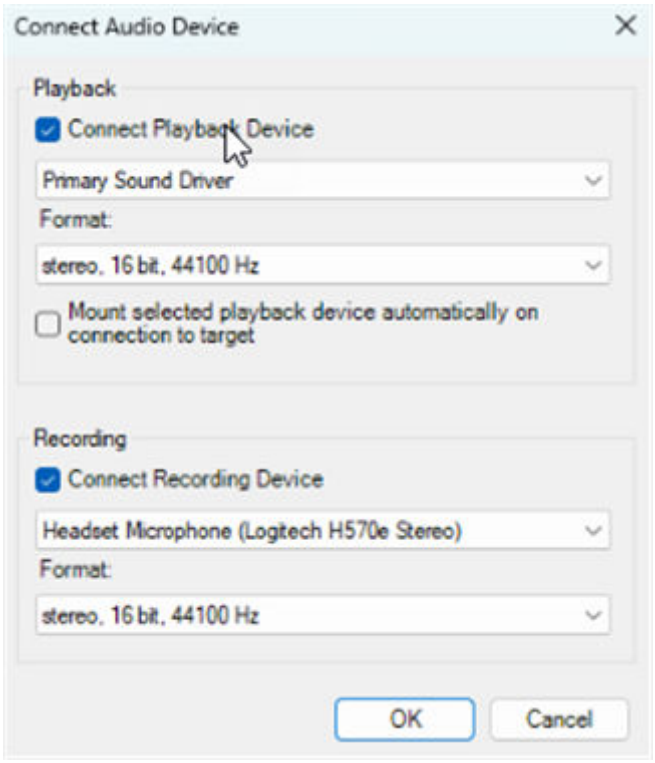
Supported Audio Device Formats

The following playback formats are supported for HDMI audio:

- Stereo, 16bit, 44.1K
- Stereo, 16bit, 32K
- Stereo, 16bit, 48K

The following format is supported for USB Audio:

- Stereo, 16bit, 44.1K



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	Playback is not supported. Microphone icon appears grayed out.
	Speaker/ Microphone	These icons appear when USB audio recoding is connected.

Audio Playback 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 device, not from the client audio device control.

Bandwidth Requirements

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

Audio format	Network bandwidth requirement
44.1 KHz, 16bit stereo	176 KB/s
32 KHz, 16bit stereo,	128KB/s
48 KHz, 16bit stereo	192KB/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.

Saving Audio Settings

Audio device settings are applied on a per Dominion KX IV–101 device basis.

Once the audio devices settings are configured and saved on the Dominion KX IV–101, the same settings are applied to it.

See: Connecting and Disconnecting from a Digital Audio Device 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 and Disconnecting a Digital Audio Device

Audio device settings are applied on a per Dominion KX IV–101 device basis.

Once the audio devices settings are configured and saved on the Dominion KX IV–101, the same settings are applied to it.

See Saving Audio Settings (on page 80) for more 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 Dominion KX IV–101.
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 "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.
7. 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.

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 Playback Buffer Size

Capture buffer size is not adjustable on Dominion KX IV–101. Playback buffer can be adjusted as needed once an audio device is connected.

This feature is useful for controlling the quality of the audio, which may be impacted by bandwidth limitations or network spikes. Increasing the buffer size improves the audio quality but may impact the delivery speed. The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

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

Audio settings are configured in VKC or AKC.

► *To adjust audio settings:*

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

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.

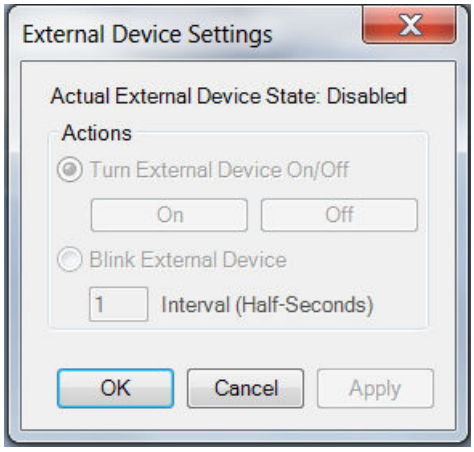
The menu option is disabled if you do not have permission for power control, and when outlets are not associated with the port.

External Device

The External Device menu allows you to control the device connected at the terminal block of the Dominion KX IV–101.

► *External Device Settings:*

1. Choose External Device > Settings to view the dialog.
2. The device state is listed.
3. Enabled devices can be controlled using the Actions options.
   - Turn External Device On/Off: Click On or Off to control terminal output relay.
   - Blink External Device: Enter the half-second interval to control blinking of the external device.



4. Click OK or Apply to save.

Version Information

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

► *Virtual KVM Client:*

- Choose Help > About Raritan Virtual KVM Client.

► *Active KVM Client:*

- Choose Help > About Raritan Active KVM Client.

► *HTML KVM Client:*

- Choose Help > About Raritan HTML KVM Client.

Active KVM Client (AKC)

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

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

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

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

AKC Supported Microsoft .NET Framework

The Active KVM Client (AKC) requires Windows .NET®. See the Release Notes for supported versions.

AKC Supported Browsers

See the Release Notes for supported browser versions.

AKC Supported Operating Systems

When launched from Edge®, the Active KVM Client (AKC) allows you to reach target servers via the Dominion KX IV–101.

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.

Prerequisites for Using AKC

Allow Cookies

Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.

Include Dominion KX IV–101 IP Address in 'Trusted Sites Zone'

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

Disable 'Protected Mode'

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

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 Dominion KX IV–101 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).

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.

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

► *Supported Features:*

- Connection Properties
- Input Settings
- Audio Playback
- Virtual Media
- Keyboard Macros
- Import and Export of Keyboard Macros
- Send Text to Target
- Keyboard and Mouse Settings
- Single Mouse Mode
- External Device
- Power Control

► *Not supported:*

- Limited Tools option: Client Settings and Launch Settings supported
- Limited keyboard support: US-English, UK-English, French, German, Swiss-German, and Japan keyboards are supported
- Hotkeys for keyboard macros
- Can only create Macros from keys that exist on the client PC (US-English, UK-English, French, German, Swiss-German, or Japan), no special function keys
- Virtual Media write not supported
- Local File Transfer
- USB drive connects

► *Known Issues:*

- If HKC does not load, but rather displays a white screen, your browser memory may be full. Close all browser windows and try again.
- On Edge & Chrome, disable the background throttling to prevent background tabs from disconnecting after a certain amount of time. Go to chrome://flags, then search for "throttle". Set "Throttle Javascript timers in backgound" and "Calculate window occlusion on Windows" to "Disabled". Restart chrome to apply settings.

Connection Properties

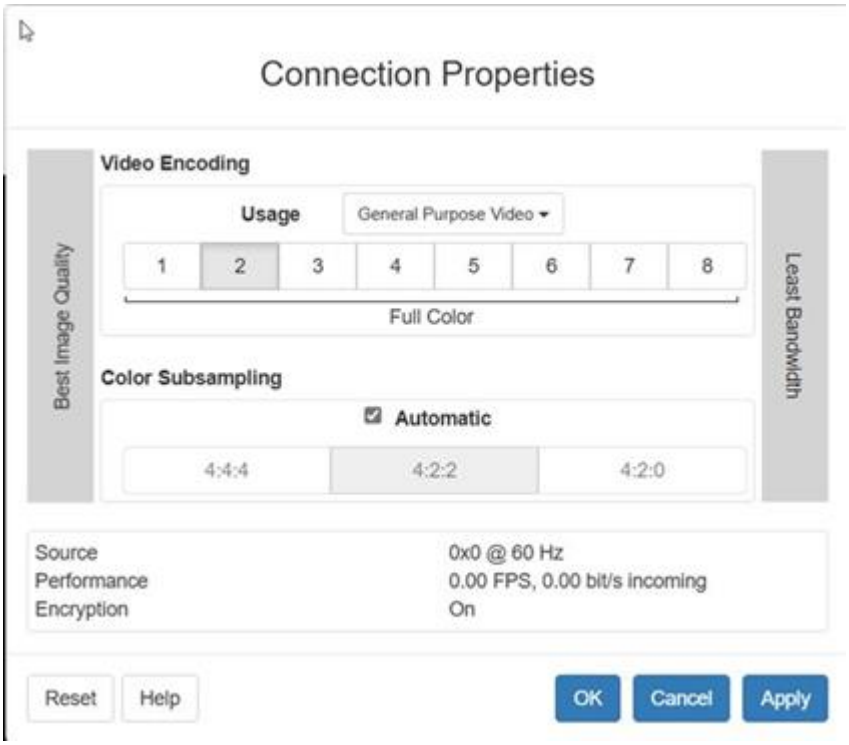
Connection properties manage streaming video performance over remote connections to target servers.

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

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

► *To view connection properties:*

- Choose File > Connection Properties.



► *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

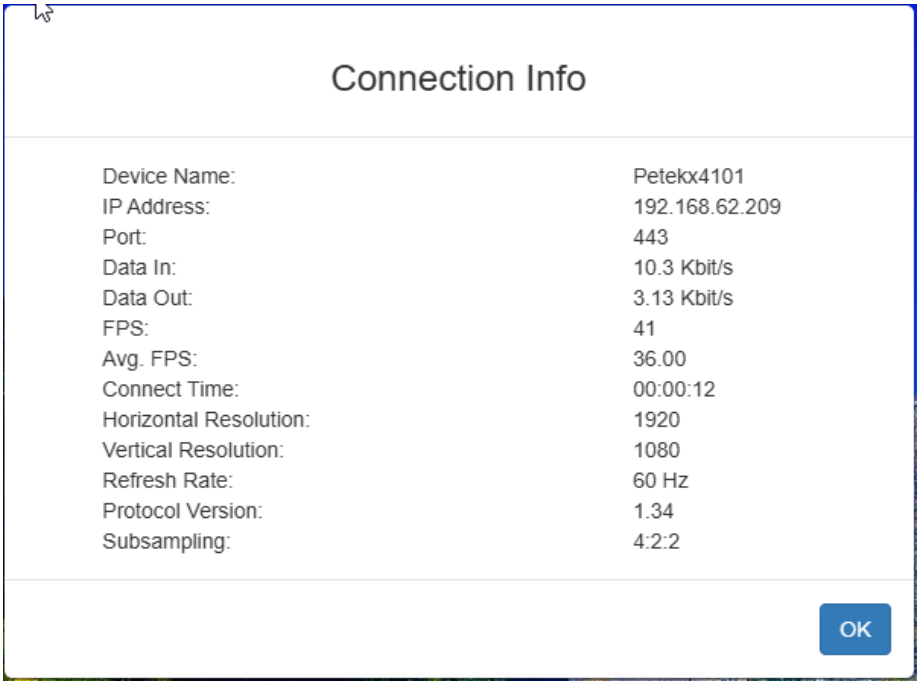
Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See Default Connection Properties for help configuring the connection properties.

- Name of the device
- IP address of the device
- Port - The KVM communication TCP/IP port used to access the device
- Data In/Second - Data rate received from the device
- Data Out/Second - Data rate sent to the device
- FPS - Video frames per second from the device.
- Average FPS - Average number of video frames per second.
- Connect Time - The duration of the current connection.
- Resolution - The target server's horizontal and vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - communications protocol version.
- Subsampling - Adaptive color subsampling

► *To view connection info:*

- Choose File > Connection Info.



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

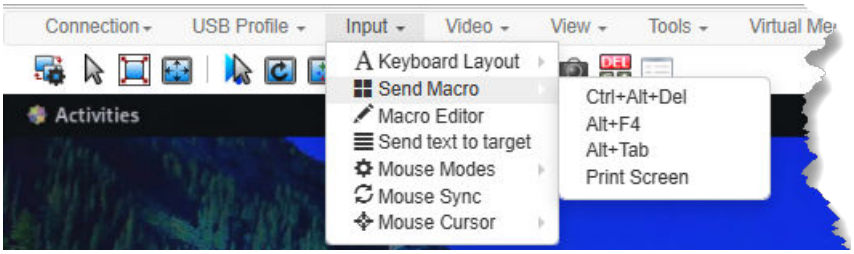
Send Macro

Due to frequent use, several keyboard macros are preprogrammed.

► *To send a preprogrammed macro:*

- Choose Input > Send Macro, then select the macro:

- Ctrl+Alt+Del: Sends the key sequence to the target without affecting the client.
- Alt+F4: Closes a window on a target server.
- Alt+Tab: Switch between open windows on a target server.
- Print Screen: Take a screenshot of the target server.



Macro Editor

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

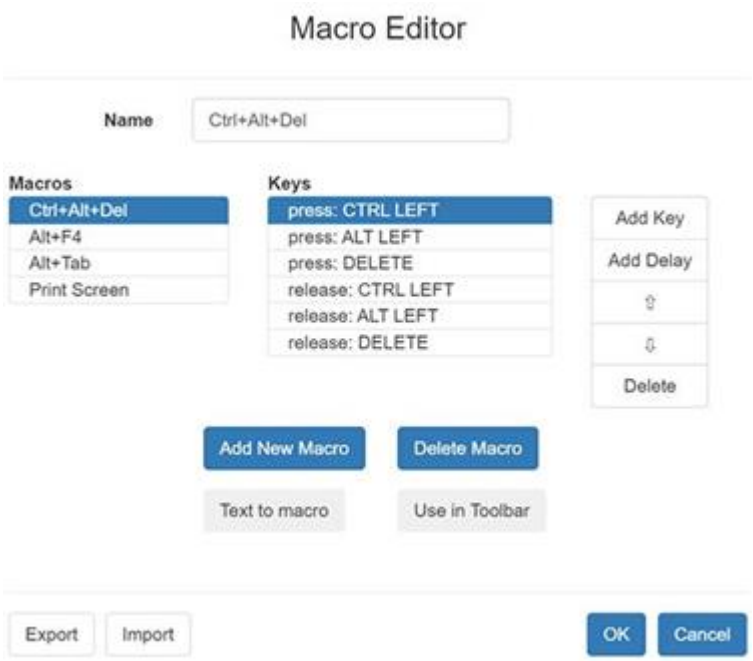
Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

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

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one Dominion KX IV–101, your macros will only be available on the browser and Dominion KX IV–101 where they were created. To reuse your macros in another Dominion KX IV–101 device, you can import and export the macro files. See Import and Export Macros (on page 96).

► *To Access the Macro Editor:*

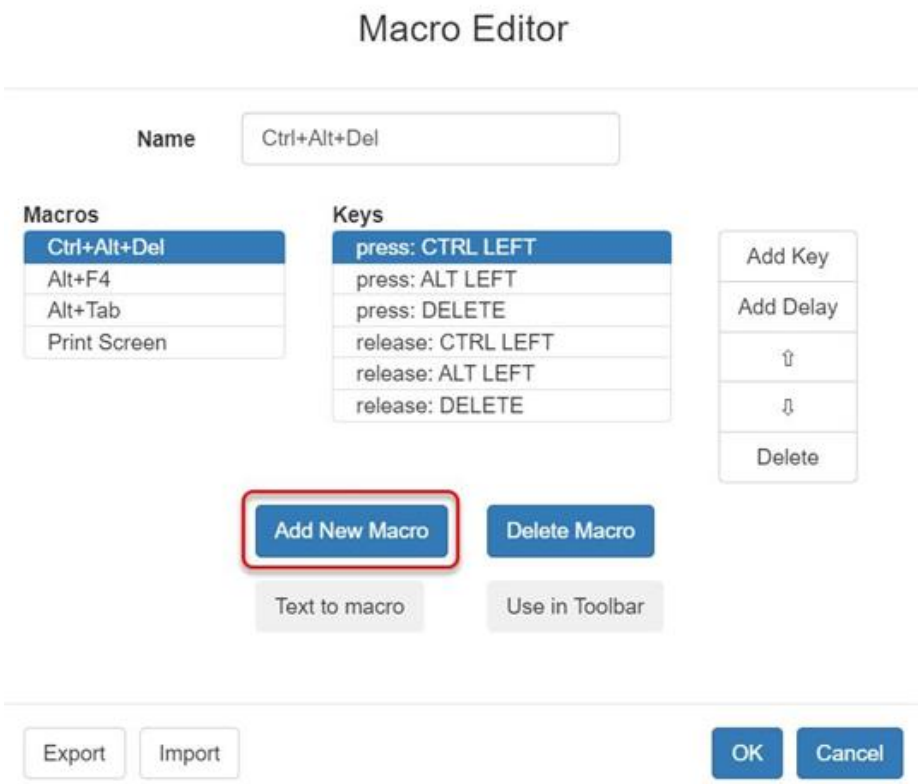
- Choose Inputs > Macro Editor.
- Select a macro from the Macros list to view the key combination.



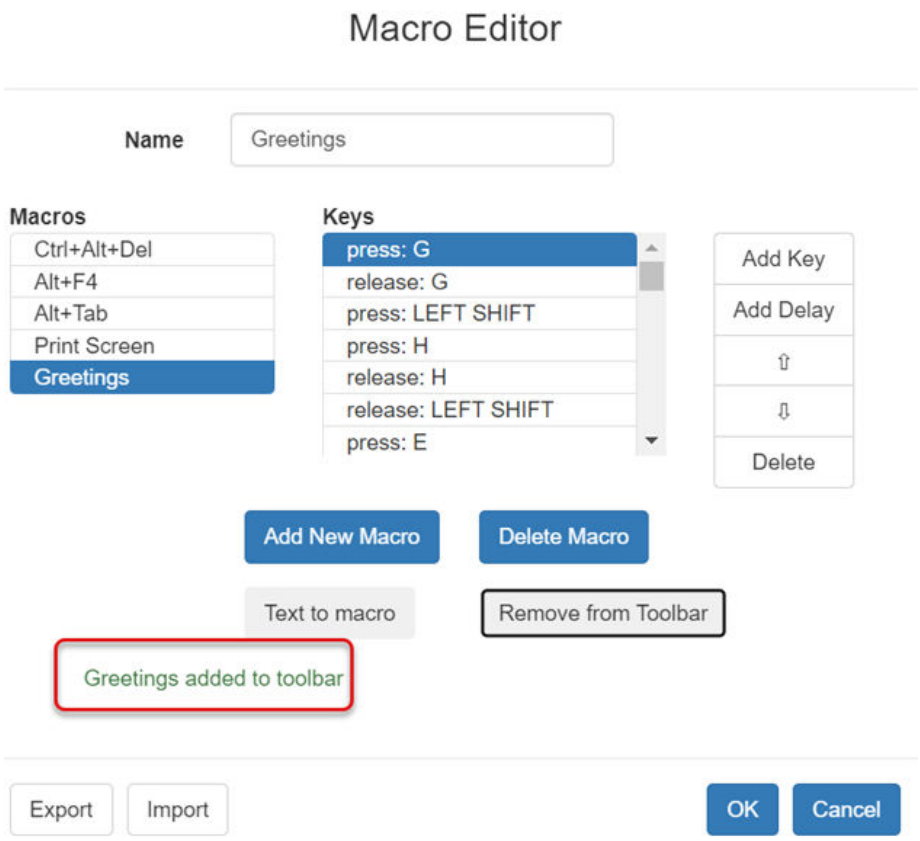
Add New Macro

► *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 (on page 93) for more details.



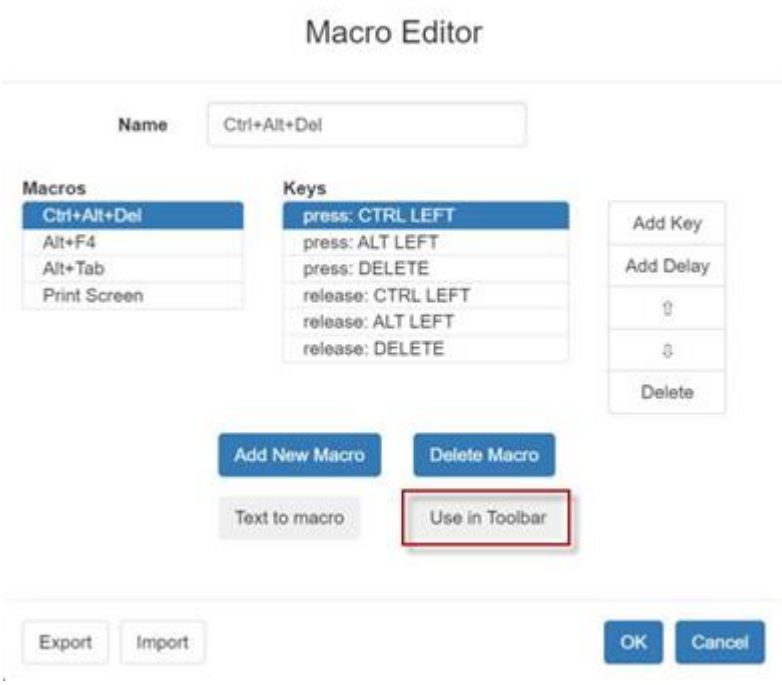
This example shows a macro for a Mac bootup sequence that requires a 2-second delay.

Add a Macro to the Toolbar

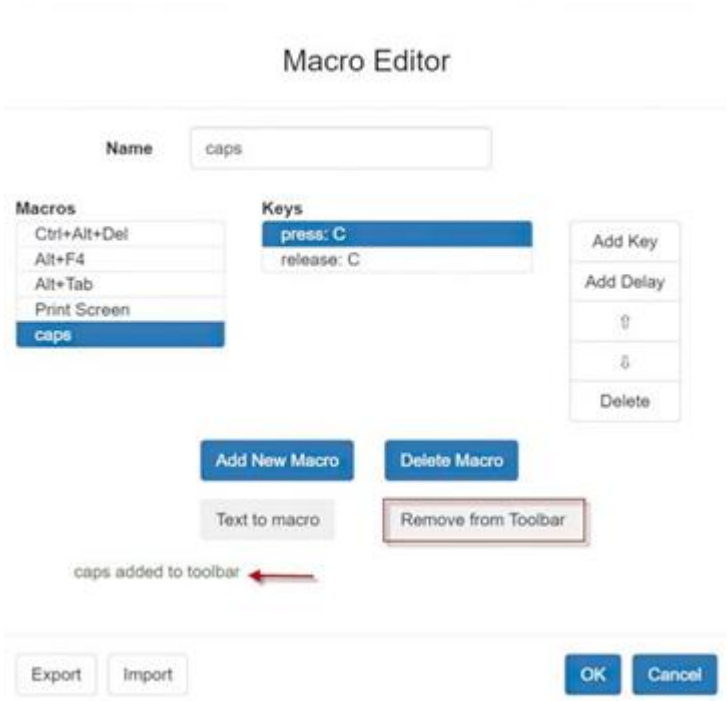
You can add a single macro to your HKC toolbar, so that you can use the macro by clicking an icon.

► *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.

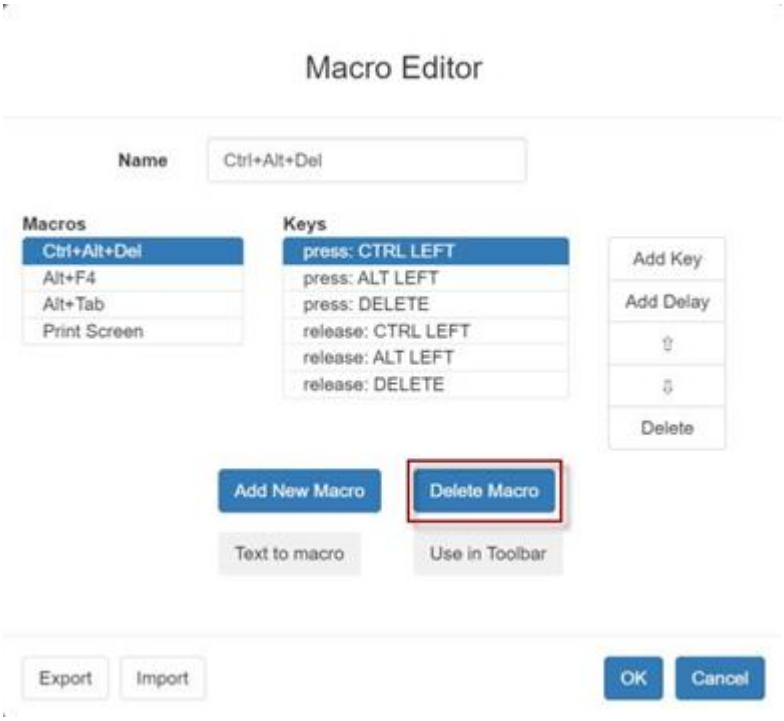


5. Click OK and exit the Macro Editor. The macro icon is added to the toolbar when one has been set.

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 Dominion KX IV–101, your macros will only be available on the browser and Dominion KX IV–101 where they were created. To reuse your macros in another Dominion KX IV–101 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.

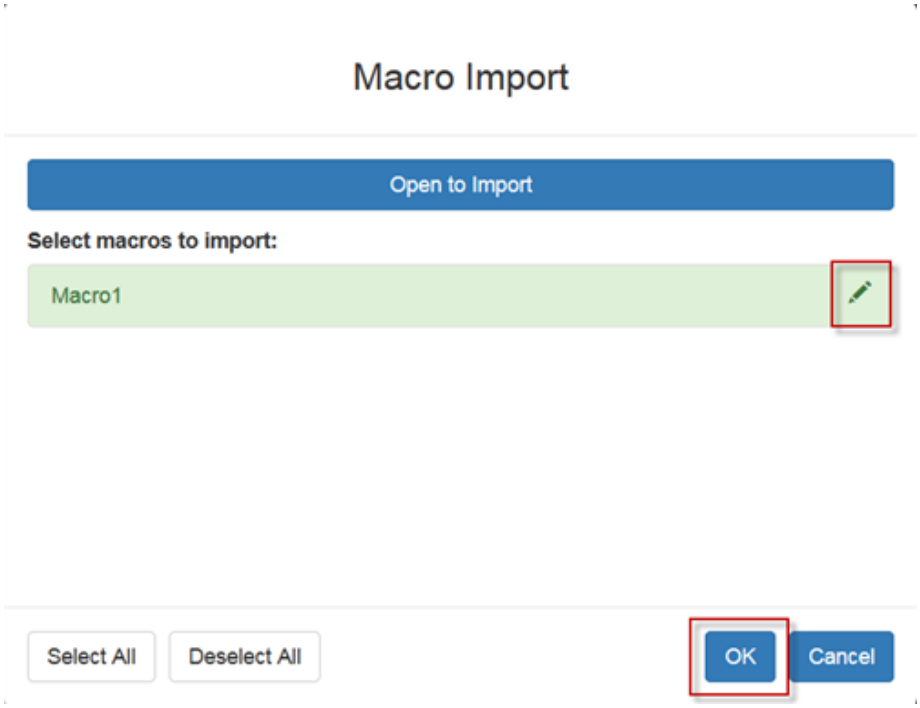
Macros are exported to an xml file named "usermacros.xml". Files are saved in your browser's default download location. Default macros are not exported.

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 Dominion KX IV–101 displays in the Macro Editor dialog.
2. To export the list, click the Export button, then save the file.
3. Log in to the Dominion KX IV–101 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.

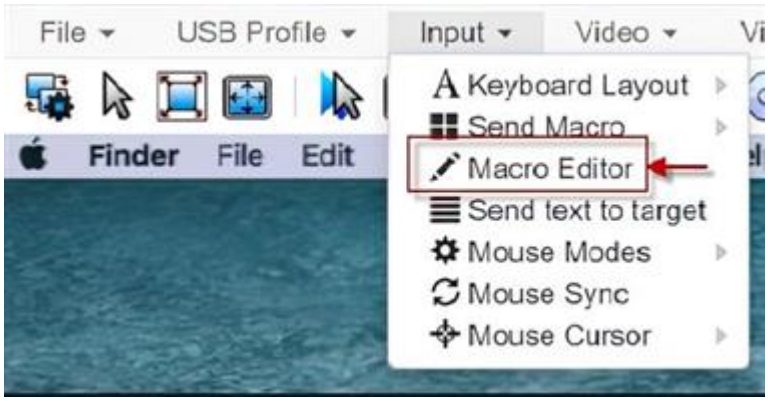


Text to macro

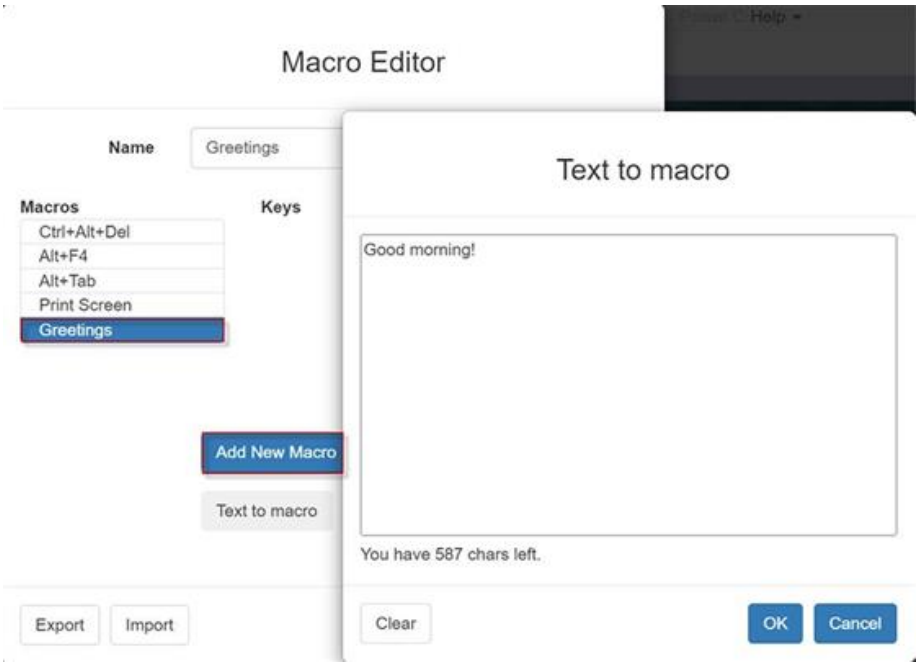
Text to macros will enable you to work more efficiently by producing frequently used phrases and paragraphs with a single command. Create a new macro and then assign text to it.

► *To add text to a macro:*

1. Choose Input > Macro Editor.



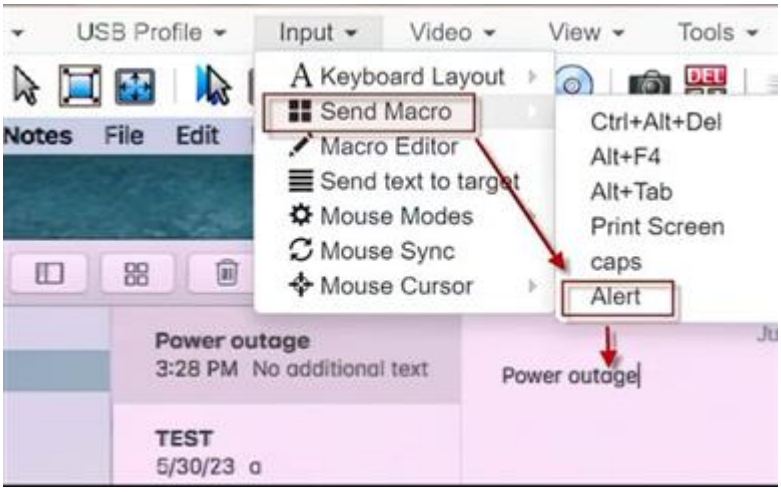
2. Select to add new macro and enter a macro name.
3. Click Text to macro.



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.



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 Dominion KX IV–101 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.

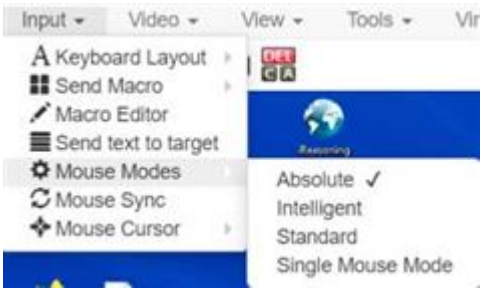
You can toggle between these two modes (single mouse and dual mouse).

Absolute

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

► *To enter Absolute Mouse Synchronization Mode:*

- Choose Input > Mouse Modes > Absolute.

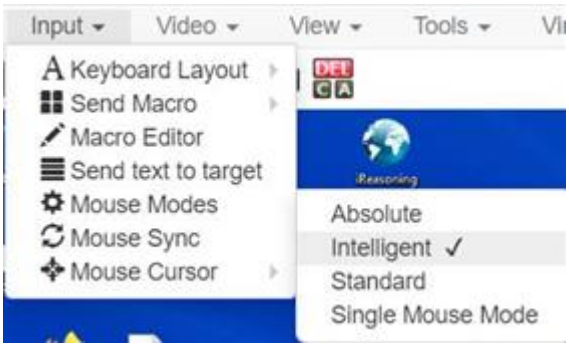


Intelligent

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

► *To enter Intelligent mouse mode:*

- Choose Input > Mouse Mode > Intelligent. The mouse will sync. See Intelligent Mouse Synchronization Conditions (on page 65), Intelligent Mouse Synchronization Conditions (on page 102).



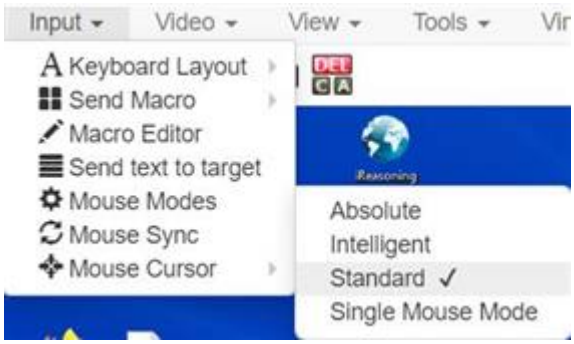
Standard

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

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

► *To enter Standard mouse mode:*

- Choose Input > Mouse Modes > Standard.



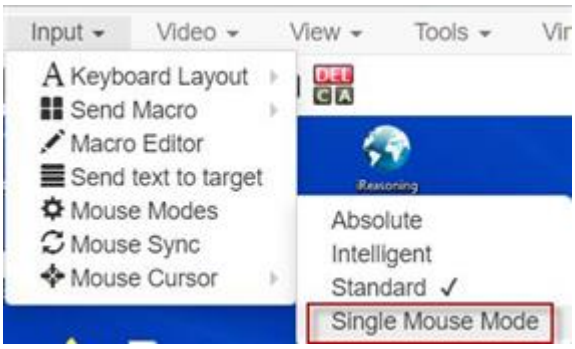
Single

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

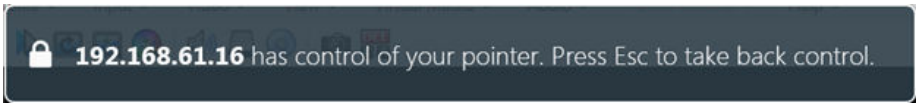
Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine. Single mouse mode is not available on Edge.

► *To enter Single mouse mode:*

- Choose Inputs > Mouse Modes > Single.



- A message appears at the top of the client window: Press Esc to show your cursor.



► *To exit Single mouse mode:*

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

Mouse Sync

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

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

► *To synchronize the mouse cursors:*

- Choose Inputs > Mouse Sync.

Intelligent Mouse Synchronization Conditions

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

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- 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.

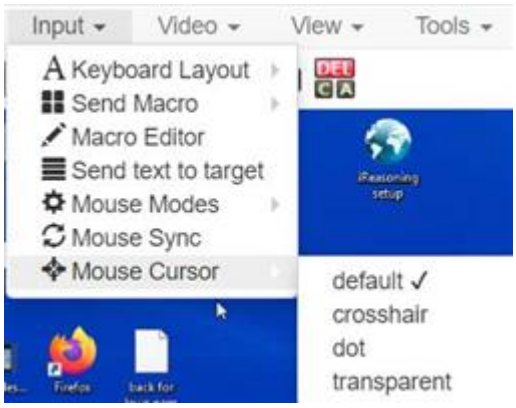
Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

Mouse Cursor

In dual mouse modes, you can select a custom cursor shape for your session. To make the cursor selection permanent, see .Tools Menu (on page 105)

► *To change the cursor shape:*

- Choose Input > Mouse Cursor, then select from the list.
  - default
  - crosshair
  - dot
  - transparent



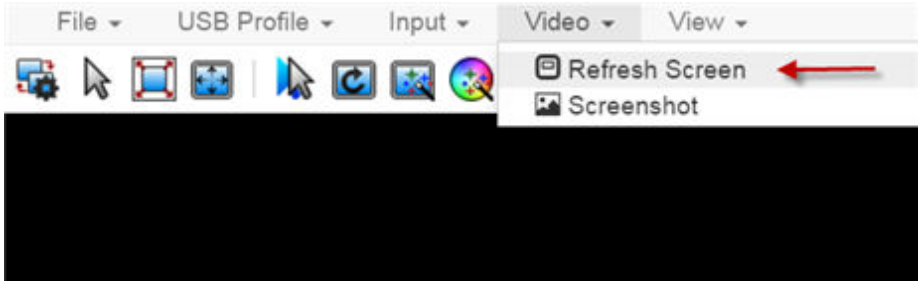
Video Menu

Refresh Screen

The Refresh Screen command forces a refresh of the video screen.

► *To force a refresh of the video screen:*

- Choose Video > Refresh Video.

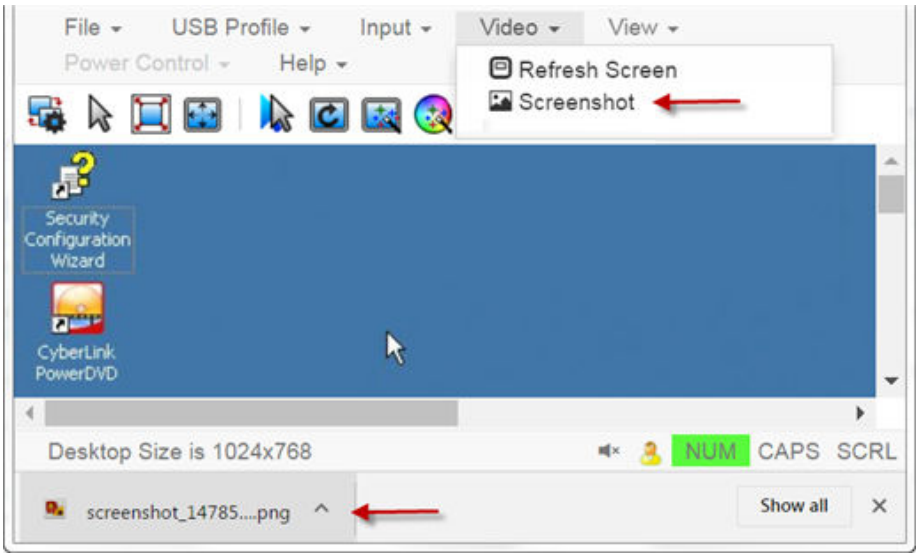


Screenshot

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

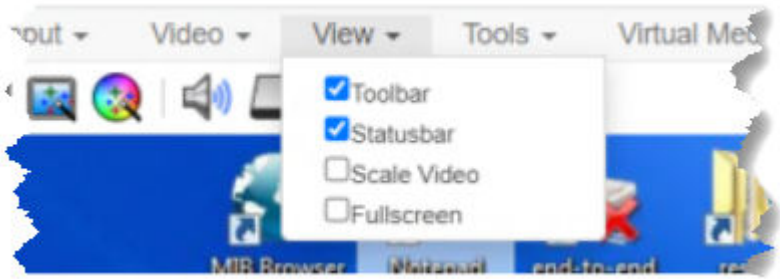
► *To take a screenshot of the target server:*

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



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.

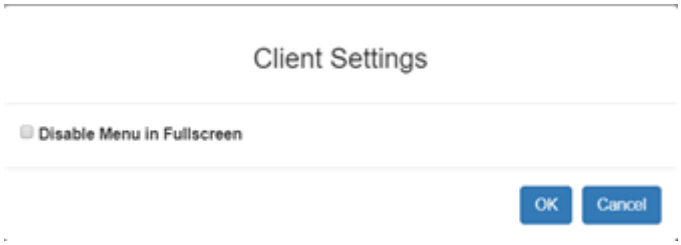
- Press Esc to exit fullscreen.

Tools Menu

The Tools menu contains options for HKC target connection settings.

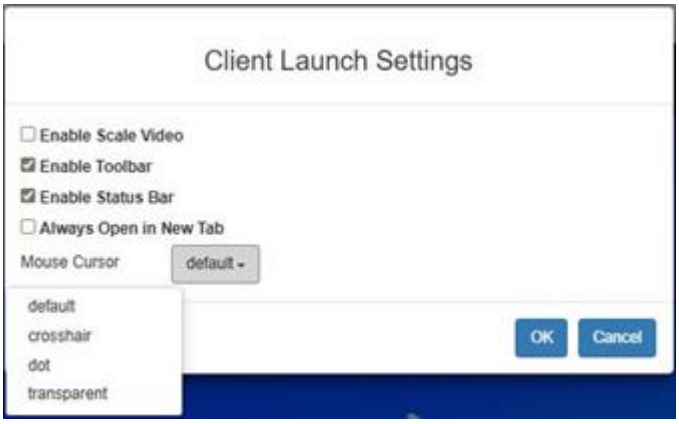
► *Client Settings:*

- 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, Always Open in New Tab, and Mouse Cursor at target launch.



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

► *Touch Settings - enabled for iOS clients:*

- Tap Tools > Touch Settings to access the Client Touch Settings. Customize the Touch Input and Gesture Scrolling settings for your mobile device.
  - Double Click Time: Time between two touch taps for the equivalent of a mouse double click.
  - Mouse Click Hold Time: Time to hold after touch down for the equivalent of a mouse right click.
  - Use Left Hand Mouse: Enable if the target OS's primary mouse button is set to Right.
  - Enable Inverted Scroll x-Axis: If selected, two-finger movement to the right moves the screen to the left instead of the default right.
  - Enable Inverted Scroll y-Axis: If selected, two-finger movement up moves the screen down instead of the default up.

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

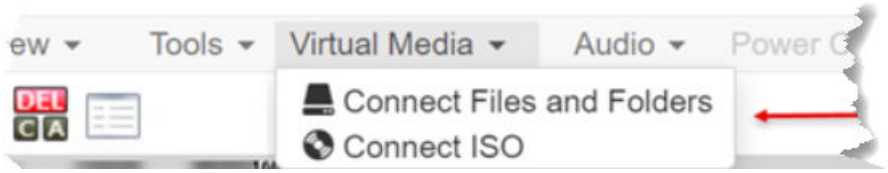
The Connect Files and Folders command provides an area to drag and drop files or folders that you want to connect by means of virtual media.

Supported browsers: Chrome, Firefox, Safari, Edge.

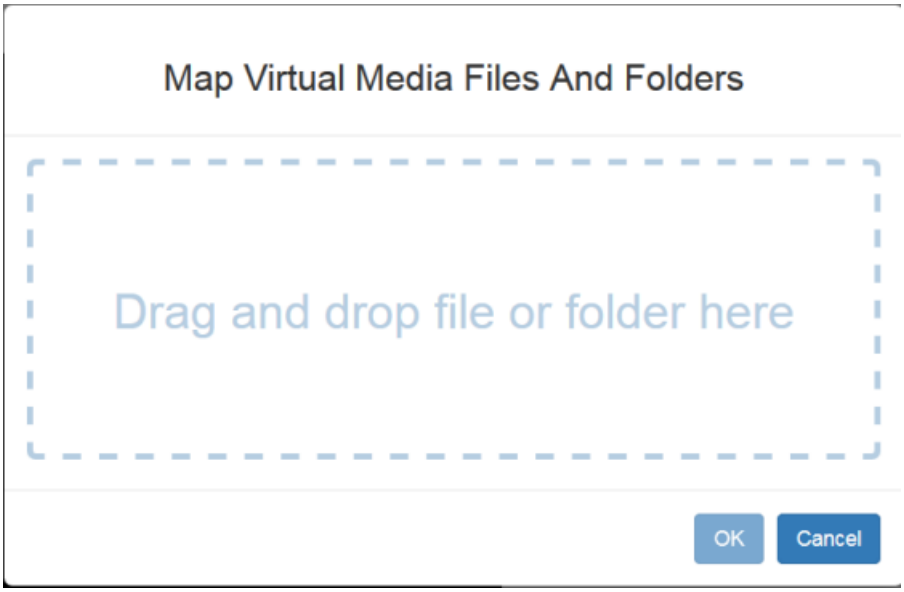
File size limit: 4GB per file

► *To connect files and folders:*

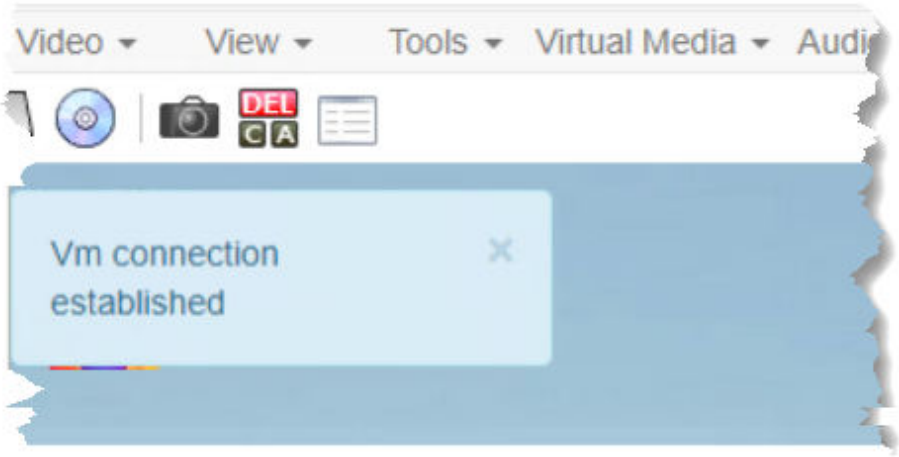
1. Choose Virtual Media > Connect Files and Folders. Or, click the matching icon in toolbar.



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

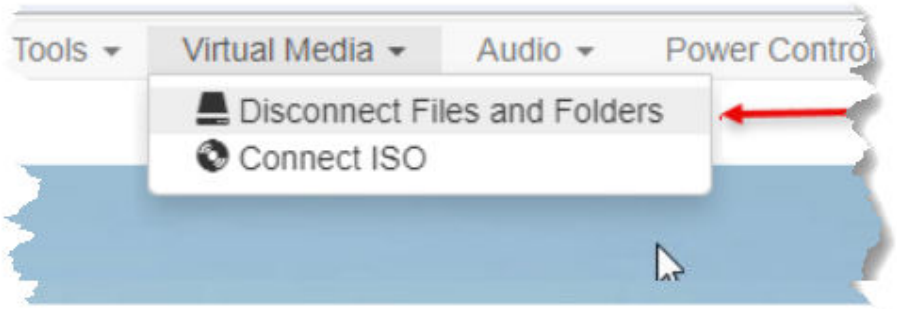


3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.



► *To disconnect files and folders:*

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



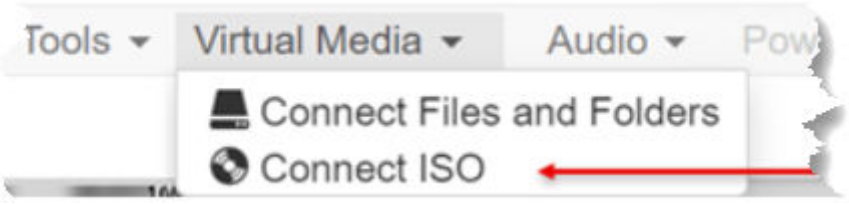
Connect ISO

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.

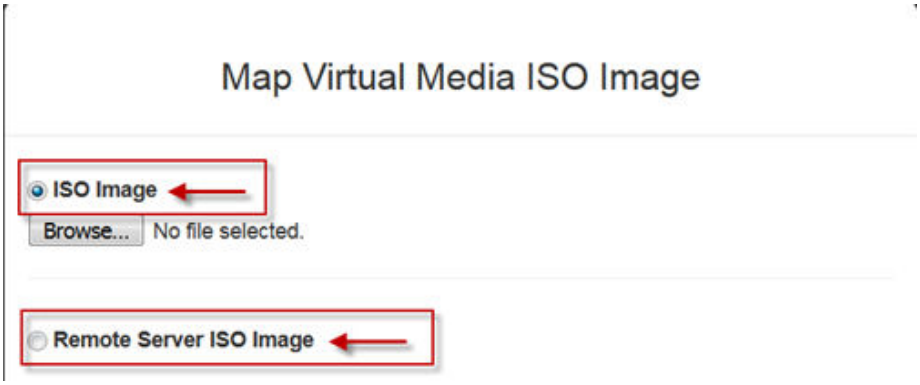
Note: If connection to your SAMBA server is lost while transferring files from your image file to the target, keyboard and mouse control will be lost for several minutes, but will recover.

► *To map virtual media image files:*

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



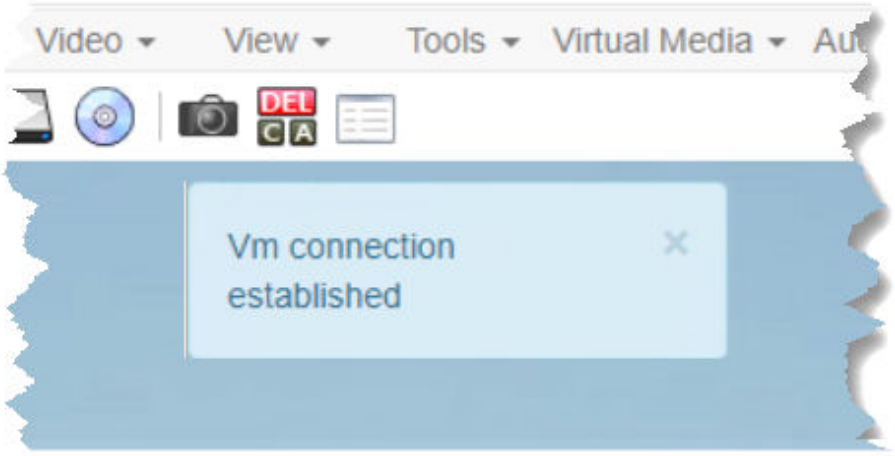
2. Select the option for your file's location:



- 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.

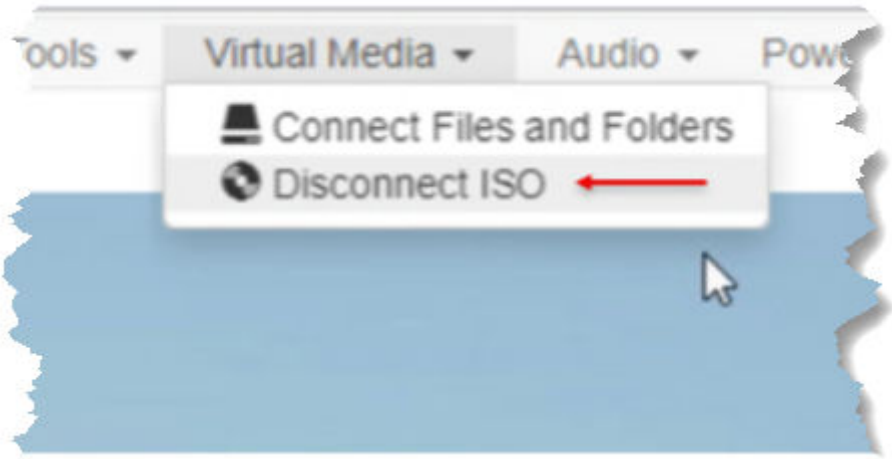
- Select Remote Server ISO Image for ISO files on a remote server. Remote ISO files must be pre-configured by an administrator for the mapping to appear here. See Virtual Media File Server Setup (File Server ISO Images Only). Select the Hostname, then select the image file from the Image list. Enter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

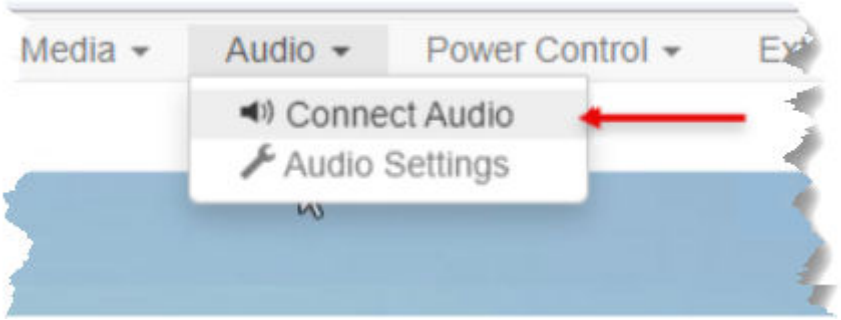
The Connect Audio command connects your playback device, selects audio format and gives an option to mount the selected playback device automatically when you connect to the target.

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.

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

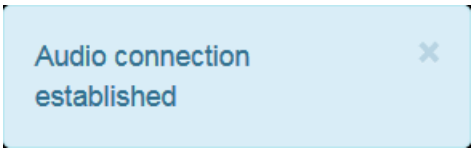
► *To connect audio:*

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



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

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



► *To disconnect audio:*

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

Audio Settings

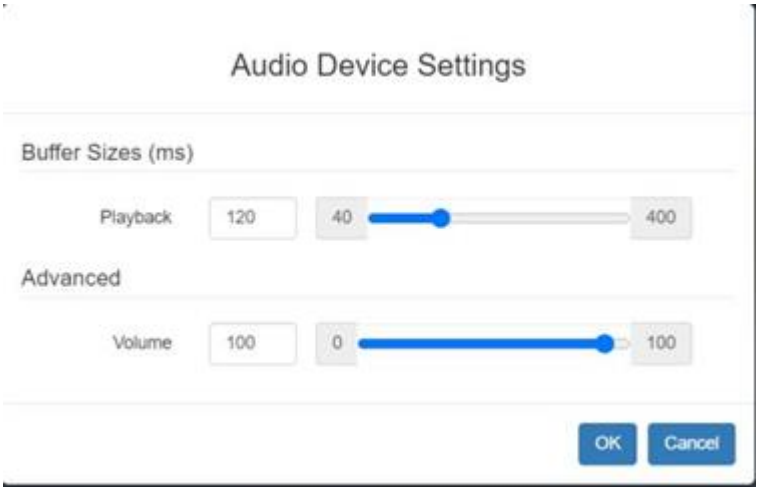
The Audio Settings option is enabled when audio is connected. Use the Audio Settings to set the buffer and volume.

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

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

► *To configure audio settings:*

1. Choose Audio > Audio Settings while Audio is connected.
2. Set the Buffer and Volume using the arrows or sliders.



3. Click OK.

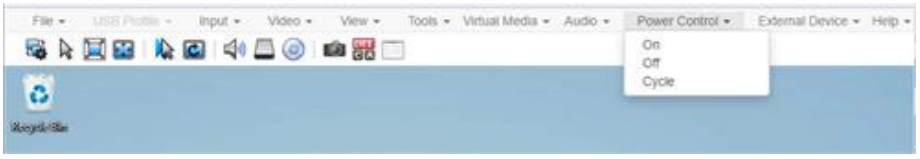
Auto Play in Safari

For HKC connections in the Safari browser that have auto mounted audio devices, make sure that the "Auto Play" setting is "Allow all Auto Play".

https://support.apple.com/guide/safari/customize-settings-per-website-ibrw7f78f7fe/mac

Power Control

You can power on, power off, and power cycle a target. Access the target, and then select a power control option from the Power Control menu.



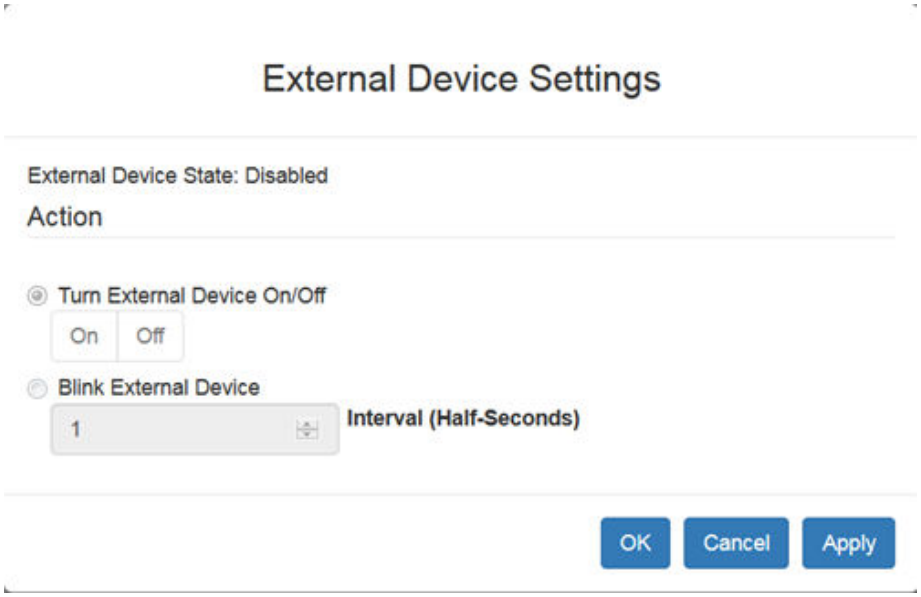
The menu option is disabled if you do not have permission for power control, and when outlets are not associated with the port.

External Device Menu

The External Device menu allows you to control the device connected at the terminal block of the Dominion KX IV–101.

► *External Device Settings:*

1. Choose External Device > Settings to view the dialog.
2. The device state is listed.
3. Enabled devices can be controlled using the Actions options.
   - Turn External Device On/Off: Click On or Off to control terminal output relay.
   - Blink External Device: Enter the half-second interval to control blinking of the external device.



4. Click OK or Apply to complete the action.

Using HKC on Apple iOS Devices

Dominion KX IV–101 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 119).

Install Certificate on Apple iOS Device

You must install a CA-signed certificate on your Apple iOS device before you can connect to Dominion KX IV–101. 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".

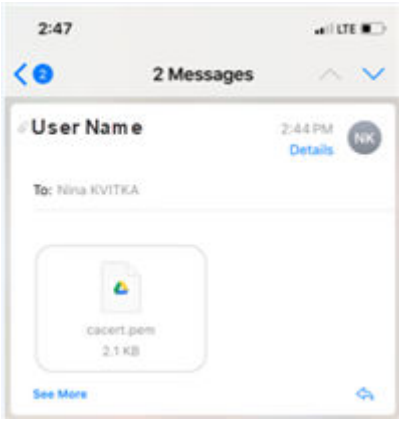
When creating certificates, the certificate Common name should match the IP address/Hostname used to connect to the device.

Install both the Dominion KX IV–101 certificate and the CA certificate used to sign the Dominion KX IV–101 certificate.

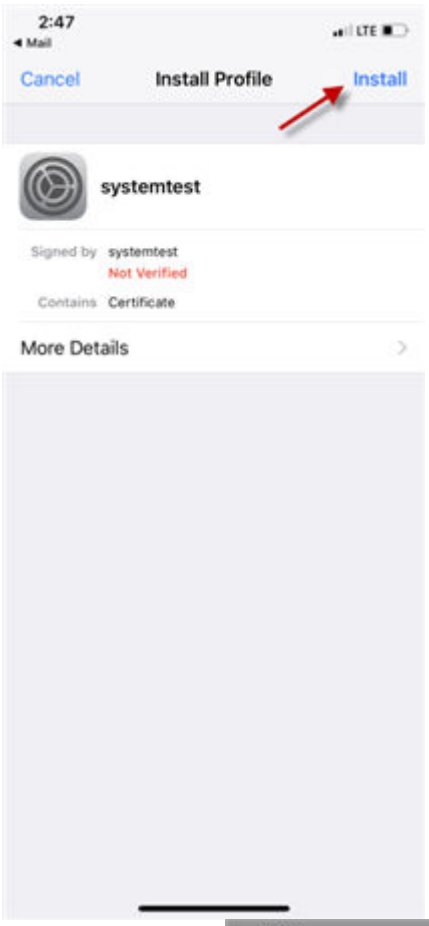
Note: If you have issues launching connections from IOS devices, check that the certificate meets Apple requirements: https://support.apple.com/en-us/HT210176

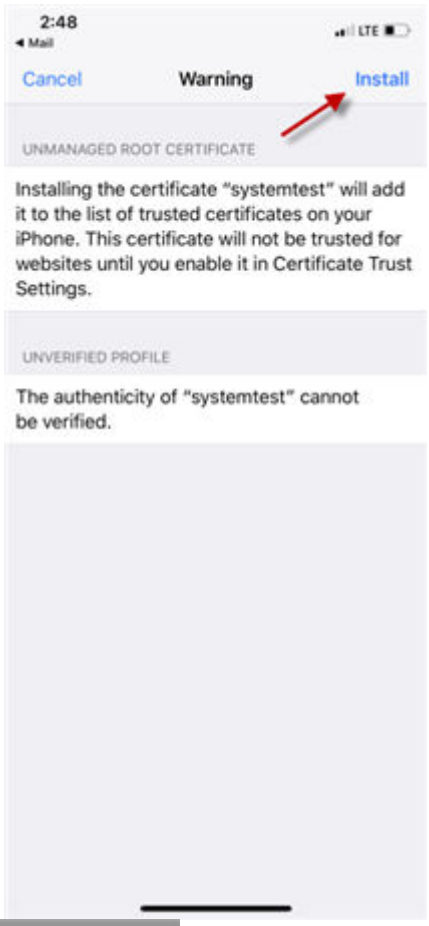
► *To install the certificate on an IOS device:*

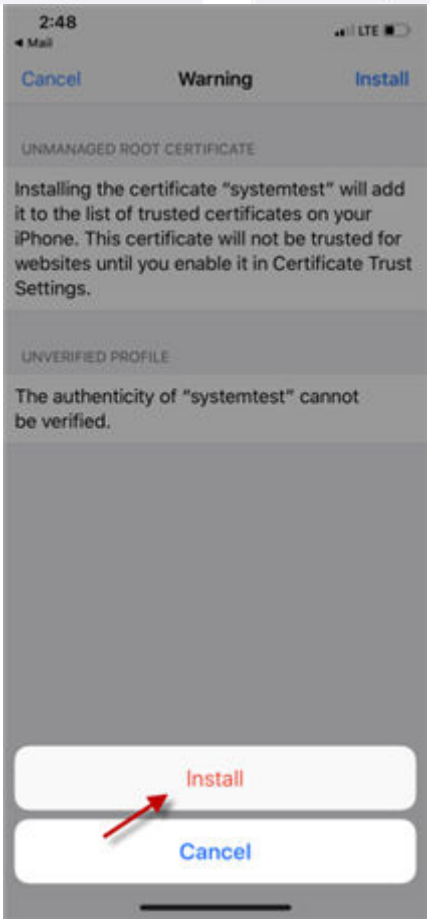
1. Email the certificate file to an email account that can be opened on the iOS device. Open the email and tap the attachment.



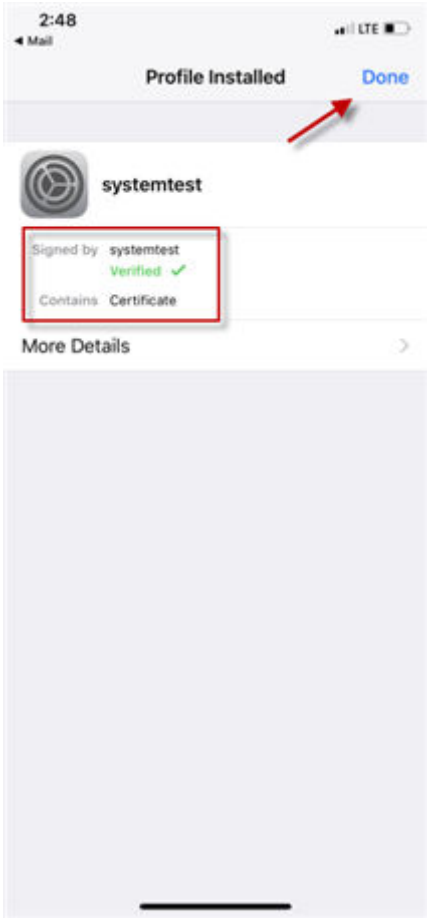
2. The certificate downloads as a "profile" that you have to install. You can have only one profile ready to install at a time. For example, if you download a profile and don't install it, and then download a second profile, only the second profile is available to be installed. If a profile is not installed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

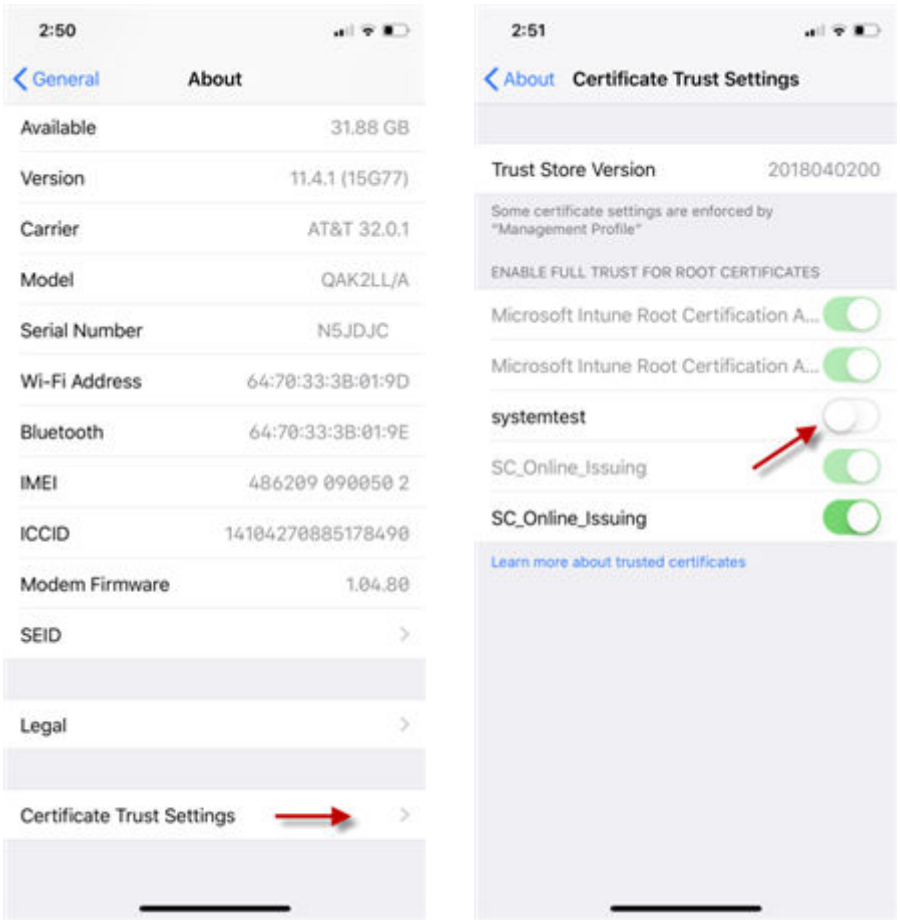

2:48
Mail
LTE
Cancel
Warning
Install
UNMANAGED ROOT CERTIFICATE
Installing the certificate "systemtest" will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.
UNVERIFIED PROFILE
The authenticity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

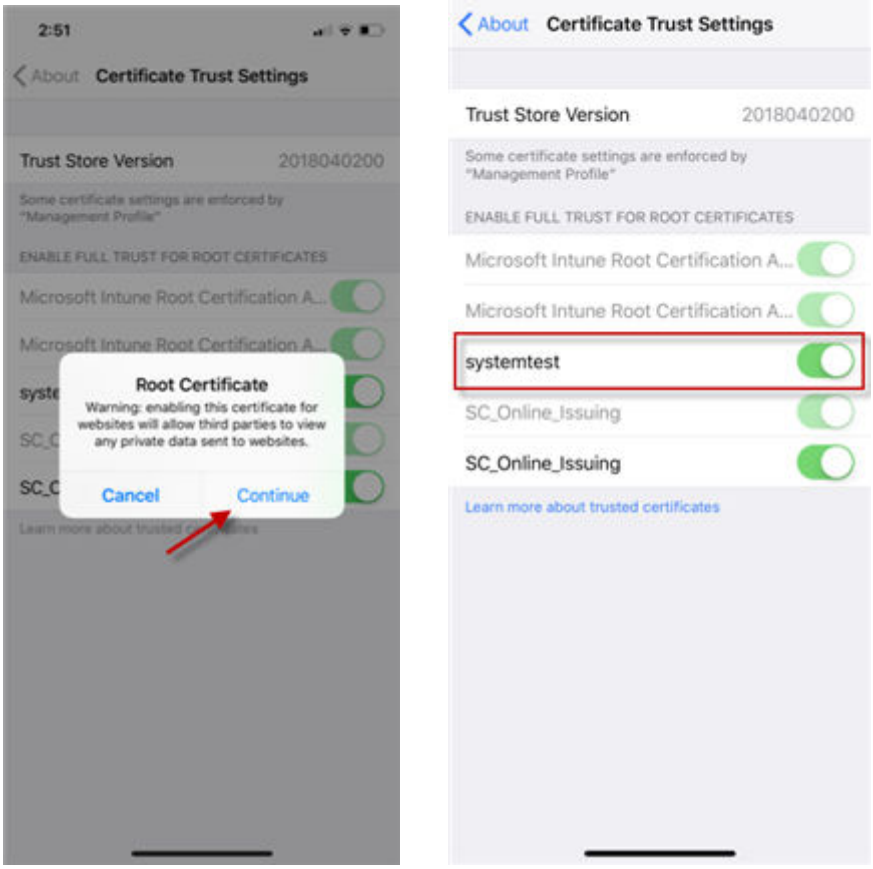
5. When complete the certificate is marked Verified. Tap Done.



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 105).

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

Keyboard Access on Mobile

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

Manage HKC iOS Client Keyboard Macros

The HKC iOS client includes a list of default macros. You can create additional macros using the HKC Macro Editor or import macros from a file. See Macro Editor (on page 90) and Import and Export Macros (on page 96).

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.

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 118).
- 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

Tips for Accessing Dominion KX IV–101 With Dual Monitor Setups

When remotely accessing a Dominion KX IV–101 in a dual monitor setup, make sure the monitor out to Dominion KX IV–101 is set as the Primary Display. Align the two monitors horizontally with the monitor out to KX4-101 in the left position. To ensure good mouse alignment in this scenario, use Intelligent Mouse Mode.

Note: For Windows 10 targets, you must disable all acceleration when using Intelligent Mouse Mode.

Dominion User Station Access to Multi KX4-101 Setups

Two or more Dominion KX4-101 devices can be accessed as a multi-KVM channel using Dominion User Station.

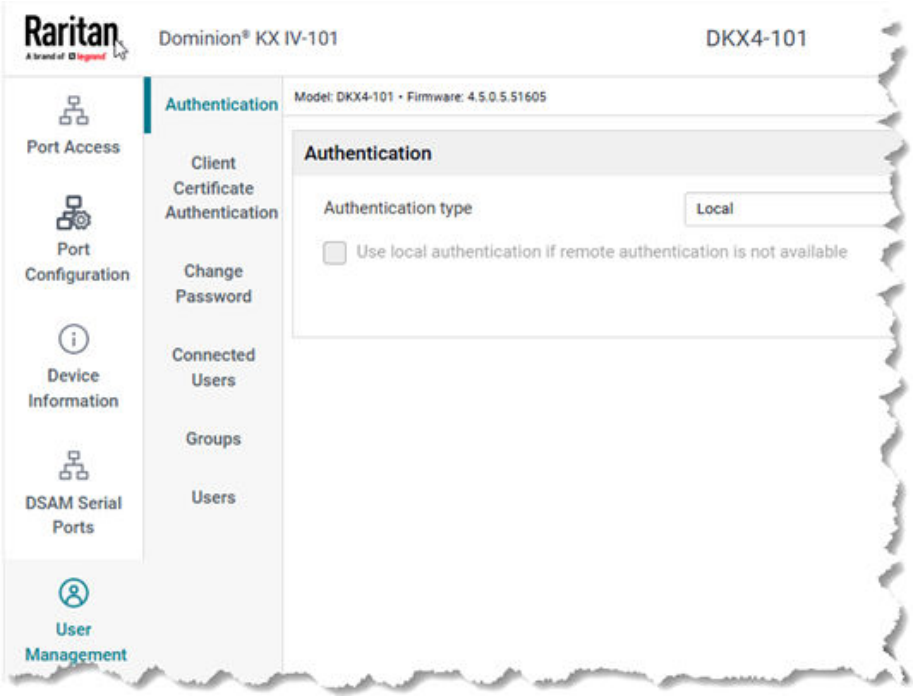
The access must be configured in Dominion User Station: https://help.raritan.com/kxus/v5.0.0/en/#/index/10/11

User Management

Dominion KX IV–101 can be configured for local or remote authentication. To prepare for configuring external authentication, see Gathering LDAP/Radius Information (on page 122).

Dominion KX IV–101 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 (on page 184).

Click User Management to view the submenu options.



In This Chapter

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 Dominion KX IV–101 supports :

- Local user database on the Dominion KX IV–101
- LDAP
- Radius

By default, the Dominion KX IV–101 is configured for local authentication. If you use this method, you only need to create user accounts.

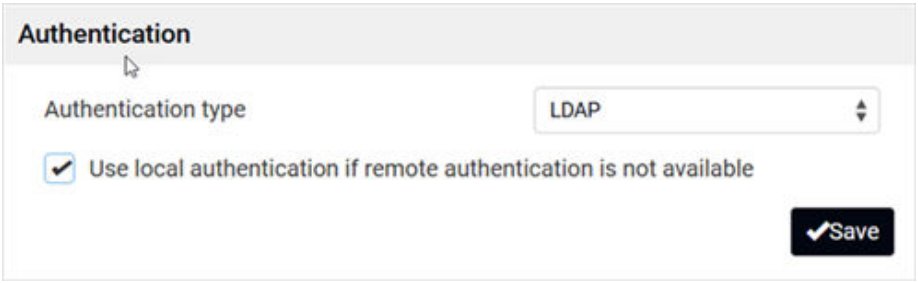
If you prefer external authentication, you must provide the Dominion KX IV–101 with information about the external Authentication and Authorization (AA) server.

If you would like local authentication to be available as a backup method when external authentication is not available, create user accounts on the Dominion KX IV–101 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 Dominion KX IV–101 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 Dominion KX IV–101.

► *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 123) and Radius Authentication (on page 131). For help with adding users, see Users and Groups (on page 138).



LDAP Authentication

Gather the information you need to add your LDAP servers to Dominion KX IV–101. For help, see: Gathering LDAP/Radius Information (on page 122).

► *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 Dominion KX IV–101. 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 Dominion KX IV–101 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.
Enable verification of LDAP Server Certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the Dominion KX IV–101 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.*

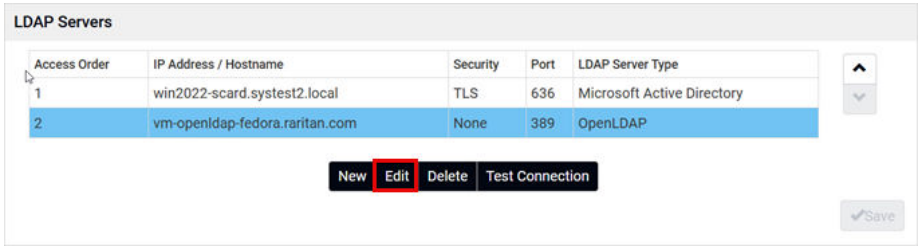
Field/setting	Description
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated 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.
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 Dominion KX IV–101 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 (on page 122).

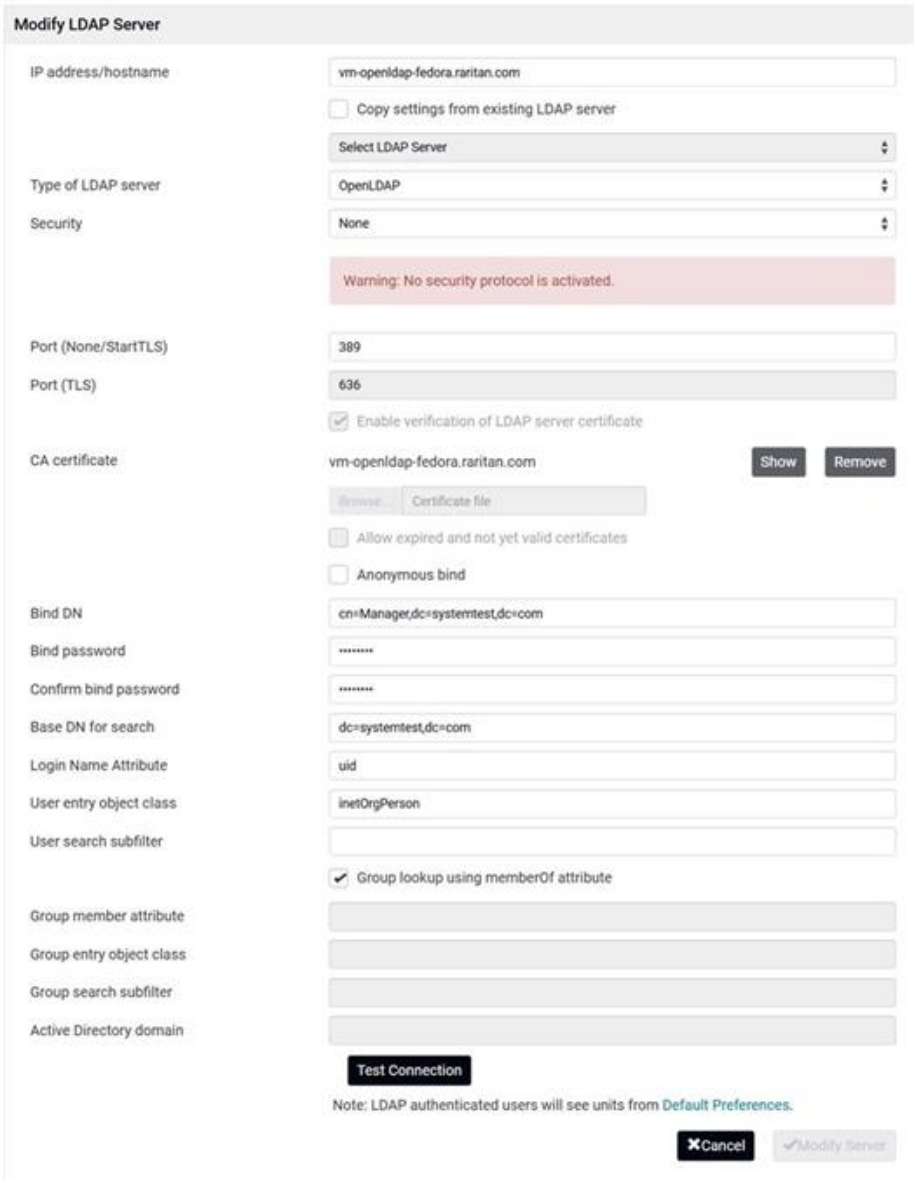
Edit and Delete LDAP Server

► *To Edit LDAP server:*

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

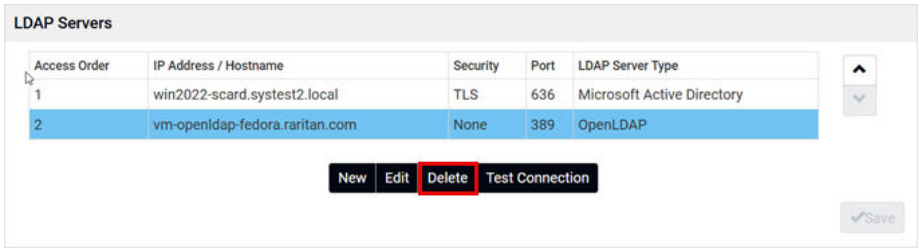


4. Modify LDAP Server opens up.
5. Make updates and click Modify Server.
6. Click Save to confirm.

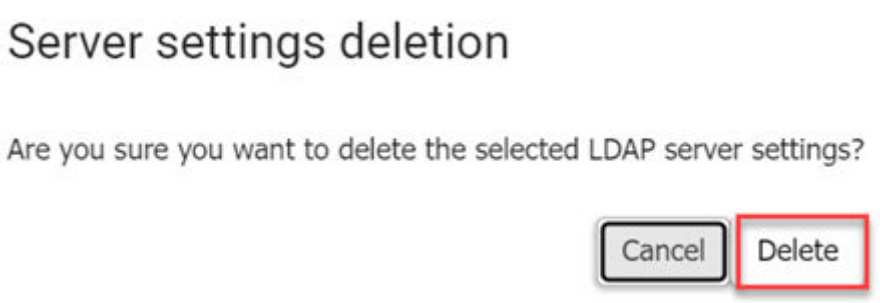


► *To Delete LDAP servers:*

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 Dominion KX IV–101

A group on the Dominion KX IV–101 determines the permissions. You must create the groups whose names are identical to the user groups created for the Dominion KX IV–101 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 Dominion KX IV–101. 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.

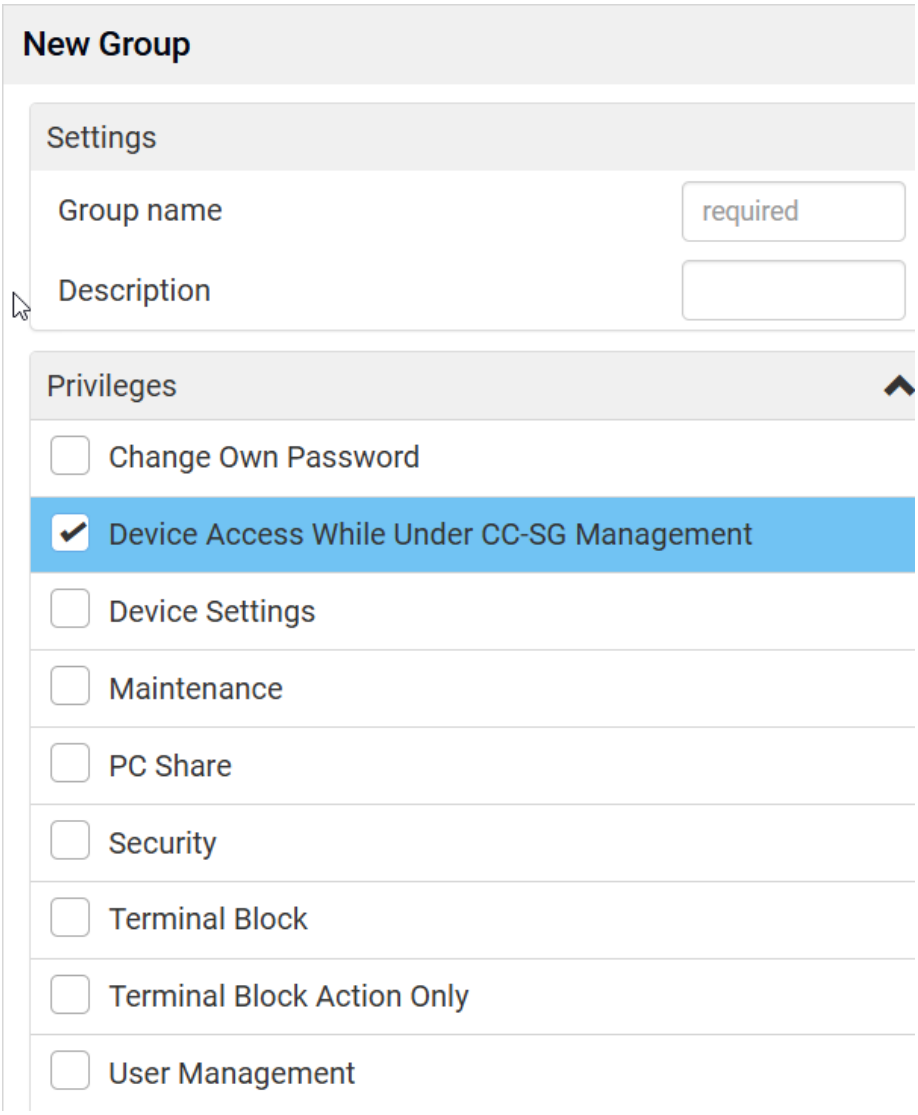
User group	User accounts (members)
KX_User	usera
	kxuser2
KX_Admin	userb
	kxuser

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.

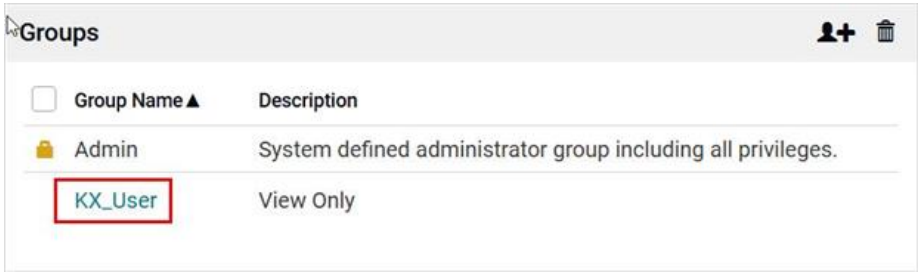
► *To create the KX_User group with appropriate permissions assigned:*

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.

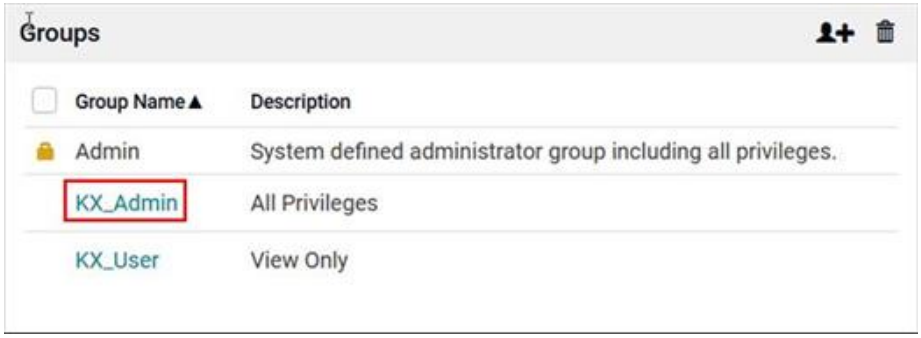
3. The KX_User group is created.



► *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 the 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 Dominion KX IV–101 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 Dominion KX IV–101. For help, see: Gathering LDAP/Radius Information (on page 122).

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.

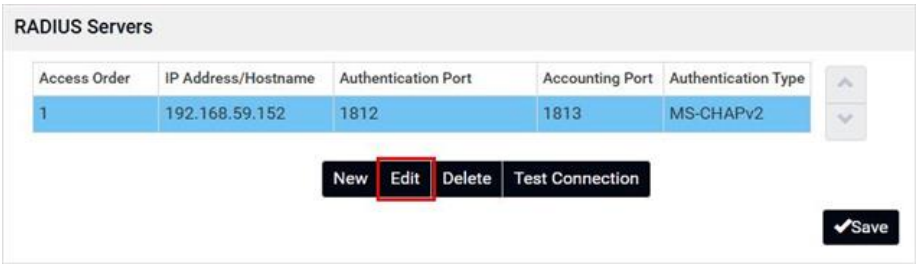
Field/setting	Description
IP Address / Hostname	The IP address or hostname of your Radius server.
Type of RADIUS Authentication	Select an authentication protocol. • PAP (Password Authentication Protocol) • MS-CHAP v2 (Microsoft's Point-to-Point Tunneling Protocol) • CHAP (Challenge Handshake Authentication 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 Dominion KX IV–101 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 (on page 122).

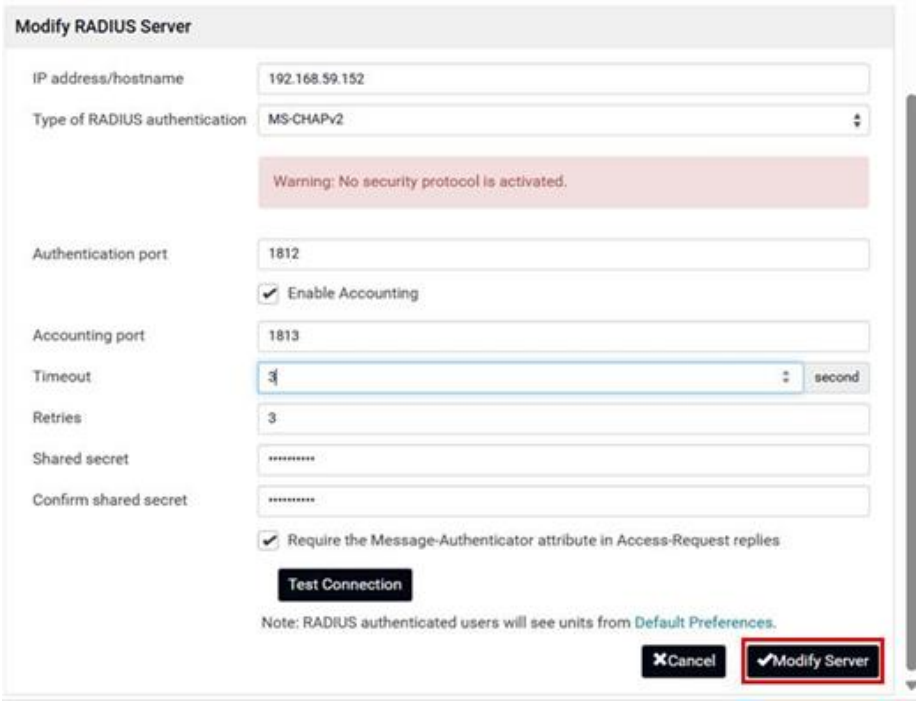
Edit and Delete Radius Server

► *To Edit Radius server:*

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

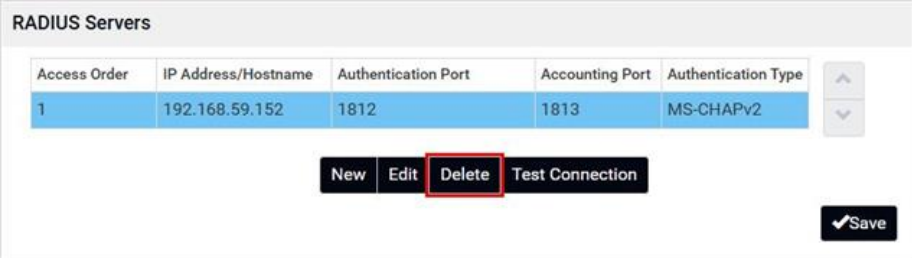


4. Modify Radius Server opens up.
5. Make updates and click Modify Server.
6. Click Save to finalize the changes.

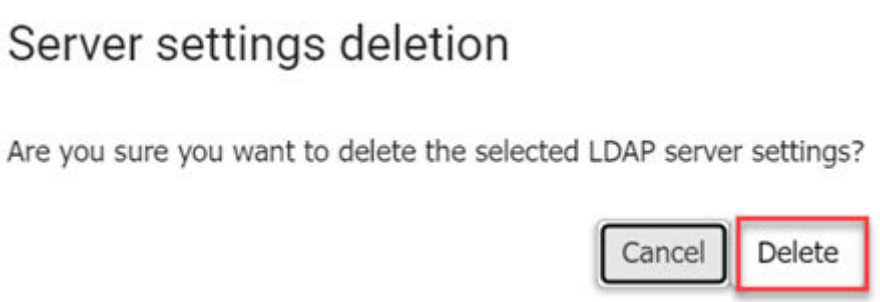


► *To Delete Radius servers:*

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 Dominion KX IV–101 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

Dominion KX IV–101 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

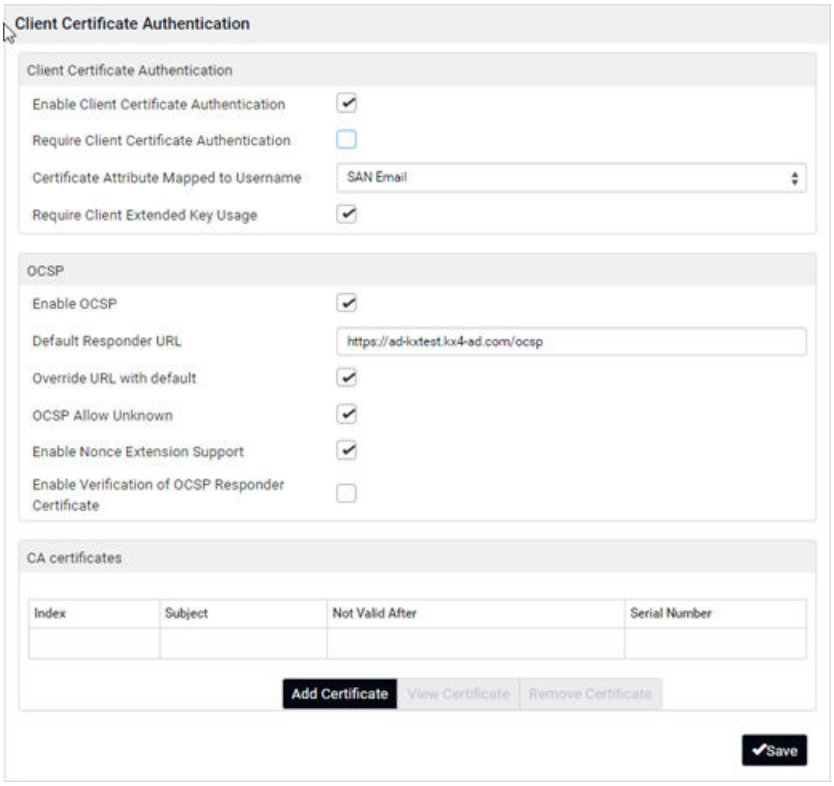
When enabled, Client Certificate Authentication applies to smart card and TLS certificate authentication.

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 a method 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 Dominion KX IV–101 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, Dominion KX IV–101 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 Dominion KX IV–101 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 sends 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.
7. Click OK to save.

Note: Once a TLS certificate is imported onto a user's PC, all subsequent logins will be authenticated using the client certificate.

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 Dominion KX IV–101 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.
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.

Users and 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.

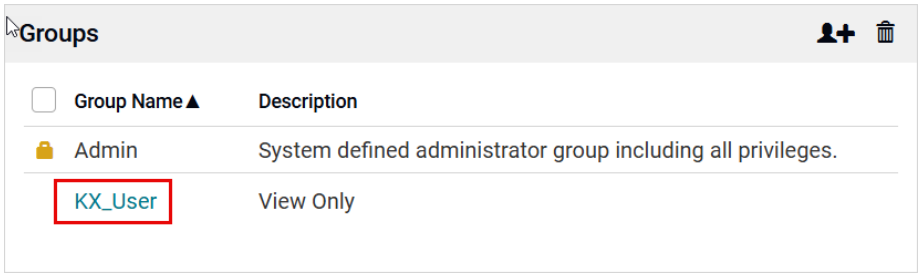
Privileges are assigned at the Group level, so you must also add groups, and assign your users to Groups. An admin group is created by default and has exclusive privileges. See Admin Group Special Privileges (on page 147).

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:*

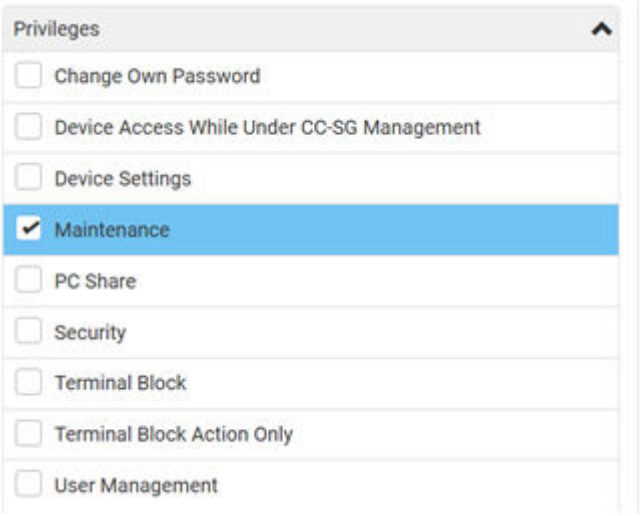
1. Click User Management > Groups, then click the add group icon 



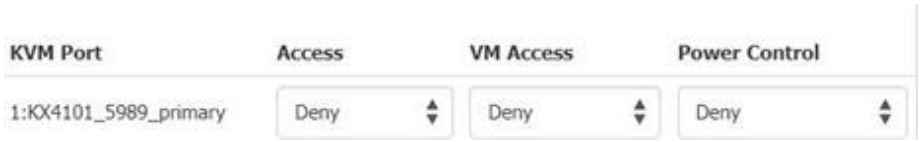
2. Complete the New Group information:

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 (on page 147).
   - Change Own Password: Allows users to change their own password.
   - Device Access While Under CC-SG Management: Allows users to directly access the Dominion KX IV–101 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 Dominion KX IV–101. User authentication is performed based on Dominion KX IV–101 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
   - Terminal Block: All settings in Device Settings > Terminal Block, and access to the externally connected device using the KVM client
   - Terminal Block Action Only: All functions in Device Settings > Allow user to use the "External Device Settings" in the KVM-Client
   - User Management: All functions in the User Management menu except Disconnect Users



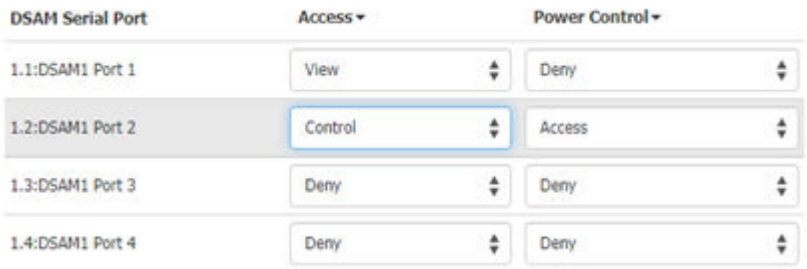
2. Select the Access and VM privileges for the KVM Port.



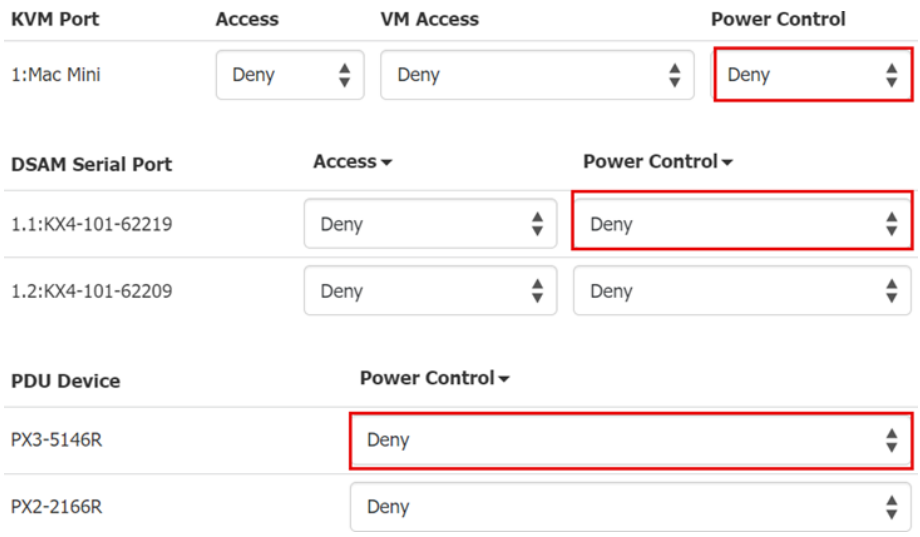
- Access: Deny, View, Control
- VM Access: Deny, Read-only, Read-write
- Power Control: Access, Deny

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

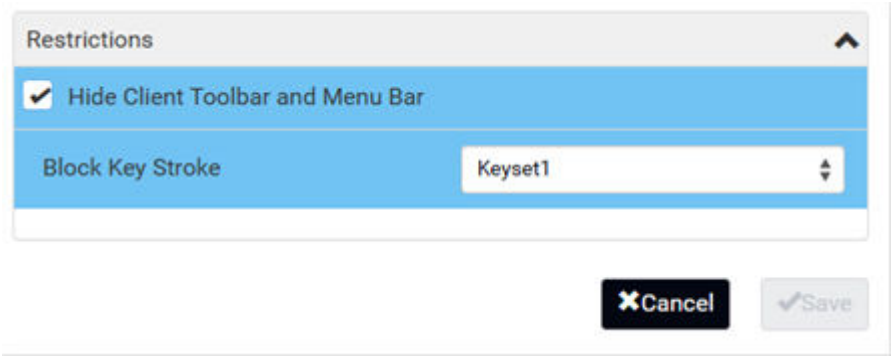
3. When a DSAM unit is connected, the Serial Port section is available to select the Access privileges for the Serial Ports.
   - Access: Deny, View, Control



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.



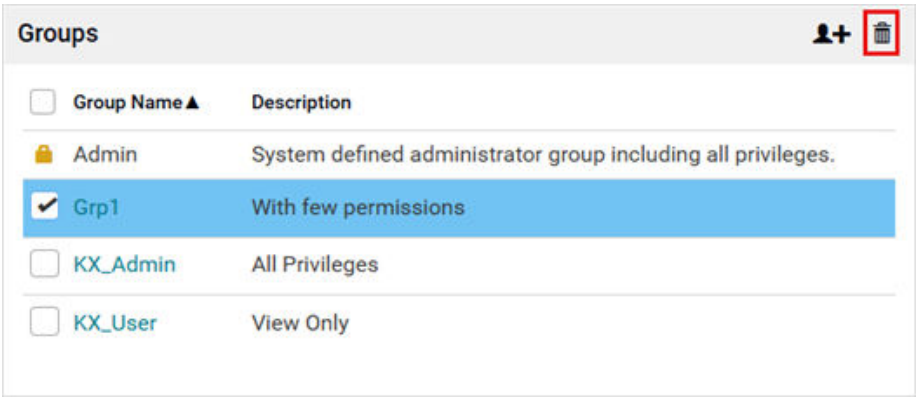
6. The Restrictions section has options for restricting client views and blocking keys.
   - Select Hide Client Toolbar and Menu Bar to remove these components from view for this group. Scaling and hotkeys for Single Mouse, Full-Screen, Scale Video and Disconnect from Target will be available.
   - In 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 161).



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

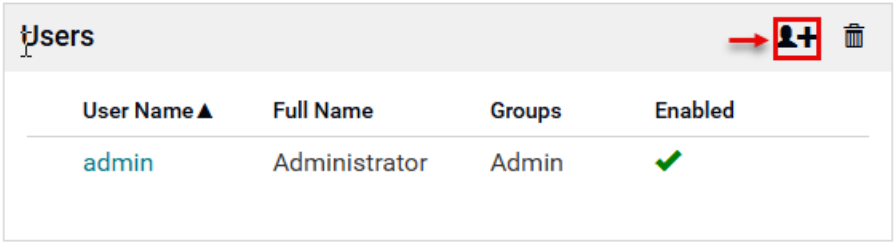
► *To delete a group:*

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.



► *To add users:*

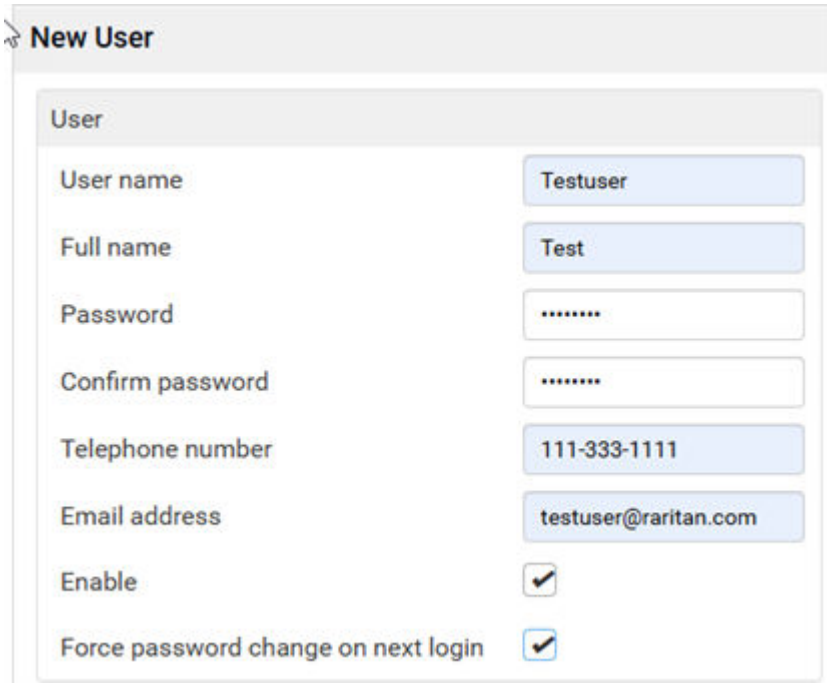
1. Click User Management > Users, then click the add user icon .



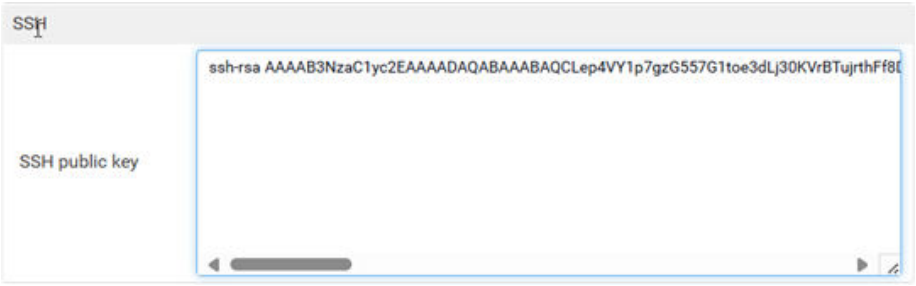
2. Complete the User information:

Field/setting	Description
Username	The name the user enters to log in to the Dominion KX IV–101. • 4 to 32 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 Dominion KX IV–101.

Field/setting	Description
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in.



1. SSH: The SSH public key is required when public key authentication for SSH is enabled. See SSH Settings (on page 169).
2. Open the SSH public key with a text editor.
3. Copy and paste all content in the text editor into the SSH Public Key field.



4. 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.

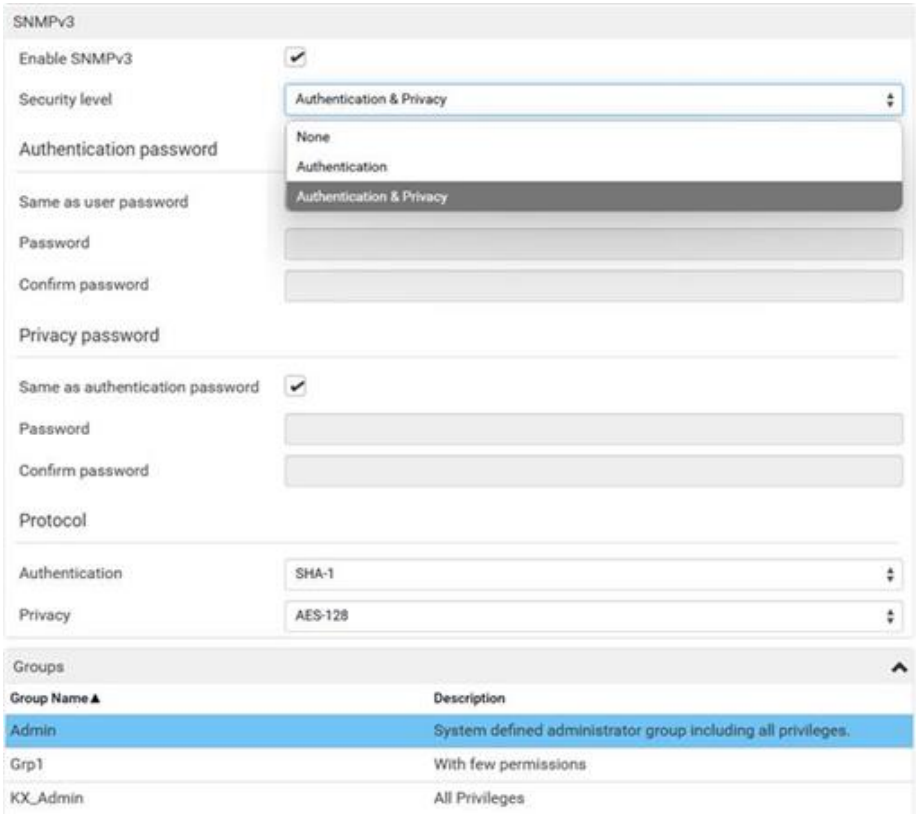
- Privacy Password: This section is configurable only when 'Authentication & Privacy' is selected.

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)

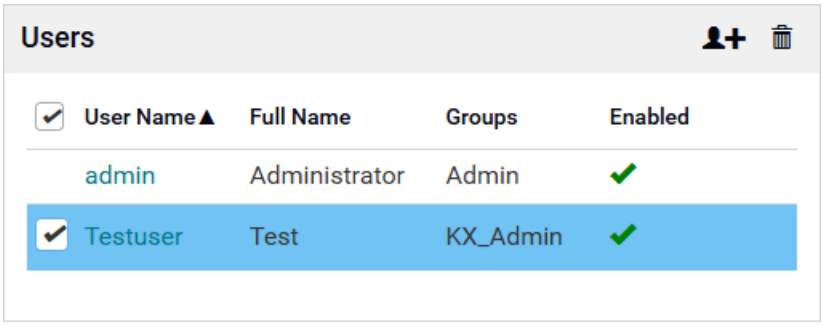
Field/setting	Description
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: • DES • AES-128 (default)



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:*

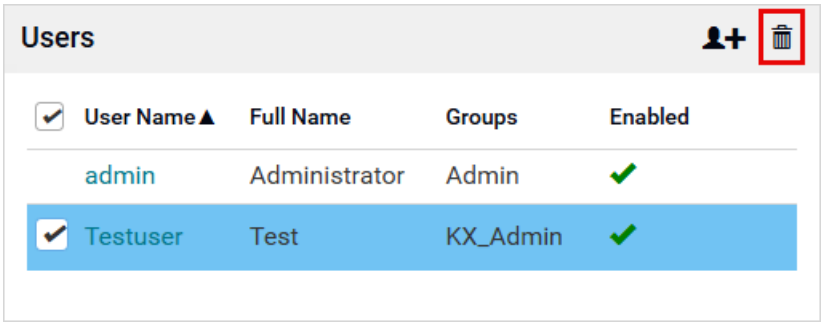
1. Click User Management > Users, then click to select the user you want to edit.



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.



Admin Group Special Privileges

The following special privileges are exclusively available to the admin group.

- Backup/Restore
- Disconnect Connected users
- Reset to Factory Defaults
- Diagnostics
- Enable SNMPv3 in the SNMP agent (SNMP gets and sets)
- Configure SNMPMv3 user parameters
  - Security Level
  - Authentication Protocol
  - Authentication Password
  - Privacy Password
  - Privacy Protocol

Device Settings and Information

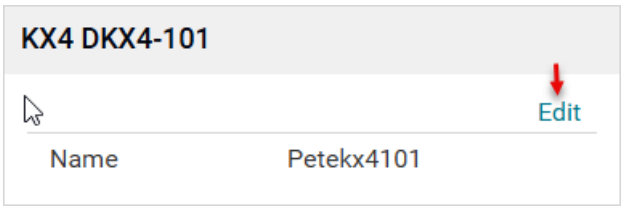
In This Chapter

Device Information

Click Device Information to view name, system, and network details about your Dominion KX IV–101. In this page you can also rename your device, and view open source license information.

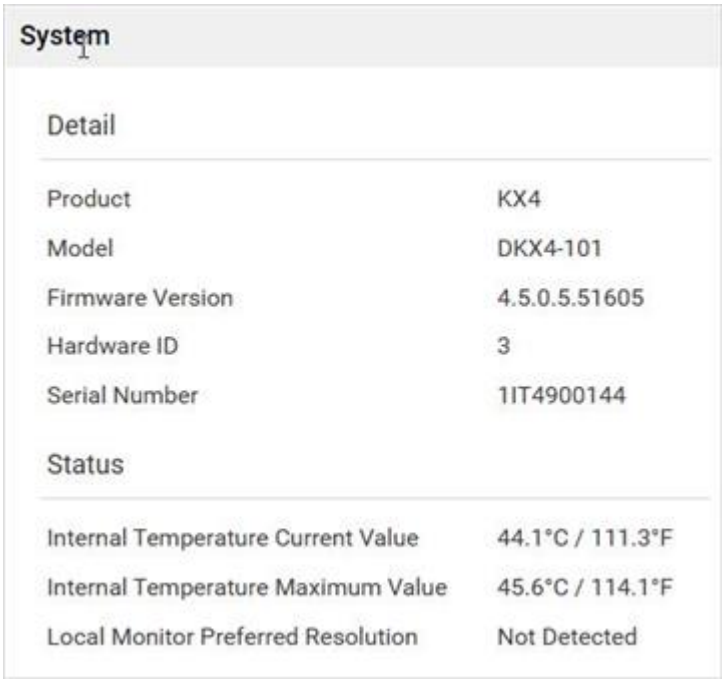
► *To edit your device name:*

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



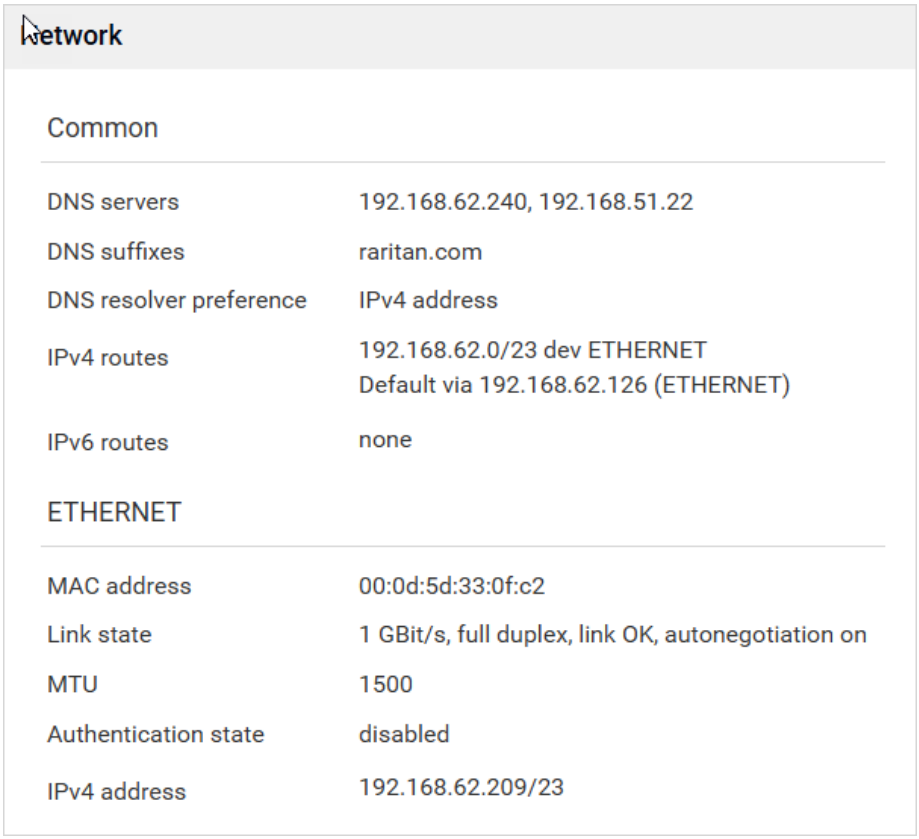
► *To view system details and status:*

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



► *To view network details:*

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



► *To view DSAM details:*

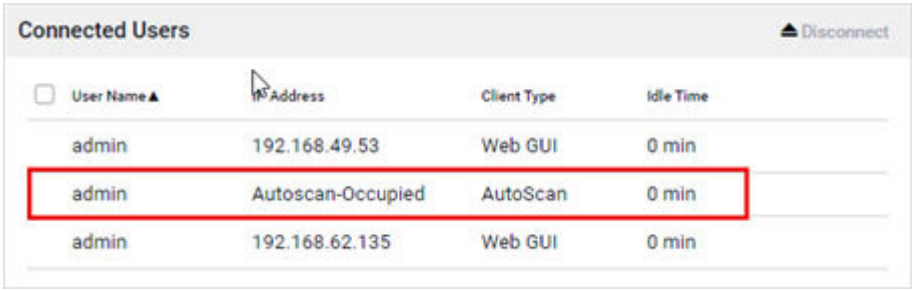
- When a DSAM unit is attached, view the hardware details: name, port number, USB port location, model, firmware version, hardware ID, serial number.

Auto Scan

The Auto Scan feature uses the Dominion KX IV–101 video channel to automatically scan and capture a screenshot of your target video at a specified time interval. 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.

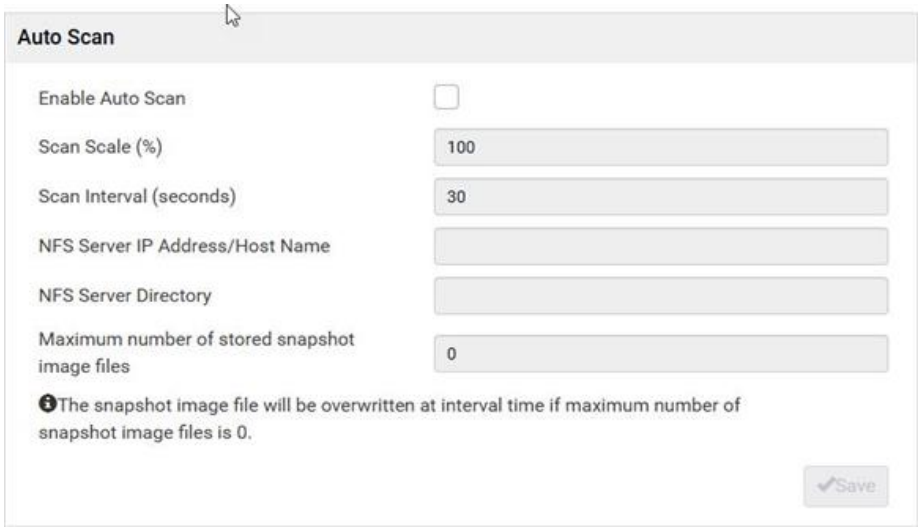
PC Share Mode should be enabled when using Auto Scan to ensure images can be captured and sent to the NFS server. When PC Share Mode is disabled, Auto Scan cannot capture a port image when the port is already occupied by another user. Go to Security > KVM Security to enable PC Share Mode.

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. 1 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. Maximum number of stored snapshot image files: Enter the total number of snapshots to be saved. When the maximum number of image files is reached, the oldest file will be replaced with the new image file.
8. Click Save to apply the settings.
9. When Auto Scan is enabled, view the status in the Device Info page. Go to Device Info, then check Auto Scan NFS in the System section.



► *Auto Scan NFS Status:*

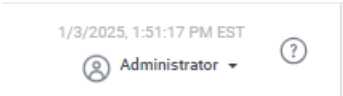
When Auto Scan is disabled, it does not appear in Device Info > Status. When enabled, possible status are:

- On
- Suspended
- Failed
- Connecting

Date and Time

Set the internal clock on the Dominion KX IV–101 manually, or link to a Network Time Protocol (NTP) server.

The Dominion KX IV–101 system date and time appears in the upper right corner of the web interface.



► *To set the date and time:*

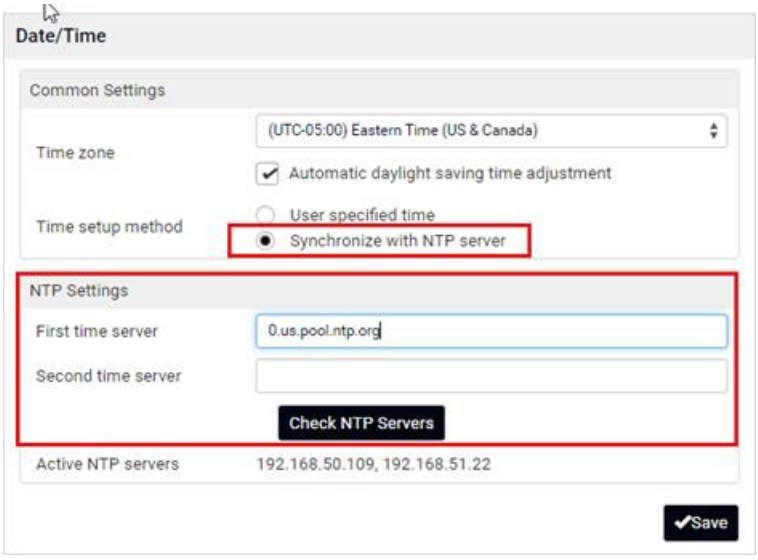
1. Click Device Settings > Date/Time.
2. Select your Time Zone.
3. If your area participates in daylight saving time, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.
4. Select the Time Setup Method:
   - User Specified Time: Set the time manually.
   - Synchronize with NTP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



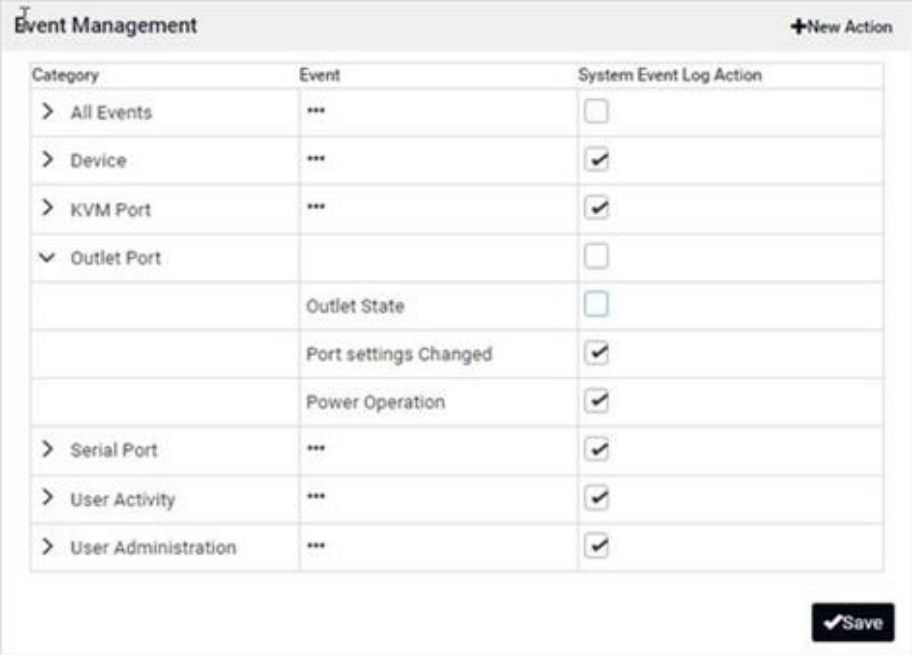
- Click Check NTP Servers to verify the validity and accessibility of the NTP servers.

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.

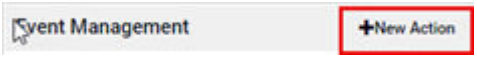
► *Configuring events and actions:*

1. Click Device Settings > Event Management.
   - The Event Management page shows events by Category. Click a category to view individual events. In this example, New Action1 syslog, New Action1 snmp, and System Event Log Action have been added and assigned to all User Activity and User Administration events.
2. Select the event check boxes to assign an action to an event. Click Save.
3. 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.



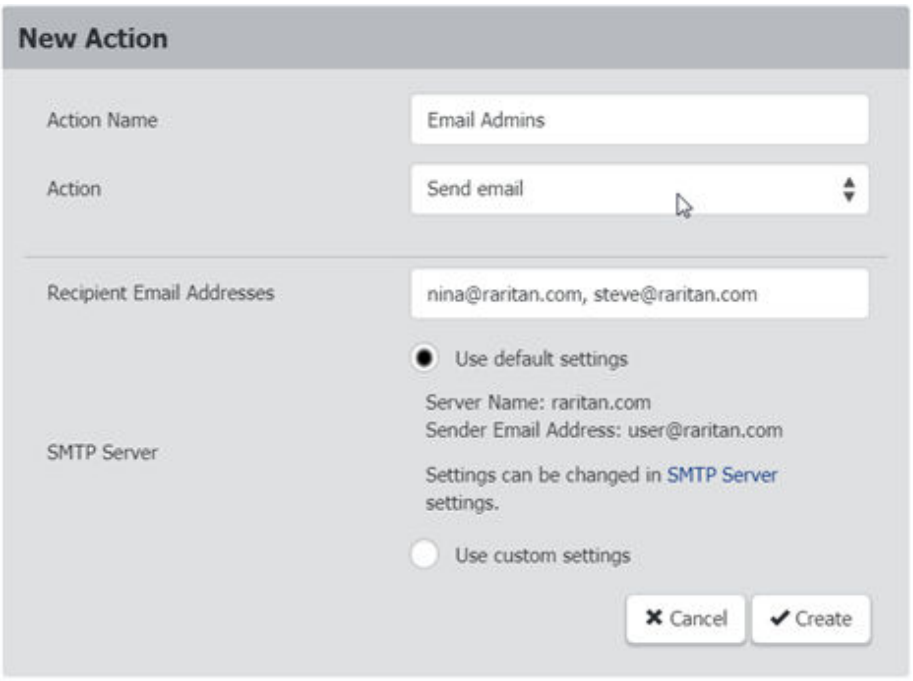
2. Assign a name to this action.
3. Select the desired action and configure it.
   - Email Actions: See Send Email (on page 154)
   - SNMP Actions: See SNMP Notifications (on page 155)
   - Syslog Actions: See Syslog Messages (on page 158)
4. Click Create.

Send Email

Use this action to send an email according to your preconfigured SMTP settings, or create actions with one or more customized SMTP settings.

See Event Management (on page 153) for help assigning this action to an event.

► *To create the send email action:*



1. Select Send Email from the Action list.
2. In the Recipient Email Addresses field, enter the email addresses of the recipients. Use a comma to separate multiple email addresses.
3. By default, the SMTP server settings will be used to complete this action. To view or change those settings, click the SMTP Server hyperlink.
   - To use a different SMTP server, click the "Use custom settings" radio button. The fields for customized SMTP settings appear. See SMTP Server Settings (on page 167).
4. Click Create.

SNMP Notifications

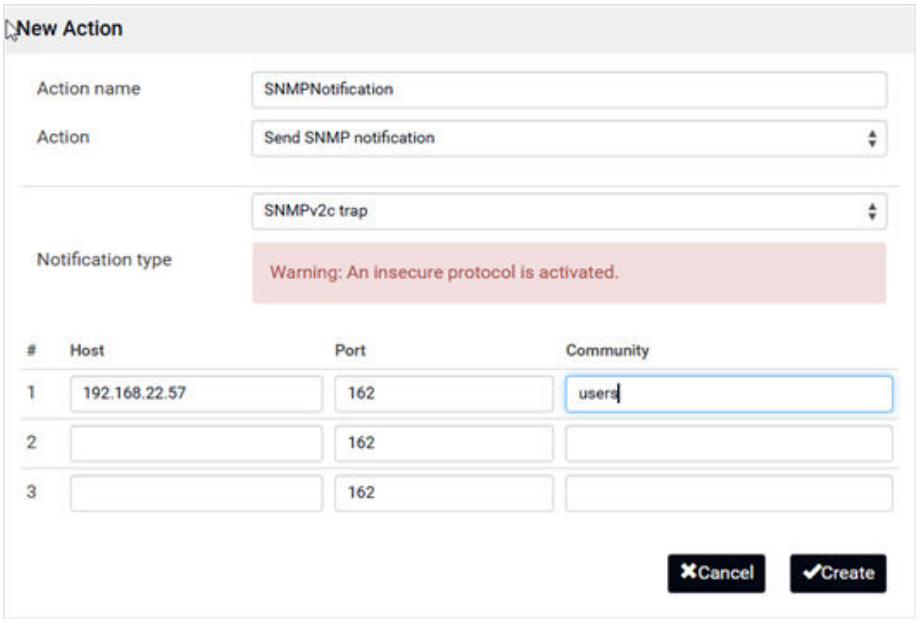
Use this action to send an SNMP notification to one or more SNMP servers.

See Event Management (on page 153) for help assigning this action to an event.

► *To create the SNMP notification action:*

1. Select Send SNMP Notification from the Action list.
2. Select the type of SNMP notification. Follow the procedure below based on your selection.

► *SNMP v2c notifications:*

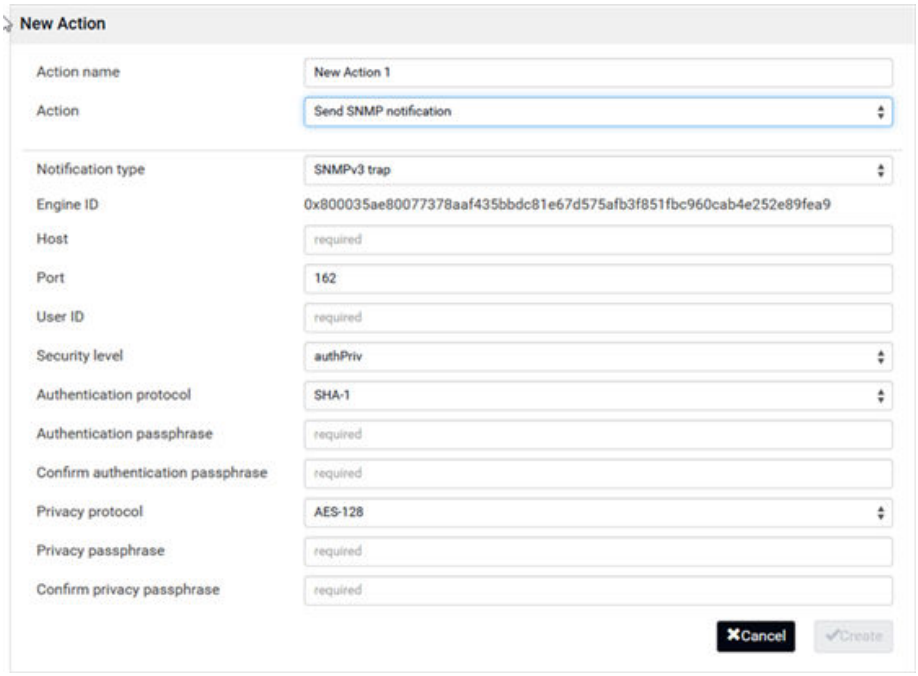


1. In the Notification Type field, select SNMPv2c Trap.
2. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
3. In the Port fields, enter the port number used to access the device(s).
4. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the Dominion KX IV–101 and all SNMP management stations.
5. Click Create.

Tip: An SNMP v2c notification action permits a maximum of three SNMP destinations. If you need to assign more than 3 SNMP destinations to an event, you can create and assign multiple actions comprising all the destinations.

► *SNMP v3 notifications:*

Note: Duplicated SNMP Trap v3 secName (User ID) is not supported when multiple SNMP Trap destinations are configured.



1. In the Notification Type field, select SNMPv3 Trap. The engine ID is prepopulated.
2. Enter the following as needed and then click OK to apply the settings:
   a. Host: Enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
   b. Port number
   c. User ID for accessing the host -- make sure the User ID has SNMPv3 permission.
   d. Select the host security level:

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. Select the authentication protocol - MD5 or SHA Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. Select the authentication protocol - MD5 or SHA Enter the authentication passphrase and confirm the authentication passphrase Select the Privacy Protocol - DES or AES Enter the privacy passphrase and then confirm the privacy passphrase

3. Click Create.

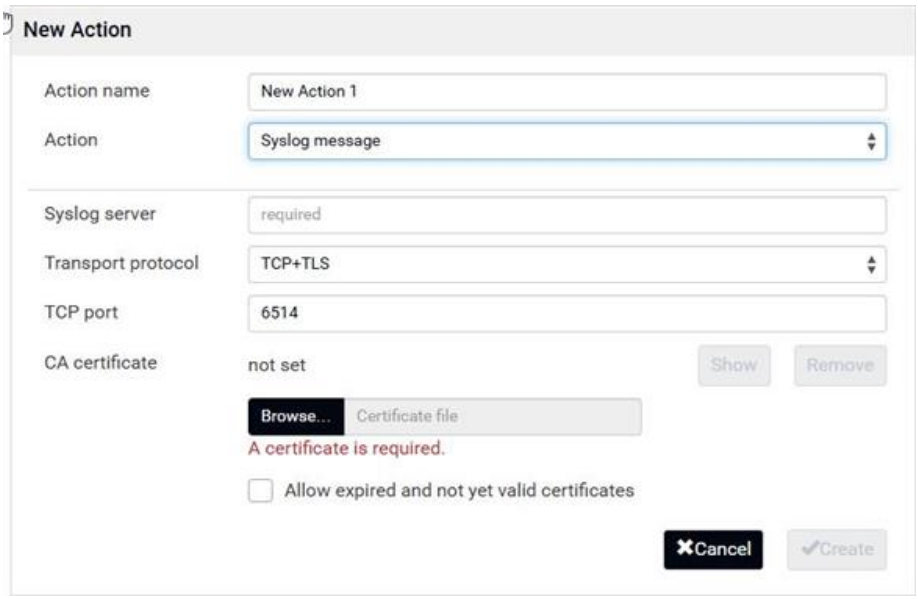
Syslog Messages

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up.

Dominion KX IV–101 may or may not detect syslog message transmission failure. Detected syslog failures and reasons are saved in the event log.

See Event Management (on page 153) for help assigning this action to an event.

► *To create the syslog message action:*



1. Select Syslog Message from the Action list.
2. In the Syslog Server field, specify the IP address to which the syslog is forwarded.
3. In the Transport Protocol field, select one of the syslog protocols: UDP, TCP, or TCP+TLS. The default is TCP+TLS.

Transport protocols	Next steps
UDP	• In the UDP Port field, type an appropriate port number. Default is 514. • Select the "Legacy BSD Syslog Protocol" checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the TCP Port field.

Transport protocols	Next steps
TCP+TLS	A TLS certificate is required. • Type an appropriate port number in the "TCP Port" field. Default is 6514. • In the CA Certificate field, click Browse... to select a TLS certificate. After importing the certificate, click Show to view its contents, or click Remove to delete. • To allow event messages even if any TLS certificate in the selected certificate chain is outdated or not valid yet, select the "Allow expired and not yet valid certificates" checkbox.

4. Click Create.

Dominion KX IV–101 Events

- Event log cleared - Event log was cleared
- CC Management Started - CC-SG management started
- CC Management Stopped - CC-SG management stopped
- Device clock changed - Device clock was changed
- Device Identification changed - Device identity was changed
- Device settings restored - Device settings were restored
- Device settings saved - Device settings were backed up
- Device State changed - Device state was changed
- DSAM Connected - A DSAM connected to KX4-101
- DSAM Disconnected - A DSAM disconnected from KX4-101
- 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
- Firmware update completed - KX4-101 firmware update completed
- Firmware update failed - KX4-101 firmware update failed
- Firmware update started - KX4-101 firmware update started
- Firmware validation failed - KX4-101 firmware validation failed
- FIPS mode changed - FIPS settings were changed
- 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 KX4-101
- PDU Disconnected - A PDU disconnected from KX4-101
- 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
- Terminal block settings changed - Terminal block settings changed
- Terminal block status changed - Terminal block status changed
- KVM Port Connected - KVM Port was connected
- KVM Port Disconnected - KVM Port was disconnected
- KVM Port settings Changed - KVM Port settings changed
- KVM Port Audio Connected - KVM Port audio connected
- KVM Port Audio Disconnected - KVM Port audio disconnected
- KVM Port Status Changed - KVM Port status 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 Changed - Serial port status 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

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 (on page 138).

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 (on page 138).

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 (on page 148). Dominion KX IV–101 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::10/64*

► *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).

Field	Description
Duplex	• Select a duplex mode. • Auto: The Dominion KX IV–101 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 Dominion KX IV–101) 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.
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.

Field	Description
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.
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 Dominion KX IV–101 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 Dominion KX IV–101 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.

Field/setting	Description
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.
Allow connection if system clock is incorrect	If powered off for a long time, the system time may be incorrect. When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the system time is earlier than the firmware build before synchronizing with any NTP server.

► *Common Network Settings:*

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

Field	Description
DNS resolver preference	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 Dominion KX IV–101 will use DHCP-assigned DNS servers.

Field	Description
Send MAC address to DHCP server	When this checkbox is selected, the MAC address is sent to the DHCP server. By default, the checkbox remains unchecked, and the serial number of Dominion KX IV–101 is sent instead.

Network Services

The Dominion KX IV–101 supports the following network communication services:

- Discovery
- HTTP/HTTPS
- SMTP Server
- SNMP
- SSH

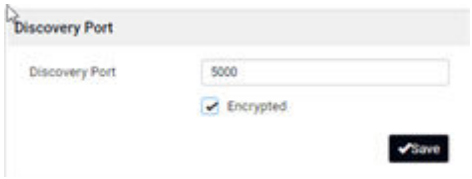
Discovery Port

Dominion KX IV–101 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.



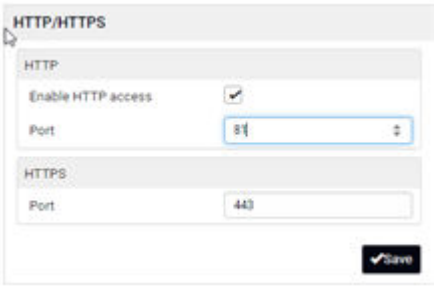
HTTP/HTTPS Ports

Dominion KX IV–101 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 (on page 153).

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See Event Log (on page 201).

► *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
Time between sending retries	Type the interval between email retries in minutes. • Default is 2 minutes.

Field	Description
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 Dominion KX IV–101 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

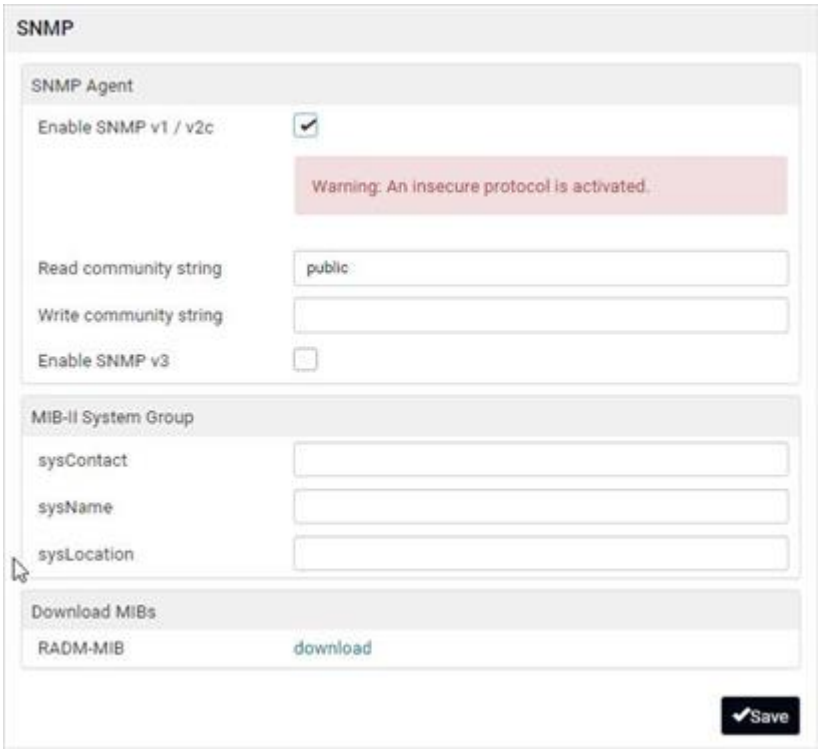
You can enable or disable SNMP communication between an SNMP manager and the Dominion KX IV–101.

► *To configure SNMP communication:*

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 MIB to use with your SNMP manager.
5. Click Save.



SSH Settings

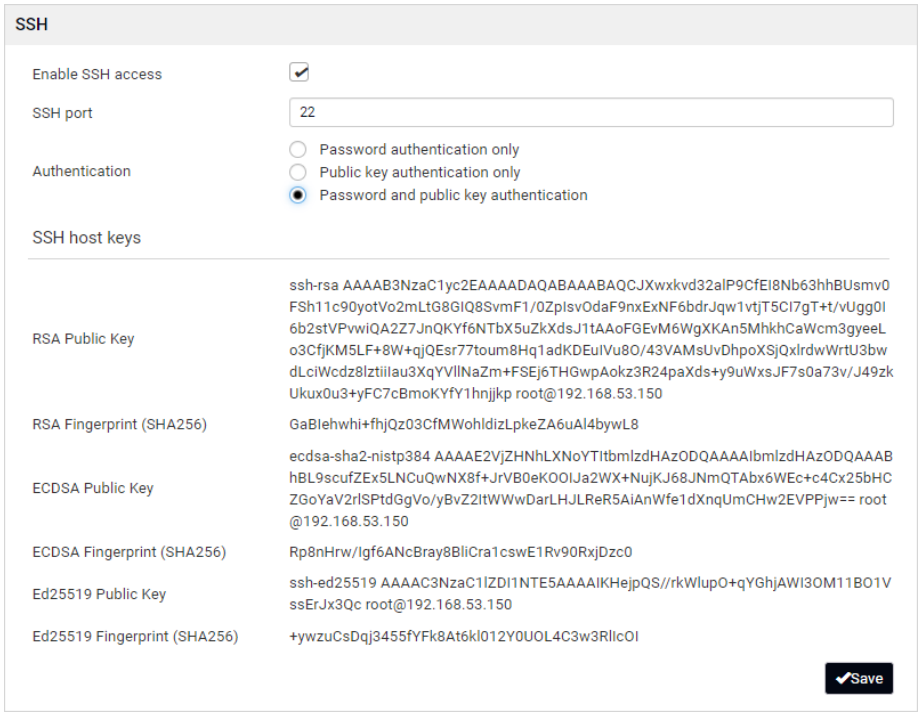
Enable or disable SSH access to the CLI, change the TCP port, or set a password or public key for login over SSH.

► *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 (on page 138)

5. Click Save.



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

PDU Management

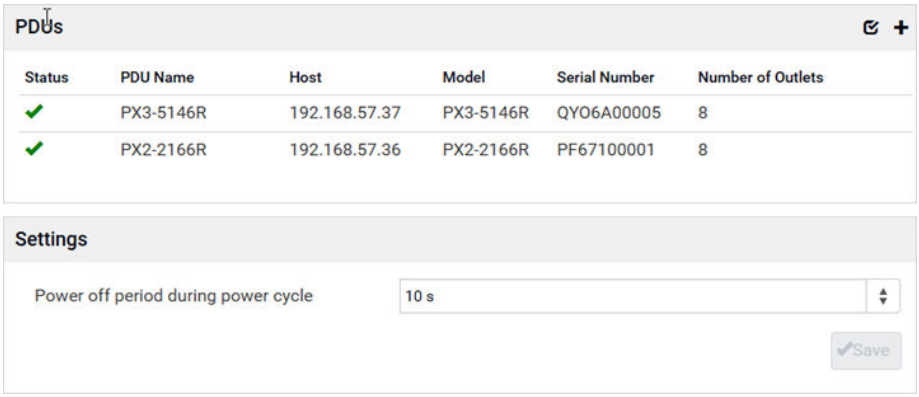
Power Distribution Units (PDUs), including Raritan PX2, PX3 and PX4 and Server Technology PRO3X and PRO4X can be added to the Dominion KX IV–101 using SNMP. You can configure up to 8 PDUs in the Dominion KX IV–101 and get their current status. You can see all the added PDUs on the PDU Management page. The Dominion KX IV–101 checks the connection status of the configured PDU every 30 seconds. If it fails 10 times consecutively, the Dominion KX IV–101 will stop further checks. After adding PDUs, you can configure power associations to targets. See Port Configuration: Power Association (on page 28).

► *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.

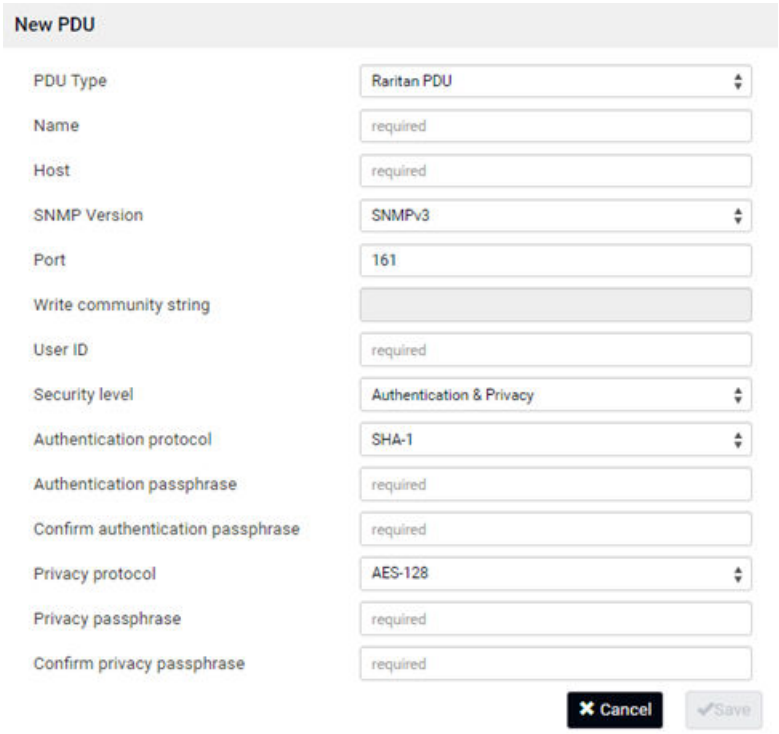
Adding PDUs

Dominion KX IV–101 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 a 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,a 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.

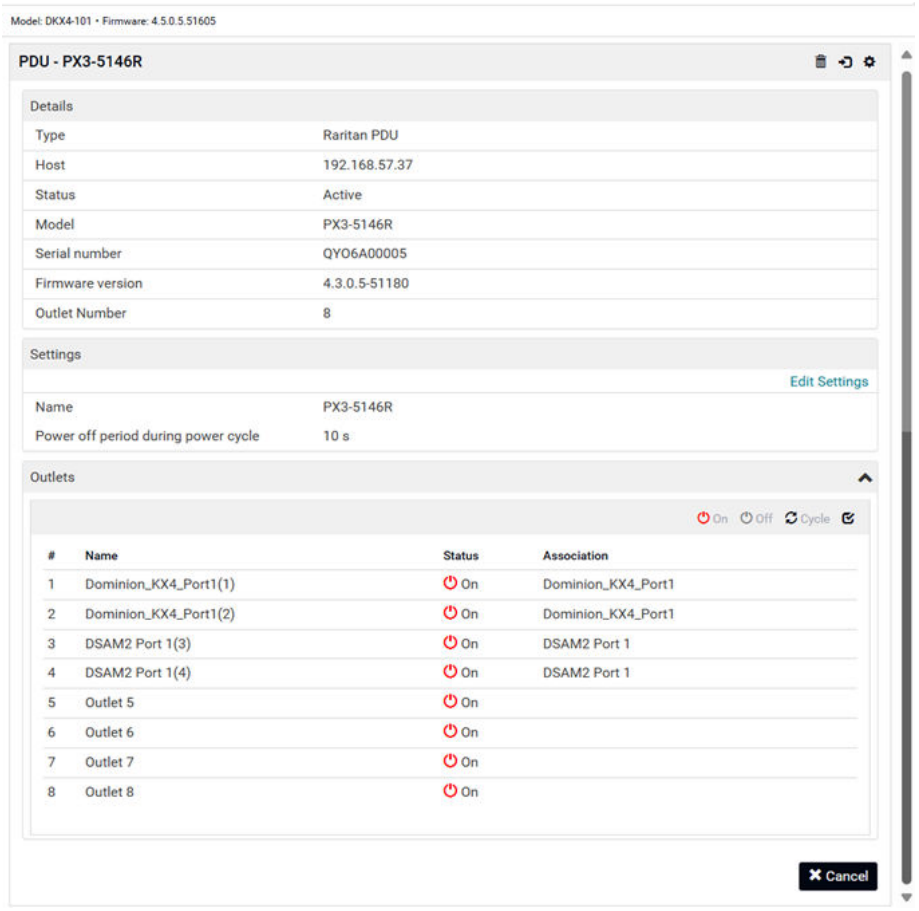
PDU and Outlet Details

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/IP Address: 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 Dominion KX IV–101. However, when the Dominion KX IV–101 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 Dominion KX IV–101.

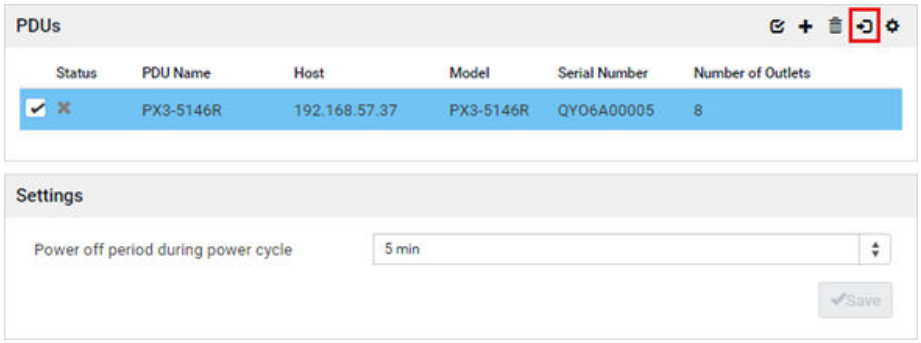
► *To Edit a PDU:*

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 Dominion KX IV–101, 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 Dominion KX IV–101.



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.

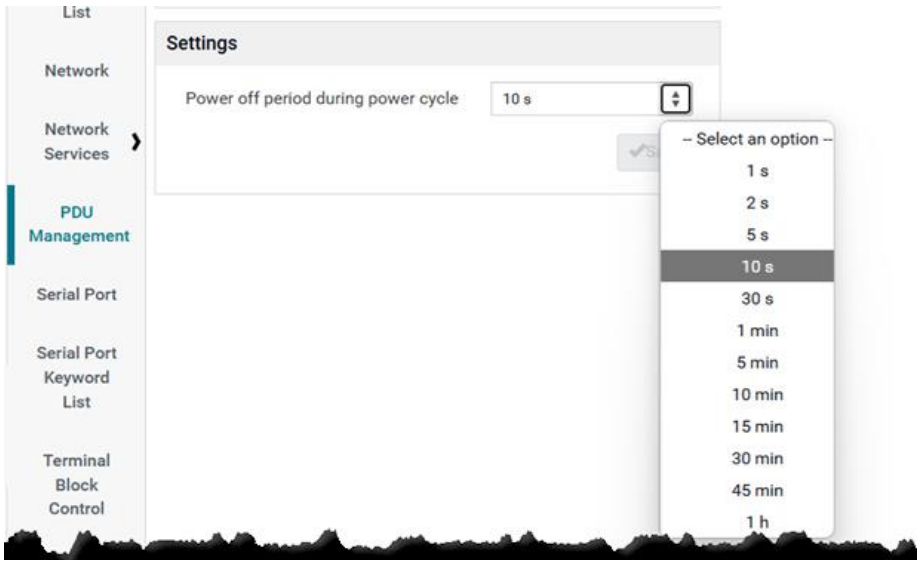
Settings for Power Cycling

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*

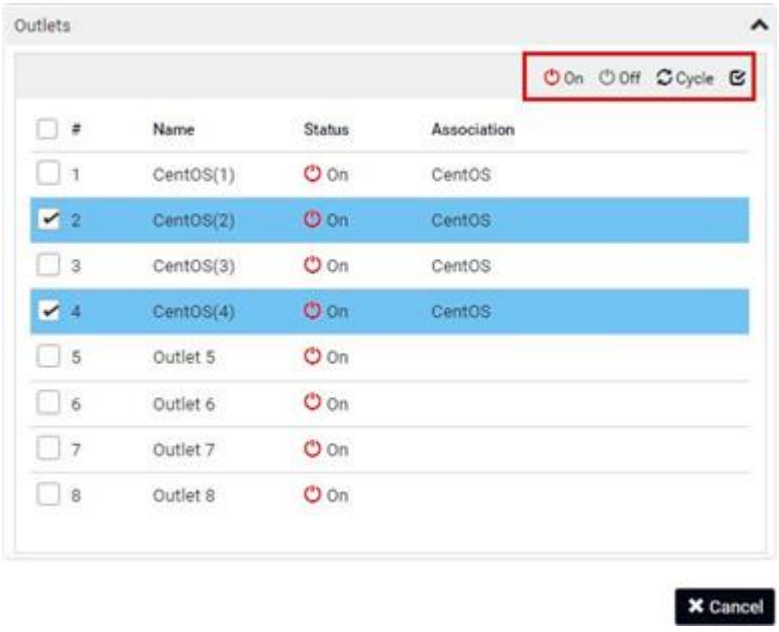
1. Click the Select icon to enable the checkboxes in the PDUs list.
2. Select one or multiple outlets.
3. Click On and then click Switch on to confirm.
4. All selected outlets turn on and show On status.

► *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.

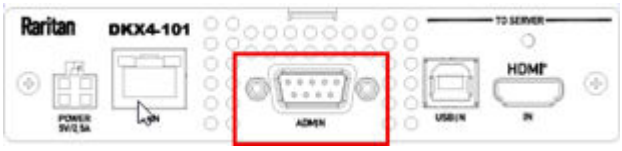
► *Power Cycle*

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.



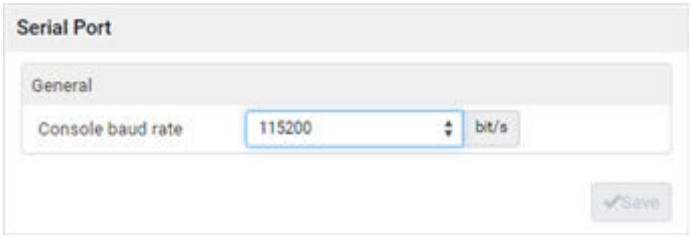
Serial Port

The Serial Port setting controls the baud rate of the Dominion KX IV–101 serial port. Dominion KX IV–101'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

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.

Terminal Block Control

The Terminal Block Control feature allows you to configure an external device that is connected to the terminal block of the Dominion KX IV–101.

The Dominion KX IV–101 has one input terminal and one output terminal.

► *Input Terminal:*

- Two pins
- Supports an external push button or switch input
- Binary switches only
- Use case: turning off remote access when maintenance is being performed on the target

► *Output Terminal:*

- Three pins
- Two relays. One Normally Open (NO), and Normally Closed (NC). Both relays share the same common, so it is preferred to use only one. When using both at the same time, the common must be wired correctly.
- Use cases: performing remote power control of a server via its power button, turning on a light when a remote user is connected, or turning on a door lock or camera.
- Supported output devices: LED, Buzzer, PC Power Button. Output devices must provide their own power.

► *Permissions:*

There are several types of permissions involved in configuring and using terminal block control.

- To configure the terminal block settings, you must have the Terminal Block privilege. See Users and Groups (on page 138). With this privilege, you can access the Device Settings > Terminal Block Control page, which allows you to enable or disable input and output, and set permissions to allow input control for remote and local users, and configure the action of the output control. See procedure below.
- In addition to setting the permissions in the Terminal Block page, you must give all remote and local users Port Access permissions. The KVM Client's External Device menu will be accessible to users with the correct combined permissions. See Users and Groups (on page 138).
- You must enable local port output. The setting Security > KVM Security > Disable Local Port Output will override all other permissions. See KVM Security (on page 187).

► *Terminal Block Control Settings: Input*

1. Click Device Settings > Terminal Block Control.

Input Configuration	
Enable External Input Switch	Enable or disable the input switch.

Input Configuration	
Input State For Access Control	The input state for access control: Open or Closed. Default value is Closed.
Current External Input Switch State	The current state: Open or Closed. Input state allows control of the device access.
Give Remote Console User	Select the access permission for remote console users. • Full Access: Default setting. • Video Only • No Access: No video, keyboard, and mouse activity allowed, VM session terminated, KVM session terminated, Connection to target disallowed.
Give Local Console User	Select the access permission for local console users. • Full Access • Video Only • No Access

2. Click Save.

► *Terminal Block Control Output Settings and Actions:*

1. Click Device Settings > Terminal Block Control.
2. Scroll down for the Output settings and actions.

Output Configuration	
Enable External Device	Enable or disable the external device.

Output Configuration	
External Device State	The external device state is displayed: • On • Off • Blinking
Action	Select the radio button for the output action you want to perform on the external device: • Turn External Device On/Off: Click On or Off. • Pulse External Device: Sends a pulse to the device, either off to on, or on to off. Initial state of pulse can be changed by clicking button "On" and "Off". • Blink External Device: Make sure the blink interval is set as desired. • Turn External Device Based On KVM Port Status: Allows KVM Port Status Association • KVM Port Status Association: Turn On when KVM Port Busy or Connected or Turn On when KVM Port Idle.
Blink/Pulse Interval	Set interval between blinks or pulses in half-seconds. Default is 1. • Blink range: 1-100 half-seconds • Pulse range: 1 - 100 half-seconds

1. Click Save.

Connecting the Terminal Block to a Motherboard

Dominion KX IV–101 can control one external switch, either power SW or reset SW, by connecting the terminal block to the pins on a motherboard of the external device.

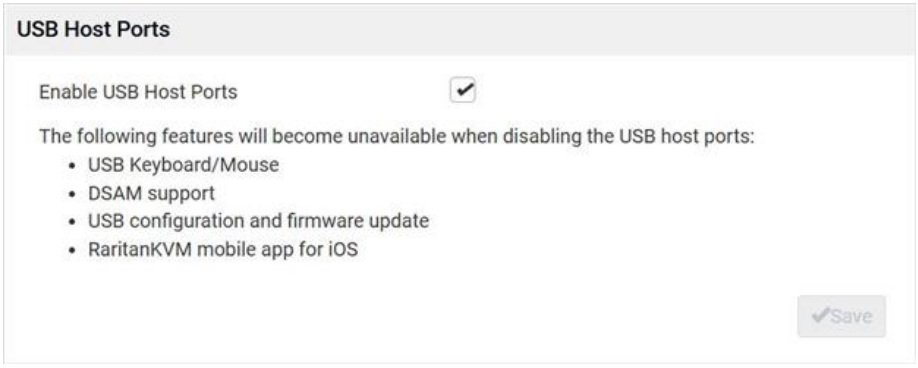
There are power SW and reset SW headers on most motherboards. They are normally connected to the push buttons on the front panel of the case.

- Connect the two pin header to NO(normally open) of the terminal block on the Dominion KX IV–101.

USB Port

USB ports on the device can be enabled or disabled.

Caution: By disabling the USB A ports, you will also lose the keyboard/mouse from the local console.



► *Enable USB Host Ports:*

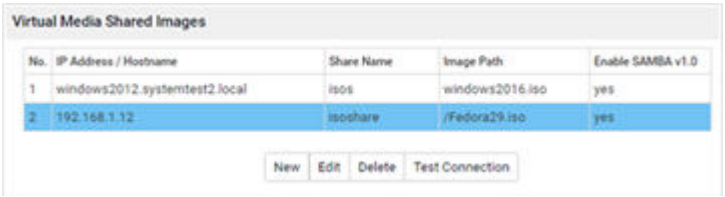
1. Select Device Settings > USB Port
2. Select the check box "Enable USB Host Ports" to enable the USB A ports or
3. Uncheck the check box "Enable USB Host Ports" to disable the USB A ports

When disabled, the following features are unavailable:

- USB Keboard/Mouse
- DSAM Support
- USB configuration and firmware update
- RaritanKVM mobile app for iOS

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, /path0/image0.iso, \path1\image1.iso, and so on.
   - Select the Enable Samba 1.0 checkbox to allow Dominion KX IV–101 to use an older Samba version. When unchecked, Samba 3.0 is used.
4. Click Test Connection to verify.
5. Click Add Shared Image.

Security

In This Chapter

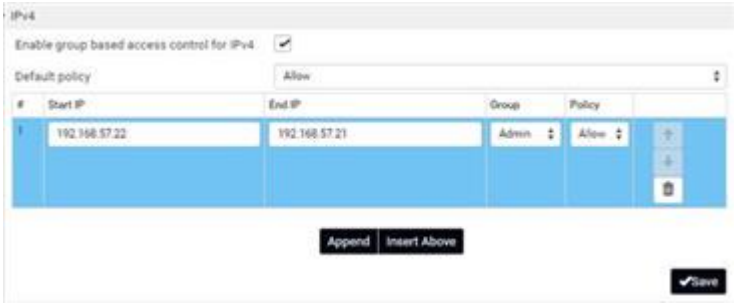
Group Based Access Control

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 Dominion KX IV–101 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 Dominion KX IV–101 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.

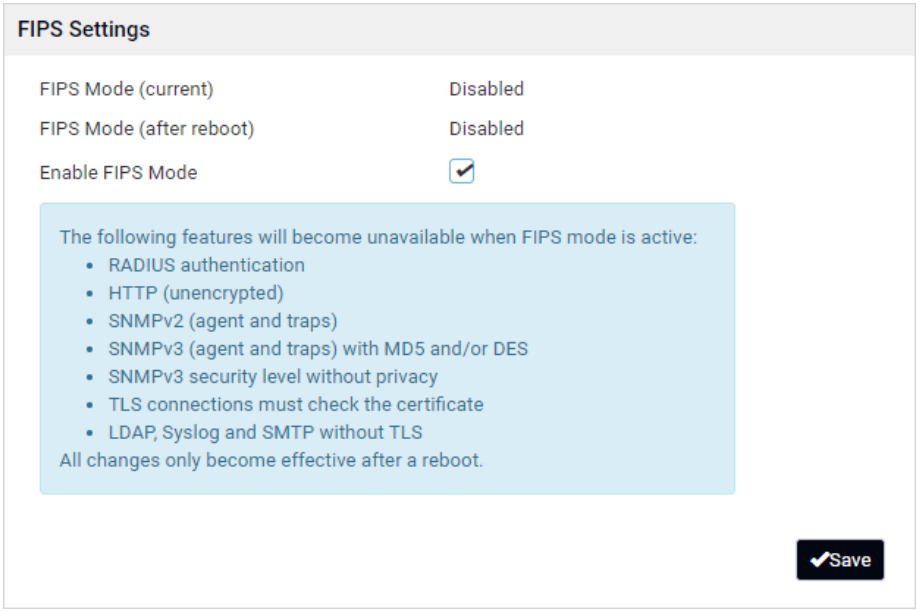
You will utilize FIPS 140-2 approved algorithms for external communications once in FIPS 140-2 mode. The FIPS cryptographic module is used for encryption of session traffic consisting of video, keyboard, mouse, virtual media and smart card data.

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'. The most recently created CSR will be associated internally with the key file.

Note: 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 Dominion KX IV–101.



FIPS 140-2 Support Requirements

The Dominion KX IV–101 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 Dominion KX IV–101, 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 Dominion KX IV–101, 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.

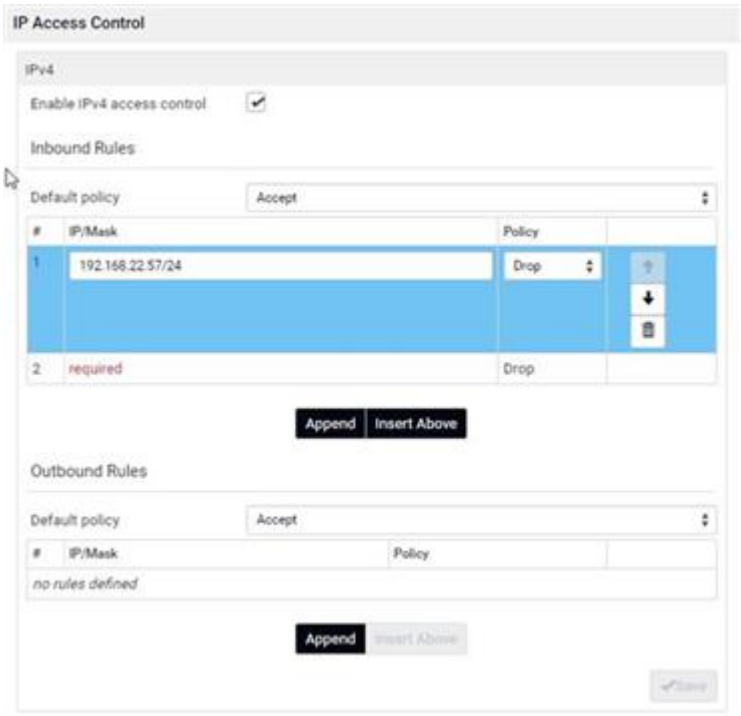
  When typing the IP address, you must specify it in the CIDR notation. That is, BOTH the address and the prefix length are included. For example, to specify a single address with the 32-bit prefix length, use this format:

  x.x.x.x/32

  /32 = 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 Dominion KX IV–101.
   - Outbound rules control the data sent from the Dominion KX IV–101.
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.



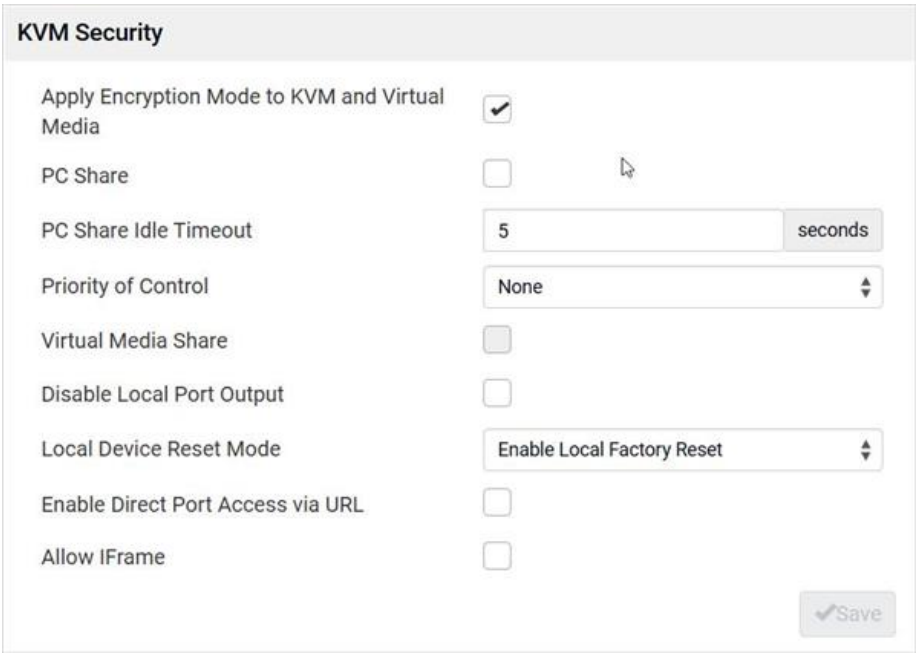
6. Click Save. Note that IPv4 and IPv6 rules are saved separately.

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 Dominion KX IV–101 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 (on page 150).
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. Note: The default is 5 seconds but values can range from 0 to 600 seconds. This value can be updated even if PC Share is not enabled.

Field/setting	Description
Priority of Control	This option assigns the keyboard and mouse priority of control to None, Local User or Remote User. None (Default) - The first user to connect to either the local or remote client has priority of control, until the PC Share Idle Timeout period expires. Once the idle timeout period ends, a different user client session can gain priority of control by using their mouse or keyboard. Local User - The local client will always have priority of control over the remote client. It will re-take control immediately from a remote client session, without having to wait for the PC Share Idle Timeout period to expire. Remote User - The remote client will always have priority of control over the local client. It will re-take control immediately from a local client session, without having to wait for the PC Share Idle Timeout period to expire.
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.
Disable Local Port Output	If you will be using the Terminal Block Control feature, make sure this checkbox is cleared. When Disable Local Port Output is selected, this setting will override all other permissions for terminal block control. See Terminal Block Control (on page 179).
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 Dominion KX IV–101 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 Dominion KX IV–101 in a URL. See Direct Port Access URL (on page 189).
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 Dominion KX IV–101 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 "1".
- 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 Dominion KX IV–101 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 Dominion KX IV–101, 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 Dominion KX IV–101.

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

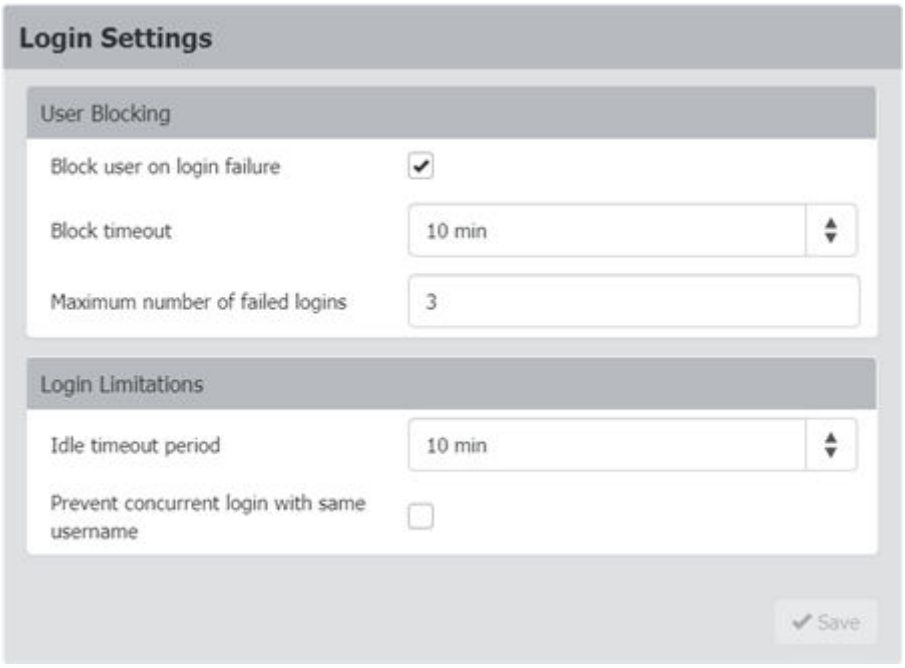
The Login Settings page contains options for user blocking and login limitations.

The default Login Setting is:

- Block user on login failure: Enabled
- Block timeout: 5 minutes
- Maximum number of failed logins: 3

► *To configure login settings:*

1. Click Security > Login Settings.
2. To block users for failed logins, select the Block user on login failure checkbox, then configure the parameters.
   - Block timeout: Select the time period that users with failed logins will be blocked from logging in.
   - Maximum number of failed logins: Enter the number of failed login attempts that users can make before they are blocked.
3. To automatically logout users after an idle period, select a time in the Idle timeout period field. To allow idle users to remain logged in, select "infinite."
4. Select "Prevent concurrent login with same username" to prevent logins by more than one user with the same username. This setting does not apply to the default admin user.



5. Click Save.

Password Policy

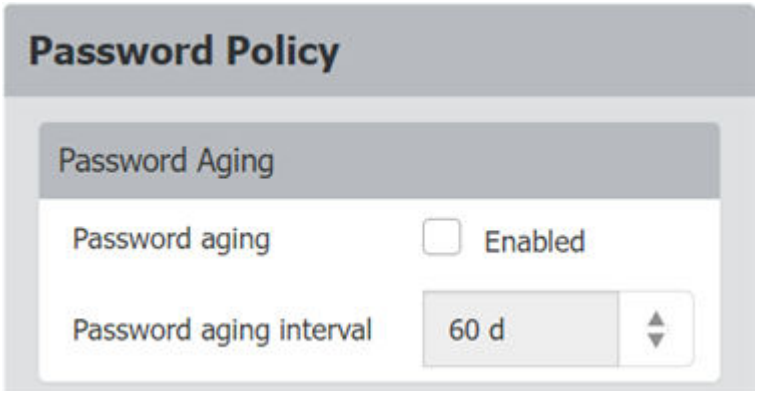
The Password Policy page contains settings for password aging and strong passwords.

The default Password Policy is:

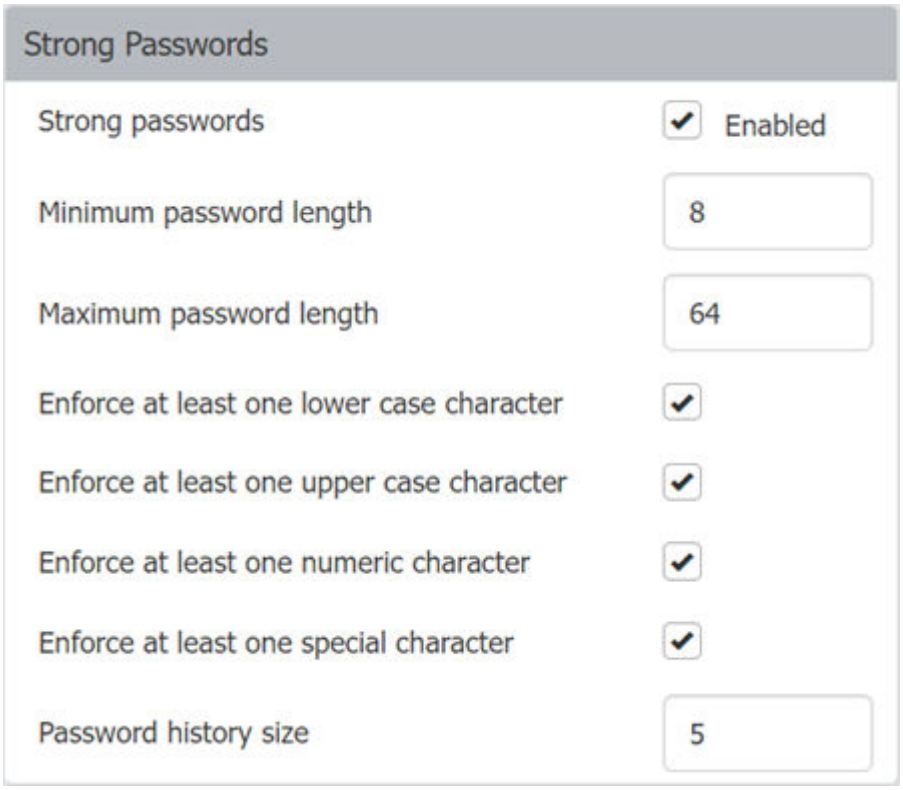
- Password Aging: Disabled
- Strong Passwords: Enabled

► *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.



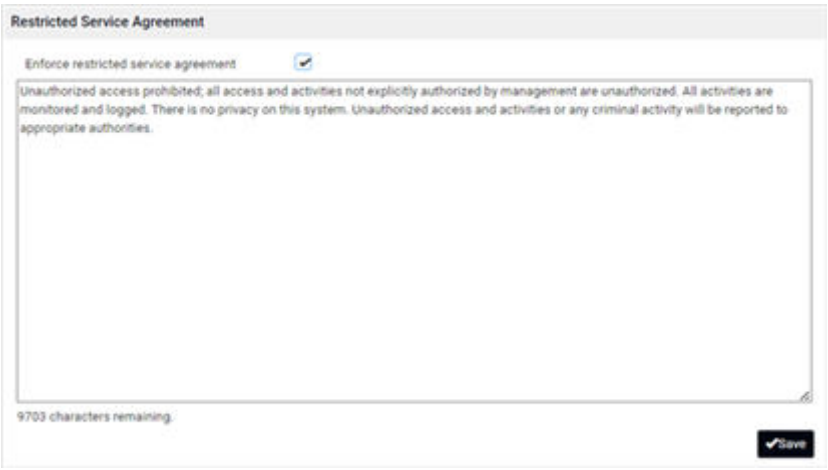
4. Click Save.

Service Agreement

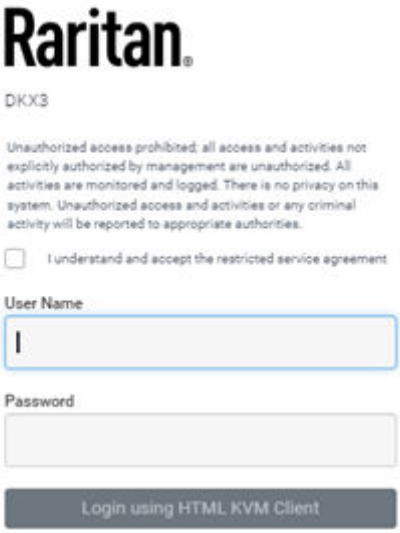
The Service Agreement page allows you to enable an agreement that appears on the login page of the Dominion KX IV–101. Users must select a checkbox on the agreement before logging in.

► *To configure the service agreement:*

1. Click Security > Service Agreement.



2. Select the Enforce Service Agreement checkbox.
3. 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

Dominion KX IV–101 uses TLS 1.3 for any encrypted network traffic between itself and a connected client. When establishing a connection, Dominion KX IV–101 has to identify itself to a client using a cryptographic certificate. The Dominion KX IV–101 contains a default certificate that you should replace with your own.

Dominion KX IV–101 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 Dominion KX IV–101 date/time is set correctly.

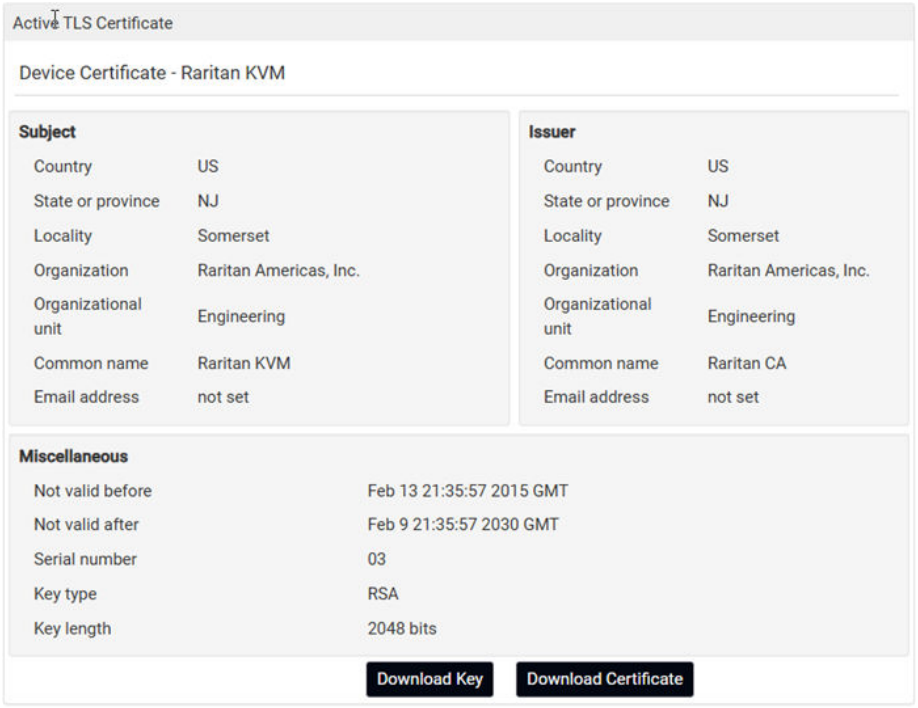
When a self-signed certificate is created, the Dominion KX IV–101 date and time are used to calculate the validity period. If the Dominion KX IV–101 date and time are not accurate, the certificate's valid date range may be incorrect, causing certificate validation to fail. See: Date and Time (on page 152).

Note: The CSR must be generated on the Dominion KX IV–101 or generated separately by CA.

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.

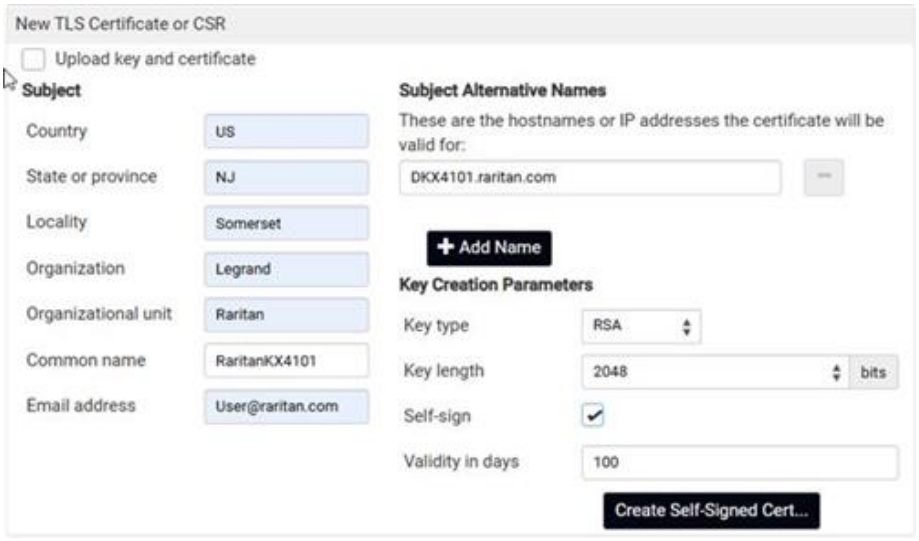
- Organization - The name of the organization to which the Dominion KX IV–101 belongs.
- Organizational unit - This field is used for specifying to which department within an organization the Dominion KX IV–101 belongs.
- Common name - The network name of the Dominion KX IV–101 once it is installed on your network (usually the fully qualified domain name). The common name is identical to the name used to access the Dominion KX IV–101 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 Dominion KX IV–101 is accessed using HTTPS.
- Email address - The email address of a contact person that is responsible for the Dominion KX IV–101 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.

---

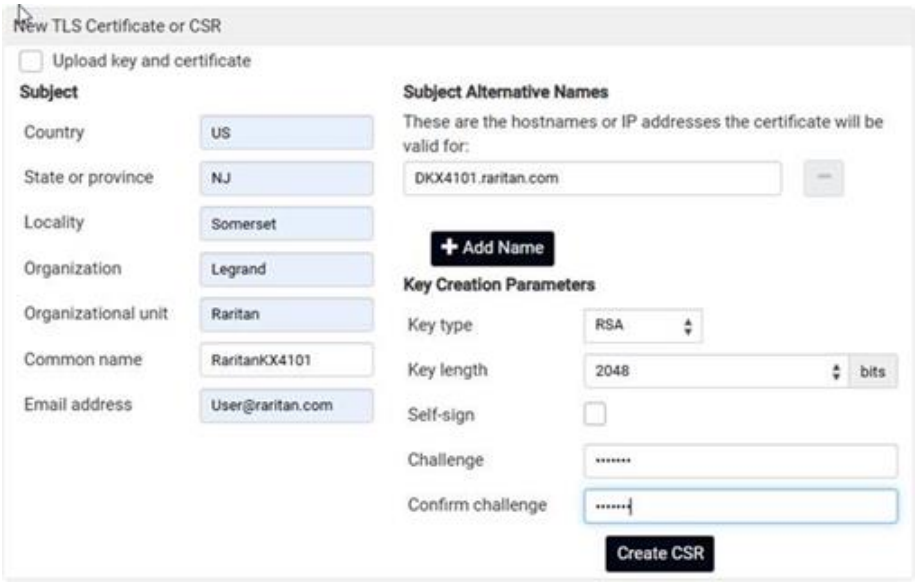
1. To generate self-signed certificate, do the following:
   a. In the Key Creation Parameters, select the Self-Sign checkbox . When you select this option, the Dominion KX IV–101 generates the certificate based on your entries, and acts as the signing certificate authority. The CSR does not need to 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 Dominion KX IV–101 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.

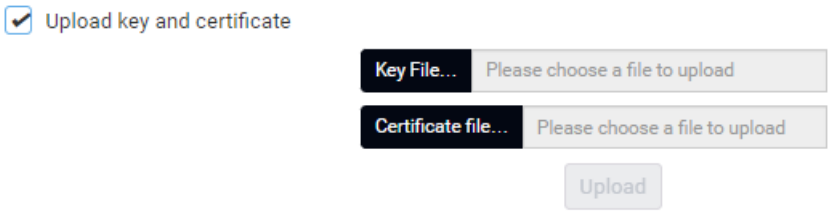
Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.

- Once you get the certificate from the CA, return to this page to upload it to the Dominion KX IV–101. 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

In This Chapter

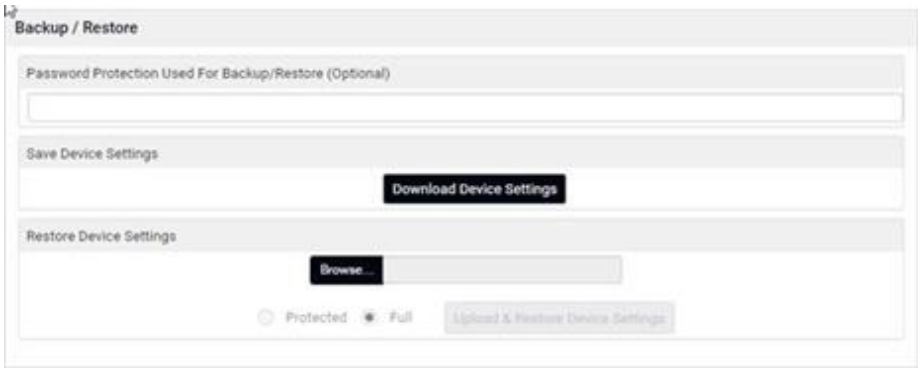
Backup and Restore

You must be a member of the admin group to download a backup file, and to restore a Dominion KX IV–101 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 Dominion KX IV–101 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 Dominion KX IV–101 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.

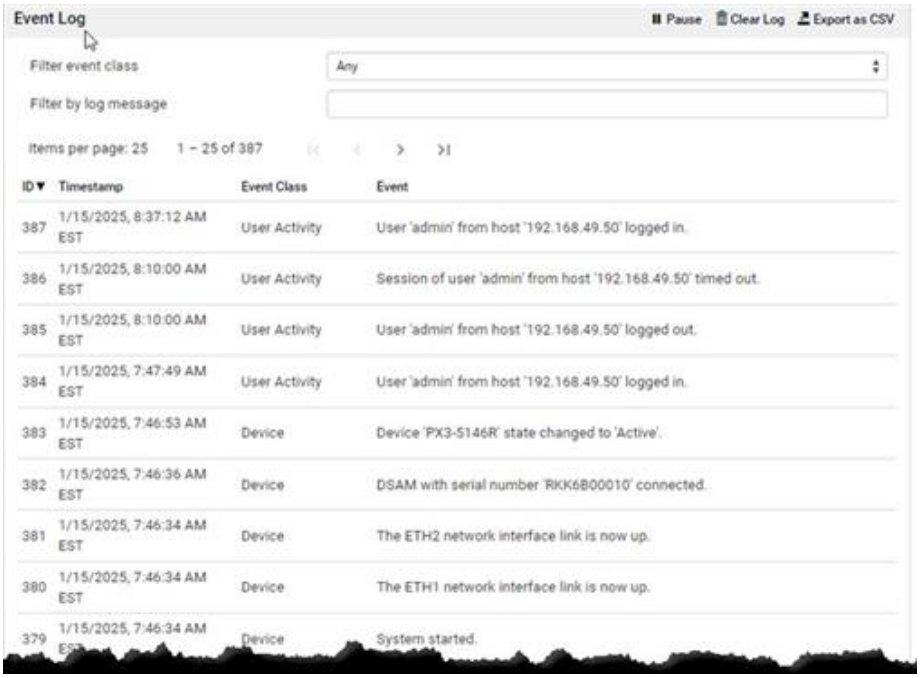
Event Log

The Dominion KX IV–101 captures certain system events and saves them in a local event log.

You can view over 2000 historical events that occurred on the Dominion KX IV–101 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 Dominion KX IV–101 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:*

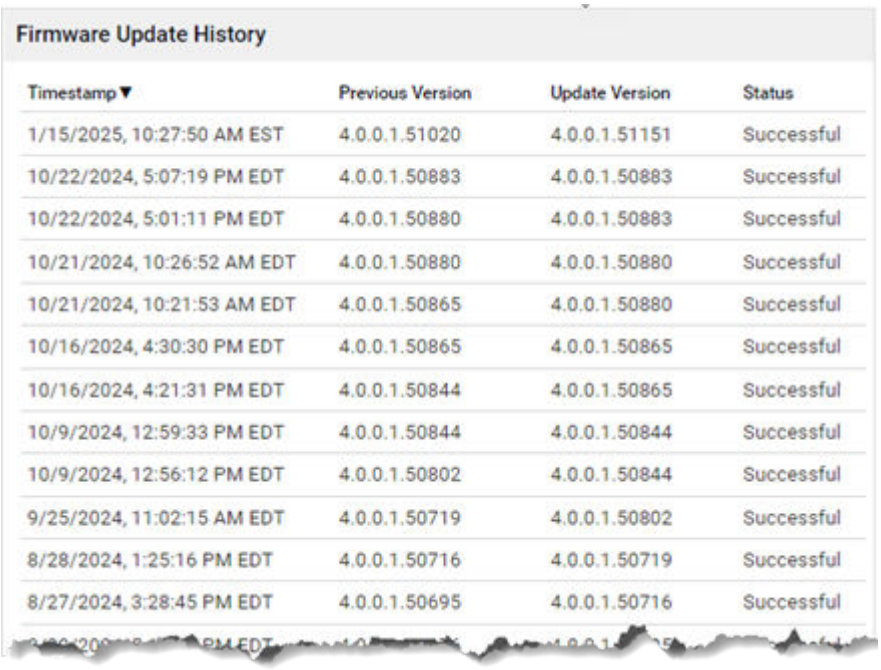
1. Click the Export as CSV icon  on the top right corner.
2. CSV file with event logs downloads to local folder.

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

DSAM Firmware History

The DSAM 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 DSAM firmware update history:*

- Choose Maintenance >DSAM Firmware History.
  Each firmware update event consists of:
  - Update date and time
  - Serial Number
  - Port number where DSAM is connected
  - Previous firmware version
  - Update firmware version
  - Update result

DSAM Firmware Update History

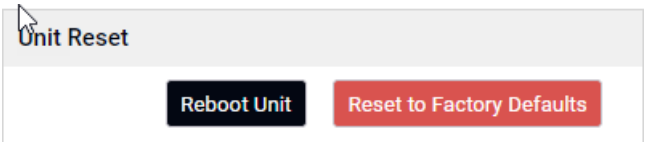
Timestamp ▼	Serial Number	Port	Previous Version	Update Version	Status
8/9/2023, 4:08:15 PM EDT	RKK1200079	2	1.0	1.0	Successful
4/26/2022, 11:46:52 AM EDT	RKJ6B00002	1	1.0	1.0	Successful
4/26/2022, 10:44:05 AM EDT	RKJ6B00002	1	1.0	1.0	Successful
3/8/2022, 12:28:45 PM EST	RKK1200079	2	1.0	1.0	Successful
2/17/2022, 6:19:29 PM EST	RKK1200079	2	1.0	1.0	Successful
11/3/2021, 2:45:27 PM EDT	RKK1200079	1	1.0	1.0	Successful
9/30/2021, 4:14:12 PM EDT	RKK1200079	1	1.0	1.0	Successful
9/29/2021, 11:01:41 AM EDT	RKK1200079	1	1.0	1.0	Successful
7/8/2021, 3:59:45 PM EDT	RKK1200079	1	1.0	1.0	Successful

Note: This option is available only when DSAM is connected to the Dominion KX IV–101.

Unit Reset

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

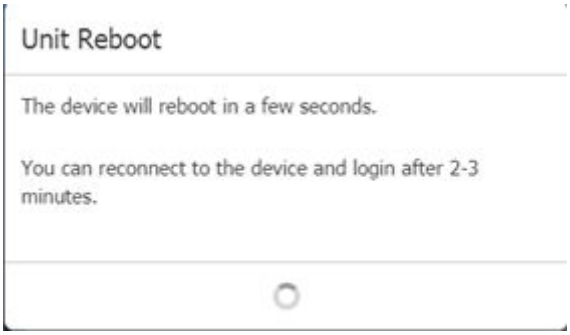
- Reboot Unit: Restarts the Dominion KX IV–101.
- Reset to Factory Defaults: Removes all customized settings and returns the Dominion KX IV–101 to the factory default settings. Requires admin privilege.



► *To reboot the device:*

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

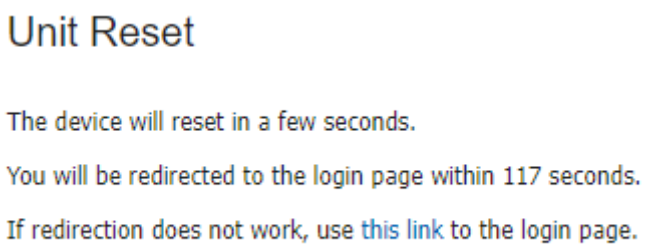
A countdown timer appears.



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 few seconds to complete.
6. When the reset is complete, proceed with initial configuration. See Initial Configuration (on page 12).



► *Other factory reset options:*

- Use the reset button on the Dominion KX IV–101 device. Press the reset button for 5 seconds. Device will reset and reboot.
- Perform the CLI command. See CLI: reset (on page 244)

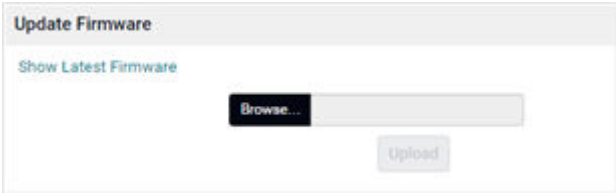
Update Firmware

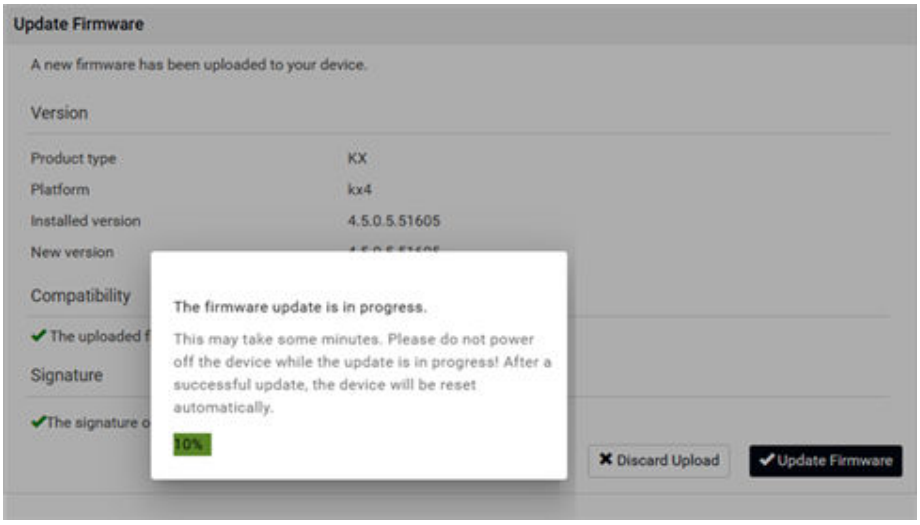
"Show Latest Firmware" link brings up Raritan's Support page: www.raritan.com/support where firmware files are available.

You must have the Maintenance privilege to update the Dominion KX IV–101 firmware.

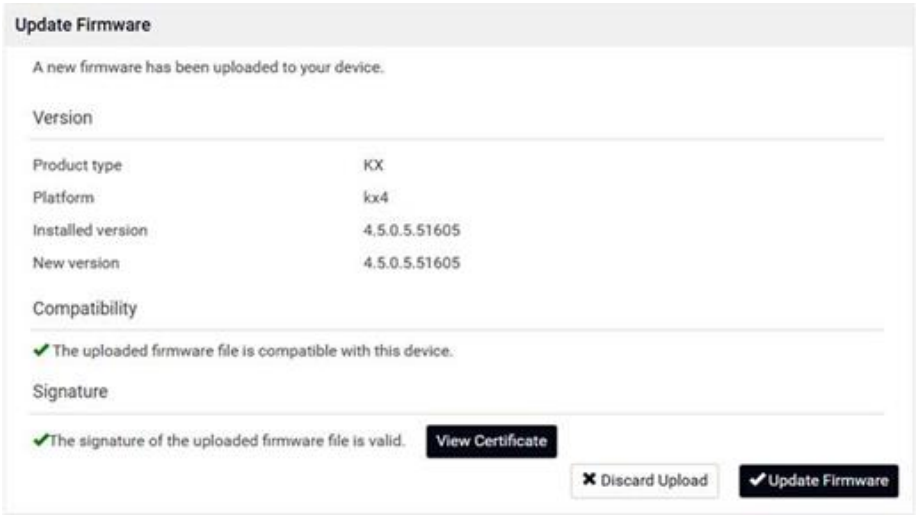
► *To update the firmware:*

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.





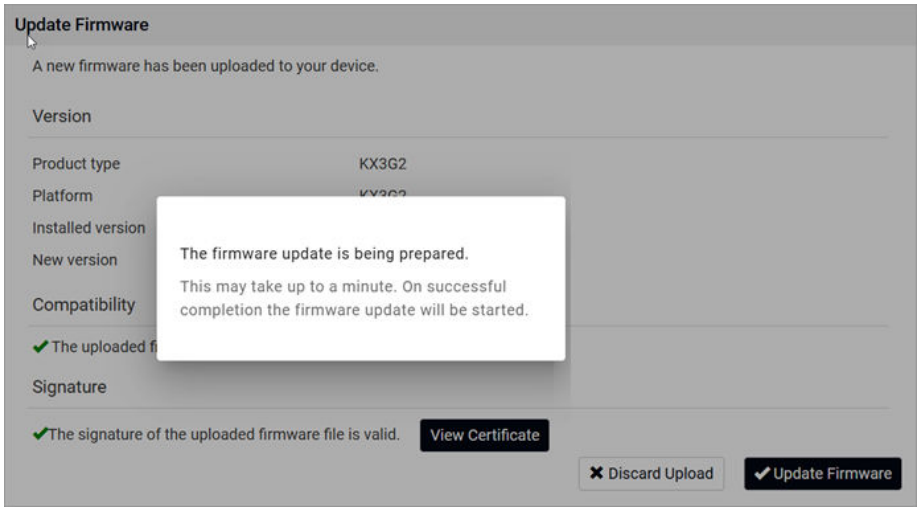
3. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.



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

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

Warning: Do NOT power off the Dominion KX IV–101 during the update. The power LED on the device fast-blinks green during update.



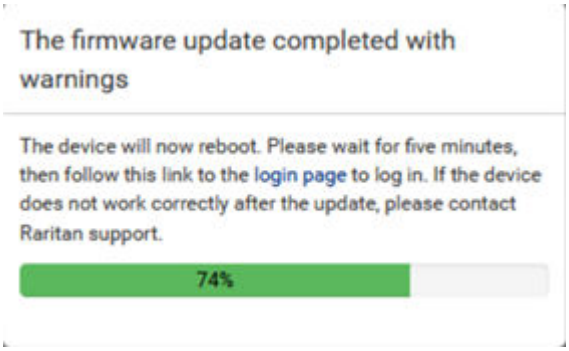
Note: No users can successfully log in during the update. Logged in users are forced to suspend operations.

1. When the update is complete, the Dominion KX IV–101 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 Dominion KX IV–101 again to check the update results.

After Updating: The Dominion KX IV–101 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 (on page 168).

► *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 Dominion KX IV–101. This warning does not indicate any problems or that the update failed.



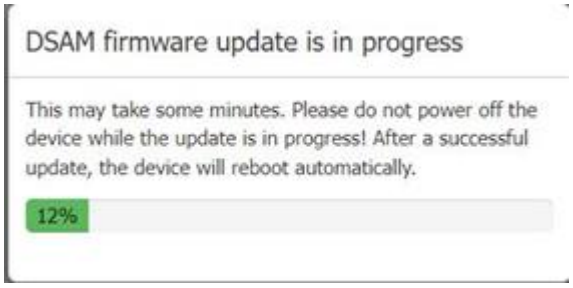
Update DSAM Firmware

You must connect DSAM to the <ProductName. To update the DSAM firmware you must have the Maintenance privilege.

► *To update the DSAM firmware:*

1. Click Maintenance > Update DSAM Firmware.
2. Select the DSAM and click the Update Firmware.

3. Click Update to confirm.
4. DSAM firmware update is being prepared message appears and after that progress bar appears to indicate the update progress.



5. The Dominion KX IV–101 reboots after the completion of DSAM Firmware upgrade.

Update Firmware Using SCP

While updating firmware using SCP, all user management operations are suspended and all login attempts fail.

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

► *To update the firmware via SCP:*

1. Type the following SCP command and press Enter.

```
scp <firmware file> <user name>@<device ip>:/fwupdate
```

   - <firmware file> is the Dominion KX IV–101 firmware's filename. If the firmware file is not in the current directory, you must include the path in the filename.
   - <user name> is the "admin" or any user profile with the Firmware Update permission.
   - <device ip> is the IP address or hostname of the Dominion KX IV–101 where you want to upload the specified file.

2. Type the password when prompted, and press Enter.

The system transmits the specified firmware file to the Dominion KX IV–101, and shows the transmission speed and percentage.

When the transmission is complete, it exits without a message. Dominion KX IV–101 will start to update its firmware after transmission is done successfully.

3. Check the Dominion KX IV–101 web interface for update progress and success message when update is complete.

► *SCP example*

```
scp kx-kx4-040100-47253.rfp admin@192.168.87.50:/fwupdate
```

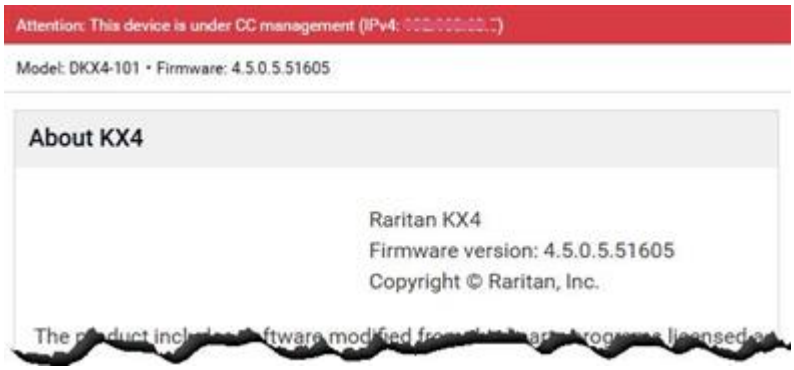
► *Windows PSCP command:*

PSCP in Windows works in a similar way to the SCP.

- `pscp <firmware file> <user name>@<device ip>:/fwupdate`

Stop CC-SG Management

While Dominion KX IV–101 is under CC-SG management, if you try to access the device directly, you are notified that the device is under CC-SG management.

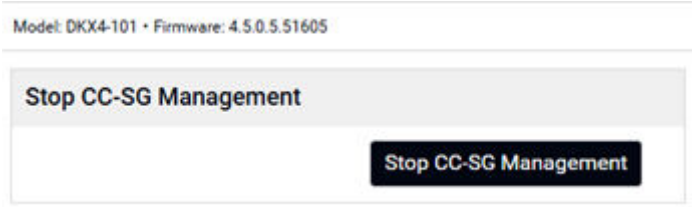


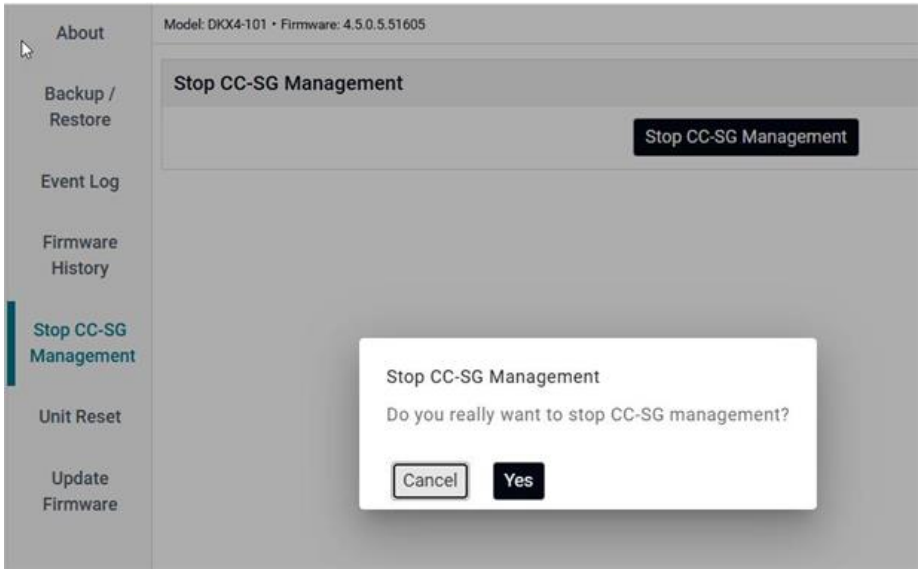
If you are managing Dominion KX IV–101 through CC-SG and connectivity between CC-SG and the Dominion KX IV–101 is lost after the specified timeout interval (typically 10 minutes), you are able to end the CC-SG management session from the Dominion KX IV–101 console.

Note: You must have the appropriate permissions to end CC-SG management of Dominion KX IV–101.

---

1. Click Maintenance > Stop CC-SG Management. A message indicating that the device is being managed by CC-SG will be displayed. An option to remove the device from CC-SG management will also be displayed.





2. Click Yes to begin the process of removing the device from CC-SG management.
3. A confirmation message of "Successfully saved" displays when CC-SG management has ended.

Virtual Media

In This Chapter

Overview

All Dominion KX IV–101 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 Dominion KX IV–101 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

Virtual Media Performance Recommendations

Additional studies of virtual media performance show that KX4-101 virtual media performance can range up to 175 Mbps. This is significantly faster than the KX3 switches (8-10 Mbps).

► *For maximum performance:*

- Turn off encryption. Encryption has a large effect on performance.
- Utilize a high-speed laptop/PC with AKC or VKC KVM Clients.
- Utilize the KX IV User Station (DKX4-UST).

- Writing to a virtual media drive connected to the KVM Client may be slower than reading from the drive.
- There may be performance variations across different USB drives.
- Network performance is also a factor.

Prerequisites for Using Virtual Media

Dominion KX IV–101 Virtual Media Prerequisites

- For users requiring access to virtual media, the Dominion KX IV–101 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 ShareSecurity Settings must also be enabled in the Security Settings page (Optional).
- A USB connection must exist between the CIM and the target server.
- You must choose the correct USB connection settings for the KVM target server you are connecting to.

Client 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.

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 Tasks Via Virtual Media

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

- Transferring files
- Running diagnostics
- Installing or patching applications
- Complete installation of the operating system

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

Supported Virtual Media Types

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

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 (on page 77).

► *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

Appendices

CLI Commands

The Dominion KX IV–101 supports the following categories of commands in the CLI:

check	Check services
clear	Clear logs
config	Enter configuration view
connect	Connect to a target
diag	Enter diagnostics view
exit	Exit CLI session
reset	Reset device
show	Shows various device information

In This Chapter

CLI: check

check

check ntp

CLI: clear

clear

clear eventlog

Do you really want to clear the event log? [y/n]

CLI: config

config

#config

config:#

► *Available commands:*

apply	Save changed settings and leave config mode
authentication	Configure authentication settings
autoscan	Configure auto scan settings
cancel	Discard changed settings and leave config mode
check	Check services
device	Configure Device
group	Configure user groups
keyset	Configure keyset settings
keyword	Configure keyword for DSAM serial ports
network	Configure network settings
password	Change password of currently logged in user
pdu	Configure PDU settings
port	Configure DSAM serial port settings
security	Configure security settings
serial	Configure serial port settings
terminalblock	Configure terminal block settings
time	Configure date/time settings
usbport	Configure usb port 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> <type > <authport> <acctport> <timeout> <retries>

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) (1..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>]

Create a new group

name Group name

privileges Group privileges (one or more (separated by '/') of allowTerminalBlockActionOnly/changePassword/changeTerminalBlockSettings/deviceAccessUnderCcsg/deviceSettings/maintenance/pcShare/portControl:all/portControl:1/portControl:201/portControl:202/portViewOnly:all/portViewOnly:1/portViewOnly:201/portViewOnly:202/portVmROnly:all/portVmROnly:1/portVmRW:all/portVmRW:1/powerControl:all/powerControl:1/powerControl:201/powerControl:202/powerControl:2/powerControl:3/securitySettings/userManagement)

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>] [addRestrictions <addrestricts>] [removeRestrictions <removerestricts>]

Edit a group

name Group name (Admin/KX_Admin/KX_User)

description Group description

addPrivileges Add group privileges (one or more (separated by '/') of allowTerminalBlockActionOnly/changePassword/changeTerminalBlockSettings/deviceAccessUnderCcsg/deviceSettings/maintenance/pcShare/portControl:all/portControl:1/portControl:201/portControl:202/portViewOnly:all/portViewOnly:1/portViewOnly:201/portViewOnly:202/portVmROnly:all/portVmROnly:1/portVmRW:all/portVmRW:1/powerControl:all/powerControl:1/powerControl:201/powerControl:202/powerControl:2/powerControl:3/securitySettings/userManagement)

removePrivileges Remove group privileges (one or more (separated by '/') of allowTerminalBlockActionOnly/changePassword/changeTerminalBlockSettings/deviceAccessUnderCcsg/deviceSettings/maintenance/pcShare/portControl:all/portControl:1/portControl:201/portControl:202/portViewOnly:all/portViewOnly:1/portViewOnly:201/portViewOnly:202/portVmROnly:all/portVmROnly:1/portVmRW:all/portVmRW:1/powerControl:all/powerControl:1/powerControl:201/powerControl:202/powerControl:2/powerControl:3/securitySettings/userManagement)

addRestrictions Add group restrictions (hideClientToolbar)

removeRestrictions Remove group restrictions (hideClientToolbar)

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 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-1/SHA-224/SHA-256/SHA-384/SHA-512)

authPass Authentication pass phrase

privProto Privacy protocol (DES/AES-128/AES-192/AES-256/AES-192-3DES/AES-256-3DES)

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>] [controlPriority <controlPriority>]

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) (0..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)

controlPriority Set control priority (none/local/remote)

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 network

network

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 macclientid [enabled <enabled>]

Configure sending mac as client id to DHCP servers

enabled Enable/disable sending mac as client id to DHCP server (true/false)

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 terminalblock

config:# terminalblock [inputEnable <inputEnable>] [inputRemote <inputRemote>] [inputLocal <inputLocal>] [outputEnable <outputEnable>] [outputAction <outputAction>] [blinkInterval <blinkInterval>]

Configure terminal block settings

inputEnable Enable/Disable input switch (enable/disable)

inputRemote Setup input remote console (fullAccess/videoOnly/noAccess)

inputLocal Setup input local console (fullAccess/videoOnly/noAccess)

outputEnable Enable/Disable output device (enable/disable)

outputAction Setup output action (deviceOff/deviceOn/blinkDevice)

blinkInterval Setup device blink interval(in half-seconds) (1..10)

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 usbport

config:# usbport [enable <enable>]

Configure usb port settings

enable Enable/Disable usb port (true/false)

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: 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: exit

exit

exit

CLI: show

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***
network	***Shows all network information***
pdu	***Shows PDU information***
port	***Shows DSAM serial port parameters***
security	***Shows security settings***
serial	***Shows serial port parameters***
terminalblock	***Shows terminal block settings***
time	***Shows date/time information***
usbport	***Shows usb port settings***
user	***Shows user information***
vmshare	***Shows information about auto virtual media shared images***

show authentication

Authentication type: Local

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 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

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: 4.5.0.5.51605

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 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

Power cycle delay: 10 Seconds

#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

Priority of control: None

SSH DPA: Disabled

show serial

Configured baud rate: 9600 bit/s

Device detection type: Force console

Detected device: Console

show terminalblock

External input switch: Disabled

Input state for access control: Closed

Current external switch state: Open

Give remote console user: Full Access

Give local console user: Full Access

External output device: Disabled

External device state: Disabled

Output action: Turn Device Off

Device blink interval: 1 (half-seconds)

Turn on based on KVM status: busy_connected / idle"

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 usbport

Enable Usb Port: Enabled

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

Appendix A Specifications

Case Dimension:	• 140mm (W) x 144mm (D)x 30mm (H), 5.51” (W) x 5.67 “ (D) x “ 1.18(H)
Weight (excluding power adapter):	• 0.65kg (1.42lb)
Operating Temperature:	• 0 °C -- 55 °C (32 °F --131 °F)
Storage Temperature: -	• 20 °C -- 80 °C (-4 °F --176 °F)
Operating Humidity:	• 20%-80% RH
Storage Humidity:	• 10%-90% RH
Maximum Power Consumption:	• 12.5W under 4K@30 video stream and without local USB device. DKX4-101 can support two USB devices with up to 500mA for each.
Power adapter:	• ATS024T-W050V with different plugs: • Input: Universal 100VAC-240VAC 50/60Hz • Output: 5VDC/4A • C14 Socket • Safety certification: UL / CUL / PSE / BSMI / RCM / GS • EMI: FCC / CE Class B ； Conduction and Radiation Met.
Additional power adapter:	• ATS24T-P050 with C14 socket input. • Input: Universal 100VAC-240VAC 50/60Hz • Output: 5VDC/4A • Plug: US, EU, AU, UK, CN, Korea • Safety certification: UL / CUL / PSE / BSMI / RCM / GS • EMI: FCC / CE Class B ； Conduction and Radiation Met.
Terminal block output:	• Dry contact output supports load with up to 2A/30VDC, or 0.5A/60VDC, or 0.3A/125VAC.
Terminal block input:	• Dry contact input only. Does not support any power input.
Cables and adapters for additional interface support: See D4CBL Adapters (on page 257)	• D4CBL-DP-HDMI • D4CBL-MDP-HDMI • D4CBL-DVI-HDMI • D4CBL-USBC-HDMI • D4CBL-VGA-HDMI
Mounting bracket:	• Includes Bracket "L" KX101 (part number 250-62-3011-00)
Optional mounting hardware:	• Metal Hook DSAM-4 • 1U bracket RACK-KIT-DKX4-101-3 for mounting three DKX4-101 units • Universal HDMI Cable Lock P/N: 254-01-0055-00

In This Chapter

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)

Apple Mac M1 BIOS Access

BIOS access to the MAC M1 is only through the power button. It requires the power button to be pressed for 10 seconds.

It is not possible to access from KVM connections or using shortcuts.

D4CBL Adapters

D4CBL adapters are used for additional interface support. Following are the video resolutions supported by these adapters.

D4CBL-DP-HDMI, D4CBL-MDP-HDMI,and D4CBL-USBC-HDMI: support up to 4K@30 video resolution.

D4CBL-DVI-HDMI: support up to 1920 x 1200 x60 with RB.

D4CBL-VGA-HDMI: support following video resolutions, but not limited to these.

- 800x600 56Hz/60Hz/72Hz/75Hz
- 1024x768 60Hz/70Hz/75Hz
- 1152x864 60Hz/70
- 1280x720 50Hz/60Hz/75Hz
- 1280x768 50Hz/60Hz/75Hz
- 1280x1024 60Hz/72Hz/75Hz
- 1366x768 60Hz
- 1400x1050 60Hz/75Hz
- 1440x900 60Hz/75Hz
- 1600x900 60Hz/75Hz
- 1600x1024 60Hz/75Hz
- 1600x1200 60Hz/65Hz/70Hz/75Hz
- 1680x1050 60Hz/75Hz
- 1920x1080i 50Hz/60Hz
- 1920x1080P 50Hz/60Hz
- 1920x1200x60 with RB0Hz
- 1920x1200x60 with RB

Diagnostics

In This Chapter

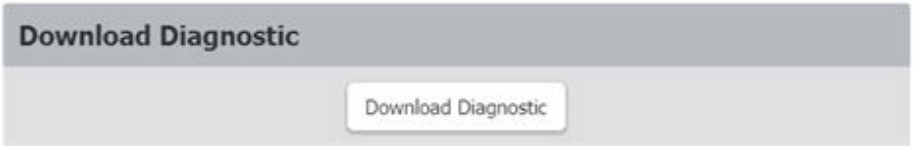
Download Diagnostic

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

You can download a diagnostic file from the Dominion KX IV–101 to a client machine. The file is compressed into a .zip file and should be sent to Raritan Technical Support.

You must be a member of the admin group.

► *To download a diagnostic file:*



1. Click Diagnostics> Download Diagnostic.
2. Click Download Diagnostic, then save the file.
3. Send this file as instructed by Raritan Technical Support.

Network Diagnostics

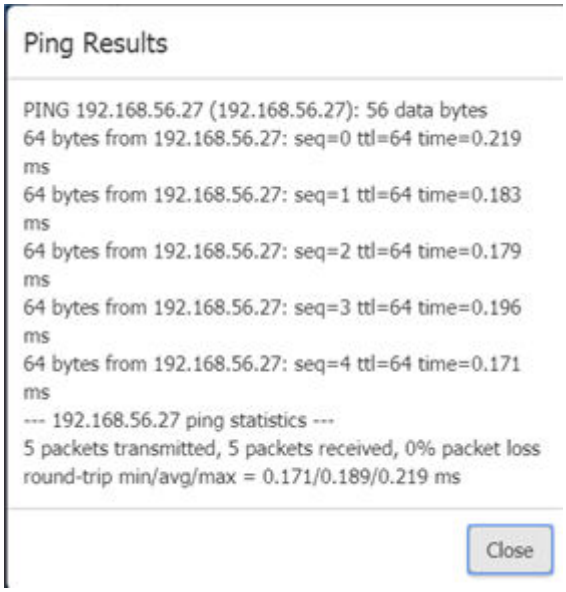
Dominion KX IV–101 provides the following tools to diagnose potential networking issues.

- 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.

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

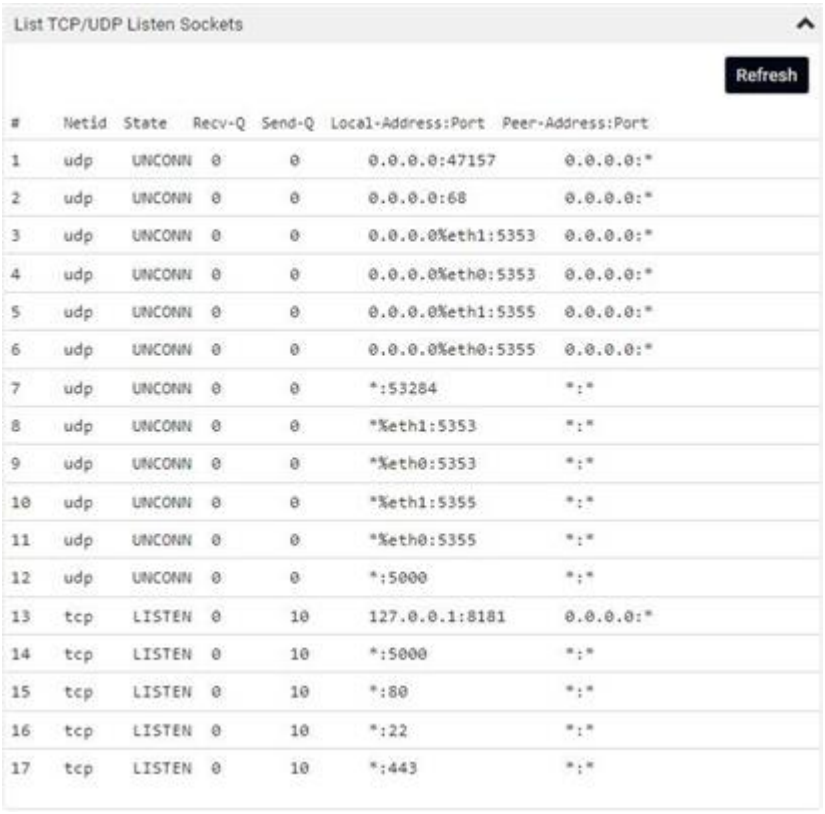
► *List TCP Connections:*

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.



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

Appendix B LDAP Configuration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP 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 AD server
c. Configure LDAP authentication on the device
d. Configure roles on the device

Important: TLS is used 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.

In This Chapter

Configure User Groups on the AD Server

You must create the groups for the Dominion KX IV–101 on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups for the Dominion KX IV–101 are named *KX_Admin* and *KX_User*. See Configure Group on the Dominion KX IV–101 (on page 128).
- User accounts *kxuser, kxuser2*, *usera* and *userb* already exist on the AD server.

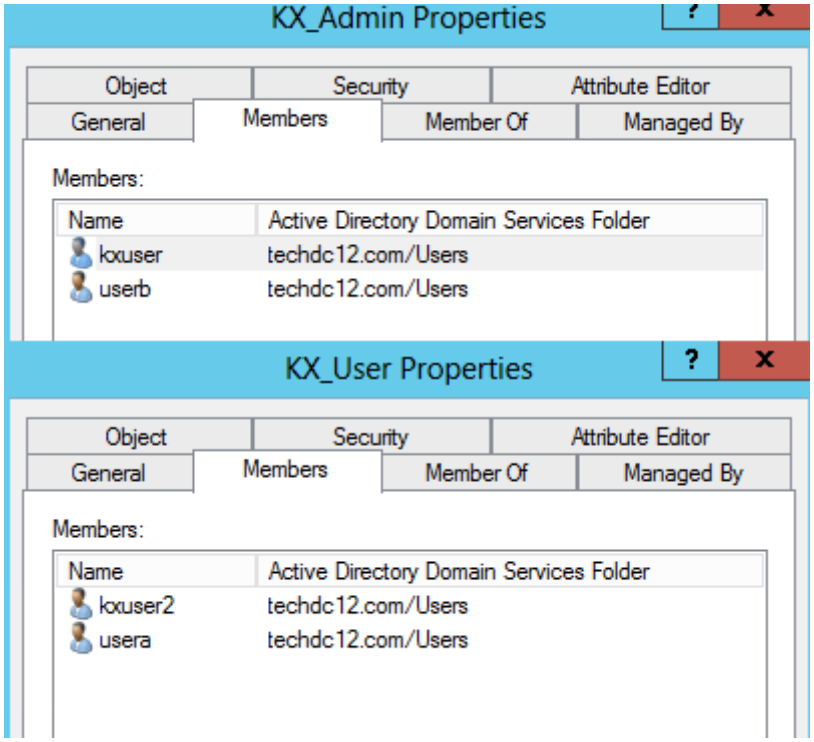
► *To configure user groups on the AD server:*

1. On the AD server, create new groups -- *KX_Admin* and *KX_User*.

Note: Refer to the documentation or online help accompanying Microsoft AD for detailed instructions.

---

2. Add the *kxuser2* and *usera* accounts to the KX_User group.
3. Add the *kxuser* and *userb* accounts to the KX_Admin group.
4. Verify whether each group comprises correct users.


KX_Admin Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
kxuser
techdc12.com/Users
userb
techdc12.com/Users
KX_User Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
kxuser2
techdc12.com/Users
usera
techdc12.com/Users

Appendix C Reserving IP Addresses in DHCP Servers

Dominion KX IV–101 uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the Dominion KX IV–101 in a DHCP server, use the Dominion KX IV–101 device's serial number as the unique ID instead of the MAC address.

Since all network interfaces can be simultaneously enabled and configured with diverse static IP addresses, the client identifier of each network interface is different. The main difference is the absence/presence of a suffix, which is the interface name added to the end of the serial number. The table below lists the client identifiers of all network interfaces.

Interface	Client identifier
ETH1	serial number
ETH2	serial number plus the uppercase suffix "-ETH2"
WIRELESS	serial number plus the uppercase suffix "-WIRELESS"
BRIDGE	serial number

You can reserve the IP addresses of more than one interfaces in the DHCP server if preferred. Note that you must choose/configure the bridge interface if your device is set to the bridging mode.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

In This Chapter

Reserving IP in Windows

To reserve the IP address of any network interface in the Windows DHCP server, you must convert that interface's client identifier into *hexadecimal* ASCII codes.

In the following illustration, it is assumed that the serial number is PEG1A00003.

► *Windows IP address reservation illustration:*

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-ETH2 = 50 45 47 31 41 30 30 30 30 33 2D 45 54 48 32 • The suffix comprising the dash symbol and the word "ETH2" is also converted.

Interface	Client identifier conversion
WIRELESS	PEG1A00003-WIRELESS = 50 45 47 31 41 30 30 30 30 33 2D 57 49 52 45 4C 45 53 53 • The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. In your DHCP server, go to the New Reservation dialog, and enter the converted ASCII codes without spaces.

For example, to reserve the ETH1 interface's IP address, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. 5045473141303030303033
Other fields	Configure as needed.

Reserving IP in Linux

There are two methods to reserve the IP address of any network interface in the standard Linux DHCP server (ISC DHCP server):

- Convert an interface's client identifier into *hexadecimal* ASCII codes.
- Use an interface's original client identifier without converting it into ASCII codes.

In the following illustrations, it is assumed that the Dominion KX IV–101 serial number is PEG1A00003, and the IP address you want to reserve is 192.168.20.1.

► *Illustration with ASCII code conversion:*

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-ETH2 = 50 45 47 31 41 30 30 30 30 33 2D 45 54 48 32 • The suffix comprising the dash symbol and the word "ETH2" is also converted.
WIRELESS	PEG1A00003-WIRELESS = 50 45 47 31 41 30 30 30 30 33 2D 57 49 52 45 4C 45 53 53 • The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. Separate the converted ASCII codes with a colon, and a prefix "00:" must be added to the beginning of the converted codes.

For example, the *converted* client identifier of the ETH1 interface looks like the following:

`00:50:45:47:31:41:30:30:30:30:33`

3. Now enter the converted client identifier with the following syntax.

```
host mypx {
option dhcp-client-identifier = 00:50:45:47:31:41:30:30:30:30:33;
fixed-address 192.168.20.1;
}
```

► *Illustration without ASCII code conversion:*

1. Use the original client identifier of the desired network interface. DO NOT convert them into ASCII codes.
2. A prefix "\000" must be added to the beginning of the client identifier.

For example, the client identifier of the ETH1 interface looks like the following:

`\000`PEG1A00003

3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

```
host mypx {
option dhcp-client-identifier = "\000PEG1A00003";
fixed-address 192.168.20.1;
}
```

Appendix D Third Party Licenses

This appendix contains third party licenses for software used by Dominion KX IV–101 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

Copyright (c) 2021 Google LLC.

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/common

MIT

@angular/core

MIT

@angular/forms

MIT

@angular/material

MIT

The MIT License

Copyright (c) 2021 Google LLC.

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/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

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2013, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 10: Lennart Poettering copyright notice (BSD-like) -----

Copyright 2010 Lennart Poettering

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Part 11: IETF copyright notice (BSD) -----

Copyright (c) 2013 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Internet Society, IETF or IETF Trust, nor the names of specific contributors, may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 12: Arista Networks copyright notice (BSD) ----

Copyright (c) 2013, Arista Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Arista Networks, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 13: VMware, Inc. copyright notice (BSD) -----

Copyright (c) 2016, VMware, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of VMware, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 14: USC/Information Sciences Institute copyright notice (BSD) -----

Copyright (c) 2017-2018, Information Sciences Institute

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Information Sciences Institue nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - WPA Supplicant and Hostapd

Copyright (c) 2002-2019, Jouni Malinen <j@w1.fi> and contributors

All Rights Reserved.

These programs are licensed under the BSD license (the one with advertisement clause removed).

If you are submitting changes to the project, please see CONTRIBUTIONS file for more instructions.

This package may include either wpa_supplicant, hostapd, or both. See README file respective subdirectories (wpa_supplicant/README or hostapd/README) for more details.

Source code files were moved around in v0.6.x releases and compared to earlier releases, the programs are now built by first going to a subdirectory (wpa_supplicant or hostapd) and creating build configuration (.config) and running 'make' there (for Linux/BSD/cygwin builds).

License

This software may be distributed, used, and modified under the terms of BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V