Dominion KX IV-101

User Guide

Release 4.0.0

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

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

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

Contents

Chapter 4   User Management   61

Chapter 5   Device Settings and Information   76

Chapter 1   Installation and Initial Configuration

In This Chapter

Supported Browsers

- Chrome 71, 72, 73
- Edge 42
- Firefox 65, 66
- Internet Explorer 11
- Safari 12

See the Release Notes for more details on 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 locking power cord
- 1 HDMI cable
- 1 USB-B to USB-A cable
- 1 mounting bracket kit

Front View
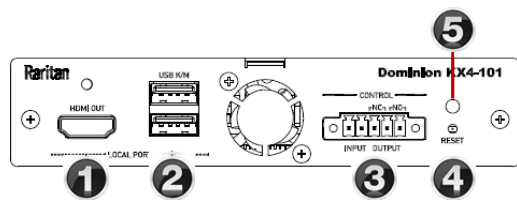
① Local Port HDMI Out to local port monitor

② Local Port USB K/M

③ Input/Output

④ Reset

5 Power Status LED:
- Green ON: Power on
- Green BLINKING: Remote target connection

·

Rear View
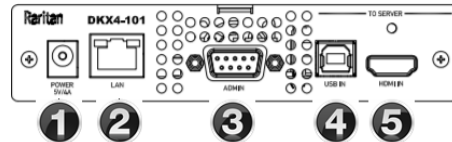
1 Power 5V/4A from power adapter

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
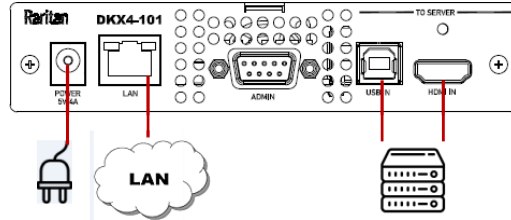
▶ **Connect the Dominion KX IV–101 to the network:**

- 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:**

- Connect the power adapter to the Dominion KX IV–101 with the arrow facing up. Push in firmly and twist clockwise to lock. Check to ensure it is locked.
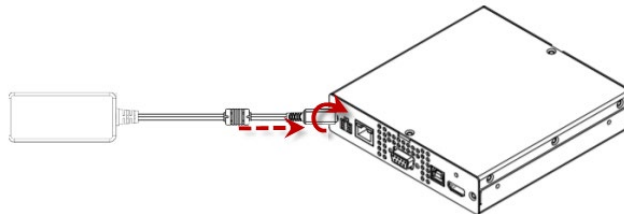
Power on all devices.

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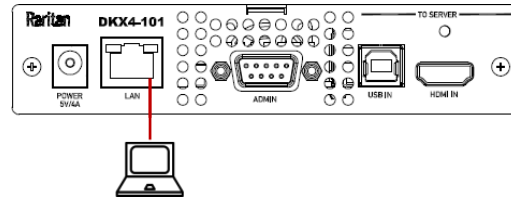
- Disable the wireless interface of the PC.
- Connect a network cable between the PC and Dominion KX IV–101 LAN port.
- Open a browser. Enter the URL "https://kvm.local". The login page appears.
- Follow the prompts to change the default password.

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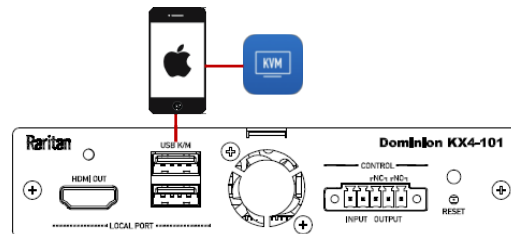
- Launch the Raritan KVM app on an iOS device.
- Connect the iOS device with the Raritan KVM app to the Dominion KX IV–101 USB port.
- Wait until the app detects the connected Dominion KX IV–101.
- Follow the prompts to change the default password.

Option 3: Serial configuration
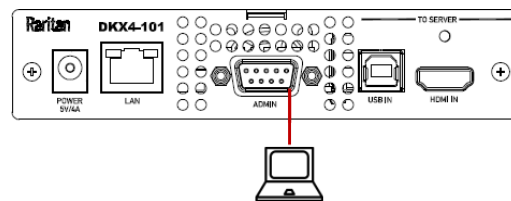
- Connect a DB9 serial cable or USB-Serial adapter between the PC and the Dominion KX IV–101 serial Admin port.
- Serial console configuration: (default) 115200bps/None/8bits/1stop
- To find the default DHCP IP address, use the "show" command to "show network".
- For help with all commands, see *CLI Commands* (on page 119).

Next Steps

- Configure network settings: See *Network* (on page 85)
- Configure time settings: See *Date and Time* (on page 78)
- Install certificates: See *SSL Certificate* (on page 105)
- Configure users: See *User Management* (on page 61)
- Configure port settings: *Port Configuration: KVM Port Settings* (on page 9)

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.
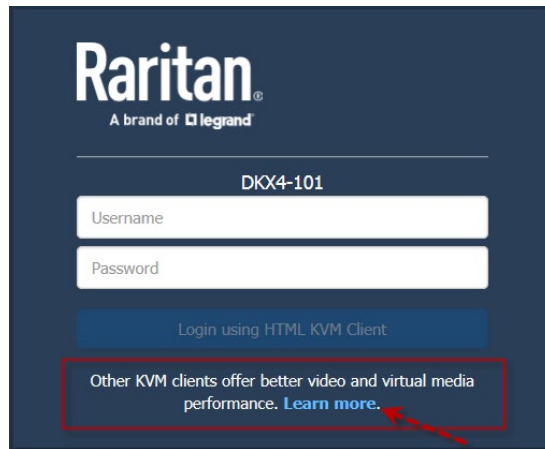
- The **Learn more** link launches a client options dialog. Click the provided links to launch a different client.
  - https://<IP address> launches HKC
  - https://<IP address>/akc launches AKC

- https://<IP address>/vkcs launches VKC

KX4-101 Client Options

Three different clients are available to launch KVM sessions or administer your device, each with its own benefits. Note that you must log into each client separately.

Client Name	How to Launch	Notes
HTML KVM Client (HKC)	On any browser, including mobile, go to **https://192.168.56.27**	This is what you're running now. Quickest and easiest to log into, but video performance and virtual media functionality are limited.
Active KVM Client (AKC)	On Windows, using Microsoft Edge™ Internet Explorer™ 11, or another browser with ClickOnce plug-in, go to **https://192.168.56.27/akc**	Recommended high-performance client for Windows. AKC will load and launch automatically when the link is clicked.
Virtual KVM Client Standalone (VKCS)	On any system with Java 1.8, go to **https://192.168.56.27/vkcs**	Recommended high-performance client for Mac and Linux. After clicking link, VKCS will download. If browser does not do it automatically, click the downloaded .jnlp file (or ctrl-click on Mac) to launch.

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 **SSL Certificate** *(on page 105) for help installing certificates that prevent these warnings.*

For more details and instructions for using all clients, see *KVM Clients* (on page 12).

Chapter 2   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 12).

Port Configuration: KVM Port Settings

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

▶ **To access all port configuration:**

- Click Port Configuration.
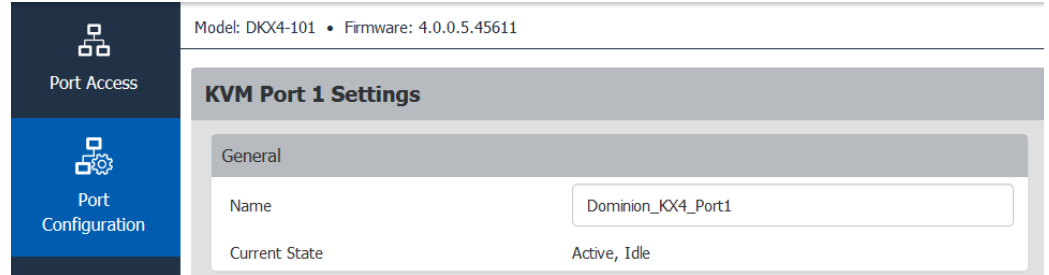
▶ **KVM Port Settings:**

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 100).
    - 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.

- 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.

- 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.

- Click Save to apply the settings.
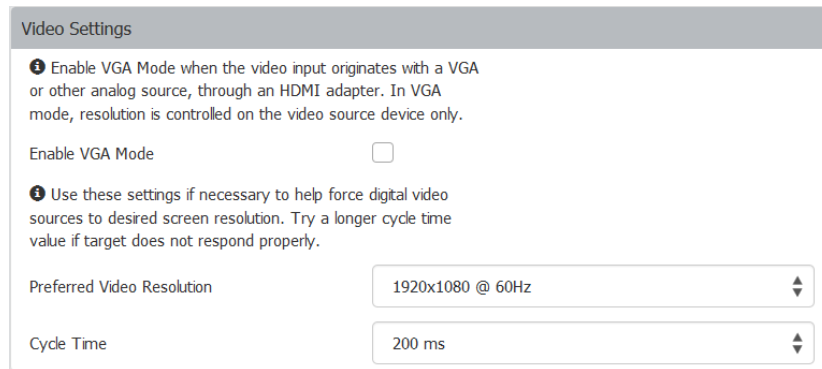
Port Configuration: USB Connection Settings

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:

  - Enable Absolute Mouse - Disable if the target does not support absolute mouse mode

  - 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.

- Click Save.

USB Connection Settings

Basic	
Enable Absolute Mouse	☑
Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices	☐
Enumerate virtual media first before keyboard and mouse	☐

- 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.

Advanced	
Virtual Media Interface #1 Type	CD-ROM ⏶⏷
Remove Unused VM Interface #1 From Device Configuration	☐
Virtual Media Interface #2 Type	Removable Disk ⏶⏷
Remove Unused VM Interface #2 From Device Configuration	☐

Raritan.
A brand of **legrand**

Chapter 3   KVM Clients

KVM Client	Name	Platforms	Features
Active KVM Client	**AKC**	▪ Windows ▪ Requires Microsoft .NET	▪ Full-featured KVM Client ▪ Java-Free
Virtual KVM Client	**VKC**	▪ Linux ▪ Mac ▪ Windows	▪ Full-featured KVM Client ▪ Requires Java
HTML KVM Client	**HKC**	▪ Linux ▪ Mac ▪ Windows ▪ HTML and Javascript	▪ Not all features are supported. ▪ See HTML KVM Client (HKC) Help for supported features. ▪ Java-Free

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

In This Chapter

Virtual KVM Client (VKCS) Help

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

Java Requirements

- Java 1.8.0_191 or higher required
- If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

▶ **VKCS Launching:**

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

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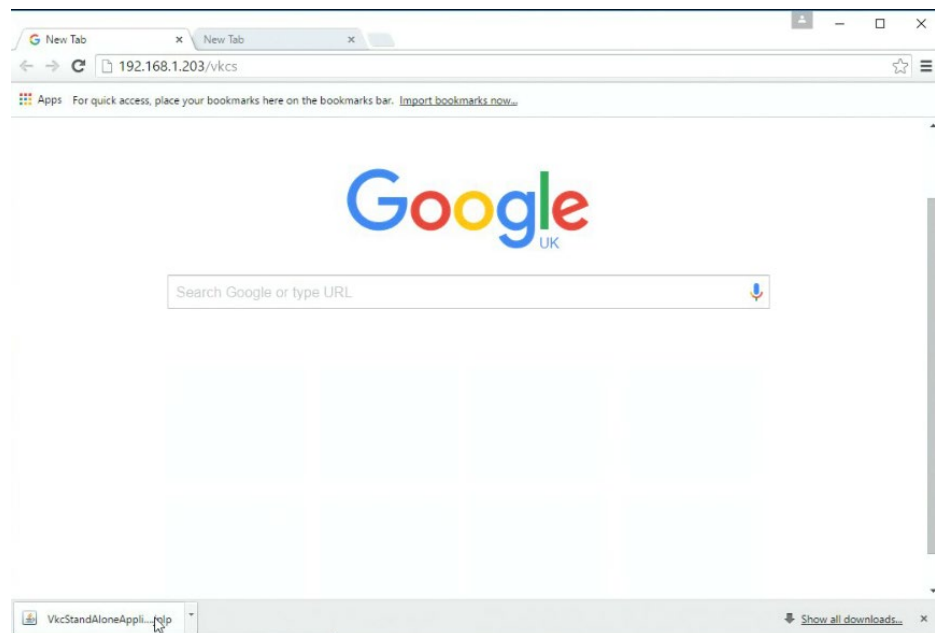
- Edge: You must click Open at the bottom of the browser to launch.
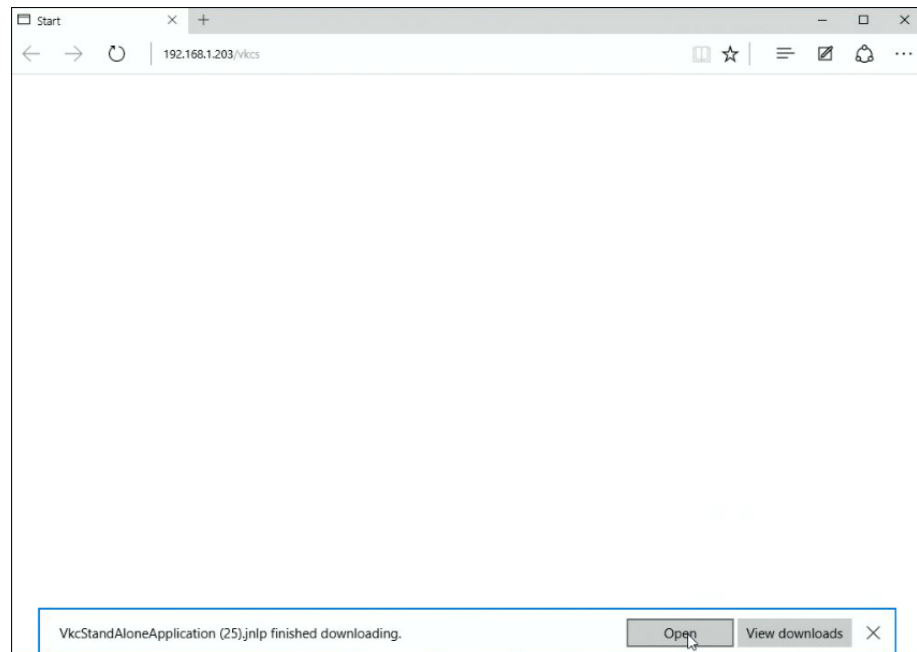
- Internet Explorer: Launches automatically.
- Firefox: Use the option "Do this automatically for files like this from now on", when the vkcs.jnlp file downloads, and it will launch automatically in future.

Proxy Server Configuration

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. Not supported for resolutions above 1920x1200, so for those resolutions color subsampling will automatically drop down to 4:2:2.
- 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".

Raritan.
A brand of legrand

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 15).

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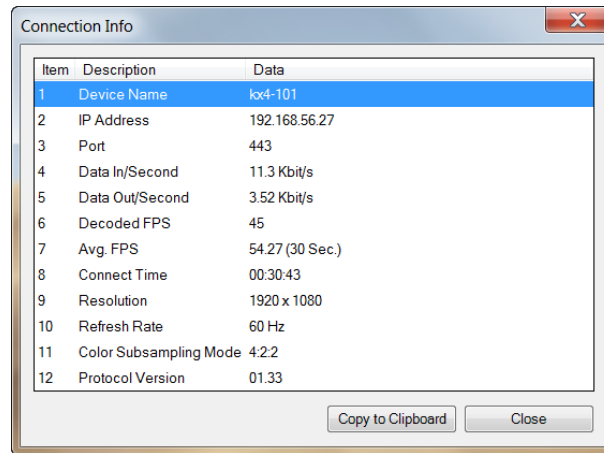
Keyboard

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. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target.

    Note: Non-English characters are not supported by the Send Text to Target function.

3. If the target uses a US/International keyboard layout, select the "Target system is set to the US/International keyboard layout" checkbox.
4. Click OK.

Keyboard Macros

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

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

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

Build a New Macro

▶ **To build a macro:**

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

For example, create a macro to close a window by selecting Left Ctrl + Esc. This appears in the Macro Sequence box as follows:

Press Left Alt

Press F4

Esc

Release F4

Esc

Release Left Alt

6. Review the Macro Sequence field to be sure the macro sequence is defined correctly.

    a. To remove a step in the sequence, select it and click Remove.

    b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.

7. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.

8. Click Close to close the Keyboard Macros dialog. The macro now appears on the Keyboard menu in the application.

9. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.

Importing and Exporting Macros

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

Import Macros

▶ **To import macros:**

1. Choose Keyboard > Import Keyboard Macros to open the Import Macros dialog. Browse to the folder location of the macro file.

2. Click on the macro file and click Open to import the macro.

    a. If too many macros are found in the file, an error message is displayed and the import terminates once OK is selected.

    b. If the import fails, an error dialog appears and a message regarding why the import failed is displayed. Select OK to continue the import without importing the macros that cannot be imported.

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

4. Click OK to begin the import.

   a. If a duplicate macro is found, the Import Macros dialog appears. Do one of the following:

- Click Yes to replace the existing macro with the imported version.

- Click Yes to All to replace the currently selected and any other duplicate macros that are found.

- Click No to keep the original macro and proceed to the next macro

- Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are skipped as well.

- Click Cancel to stop the import.

- Alternatively, click Rename to rename the macro and import it. If Rename is selected, the Rename Macro dialog appears. Enter a new name for the macro in the field and click OK. The dialog closes and the process proceeds. If the name that is entered is a duplicate of a macro, an alert appears and you are required to enter another name for the macro.

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

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

Export Macros

1. Choose Tools > Export Macros to open the Select Keyboard Macros to Export dialog.
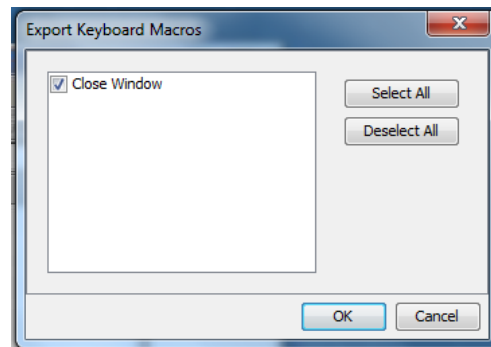
2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.

3. Click Ok. An "Export Keyboard Macros to" dialog is displayed. Locate and select the macro file. By default, the macro exists on your desktop.

4. Select the folder to save the macro file to, enter a name for the file and click Save. If the macro already exists, you receive an alert message.

5. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.

Video Properties

Refreshing the Screen

The Refresh Screen command forces a refresh of the video screen

- Choose Video > Refresh Screen, or click the Refresh Screen button ![refresh icon] 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 ![camera icon] 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.

Single Mouse Mode

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

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

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

- Choose Mouse > Single Mouse Cursor.

- Click the Single/Double Mouse Cursor button ⬉ in the toolbar.
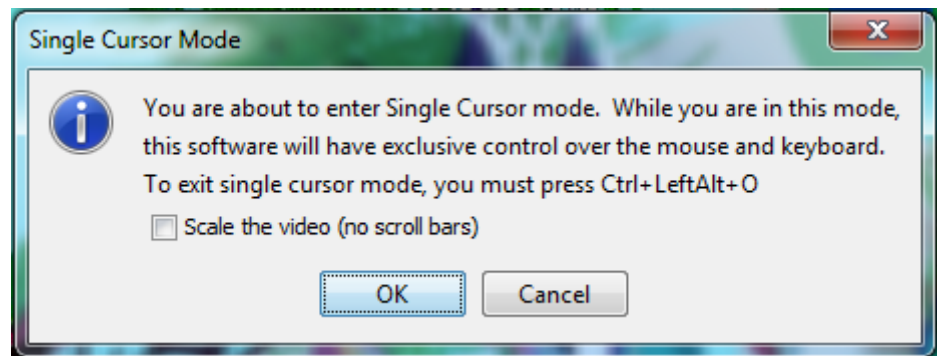
▶ **To exit single mouse mode:**

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

Tool Options

General Settings

▶ **To set the tools options:**

1. Click Tools > Options. The Options dialog appears.
2. Select the Enable Logging checkbox only if directed to by Technical Support.

   This option creates a log file in your home directory.
3. Choose the Keyboard Type from the drop-down list (if necessary).

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

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

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

4. Configure hotkeys:

- Exit Full Screen Mode - Hotkey.

  When you enter Full Screen mode, the display of the target server becomes full screen and acquires the same resolution as the target server.

  This is the hot key used for exiting this mode.

- Exit Single Cursor Mode - Hotkey.

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

  This is the hot key used to exit single cursor mode and bring back the client mouse cursor.

- Disconnect from Target - Hotkey.

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

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

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

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

Raritan.
A brand of Llegrand

5. Click OK.
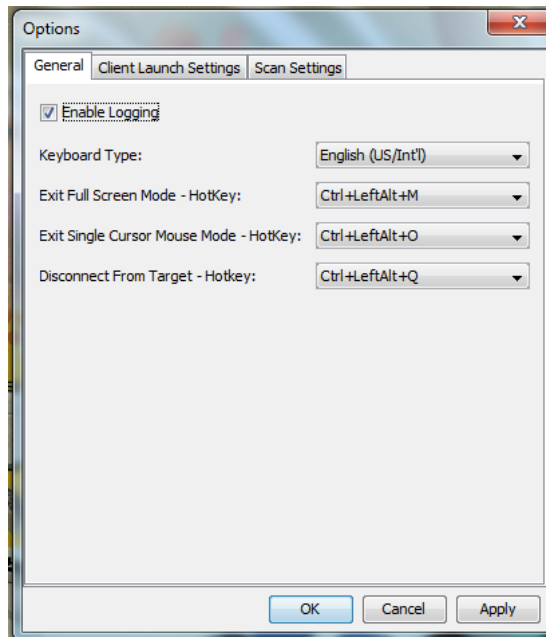
Keyboard Limitations

Turkish Keyboards

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

Slovenian Keyboards

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

Language Configuration on Linux

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

Language	Configuration method
US Intl	Default
French	Keyboard Indicator
German	System Settings (Control Center)
Japanese	System Settings (Control Center)
UK	System Settings (Control Center)
Korean	System Settings (Control Center)
Belgian	Keyboard Indicator

Language	Configuration method
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.

Client Launch Settings

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

▶ **To configure client launch settings:**

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

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

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

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

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

3. Click OK.
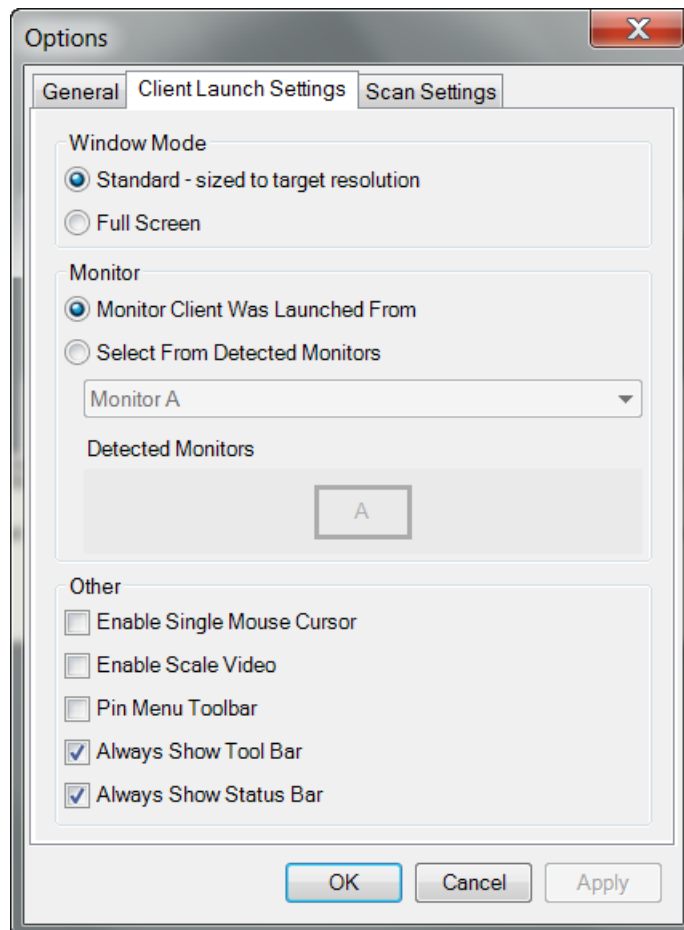
View Options

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 25).

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

If you want the menu bar to remain visible while in Full Screen mode, enable the Pin Menu Toolbar option from the Tool Options dialog. See *Tool Options* (on page 25).

▶ **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.

Digital Audio

The Dominion KX IV–101 supports audio playback over HDMI.

Supported Audio Device Formats

The following playback formats are supported:

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

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.

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.

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

- Connect audio playback at the lower quality formats. The impact of video consuming bandwidth is much less notable at 11k connections than at 44k
- Set the connection speed under Connection Properties to a value that best matches the client to server connection

Under Connection Properties, set the color depth to as low a value as possible. Reducing the color depth to 8 bit color considerably reduces the bandwidth consumed

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.

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

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

For all devices, the device type, device format, and the buffer settings applied to the device are saved.

See *Connecting and Disconnecting from a Digital Audio Device* (on page 34) 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 from 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 34) 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 audio format for the playback device from the Format: drop-down.

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

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

8. 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 ![audio icon] in the toolbar and select OK when you are prompted to confirm the disconnect. A confirmation message appears. Click OK.

Adjusting Capture and Playback Buffer Size (Audio Settings)

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

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

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

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

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

Audio settings are configured in VKC or AKC.

Adjust Audio Settings

► **To adjust audio settings:**

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

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.
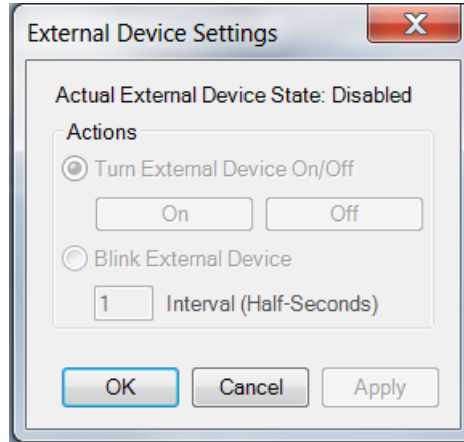
4. Click OK or Apply to save.

Version Information - Virtual KVM Client

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

- Choose Help > About Raritan Virtual KVM Client.

Active KVM Client (AKC) Help

To launch AKC, enter https://<KX4 IP address>/akc in a browser.

Overview

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

This allows you to run the client in a Windows environments without using the Java® Runtime Environment (JRE), which is required to run Virtual KVM Client (VKC).

AKC provides the same features as VKC with the exception of the following:

- Keyboard macros created in AKC cannot be used in any other client.
- Direct port access configuration
- AKC server certification validation configuration (see *Prerequisites for Using AKC* (on page 38))

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

AKC Supported Microsoft .NET Framework

The Active KVM Client (AKC) requires Windows .NET® version 4.6 or 4.7.

AKC Supported Browsers

- Internet Explorer 11 and higher
- Microsoft Edge
- Chrome and Firefox on Windows platforms. You must have the ClickOnce plugin installed. Chrome also requires .NET 3.5.

AKC Supported Operating Systems

When launched from Internet Explorer®, 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 7® operating system (up to 64 bit)
- Windows 8® operating system (up to 64 bit)
- Windows 10 ® operating system (up to 64 bit)

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

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'

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

Disable 'Protected Mode'

®Windows® 7   users should ensure that Protected Mode is not on when accessing this device.

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 Internet Explorer 11 (not supported in IE 10 or lower), 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 - not available on IE browser
- External Device

▶ **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.

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. Not supported for resolutions above 1920x1200, so for those resolutions color subsampling will automatically drop down to 4:2:2.
- 4:2:2: Good blend of image quality and bandwidth.
- 4:2:0: Maximum savings of network bandwidth and client load. Works fine for most general-purpose applications that don't emphasize high-resolution lines or text.

▶ **Current Status**

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

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

Connection Info

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

See Connection Properties for help configuring the connection properties.

- Name of the Dominion KX IV–101
- IP address of the Dominion KX IV–101
- Port - The KVM communication TCP/IP port used to access Dominion KX IV–101.
- Data In/Second - Data rate received from the Dominion KX IV–101
- Data Out/Second - Data rate sent to the Dominion KX IV–101.
- FPS - Video frames per second from the Dominion KX IV–101.
- Average FPS - Average number of video frames per second.
- Connect Time - The duration of the current connection.
- Horizontal Resolution - The target server horizontal resolution.
- Vertical Resolution - The target server vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - communications protocol version.

▶ **To view connection info:**

- Choose File > Connection Info.

Connection Info	
Device Name:	kx3-61-16
IP Address:	192.168.61.16
Port:	443
Data In/Second:	121 kB/s
Data Out/Second:	234 B/s
FPS:	17
Avg. FPS:	21.80
Connect Time:	00:00:25
Horizontal Resolution:	1024
Vertical Resolution:	768
Refresh Rate:	60 Hz
Protocol Version:	1.31

OK

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

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.
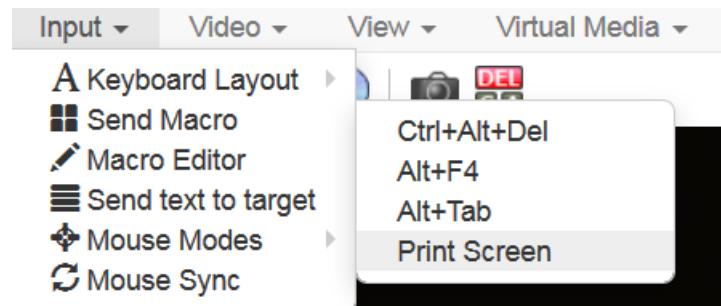
Macro Editor

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 47).

▶ **To access the Macro Editor:**

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

Macro Editor

Name	Ctrl+Alt+Del

Macros
- Ctrl+Alt+Del
- Alt+F4
- Alt+Tab
- Print Screen

Keys
- press: CTRL LEFT
- press: ALT LEFT
- press: DELETE
- release: CTRL LEFT
- release: ALT LEFT
- release: DELETE

Add Key
⇧
⇩
Delete Key

Add New Macro | Delete Macro

Export | Import | OK | Cancel

Add New Macro

▶ **To add a new macro:**

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

3. Enter a Name for the new macro. The name will appear in the Send Macro menu once the macro is saved.

4. Click Add Key, then press the key you want to add to the macro. The key press and key release appear in the Keys list.

   ▪ To add more keys, click Add Key again, and press another key.

   ▪ To remove a key, select it in the Keys list and click Delete Key

5. To put the key in the correct sequence, click to select a key in the Keys list, then click the up and down arrows.

6. Click OK to save.
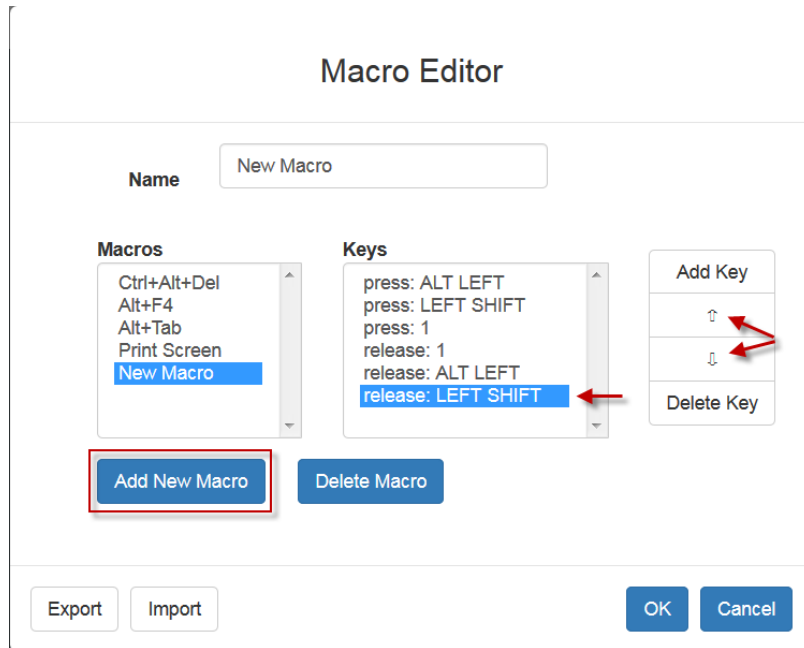
Delete a Macro

▶ **To delete a macro:**

1. Choose Inputs > Macro Editor.

2. Select the macro, then click Delete Macro.

3. Click OK.

Import and Export Macros

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one Dominion KX IV–101, your macros will only be available on the browser and Dominion KX IV–101 where they wer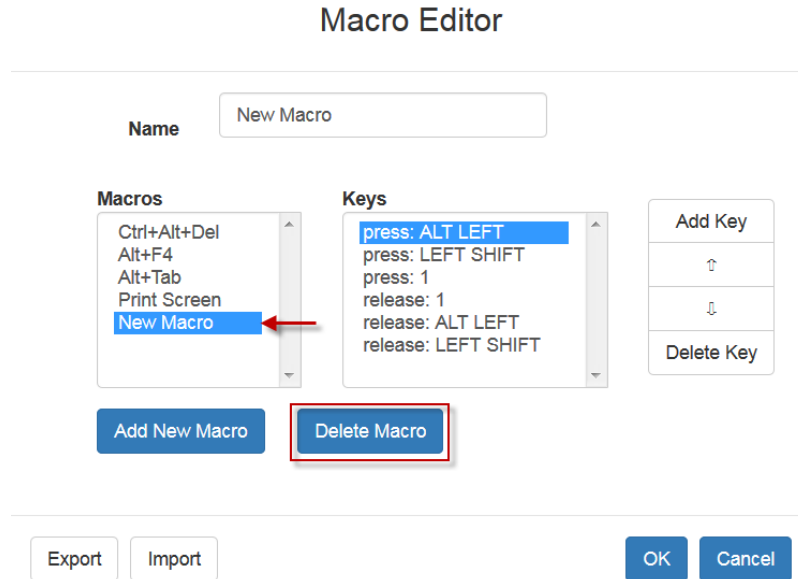e created. To reuse your macros in another Dominion KX IV–101 device, you can import and export the macro files. Imported and exported macro files created on HKC are only compatible with HKC, and cannot be used on AKC or VKC. Likewise, macro files created on AKC or VKC cannot be imported for use on HKC.

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.

▶ **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.

Macro Import

Open to Import

Select macros to import:

Macro1

Select All   Deselect All   OK   Cancel
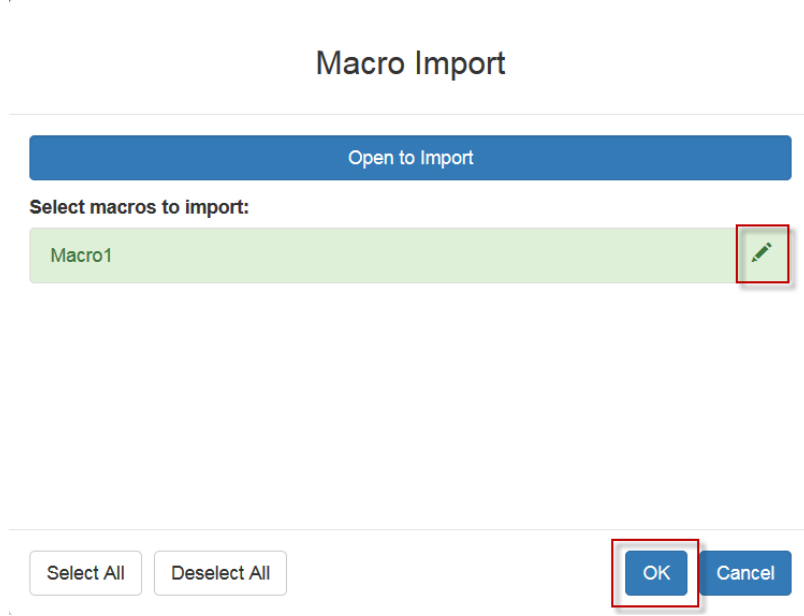
Send Text to Target

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. The Send Text to Target dialog appears.

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

3. Click OK.

Raritan.
A brand of legrand

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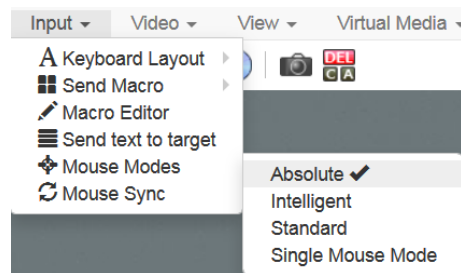
You can toggle between these two modes (single mouse and dual mouse).

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 synch. See *Intelligent Mouse Synchronization Conditions* (on page 23).
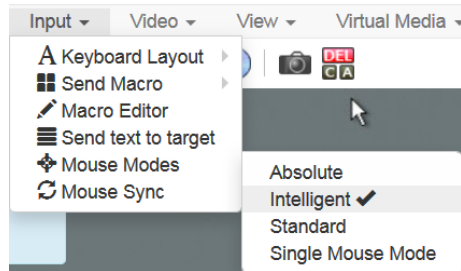
Standard

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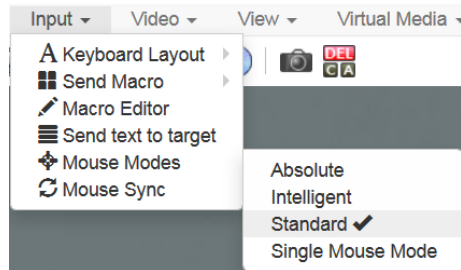
Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine. Single mouse mode is not available on Internet Explorer.

▶ **To enter Single mouse mode:**

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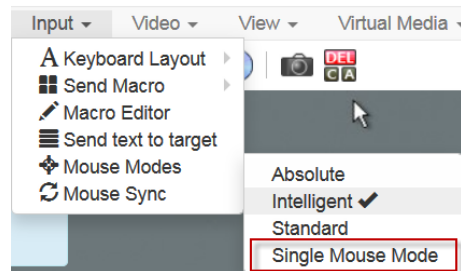
- A message appears at the top of the client window: Press Esc to show your cursor.

🔒 **192.168.61.16** has control of your pointer. Press Esc to take back control.
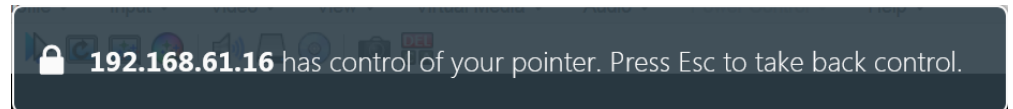
▶ **To exit Single mouse mode:**

- 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.

Raritan.
A brand of legrand

Video Menu

Refresh Screen

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

▶ **To force a refresh of the video screen:**
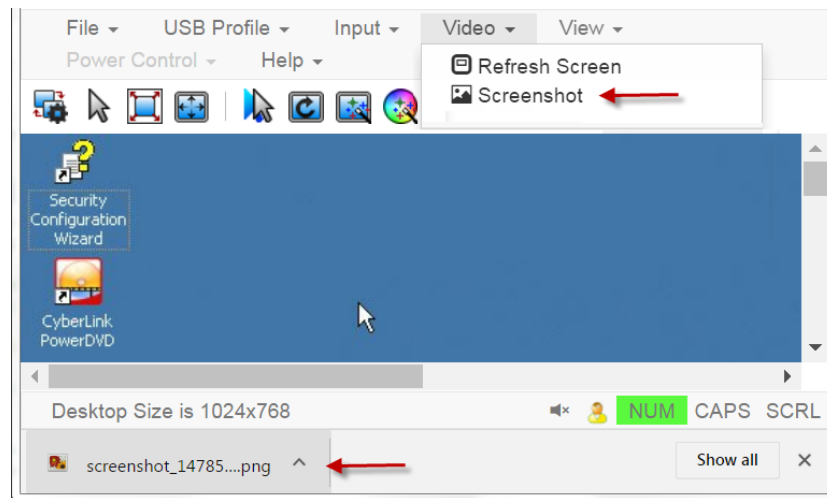
- Choose Video > Refresh Video.
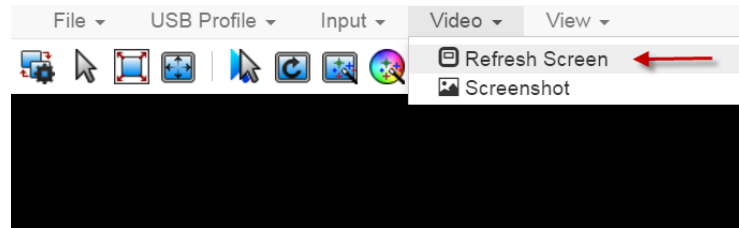
Screenshot

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.
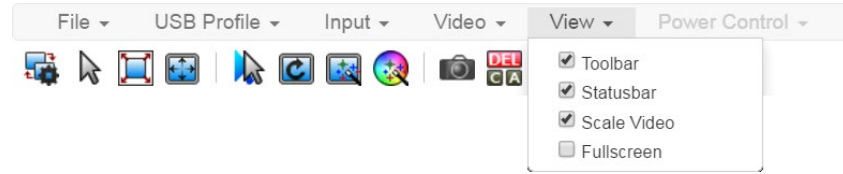
▶ **Toolbar and Statusbar:**

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.

Virtual Media Menu

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

Connect Files and Folders

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

Supported browsers: Chrome, Firefox, Safari

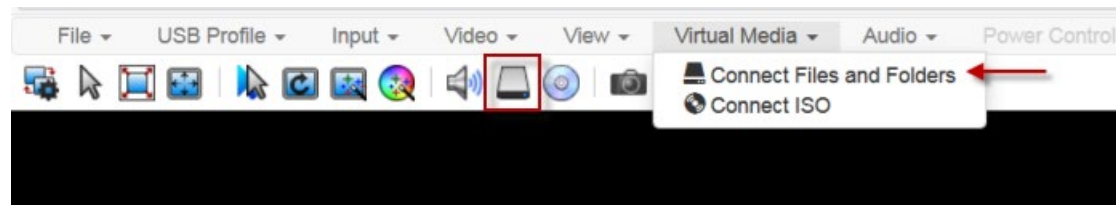File size limit: 4GB per file

▶ **To connect files and folders:**

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

2. Drag files or folders onto the Map Virtual Media Files and Folders dialog. Click OK.
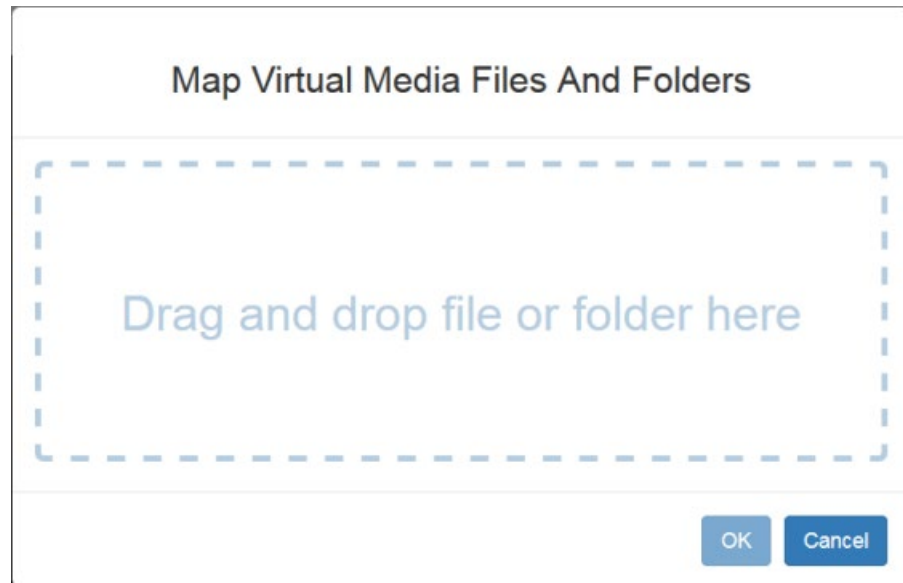
3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.
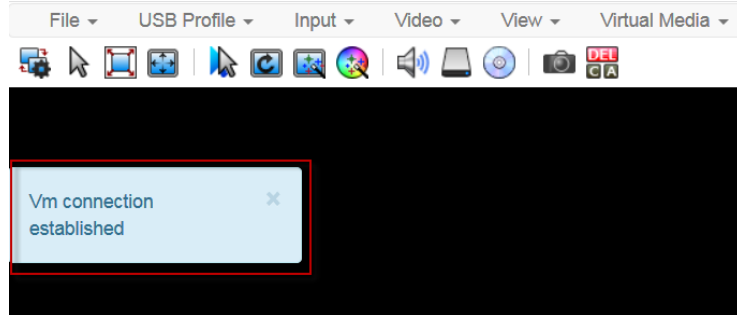
▶ **To disconnect files and folders:**

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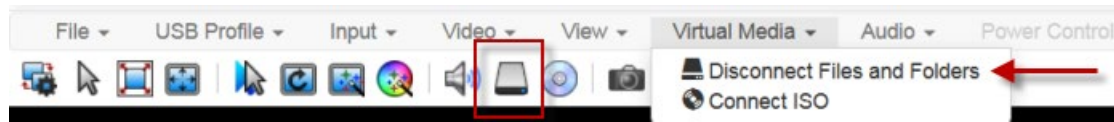
Connect ISO

The Connect ISO command maps a virtual media ISO image to the target. You can connect to ISO images on your client or on remote servers.

File size limit: 4GB per file

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

▶ **To map virtual media ISO images:**

1. Choose Virtual Media > Connect ISO. Or, click the matching icon in the toolbar.
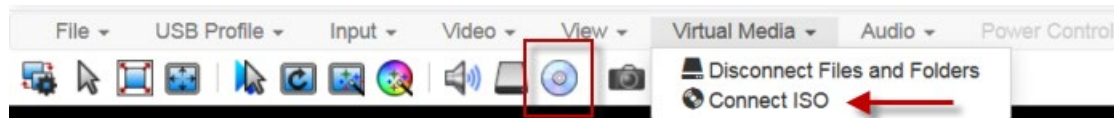
2. Select the option for your file's location:

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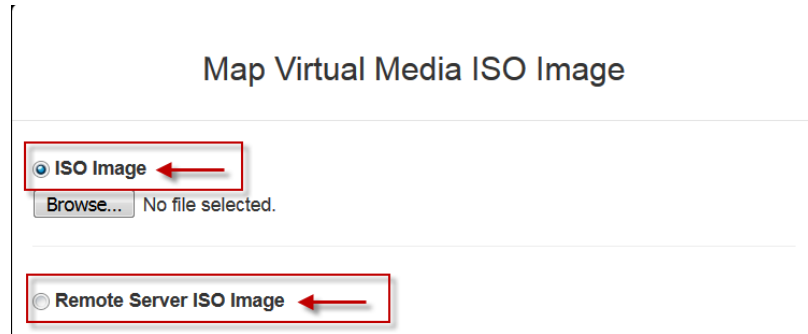
- Select ISO Image if the ISO file is directly accessible on your client. Click Browse, select the ISO file, and click OK. The filename appears next to the Browse button.

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

3. Click OK to map the selected file to the target. A message appears to show virtual media is connected.
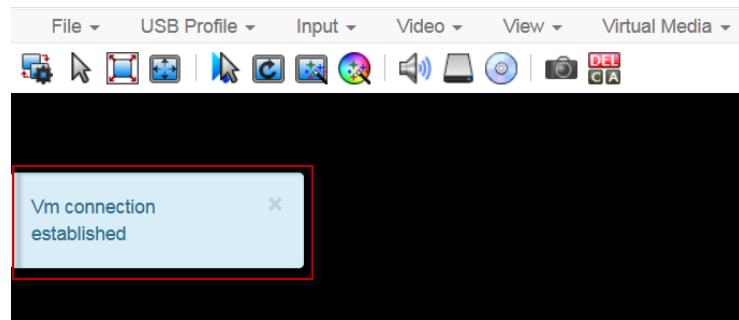
▶ **To disconnect ISO:**

- Choose Virtual Media > Disconnect ISO. Or, click the matching icon in the toolbar.
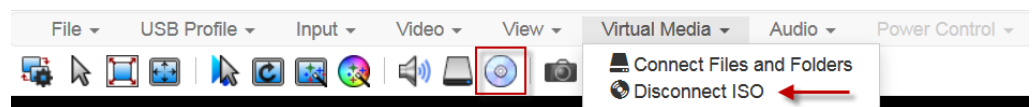
Audio Menu

The Audio menu contains audio connection and settings.

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.

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

Connect Audio

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

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

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

▶ **To connect audio:**

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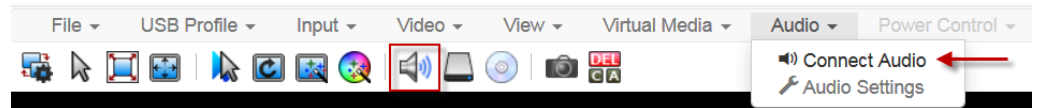
2. In the Connect Audio Device dialog, select the Connect Playback Device checkbox.

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 targets.

4. Click OK. A success message appears.

> Audio connection
> established ✕
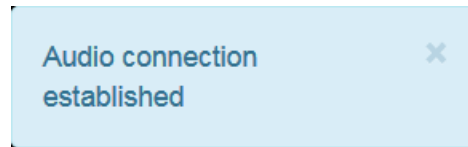
▶ **To disconnect audio:**

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.

Audio Device Settings

Buffer Sizes (ms)

| Playback | 280 | 40 | ———○——— | 400 |

Advanced

| Volume | 100 | 0 | ————————○ | 100 |

OK   Cancel
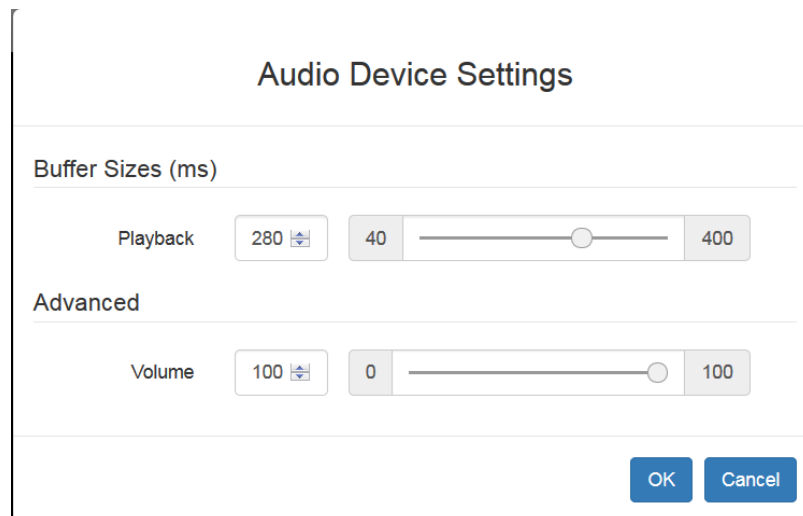
3. Click OK.

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

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.

External Device Settings

External Device State: Disabled

Action

◉ Turn External Device On/Off

| On | Off |

◯ Blink External Device

| 1 | **Interval (Half-Seconds)**

OK Cancel Apply
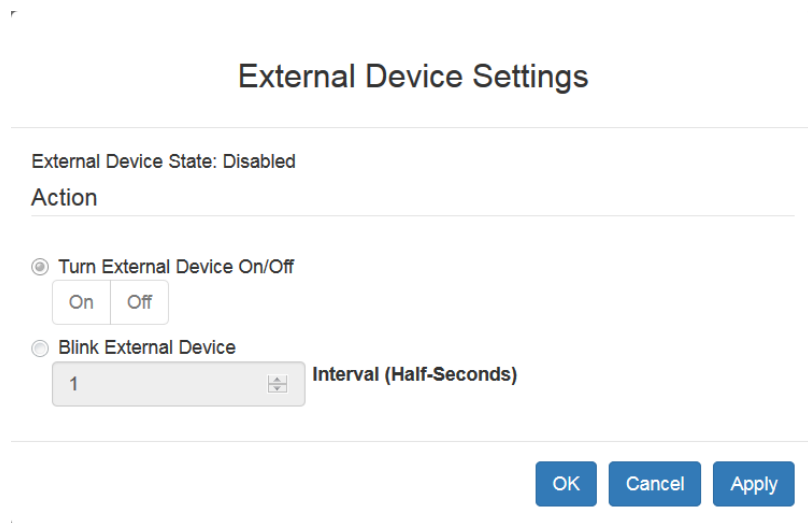
4. Click OK or Apply to complete the action.

Raritan.
A brand of legrand

Chapter 4   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 62).

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 and should change its password. For other security settings related to user management, see *Security* (on page 97).

Click User Management to view the submenu options.
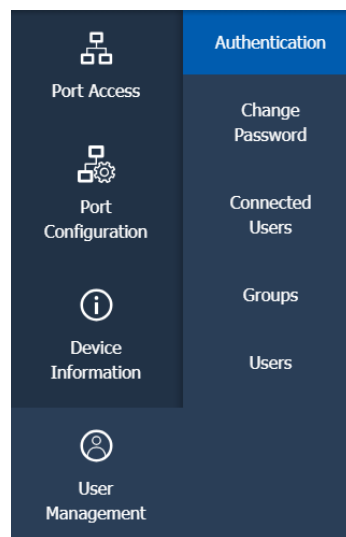
In This Chapter

Gathering LDAP/Radius Information

You must have the following information about your AA server settings to configure external authentication. 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, SmartTLS).
  - 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)

▶ **Radius authentication:**

- The IP address or host name of the Radius server
- The type of Radius Authentication used by the Radius server (PAP or CHAP)
- 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. See Creating Users.

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 64) and *Radius Authentication* (on page 67). For help with adding users, see *Users and Groups* (on page 69).

Authentication

ⓘ Local authentication is used if nothing is enabled.

Authentication Type   LDAP ⬍

☑ Use Local Authentication if Remote Authentication is not available

✔ Save

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 62).

▶ **To add LDAP servers:**

1. Click User Management > Authentication.
2. 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. .

Field/setting	Description
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.*
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.

Field/setting	Description
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.
Active Directory Domain	The name of the Active Directory Domain. ▪ Example: `testradius.com`

3. Click Test Connection to check if Dominion KX IV–101 can connect with the server.

4. 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 Order.

5. To start using these settings, make sure LDAP is selected and saved in the Authentication Type field. See *Configuring Authentication* (on page 62).

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 62).

▶ **To add Radius servers:**

1. Click User Management > Authentication.
2. In the Radius 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) ▪ 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.

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 Order.

5. To start using these settings, make sure Radius is selected and saved in the Authentication Type field. See *Configuring Authentication* (on page 62).

Disabling External Authentication

▶ **To disable external authentication:**

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

Change Your Password

▶ **To change your password:**

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

Connected Users

You can check which users have logged in to the Dominion KX IV–101 and their status. If you have administrator privileges, you can terminate any user's connection to the Dominion KX IV–101.

▶ **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. To disconnect any user, 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.

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 75).

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
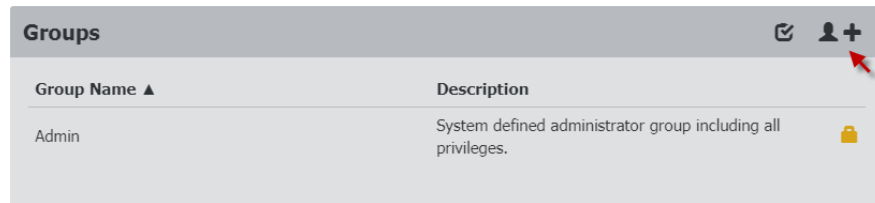
2. Complete the New Group information:

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.

3. 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 75).

- 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

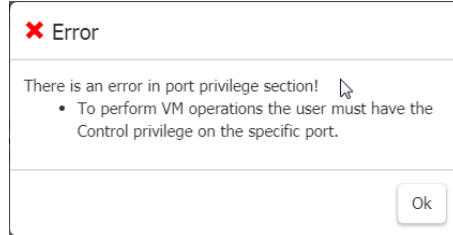- User Management: All functions in the User Management menu except Disconnect Users

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

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

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

> **✗ Error**
>
> There is an error in port privilege section!
> * To perform VM operations the user must have the Control privilege on the specific port.
>
> [Ok]

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

▶ **To add users:**

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

> **Users**   ☑ 👤➕
>
> | Enabled ▲ | User name | Full Name | Roles |
> | --- | --- | --- | --- |
> | ✔ | admin | Administrator | Admin |
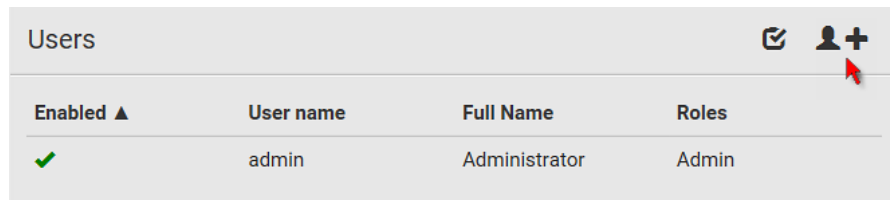
2. Complete the User information:

Field/setting	Description
User Name	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

Field/setting	Description
Enable	When selected, the user can log in to the Dominion KX IV–101.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in.

3. SSH: The SSH public key is required when public key authentication for SSH is enabled. See *SSH Settings* (on page 91).

4. Open the SSH public key with a text editor.

5. Copy and paste all content in the text editor into the SSH Public Key field.

6. SNMPv3: The SNMPv3 access permission is disabled by default. This section appears when the permission is enabled in the SNMP settings, or when a user is part of the admin group.

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. This is the default. ▪ Authentication: Authentication and no privacy. ▪ Authentication & Privacy: Authentication and privacy.

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

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

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

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

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

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

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

2. Click Save.

Admin Group Special Privileges

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

- Backup/Restore
- Bulk Configuration
- 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

Chapter 5 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.

System

Detail

Product	KX4
Model	DKX4-101
Firmware Version	4.0.0.5.45611
Hardware ID	1
Serial Number	1IT8500012

Status

Internal Temperature Current Value	45.3°C / 113.5°F
Internal Temperature Maximum Value	50.3°C / 122.6°F
Local Monitor	Not Detected

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.

Network

Ethernet

IPv4 Address	192.168.56.27/24
MAC Address	00:0d:5d:00:02:da
Link State	1 GBit/s, full duplex, link OK, autonegotiation on

Common

DNS Servers	none
DNS Suffixes	none
DNS Resolver Preference	IPv6 Address
IPv4 Routes	192.168.56.0/24 dev ETHERNET default via 192.168.56.126 (ETHERNET)
IPv6 Routes	none

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.
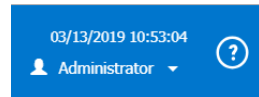
▶ **To set the date and time:**

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

▪ To use the DHCP-assigned NTP servers: **leave the First and Second time server fields blank**. DHCP-assigned NTP servers are available when either IPv4 or IPv6 DHCP is enabled. See *Network* (on page 85).

NTP Settings

First Time Server

Second Time Server

Check NTP Servers

▪ To specify NTP servers manually, enter the primary NTP server in the First Time Server field. A secondary NTP server is optional. Click Check NTP Servers to verify. Click Save.

NTP Settings

First Time Server   192.168.22.124

Second Time Server

Check NTP Servers

✔ Save

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, an action named "User events - email" has been added and assigned to all User Activity and User Administration events.
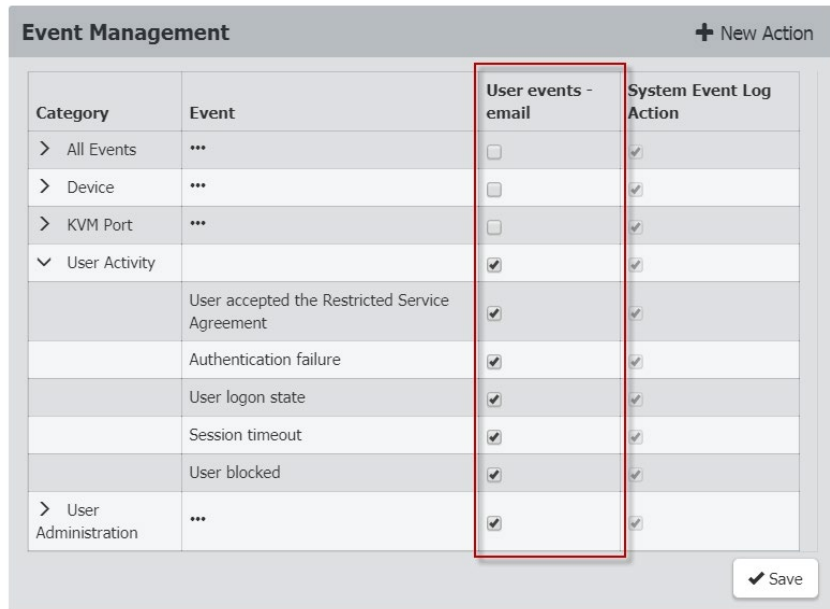
2. Select the event checkboxes to assign an action to an event. Click Save.

▶ **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 81)
    - SNMP Actions: See *SNMP Notifications* (on page 82)
    - Syslog Actions: See *Syslog Messages* (on page 84)
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 79) 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 89).
4. Click Create.

SNMP Notifications

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

See *Event Management* (on page 79) 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:**

New Action

Action Name	Syslog messages
Action	Send SNMP notification ⬍
Notification Type	SNMPv3 Trap ⬍
Engine ID	0x800035ae8000b33777b6039fc0984c22b1bdb3017 3383275011bae2170354383
Host	192.168.22.57
Port	162
User ID	user
Security Level	noAuthNoPriv ⬍

✖ Cancel   ✔ Create

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.

Security level	Description
"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 79) for help assigning this action to an event.

▶ **To create the syslog message action:**

pic here screenshot

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 UDP.

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.

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 76).

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

▶ **IPv4 settings:**

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

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
    - Consists of alphanumeric characters and/or hyphens
    - Cannot begin or end with a hyphen
    - Cannot begin with a number
    - Cannot contain punctuation marks, spaces, and other symbols
    - Maximum 253 characters
- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
    - Example: *192.168.84.99/24*

▶ **IPv6 settings:**

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

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

    Example: *fd07:2fa:6cff:1111::0/128*

▶ **Interface Settings:**

Field	Description
Speed	▪ Select a LAN speed. ▪ Auto: System determines the optimum LAN speed through auto-negotiation. ▪ 10 MBit/s: Speed is always 10 Mbps. ▪ 100 MBit/s: Speed is always 100 Mbps. ▪ 1 GBit/s: Speed is always 1 Gbps (1000 Mbps).
Duplex	▪ Select a duplex mode. ▪ Auto: The 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.

Raritan.
A brand of ▢legrand®

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.

▶ **Common Network Settings:**

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

Field	Description
DNS resolver peference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. ▪ IPv4 Address: Use the IPv4 addresses. ▪ IPv6 Address: Use the IPv6 addresses.
DNS suffixes (optional)	Specify a DNS suffix name if needed.
First/Second DNS server	Manually specify static DNS server(s). ▪ If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. ▪ If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the Dominion KX IV–101 will use DHCP-assigned DNS servers.

Network Services

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

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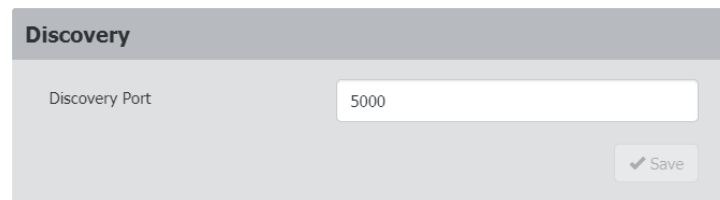
Discovery Port

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.

▶ **To change the default discovery port:**

1. Click Device Settings > Network Services > Discovery Port.
2. Enter the port number then click Save.

Discovery	
Discovery Port	5000
	✔ Save
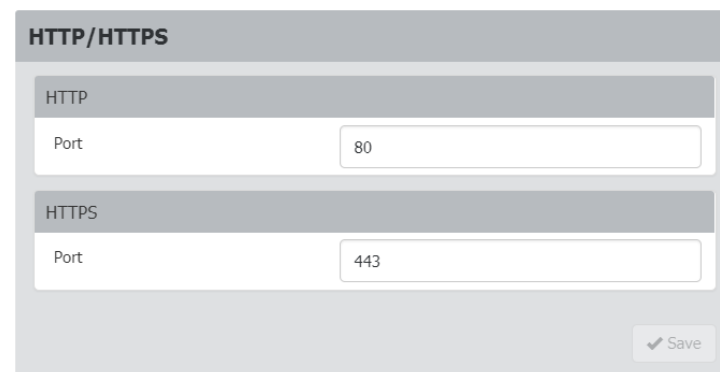
HTTP/HTTPS Ports

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. Enter the port numbers then click Save.

HTTP/HTTPS	
HTTP	
Port	80
HTTPS	
Port	443
	✔ Save

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

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 79).

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 111).

▶ **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.
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:**

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
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.

3. 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.

4. 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 Dominion KX IV–101 and the client (such as a web browser), which is impacted by the cipher priority of Dominion KX IV–101 and the client's cipher availability/settings.*

Tip: *To force Dominion KX IV–101 to use a specific AES cipher, refer to your client's user documentation for information on 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.

SNMP		
SNMP Agent		
Enable SNMP v1 / v2c	✔	
Read Community String	public	
Write Community String	private	
Enable SNMP v3	☐	
MIB-II System Group		
sysContact		
sysName		
sysLocation		
Download MIBs		
RADM-MIB	download	
		✔ 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 connection. See* **Users and Groups** *(on page 69)*
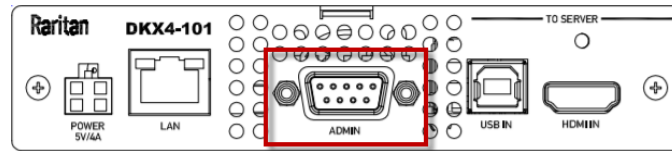
5. Click Save.

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.

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.

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 69). 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 69).
- 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 100).

▶ **Terminal Block Control Settings: Input**

1. Click Device Settings > Terminal Block Control.

Input Configuration	
Enable External Input Switch	Enable or disable the input switch.
Current External Input Switch State	The current state is displayed: Open or Closed. When switch state is open, the device functions normally.
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.
External Device State	The external device state is displayed: ▪ On ▪ Off ▪ Blinking ▪ Disabled
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. ▪ Blink External Device: Make sure the blink interval is set as desired.
Blink Interval	Set interval between blinks in half-seconds. Default is 1.

3. 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.

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.

Virtual Media Shared Images

No.	IP Address / Hostname	Share Name	Image Path	Enable SAMBA v1.0
1	192.168.1.211	isos	/fedora28.iso	no
2	windows2012.systemtestest2.local	isos	windows2016.iso	no
3	windows2012.systemtestest2.local	isos	/OSFiles/ubuntu18.iso	no
4	fedora.systemtestest2.local	sambaguest	/OSFiles/openSUSE.iso	no
5	192.168.1.12	isoshare	/Fedora29.iso	yes

New Edit Delete Test Connection

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.

Chapter 6   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 you to grant system permissions to groups, based on their IP addresses.

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.
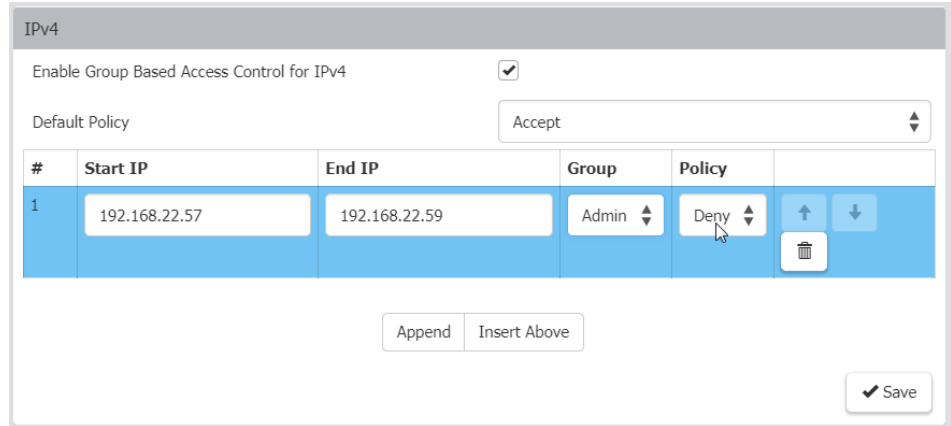
3. Determine the default policy.

    ▪ 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.

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 24-bit prefix length, use this format:

  x.x.x.x/24

  /24 = the prefix length.

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

1. Choose Security > IP Access Control.

2. Select the Enable IP Access Control for IPv4 or scroll down to select the checkbox for IPv6.

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

4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.
   - Inbound rules control the data sent to the 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.

IP Access Control

IPv4

Enable IPv4 Access Control ✔

Inbound Rules

Default Policy   Accept

#	IP/Mask	Policy	
1	192.168.22.57/24	Drop	↑ ↓ 🗑

Append   Insert Above

Outbound Rules

Default Policy   Accept

#	IP/Mask	Policy	
no rules defined			

Append   Insert Above

✔ Save

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

KVM Security

The KVM Security settings page includes options for encryption, 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
SSL Encryption Mode	▪ Auto: Recommended option. The Dominion KX IV–101 autonegotiates to the highest level of encryption possible. ▪ AES 128 ▪ AES 256
Apply Encryption Mode to KVM and Virtual Media	Select this checkbox to use encryption for virtual media as well as KVM.
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.

Field/setting	Description
PC Share Idle Timeout	Set an idle time limit for users in PC Share mode. If a user has not moved the mouse or entered keyboard input and the timeout period expires, the user relinquishes control, and another user can access keyboard and mouse control of the target.
Virtual Media Share	This option is available only when PC-Share mode is enabled. When selected, Virtual Media Share permits the sharing of virtual media and audio among multiple users, that is, several users can access the same virtual media or audio session. The default is disabled.
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 93).
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 102).

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&port=port name&client=akc

Login Settings

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

▶ **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.
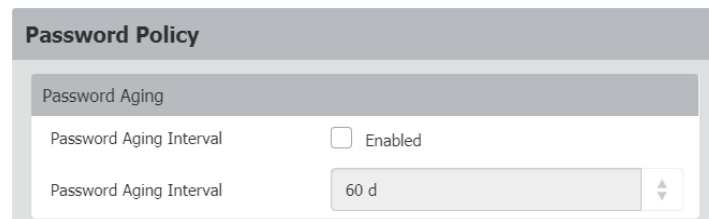

5. Click Save.

Password Policy

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

▶ **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.

Password Policy

Password Aging		
Password Aging Interval	☐ Enabled	
Password Aging Interval	60 d	▲▼

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.

Raritan.
A brand of legrand

- Specify the Password History Size, which controls how frequently passwords can be reused. Maximum is 12.

4. Click Save.

SSL Certificate

Dominion KX IV–101 uses TLS 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 78).*

Note: The CSR must be generated on the Dominion KX IV–101.

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

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

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

Active SSL Certificate

Subject			**Issuer**		
Country	US		Country	US	
State or Province	NJ		State or Province	NJ	
Locality	Somerset		Locality	Somerset	
Organization	Raritan Americas, Inc.		Organization	Raritan Americas, Inc.	
Organizational Unit	Engineering		Organizational Unit	Engineering	
Common Name	Raritan KVM		Common Name	Raritan CA	
Email Address	not set		Email Address	not set	

Miscellaneous

Not Valid Before	Feb 13 21:35:57 2015 GMT
Not Valid After	Feb 9 21:35:57 2030 GMT
Serial Number	03
Key Length	2048 bits

Download Key   Download Certificate

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

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

1. Click Security > SSL Certificate. Scroll down to the New SSL 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. To generate, do one of the following:
   - 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. 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.
   c. Click Create New SSL Key.
   d. When the page refreshes, new buttons appear in the New SSL Certificate section, to allow you to install, download or delete the newly generated self-signed certificate and key.
   e. To start using the new certificate, click Install Key and Certificate.
   f. The page may refresh as the certificate loads.
   - To generate a CSR to send to the CA for certification:
   a. In the Key Creation Parameters, enter a password in the Challenge and Confirm Challenge fields.
   b. Click Create New SSL Key.
   c. When the page refreshes, new buttons appear in the New SSL Certificate section, to allow you to download the CSR, download the key, or delete the CSR.

d. 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.

e. 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 > SSL Certificate, then scroll down to the New SSL Certificate section.

2. Select the Upload Key and Certificate checkbox. The Browse and upload controls appear.

Raritan®
A brand of legrand®

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.
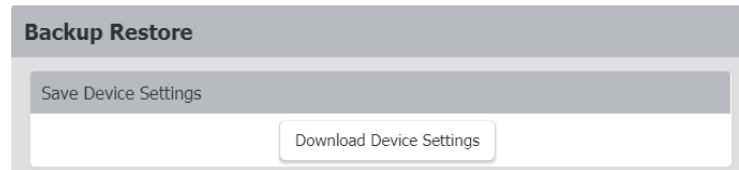
Chapter 7 Maintenance
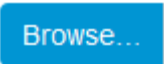
In This Chapter

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.

▶ **To download the Device Settings backup file:**

1. Click Maintenance > Backup/Restore.
2. 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 Browse... 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. Click Upload & Restore Device Settings to upload the file.
5. 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.
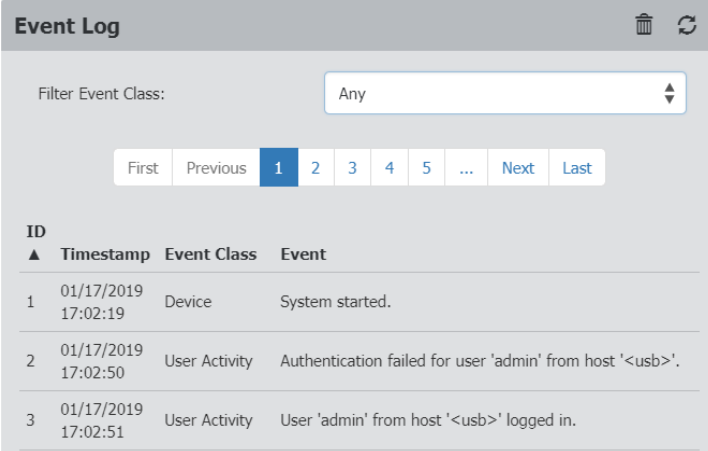
Event Log

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 256KB, each new entry overwrites the oldest one.

▶ **Event Classes:**

- Device
- KVM Port
- User Activity
- User Administration

▶ **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

- Refresh the event log by clicking the refresh icon [icon] in the top-right corner.

▶ **To view by event category:**

- Select an option in the Filter Event Class field.

▶ **To clear the local event log:**

1. Click the trash icon [icon] on the top-right corner.
2. Click Clear Log on the confirmation message.

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

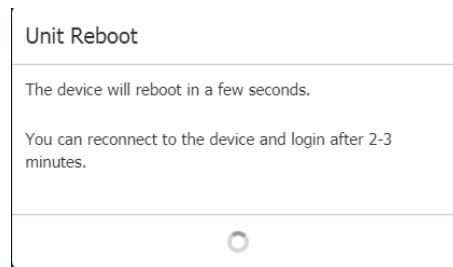| Firmware Update History			
Timestamp ▼	**Previous Version**	**Update Version**	**Status**
03/18/2019 10:05:06	4.0.0.1.45554	4.0.0.5.45611	SUCCESSFUL
03/01/2019 11:17:40	4.0.0.1.45375	4.0.0.1.45554	SUCCESSFUL

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.

Unit Reset

Reboot Unit   Reset to Factory Defaults
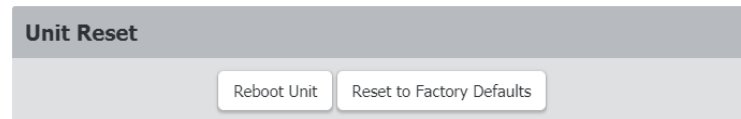
▶ **To reboot the device:**

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

   A countdown timer appears.

Unit Reboot

The device will reboot in a few seconds.

You can reconnect to the device and login after 2-3 minutes.

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. Click to confirm reset in the confirmation message.
3. A countdown timer appears. It takes about two minutes to complete.
4. When the reset is complete, proceed with initial configuration. See *Initial Configuration* (on page 4).

▶ **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.
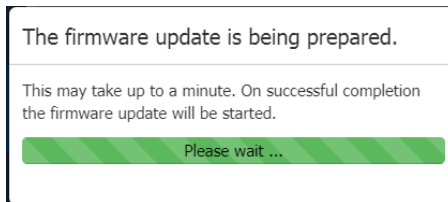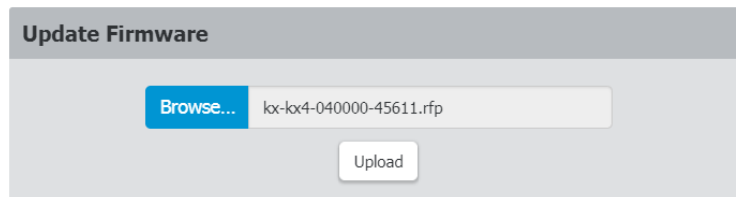- Perform the CLI command. See *CLI: reset* (on page 133)

Update Firmware

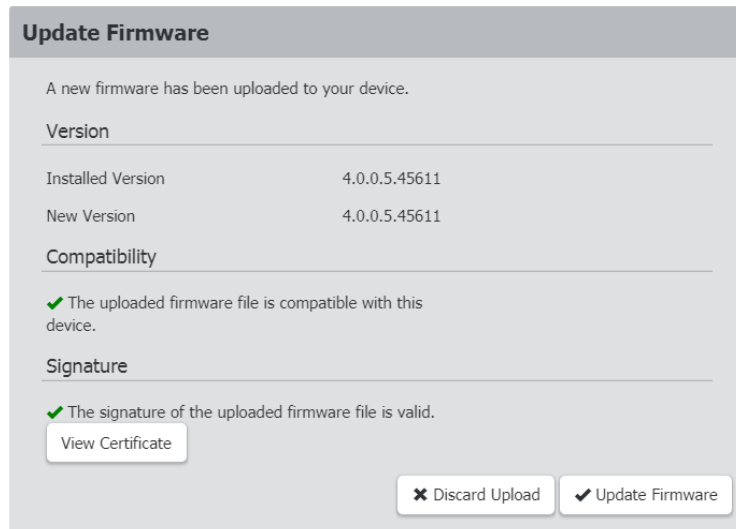Firmware files are available on Raritan's Support page: www.raritan.com/support.

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.

Update Firmware

Browse...   kx-kx4-040000-45611.rfp

Upload

The firmware update is being prepared.

This may take up to a minute. On successful completion the firmware update will be started.

Please wait ...

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

Update Firmware

A new firmware has been uploaded to your device.

Version

Installed Version	4.0.0.5.45611
New Version	4.0.0.5.45611

Compatibility

✔ The uploaded firmware file is compatible with this device.

Signature

✔ The signature of the uploaded firmware file is valid.

View Certificate

✖ Discard Upload   ✔ Update Firmware

- To cancel, click Discard Upload.

Raritan.
A brand of legrand

▪ 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–101during the update. The LAN port 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.

5. When the update is complete, the Dominion KX IV–101reboots, 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 90).

▶ **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.

# Chapter 8   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:**

Download Diagnostic

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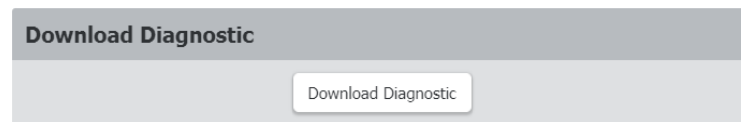
1.   Click Diagnostics> Download Diagnostic.
2.   Click Download Diagnostic, then save the file.
3.   Send this file as instructed by Raritan Technical Support.

Network Diagnostics

Dominion KX IV–101 provides the following tools diagnosing 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.

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.

```
Ping Results

PING 192.168.56.27 (192.168.56.27): 56 data bytes
64 bytes from 192.168.56.27: seq=0 ttl=64 time=0.219
ms
64 bytes from 192.168.56.27: seq=1 ttl=64 time=0.183
ms
64 bytes from 192.168.56.27: seq=2 ttl=64 time=0.179
ms
64 bytes from 192.168.56.27: seq=3 ttl=64 time=0.196
ms
64 bytes from 192.168.56.27: seq=4 ttl=64 time=0.171
ms
--- 192.168.56.27 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.171/0.189/0.219 ms

                                            Close
```

▶ **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.

▶ **List TCP Connections:**

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

#	Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
1	tcp	0	0	::ffff:192.168.56.27:443	::ffff:192.168.55.78:62654	TIME_WAIT
2	tcp	0	0	::ffff:192.168.56.27:443	::ffff:192.168.55.78:62644	TIME_WAIT

List TCP Connections

Active Internet connections (w/o servers)

Chapter 9 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

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
cancel	Discard changed settings and leave config mode
check	Check services
device	Configure Device
group	Configure user groups
history	Configure command history settings
network	Configure network settings
password	Change password of currently logged in user
security	Configure security settings
serial	Configure serial port settings
terminalblock	Configure terminal block settings
time	Configure date/time settings
user	Configure users

CLI: config device

device

config:#   device name

device [name <name>]

  Configure Device

  name   Device name

For example, to name device "KX4newname", at config menu type "device name KX4newname", 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
changeTerminalBlockSettings/deviceAccessUnderCcsg/deviceSettings/
maintenance/pcShare/portControl:1/portControl:all/portViewOnly:1/port
ViewOnly:all/portVmROnly:1/portVmROnly:all/portVmRW:1/portVmRW:al
l/securitySettings/userManagement)

config:# group delete [name <name>]

  Delete group

  name   Group name (Admin)

config:#   group modify [name <name>] [description <desc>]
[addPrivileges <addprivs>] [removePrivileges <removeprivs>]

  Edit a group

  name   Group name (Admin)

  description   Group description

  addPrivileges   Add group privileges (one or more (separated by '/')
of
changeTerminalBlockSettings/deviceAccessUnderCcsg/deviceSettings/
maintenance/pcShare/portControl:1/portControl:all/portViewOnly:1/port
ViewOnly:all/portVmROnly:1/portVmROnly:all/portVmRW:1/portVmRW:al
l/securitySettings/userManagement)

  removePrivileges   Remove group privileges (one or more (separated
by '/') of
changeTerminalBlockSettings/deviceAccessUnderCcsg/deviceSettings/
maintenance/pcShare/portControl:1/portControl:all/portViewOnly:1/port
ViewOnly:all/portVmROnly:1/portVmROnly:all/portVmRW:1/portVmRW:al
l/securitySettings/userManagement)

CLI: config history

history

config:#   history length

history length <length>

  Configure command history buffer length

  length   History buffer length (1..250)

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>]

  Configure ethernet interface

  speed   Speed (1000Mbps/100Mbps/10Mbps/auto)

  duplexMode   Duplex mode (half/full/auto)

config:#   network ipv4 gateway

network ipv4 gateway <gateway>

  Configure default IPv4 gateway

  gateway   Default IPv4 gateway

config:#   network ipv4 interface [enabled <enabled>] [configMethod <configMethod>] [preferredHostName <prefHostname>] [address <addrCidr>]

  Configure interface IPv4 settings

  enabled   Enable/disable IPv4 protocol (true/false)

  configMethod   IPv4 Configuration method (dhcp/static)

  preferredHostName   Preferred host name

  address   IPv4 address/prefix-len

config:#   network ipv6 gateway

network ipv6 gateway <gateway>

  Configure default IPv6 gateway

  gateway   Default IPv6 gateway

config:# network ipv6 interface [enabled <enabled>] [configMethod <configMethod>] [preferredHostName <prefHostname>] [address <addrCidr>]

  Configure interface IPv6 settings

  enabled   Enable/disable IPv6 protocol (true/false)

  configMethod   IPv6 Configuration method (automatic/static)

  preferredHostName   Preferred host name

  address   IPv6 address/prefix-len

config:#   network services discovery

network services discovery [port <port>]

  Configure Discovery Port

  port   RDM discovery port (1..65535)

config:# network services http [enabled <enabled>] [port <port>] [enforceHttps <enforcehttps>]

  Configure HTTP access

  enabled   Enable/disable HTTP access (true/false)

  port   HTTP access TCP port (1..65535)

  enforceHttps   Enable HTTPS enforcement for web access (true/false)

config:# network services https [enabled <enabled>] [port <port>]

  Configure HTTPS access

  enabled   Enable/disable HTTPS access (true/false)

  port   HTTPS access TCP port (1..65535)

config:# network services snmp [v1/v2c <v12enabled>] [v3 <v3enabled>] [readCommunity <readcommunity>] [writeCommunity <writecommunity>] [sysContact <syscontact>] [sysName <sysname>] [sysLocation <syslocation>]

  Configure SNMP settings

  v1/v2c   Enable SNMP v1/v2c access (enable/disable)

  v3   Enable SNMP v3 access (enable/disable)

  readCommunity   SNMP read community string

  writeCommunity   SNMP write community string

sysContact   MIB-II sysContact

sysName   MIB-II sysName

sysLocation   MIB-II sysLocation

config:# network services ssh [enabled <enabled>] [port <port>]
[authentication <authmode>]

  Configure SSH access

  enabled   Enable/disable SSH access (true/false)

  port   SSH access TCP port (1..65535)

  authentication   Authentication type
(passwordOnly/publicKeyOnly/passwordOrPublicKey)

CLI: config password

config:# password

Then press Enter key. System will prompt for current password, new
password, and confirm new password.

config:# apply

The password is changed if confirm password is correct.

CLI: config security

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 loginLimits [singleLogin <singlelogin>] [passwordAging
<pwaging>] [passwordAgingInterval <pwaginginterval>] [idleTimeout
<idletimeout>]

Raritan.
A brand of legrand®

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)

CLI: config serial

config:# serial [consoleBaudRate <consolebps>] [modemBaudRate <modembps>] [deviceDetectionType <detecttype>]

  Configure serial port settings

  consoleBaudRate   Serial console baud rate (1200/2400/4800/9600/19200/38400/57600/115200)

  modemBaudRate   Modem baud rate (1200/2400/4800/9600/19200/38400/57600/115200)

  deviceDetectionType   Device detection mode (automatic/forceConsole/forceAnalogModem/forceGsmModem)

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 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>] [password] [fullName <fullname>] [telephoneNumber <telephone>] [eMailAddress <email>] [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)

  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

Raritan.
A brand of legrand

authenticationProtocol protocol (MD5/SHA-1)	Authentication
privacyProtocol (DES/AES-128)	Privacy protocol
groups separated list of group names) (Admin)	Groups (Comma
sshPublicKey key	Set SSH public

CLI: diag

diag

diag:# netstat
netstat <mode>
 Netstat

  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..100) [5]
  size   Specify number of bytes in one request packet (1..65468) [56]
  timeout   Specify the maximum amount of time (in s) to wait for responses (1..600)

diag:# traceroute <dest> [useICMP]
 Trace route

  dest   Target host name or IP address
  useICMP   Use ICMP packets instead of UDP packets

CLI: reset

reset

reset
reset <command> [arguments...]

▶ **Available commands:**

factorydefaults   Reset device to factory defaults
unit   Reset and reboot device

reset factorydefaults
reset factorydefaults /y ...
  Reset device to factory defaults

 /y ...   Assume 'yes' as answer to questions

reset unit /y ...
  Reset and reboot device

 /y ...   Assume 'yes' as answer to questions

CLI: show

show

show <command> [arguments...]

▶ **Available commands:**

connectedusers	Shows connected user information
device	Shows Device information
eventlog	Shows event log
groups	Shows group information
history	Shows session command history
network	Shows all network information
security	Shows security settings
serial	Shows serial port parameters
terminalblock	Shows terminal block settings
time	Shows date/time information
user	Shows user information

```
# show connectedusers
--------------------------------------------------
User Name        IP Address     Client Type    Idle Time
--------------------------------------------------
admin            192.168.55.11      CLI (SSH)             0m
#
# show device
Device 'SteveKX4-101'
Product:          KX4
Model:            DKX4-101
Firmware Version: 4.0.0.1.45557
Hardware ID:      1
Serial Number:    1IT8400006
Internal Temperature Current Value: 38.7 C / 101.6 F
Internal Temperature Maximum Value: 39.6 C / 103.3 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 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

    MAC address: 00:0d:5d:00:02:d5

  IPv4

    Config method: DHCP

    Address: 192.168.50.35/24

    Preferred hostname: Not configured

    DHCP server: 192.168.50.115

  IPv6

    Disabled

\# 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
\# show serial
Configured console baud rate: 115200 bit/s
Configured modem baud rate: 115200 bit/s

Device detection type: Force console
Detected device: Console

\# show terminalblock

External input switch: Disabled

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)

show time

Device Time: 2019-03-11 13:50:26 EDT

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Setup Method: NTP synchronized

show user

User 'admin':

Enabled: Yes

Groups: Admin

SNMP v3 Access: Disabled

CLI: exit

exit

exit

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 for additional interface support:	▪ 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

Index

Raritan.
A brand of legrand

Raritan.
A brand of **legrand**