Dominion User Station User Guide

Contents

Raritan.
A brand of legrand®

Raritan.
A brand of **legrand**

Raritan®

A brand of legrand®

FCC Information

This Equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

Raritan.
A brand of legrand®

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
　取扱説明書に従って正しい取り扱いをして下さい。

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

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

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

What's New in Dominion User Station Release 5.1.0?

- Added Network Diagnostic tools to investigate network issues: Network Diagnostics (on page 272)
- 802.1x certificates and keys keys can be stored on the Dominion User Station
- New option to restore previously saved monitor settings
- Added new feature to auto save current windows layout at intervals: Window Layouts (on page 187)
- Support CC-SG 12.0

Introduction

This chapter introduces the Dominion User Station.

Overview

The Dominion User Station (DKX3/DKX4-UST, DKX3/DKX4-EUST) is designed to access servers and computer devices connected to Dominion KX III and Dominion KX IV-101 KVM and SXII Serial switches from customer LAN/WAN networks. Access to servers and devices on the network via RDP, SSH, and VNC is also supported. Additional access to web applications can be added using WEB and ESXi access points.

Note: For information on Dominion KVM and Serial switches, access the user documentation from its application or the Raritan website's Support page.

You can store the IP addresses of multiple KVM and Serial switches on the Dominion User Station so that you can remotely access any IT device connected to these KVM and Serial switches with only one click.

▶ *Illustration diagram:*
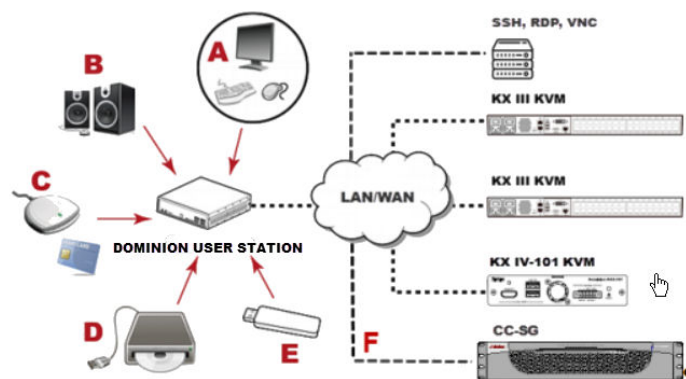
A	**A USB Keyboard, USB mouse, and one or two HDMI- or DisplayPort-interfaced monitors**
B	**Analog or digital audio appliances**
C	**Optional SmartCard reader for remote IT device authentication and SmartCard login as Cc-SG user**
D	**External drives as virtual media, such as CD-ROM**
E	**USB drives for virtual media or User Station software update**
F	**Optional integration with CC-SG**

Package Contents

DKX3/DKX4-UST and DKX3-EUST:

- Dominion User Station hardware
- Power adapter
- VESA mount kit
- Quick Setup Guide
- L-type rackmount kit (optional) is only available for DKX3/DKX4-UST and DKX3-EUST

Note: To mount the User Station in a 19-inch data center rack, you must purchase the L-type rackmount kit from Raritan. Refer to the online help or user guide for rackmount instructions.

DKX4-EUST:

- Dominion User Station hardware
- Power adapter
- VESA mount kit

Product Features

- Support KVM and Serial-over-IP connections to target servers

---

Note: The User Station CANNOT access a KVM port that is connected to a tiered KVM switch or a blade chassis server.

- Support of RDP, VNC, SSH, ESXi and Web targets
- Support a HDMI or DisplayPort-interfaced monitor
- Support for up to 4 monitors
- Support dual LAN connections
- Support virtual media, including external DVD, USB drives or network storage

---

Note: Virtual media is supported only when the accessed KX device supports it and you have permissions to use virtual media. See Virtual Media (on page 147).

- Support USB audio
- Support power control for target servers (with Raritan PX PDUs)
- Support authentication to target servers via an optional SmartCard
- Support authentication and authorization via LDAP
- Support the optional FIPS 140-2 mode
- Support authentication and authorization via CC-SG

Introduction to the User Station

Front View

DKX4-UST:

DKX3-UST Version 2:

1. Microphone input
2. Audio output
3. Power LED
4. Hard disk LED
5. Power button
6. SD card reader (not available)
7. USB 2.0 and 3.1* ports

DKX3-UST Version 1:
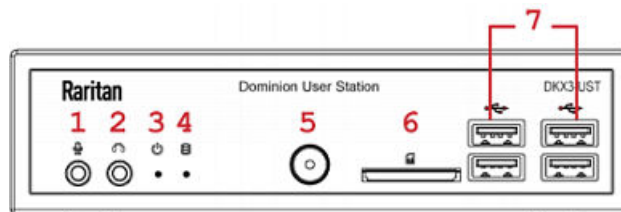
DKX4-UST and DKX3-UST Version 2 models only

DKX3-EUST:

1. Microphone output
2. Audio output
3. Power button
4. Type-A USB 3.2
5. Type -C USB 3.2
6. USB 2.0 ports

DKX4-EUST:
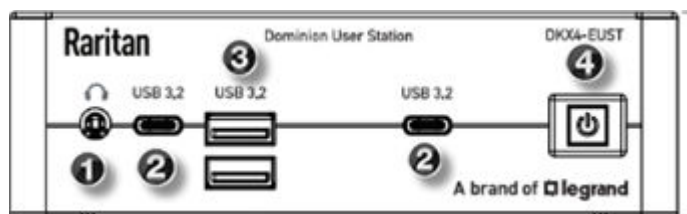
1. Audio output*
2. Type-C USB 3.2
3. Type -A USB 3.2
4. Power button

Audio output port can support speaker and microphone via a 3.5 mm stereo Y cable (not included in the package).

Rear View

DKX4-UST:

1. RS232/RS422/ RS485

2. RS232

3. DC power input

4. Gigabit LAN port 1

5. Gigabit LAN port 2

6-7. USB Ports

KX3-UST and KX3-UST Version 2: USB 2.0, 3.0

KX4-UST only: USB 3.1

8. DisplayPort (DP) video 1

9. DisplayPort (DP) video 2

10. HDMI video

11. Connector for external power button

DKX3-UST Version 2:

DKX3-UST Version 1:
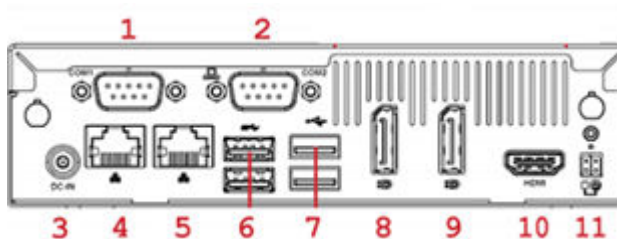
DKX4-EUST:
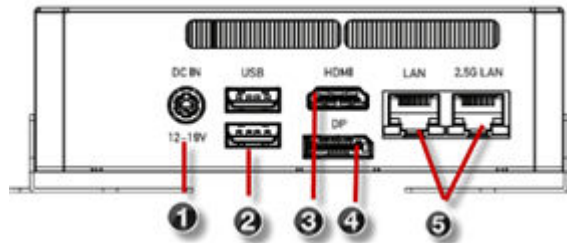
1. DC power input
2. USB ports
3. HDMI video
4. DisplayPort video
5. 1 Gigabit & 2.5 Gigabit LAN port

DKX3-EUST:

1. DC power input
2. USB ports
3. HDMI video
4. DisplayPort video
5. 2 Gigabit LAN ports

Side View
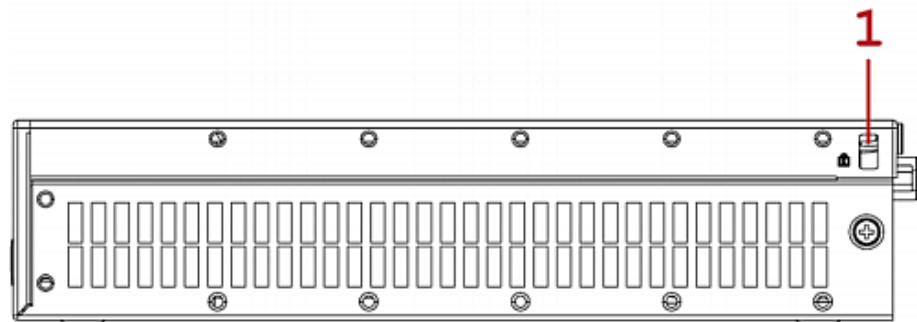
1. Kensington Lock holes

Introduction to the Software

After powering on the User Station, the Login Screen is shown.

After successfully logging in to the User Station, the Main Screen displays.

Login Screen
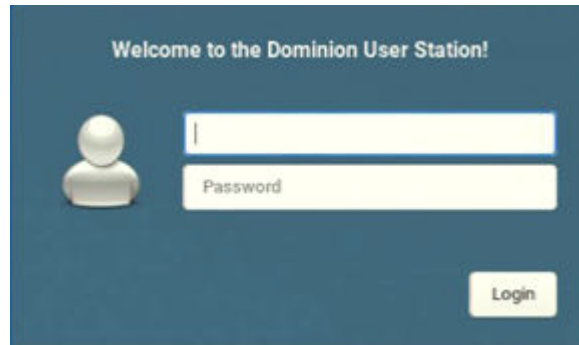
- System date and time

- Keyboard language (default US English) and Restart or Shut Down

- Login: The login icon indicates the authentication type being used: Local, LDAP, CC-SG, or SmartCard with CC-SG intergration.

- A local authentication checkbox is available whenever the user name "admin" is entered, and for all users when "Allow access for local users" is enabled in either LDAP or CC-SG integration mode.
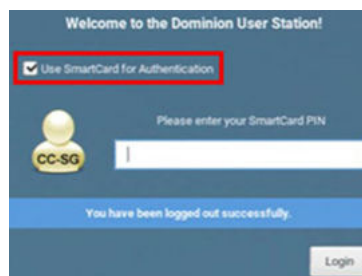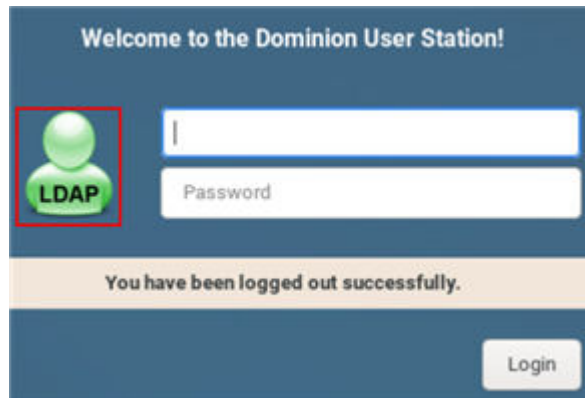
Main Menu, Port Navigator, Toolbar

The screen displayed after login is the Main Screen. When logging in for the first time, a welcome message is displayed.

The Main Menu and toolbar is located at the bottom of this screen. This toolbar shows the Main Menu, shortcut icons and lists any open User Station and KVM and Serial Client windows.

The Port Navigator opens by default, and can be closed then re-opened from the Main Menu.
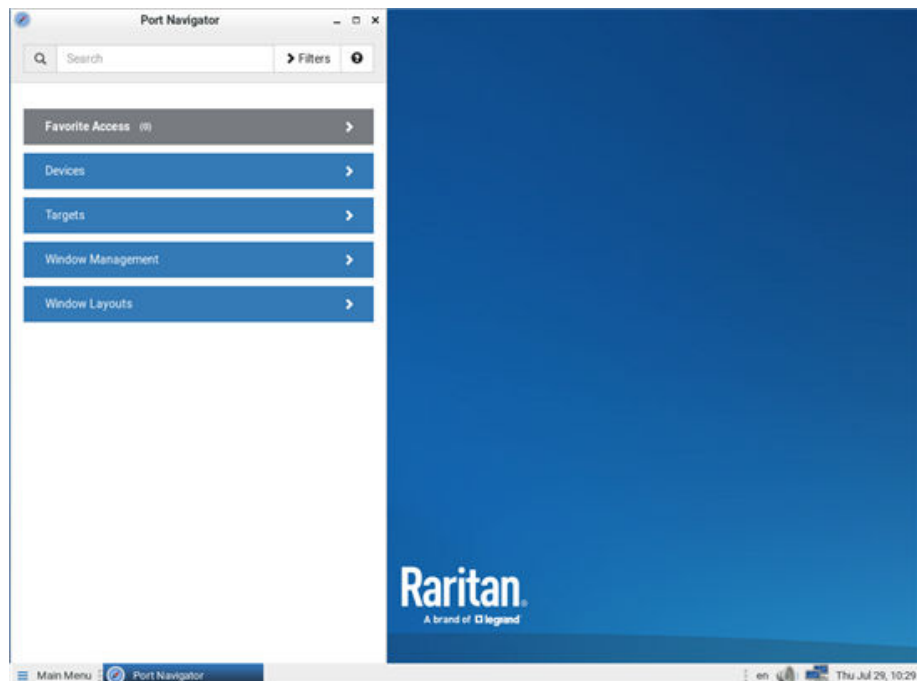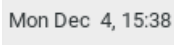
- Main Menu:

This menu contains the primary User Station commands and system settings.

- Open window(s):

  If any window is launched, its name is shown in the Toolbar. In the above diagram, only the Port Navigator window is launched.

  You can right-click any open window in the Toolbar to minimize, maximize, move, resize and so on.

- Shortcut icons for viewing/configuring system settings:

  Hover your mouse pointer over an icon to view information, or click or right-click it to configure settings.

Note: The above diagram shows factory default icons. More icons may be available if you change any system settings. For example, Monitor (on page 28).

Default icons	Description
en	The Keyboard Layout icon indicates the current keyboard layout. The default is *en* (American English). See Keyboard Layout Icon (on page 50).
🔊	This icon controls the volume. See Volume Icon (on page 50).
🖥️	This icon shows or configures the network information. See Network Icon (on page 50).
Mon Dec 4, 15:38	The Clock icon indicates the day of the week, date and current time. See Clock Icon (on page 52).

Online Help

You can access the online help for the Dominion User Station in the Main Menu.

▶ *Online help:*

- Choose Main Menu > Help > User Manual.

  You must be connected to the Internet to access Dominion User Station's online help.
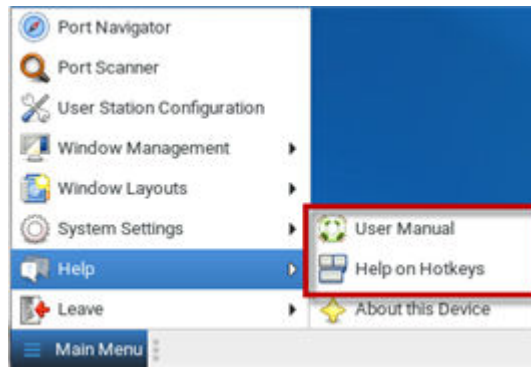
Help on Hotkeys

You can also access this list of pre-programmed and user-configurable hot keys for the User Station in the Main Menu.

- Choose Main Menu > Help > Help on Hotkeys.

► *Hotkeys in the Dominion User Station*

Dominion User Station has a number of pre-defined and user configurable hotkeys implemented to open tools, move or resize windows, open target windows or perform some operations.

Most of the desktop hotkeys can be configured by the user (Preferences > Hotkeys and Gestures), including the possibility to disable them. The key combinations listed below are the factory defaults for these hotkeys. This guide does not mention operations whose hotkeys are disabled by default.

► *Dominion User Station Functions*

- Ctrl + Alt + N

  Launch the Dominion User Station Port Navigator
- Ctrl + Alt + C

  Launch the Dominion User Station Configuration
- Ctrl + Alt + L

  Lock the Dominion User Station Screen
- Ctrl + Alt + Del

  Shut down or restart the Dominion User Station

► *Window Management Functions*

The following hotkeys are useful to close the currently active window or switch between windows.

- Alt + F4

Close the active window.

- Alt + Tab

  Switch focus to the next window.

- Shift+Alt+Tab

  Switch focus to the previous window.

The next keys are used to move and resize the open windows and switch between windows. They are not configurable individually but can be enabled or disabled globally. Note that the keypad keys are functional independently of the status of Num Lock. Keypad 4, 6. 8, 2 act as Left, Right, Up and Down respectively.

- Shift+Win + [Left/Right/Up/Down]

  Switch focus to the window in the direction specified of the currently focused window.

- Ctrl+Alt+Shift+[Left/Right]

  Move the active window to the previous/next monitor.

- Ctrl+Alt+[Left/Right/Up/Down]

  Move the active window to the left/right/top/bottom edge of the current monitor.

- Ctrl+Alt+[Keypad-1/3/9/7]

  Move the active window to the corners of the current monitor.

- Ctrl+Shift+[[Left/Right/Up/Down]

  Move the active window to the nearest edge in the direction specified.

- Ctrl+Windows + [Left/Right/Up/Down]

  Grows the active window until it touches the nearest edge in the direction specified.

  Edges are the outer edges of the other windows, monitor edges in multi nonitor setups, or hte desktop boundaries. If the window edge is at the screen edge already, it is shrunk instead.

- Alt+Windows + [Left/Right/Up/Down]

  Shrinks the active window until it touches the nearest edge in the direction specified. Edges are the outer edges of the other windows, monitor edges in multi monitor setups, or thedesktop boundaries. If no edge is found, the window is halved in size.

▶ *Access Client Functions*

The following hotkeys are only available during a running target connection.

- Control Alt M

  Leave Single Cursor Mode (KVM Clients only). Only available if in single cursor mode. Single cursor mode not available if the hotkey is disabled.

- Ctrl + Alt+ F

Enter or leave full screen mode on KVM and VNC Clients.

- Ctrl + Alt + Enter

  Enter or leave full screen mode on RDP clients.

- F11

  Enter or leave full screen mode in SSH, Serial, or ESXi clients.

► *Target Hotkeys*

You can configure target hotkeys for quick access to KVM ports or other targets. For KVM ports, open the Configuration, select a KX device, select a port, and click Edit Preferences. For other targets, select Targets, choose an Access Point to this target, then click Edit Preferences. Select the hotkey you want to use for this port and click OK.

Options include:

- Ctrl+Shift +<F key>
- Ctrl+Shift +<letter>
- Ctrl+Alt+<number>
- Ctrl+Alt+<letter>
- Shift + Alt + <F key>
- Shift + Alt + <letter>
- Ctrl+Shift+Alt+<F key>
- Ctrl + Shift +Alt + <letter>

Notes: A few hotkey combinations might be overridden by the user station system. Test all hotkey combinations to make sure they work properly.

Key combinations configured for User Station Functions or Access Client Functions cannot be used as Target Hotkeys.

Main Menu

Main menu provides access to the following items:

- Port Navigator. See: Port Navigator (on page 114)
- Port Scanner. See: Port Scanner (Launch) (on page 57)
- User Station Configuration
- Window Management. See Window Management (on page 58)
- Window Layouts. See Window Layouts (Create) (on page 56)
- System Settings. See:System Settings (on page 21)
- Help
- Leave

In This Chapter
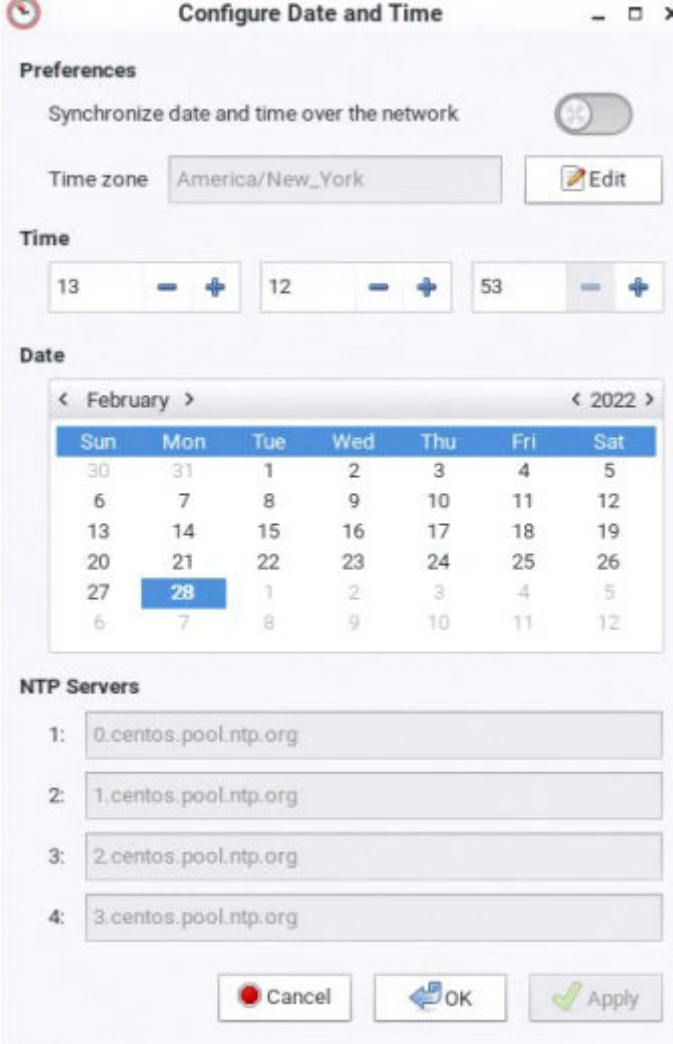
System Settings

System Settings are found in the Main Menu.
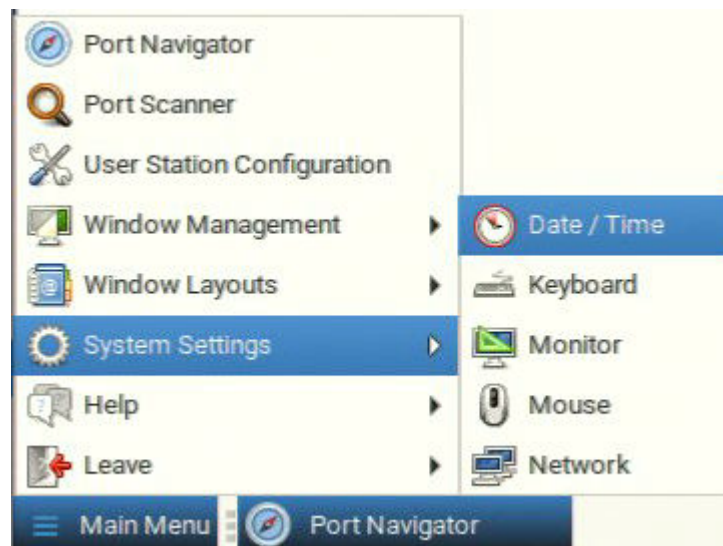
Date/Time

1. Choose Main Menu > System Settings > Date/Time. The date/time dialog appears.
2. See Time Zone (on page 23) for details on how time zone is used by manual and NTP date/time configurations.
3. Up to 4 NTP servers can be added.

Raritan.
A brand of Legrand

► *To manually set date and time:*

- Click Edit and set the correct Time Zone if needed, then use the Time and Date sections to configure the current date and time. Note that the Time section uses a 24-Hour clock. Click Apply or OK when complete.

► *To use NTP:*

- Turn on "Synchronize date and time over network".
- Click Edit and set the correct Time Zone if needed.
- Click OK.

Note: It may take a few minutes before the NTP Date and Time is applied. It is not recommended to use Windows NTP Servers.

Time Zone

The time zone setting is important for both manual and NTP-synchronized time. If it is correct, do NOT change it unless required.

- For the time synchronized with an NTP server, time zone changes affect the time displayed onscreen, daylight savings time, and internal UTC-based clock of the User Station.
- For the manual date and time, time zone changes do NOT affect the time displayed onscreen, but they affect the internal UTC-based clock.
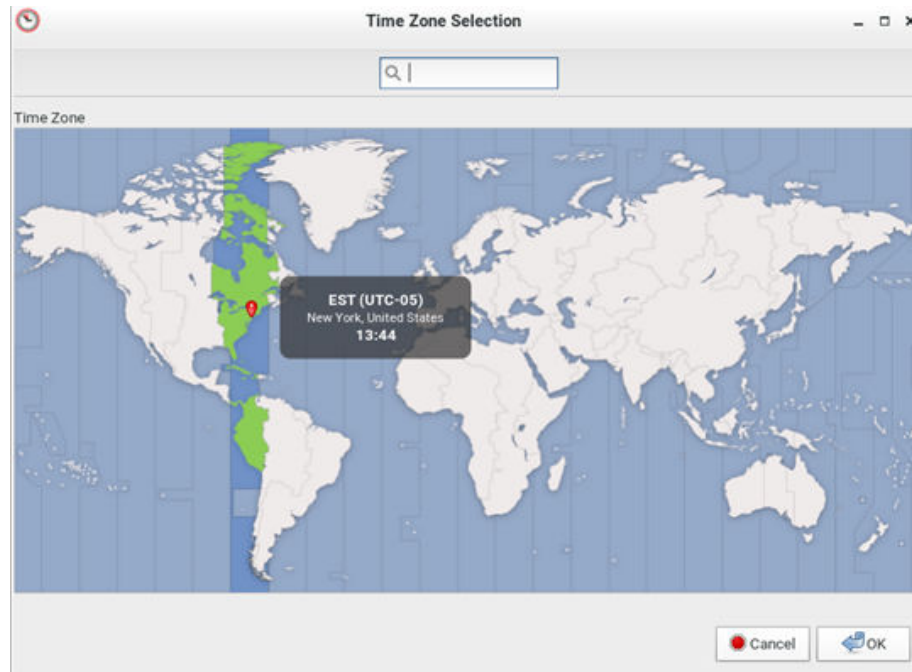
- Click Edit in the Date/Time settings to access the time zone map.
- Use the search box to find your city or zone Select it to highlight it on the map, then click OK.

Keyboard

1. Choose Main Menu > System Settings > Keyboard. The Keyboard Preferences dialog appears.

Raritan.
A brand of ☐ legrand
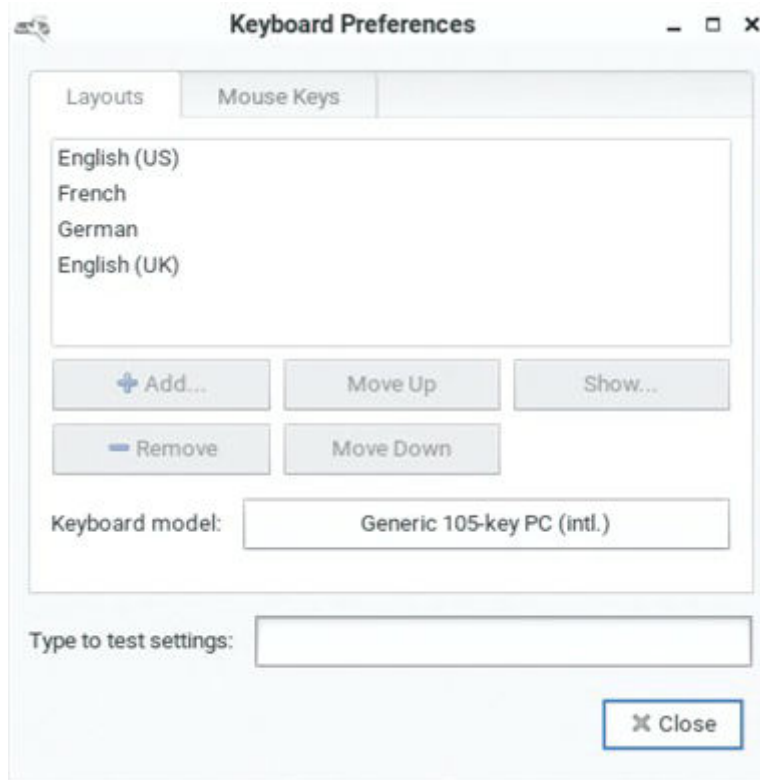
2. Click any tab to configure different keyboard settings.

- Configure the keyboard layout in the tab labeled Keyboard Layouts (on page 25).
- To use the keypad to move the mouse pointer, configure Mouse Keys (on page 27).

1. In the "Type to test settings" field, type anything to verify the current keyboard settings.

Keyboard Layouts

In the Layouts tab, available keyboard layouts are all shown. The same keyboard layout list is also available when working with the keyboard icon in the Main Toolbar. Any changes made to the dialog's keyboard changes the keyboard. Layout list also change the keyboard layout list available in the Main Toolbar. See Main Menu, Port Navigator, Toolbar (on page 16).

A maximum of four layouts are supported. If you have four layouts, you must remove one before you can add a new layout.

![Raritan logo] Raritan.
A brand of ☐ legrand

► *To manage available keyboard layouts:*
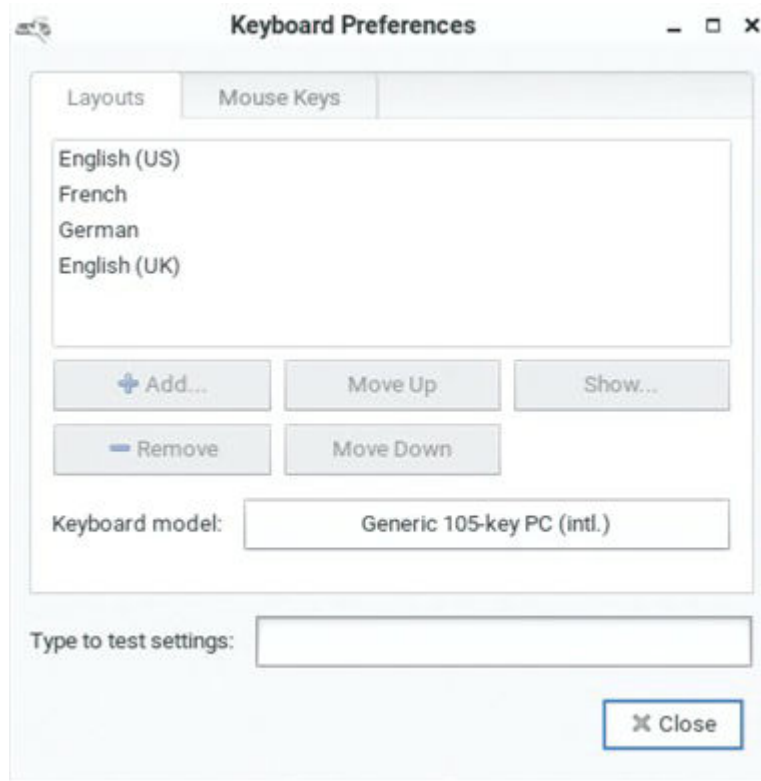
- To restore the keyboard layout list, select one layout and click Move Up or Move Down.
- To delete a layout from the list, select it and click Remove.
- To view keyboard layout, select it and click Show.
- To add a layout to the list, click Add. If four layouts are already listed, you must remove one before you can add another. After clicking Add, select a layout by County or Language to preview the keyboard layout. Click Add to add the layout to your list.
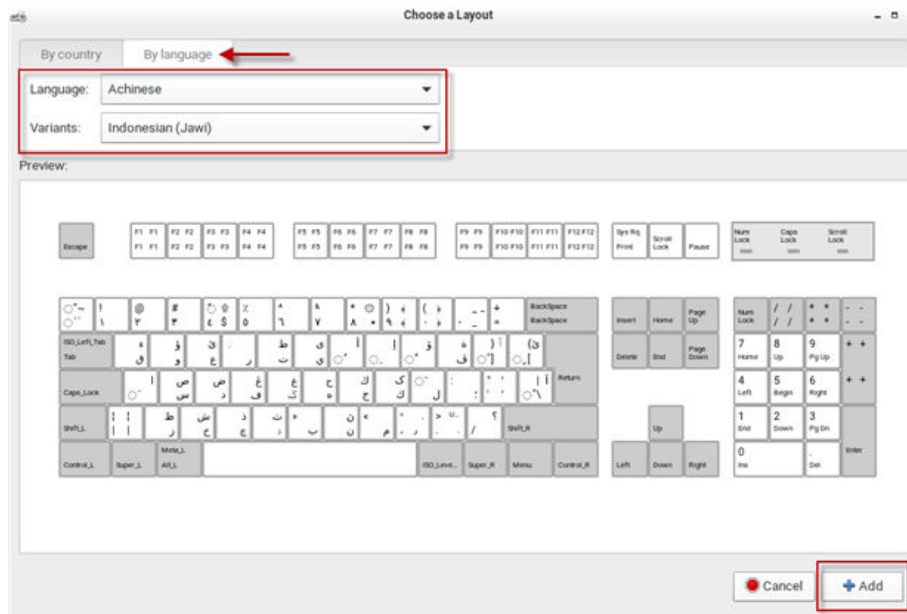
▶ *To determine the keyboard model:*

- Click the button in the "Keyboard model" field. Then select the vendor and model of your keyboard.

Mouse Keys

When you want to use the numeric keypad to control the mouse pointer/cursor, select the checkbox labeled "Pointer can be controlled using the keyboard."

When enabled, each keypad key functions as the following table.

Key	Function
0	Depress the selected button
.	Release the selected button
1	Move toward the bottom-left corner
2	Move down
3	Move toward the bottom-right corner
4	Move left
5	Click the selected button
6	Move right
7	Move toward the top-left corner
8	Move up
9	Move toward the top-right corner

Key	Function
/	Select primary button
-	Select alternate button
+	Double click the selected button
Enter	Enter

- Acceleration: Use the slider bar to adjust the pointer acceleration rate. Left side is faster and right side is slower.
- Speed: Use the slider bar to adjust the pointer speed. Left side is slower and right side is faster.
- Delay: Use the slider bar to adjust the delay prior to pointer movement. Left side is shorter and right side is faster.

Monitor

1. Choose Main Menu > System Settings > Monitor. The Monitor Preferences dialog appears.
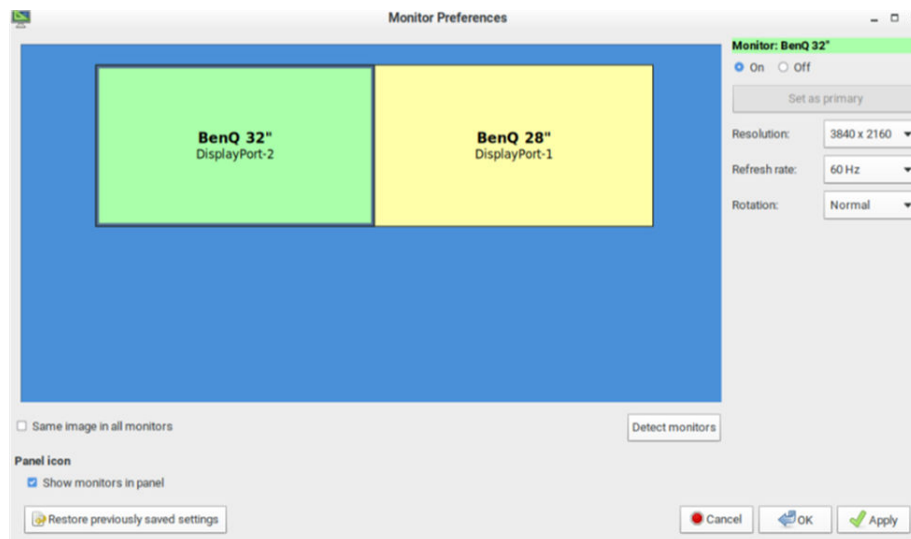
2. Perform or configure any of the following functions:

Setting/button	Function
On/Off	Turn on or off this monitor, if more than one monitor is connected to the User Station. This setting is disabled when only one monitor is connected.
Set as primary	Click this button to specify this monitor as the primary monitor, when there are multiple monitors connected. This button is disabled when: • Only one monitor is connected. • Or this monitor has been set as the primary one.
Resolution	Determine the video resolution applied to this monitor.

Raritan.
A brand of Llegrand

Setting/button	Function
Refresh rate	Determine the refresh rate applied to this monitor.
Rotation	Determine how the image on the screen should be rotated, if intended.
Same image in all monitors	If more than one monitor is a connected, determine whether all monitors show the same image. This setting is disabled when only one monitor is connected.
Detect monitors	Click this button if any connected monitor is not detected. Usually it is not necessary to use this function when there is only one monitor connected.
Show monitors in panel	Determine whether the monitor shortcut icon is added to the Main Toolbar. See Main Menu, Port Navigator, Toolbar (on page 16).
Restore previously saved settings	Click this button to restore the previous saved settings of all the monitors.

3. If any settings are changed, click OK to save and close the dialog, Apply to save and keep the dialog open, or Cancel to cancel.

- If clicking OK or Apply, a confirmation message appears. Click Restore Previous Configuration to restore to the original settings, or click Keep This Configuration to apply the new settings.

Mouse

The mouse preferences dialog affects how your mouse works in Dominion User Station screens only. These settings do not affect your mouse in the KVM Client. For those settings, see Mouse Settings (on page 134)

1. Choose Main Menu > System Settings > Mouse. The Mouse Preferences dialog appears.
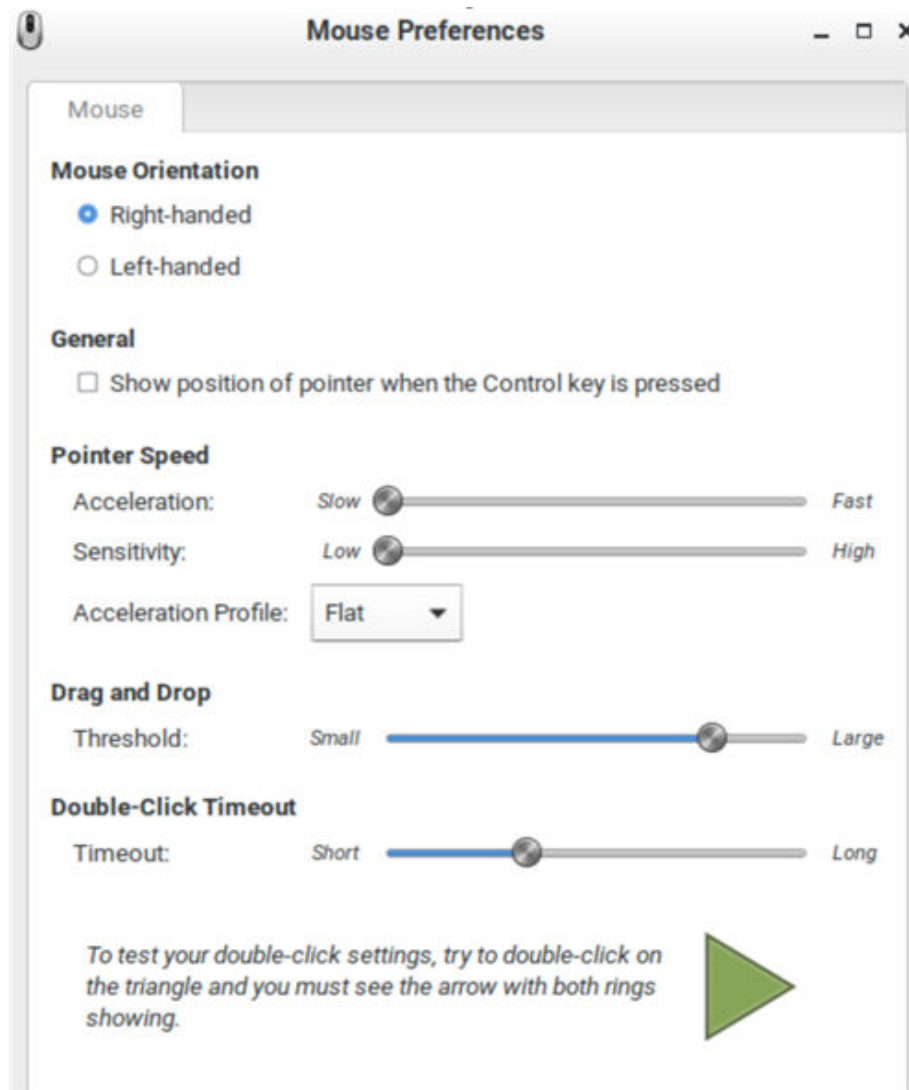
2. The following mouse settings can be adjusted:
   - Mouse Orientation: Right-handed or Left-handed
   - General: With option to show the position of the pointer when the Control key is pressed.
   - Pointer Speed: Adjust Acceleration and Sensitivity.
   - Acceleration Profile: Adaptive, Default, Flat.
   - Drag and Drop: Adjust the threshold for drag and drop operations.
   - Double-Click Timeout: Adjust from short to long. Double-click the green triangle to test the setting.
3. Click Close to exit the dialog.

Network

Network Connections - Ethernet

You can connect the two LAN ports of the User Station to the same or diverse subnets.

Raritan.
A brand of 🔲legrand

If you have connected both LAN ports to the network(s) when turning on or restarting the User Station, the User Station *randomly* selects one of the network connections as the default one. However, if you change the network settings of either or both connections, the "final" one that is changed will automatically become the default connection.

Note: You can identify the default connection in the Connection Information dialog. See Network Icon (on page 50).

By default, both IPv4 and IPv6 addressing are enabled for both LAN ports, and the following are the default network settings:

- IPv4: *Automatic (DHCP)*
- IPv6: *Automatic*

You can also set additional ethernet options, such as MTU and Wake on LAN: See Ethernet Settings (on page 33). You can also configure bond devices: See Network Connections - Bond Connections (on page 44).

► *To change network settings:*

1. Choose Main Menu > System Settings > Network. The Network Connections dialog appears, with two factory default connections listed for two LAN ports.
   - *Ethernet 1* is for LAN port 1, and *Ethernet 2* is for the other.
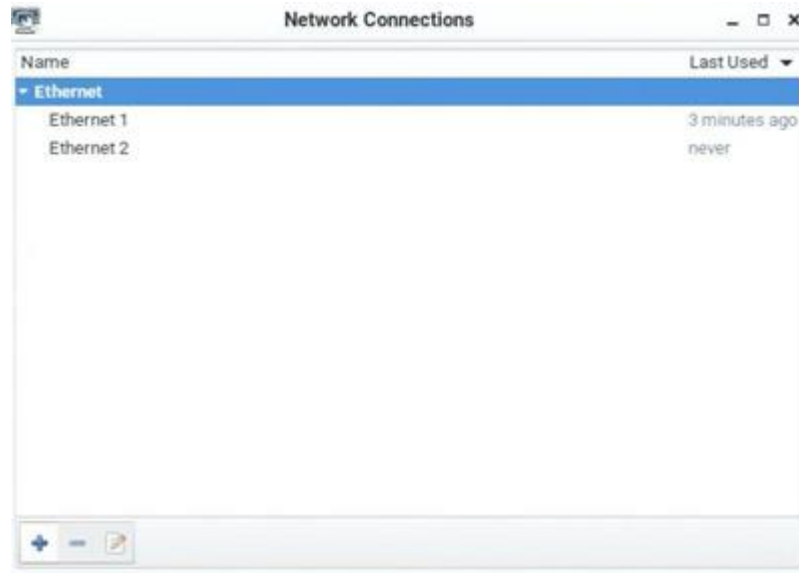
2. Select the desired connection, and click Edit. A dialog appears.
3. Enter a new name in the Connection name field if desired.
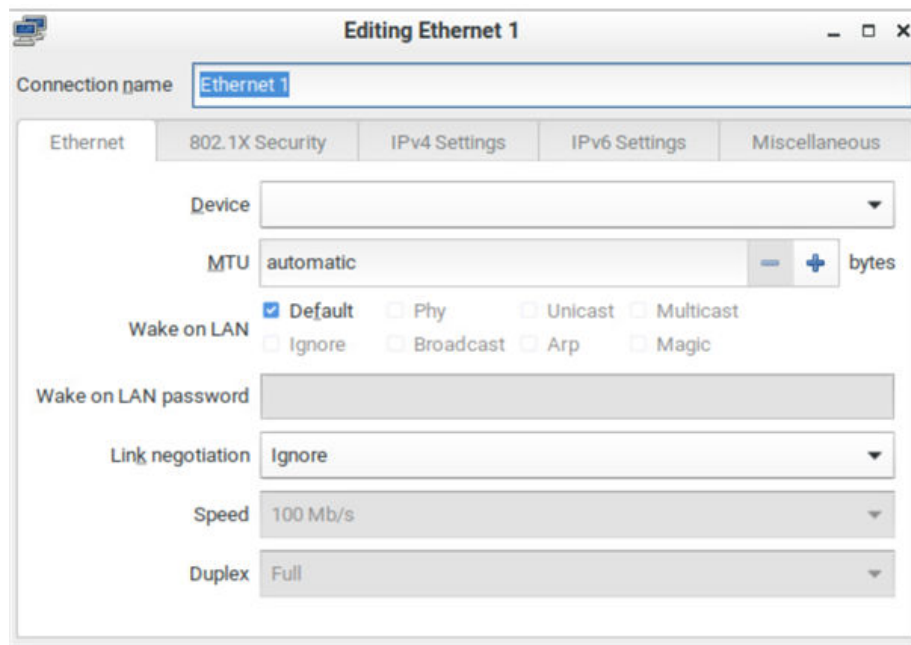
4. Click the IPv4 Settings or IPv6 Settings tab to configure network settings properly.

- IPv4 Settings:

Setting	Description
Method	Select one of the following as the connection method and configure associated settings: • Automatic (DHCP) • Automatic (DHCP) addresses only • Manual • Disabled See IPv4 Settings (on page 34).

- IPv6 Settings:

Setting	Description
Method	Select one of the following as the connection method: • Ignore • Automatic • Automatic, addresses only • Automatic, DHCP only • Manual • Disabled See IPv6 Settings (on page 36).

5. Click OK. The new network settings apply now.

Note: You can retrieve current IP addresses from the Connection Information dialog. See Network Icon (on page 50).

Ethernet Settings
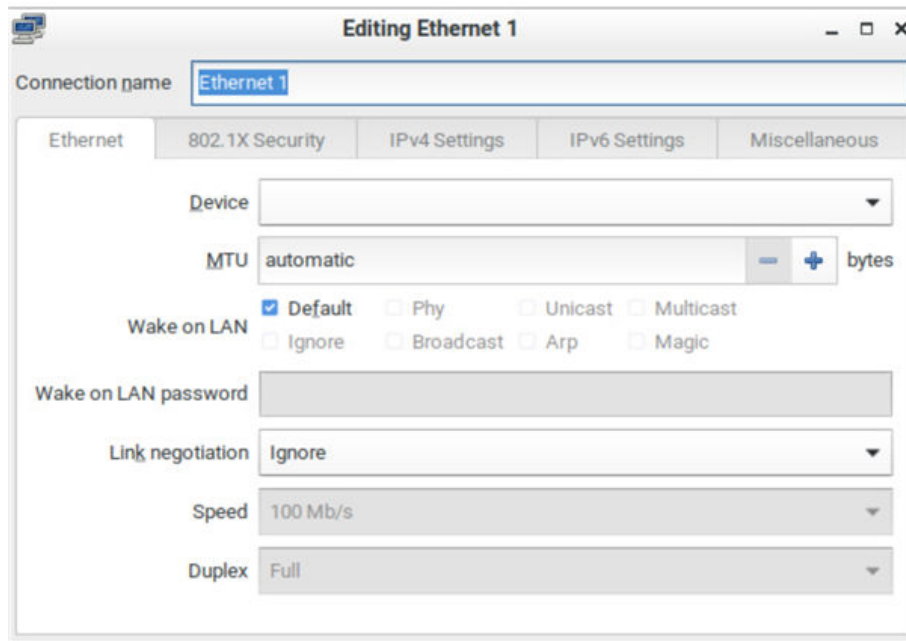
► *MTU:*

- Select Automatic, or click plus/minus to specify the maximum number of bytes per packet.

► *Wake on LAN:*

- Default: Leave as default, or deselect to enable other options.
- Phy
- Unicast
- Multicast
- Ignore
- Broadcast
- Arp
- Magic: Requires Wake on LAN password.

► *Link Negotiation:*

- Ignore
- Automatic
- Manual: Set Speed and Duplex.

IPv4 Settings

► *Automatic (DHCP):*

The DHCP server in the network automatically assigns an IPv4 address to the User Station as well as DNS server(s) and domain(s).

The following settings are configurable for this method.

Setting	Description
Additional DNS servers	Optional. You may specify IP addresses of one or multiple additional DNS servers for resolving host names. Use commas to separate multiple servers.
Additional search domains	Optional. You may specify IP addresses of one or multiple additional domains for resolving host names. Use commas to separate multiple domains.

Raritan.
A brand of ☐legrand

Setting	Description
DHCP client ID	Optional. You can specify a DHCP client ID for identifying this User Station in the network.
DHCP hostname	Optional. You can specify a preferred hostname to send to the DHCP server to use for DNS name resolution
Require IPv4 addressing for this connection to complete	When deselected, either IPv4 or IPv6 addressing can be used to establish the connection. When selected, only IPv4 addressing is used for making the connection.
Routes	Optional. Configure the IPv4 routing for this User Station. • Click Add to add one or multiple routing addresses for the User Station to reach in the network. • To remove any existing routes, select it and click Delete. • *Ignore automatically obtained routes*: Select this checkbox only when you want to use manually-specified routes. • *Use this connection only for resources on its network*: If selected, this connection will be used only when retrieving resources from the network. It will never be used as the default network connection.

Note: You can retrieve current IP addresses from the Connection Information dialog. See <u>Network Icon</u> (on page 50).

► *Automatic (DHCP) addresses only:*

The DHCP server in the network automatically assigns an IPv4 address to the User Station, but no DNS servers or domain servers are specified.

The following settings are configurable for this method.

Setting	Description
DNS servers	Specify IP addresses of one or multiple DNS servers. Use commas to separate multiple servers.
Search domains	Specify IP addresses of one or multiple domains for resolving host names. Use commas to separate multiple domains.

Setting	Description
DHCP client ID	See the above table for information of these fields/ options.
Require IPv4 addressing for this connection to complete	
DHCP hostname	
Routes	

► *Manual:*

Select this method when intending to manually assign a static IP address to the User Station.

In the Addresses section, click Add and then type the User Station's IPv4 address, netmask and gateway in this section. At least one IPv4 address, netmask and gateway must be specified.

Addresses

Address	Netmask	Gateway	
192.168.60.80	24	192.168.60.1	➕ Add
			⊗ Delete

The following settings are configurable for this method. See the above table for associated information.

- DNS servers
- Search domains
- Require IPv4 addressing for this connection to complete
- Routes

► *Disabled:*

The IPv4 networking settings are all disabled.

IPv6 Settings

Raritan.
A brand of ▢legrand

► *Automatic:*

IPv6 auto-configuration automatically assigns an IPv6 address to the User Station, and retrieves the information of DNS server(s) and domain(s) from the DHCP server.

The following settings are configurable for this method.

Setting	Description
Additional DNS servers	Optional. You may specify IP addresses of one or multiple additional DNS servers for resolving host names. Use commas to separate multiple servers.
Additional search domains	Optional. You may specify IP addresses of one or multiple additional domains for resolving host names. Use commas to separate multiple domains.

Setting	Description
IPv6 privacy extensions	Determine whether and how privacy extensions apply to the IPv6 addressing. • Disabled: Disables privacy extensions. • Enabled (prefer public address): Enables privacy extensions and a public address is preferred. • Enabled (prefer temporary address): Enables privacy extensions and a temporary address is preferred.
IPv6 address generation mode	Determine how the address is generated: • Stable privacy • EUI 64
Require IPv6 addressing for this connection to complete	When deselected, either IPv4 or IPv6 addressing can be used to establish the connection. When selected, only IPv6 addressing is used for making the connection.
Routes	Optional. Configure the IPv6 routing for this User Station. • Click Add to add one or multiple routing addresses for the User Station to reach in the network. • To remove any existing routes, select it and click Delete. • *Ignore automatically obtained routes*: Select this checkbox only when you want to use manually-specified routes. • *Use this connection only for resources on its network*: If selected, this connection will be used only when retrieving resources from the network. It will never be used as the default network connection.

Note: You can retrieve current IP addresses from the Connection Information dialog. See Network Icon (on page 50).

► *Automatic, addresses only:*

IPv6 autoconfiguration automatically assigns an IPv6 address to the User Station, but no DNS servers or domain servers are specified.

The following settings are configurable for this method.

Setting	Description
DNS servers	Specify IP addresses of one or multiple DNS servers. Use commas to separate multiple servers.

Raritan.
A brand of Llegrand

Setting	Description
Search domains	Specify IP addresses of one or multiple domains for resolving host names. Use commas to separate multiple domains.
IPv6 privacy extensions	See the above table for information of these fields/options.
Require IPv6 addressing for this connection to complete	
IPv6 address generation mode	
Routes	

► *Automatic, DHCP only:*

The DHCPv6 server in the network automatically assigns an IPv6 address to the User Station, and specify DNS server(s) and domain(s).

The following settings are configurable for this method. See the above table for associated information.

- IPv6 address generation mode
- Require IPv6 addressing for this connection to complete
- Routes

► *Manual:*

Select this method when intending to manually assign a static IP address to the User Station.

In the Addresses section, click Add and then type the User Station's IPv6 address, prefix and gateway in this section. At least one IPv6 address, prefix and gateway must be specified.

The following settings are configurable for this method. See the above table for associated information.

- DNS servers
- Search domains
- IPv6 address generation mode
- Require IPv6 addressing for this connection to complete
- Routes

► *Disabled:*

The IPv6 networking settings are all disabled.

Miscellaneous Settings

The Miscellaneous settings tab is used when you have a VPN configuration.

- Select the "Automatically connect to VPN when using this connection" to make sure your configured VPN is used automatically whenever the selected network is active.

802.1X Security Settings

IEEE 802.1X authentication can be configured independently on each LAN port to give the Dominion User Station secure access to your wired LAN. You have to configure an authentication server which supports Radius and EAP protocols.

Note: 802.1X authentication fails if FIPS 140-2 Mode is enabled on the KXUST

Dominion User Station supports following authentication methods with 802.1 security:

- MD5
- TLS
- PWD
- FAST
- Tunneled TLS
- Protected EAP (PEAP)

Raritan.
A brand of ☐ legrand
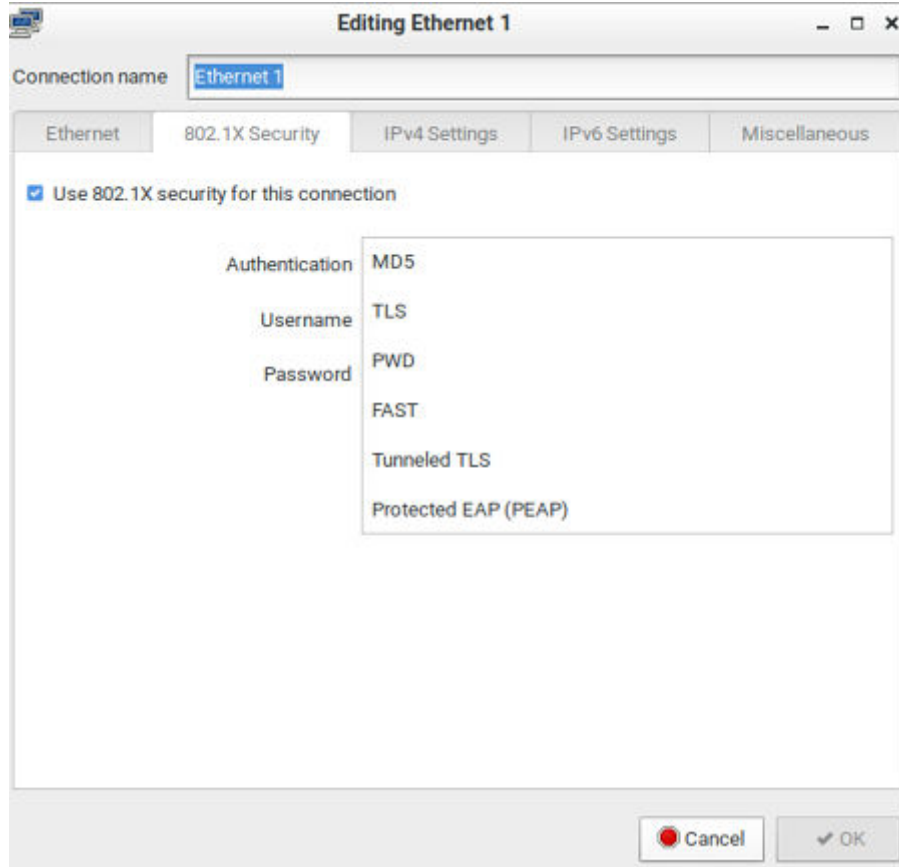
Configure 802.1X Security

► *To configure 802.1X security:*

1. Choose Main Menu > System Settings >Network >Ethernet 1 > 802.1X Security tab. The settings page opens.

Note: LAN1 and LAN2 settings are separate.
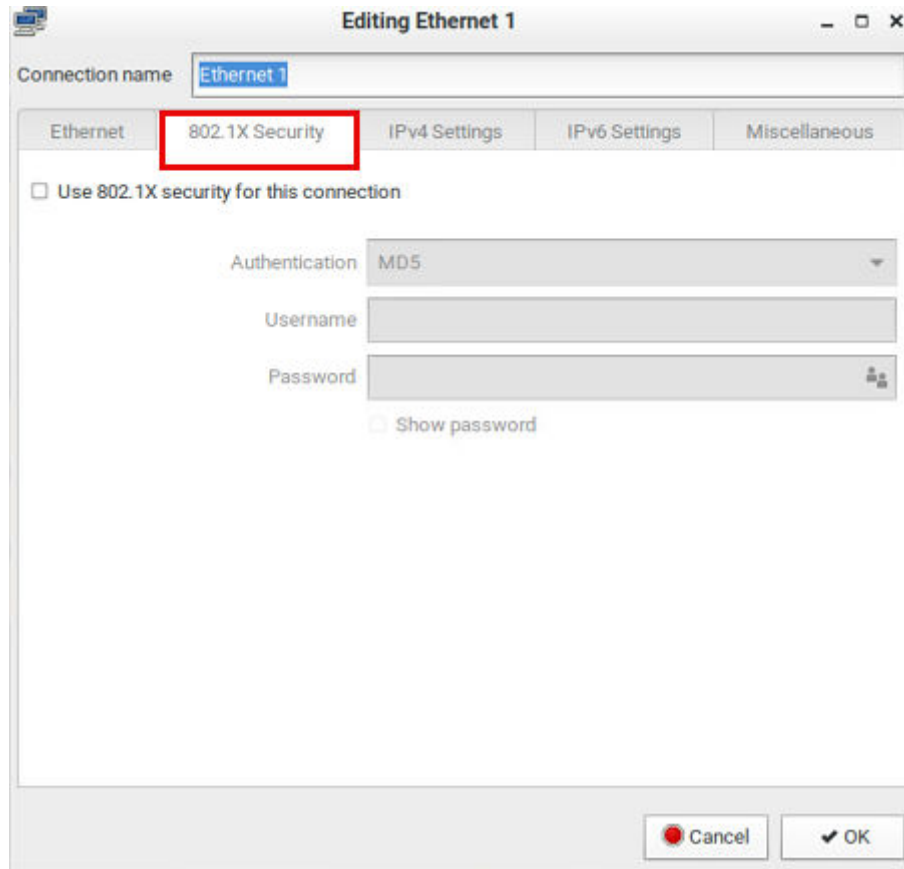
2. Select the "Use 802.1X security for this connection" check box to begin.
3. Select your Authentication method from the list.
   - MD5:
     - Enter the Username and Password.
     - Select Show password to see password unmasked.
   - TLS:
   - No CA Certificate required:
     - Enter the identity and domain.
     - Select "No CA Certificate is required" option. This will disable the CA Certificate field.
     - Choose option to select from file for User certificate.
     - Enter user certificate password if required.
     - Choose option to select from file for User private key.
     - Enter User key password.
   - Certificate required:
     - Enter a identity and domain.
     - Choose option to select from file to upload the CA certificate.
     - Enter the CA certificate password if required.
     - Select Show passwords to verify.

Raritan.
A brand of ▢legrand

- Choose option to select from file to upload User Certificate.
- Enter User certificate password if required.
- Enter User private key.
- Enter User key password.
- PWD:
  - Enter the Username and Password.
  - Select Show password to see password unmasked.
- FAST:
  - Enter Anonymous identity
  - If "Allow automatic PAC provisioning" is selected, choose a provisioning method from the list.
  - Upload PAC file.
  - Choose a method for Inner Authentication from the list.
  - Enter Username and Password.
- Tunneled TLS:
- No CA Certificate required:
  - Enter an Anonymous identity and Domain.
  - Select "No CA Certificate is required" option. This will disable the CA Certificate field.
  - Enter Inner Authentication option from the list.
  - Enter Username and Password.
- Certificate required:
  - Enter an Anonymous identity and Domain.
  - Choose option to select from file to upload the CA certificate.
  - Enter the CA certificate password if required.
  - Select Show passwords to verify.
  - Enter Inner Authentication option from the list.
  - Enter Username and Password.
- Protected EAP (PEAP):
- No Certificate required:
  - Enter an Anonymous identity and Domain.
  - Select "No CA Certificate is required" option. This will disable the CA Certificate field.
  - Select PEAP version.
  - Enter Inner Authentication option from the list.
  - Enter Username and Password.
- Certificate required:
  - Enter an Anonymous identity and Domain.
  - Choose option to select from file to upload the CA certificate.
  - Enter the CA certificate password if required.
  - Select Show passwords to verify.

- Select PEAP version.
- Enter Inner Authentication option from the list.
- Enter Username and Password.
4. Click OK.

Network Connections - Bond Connections

To create NIC redundancy, you can configure network bonding devices to replace the standard Ethernet configuration. This setup doubles the maximum network speed if both ports are used and provides redundancy. The Dominion User Station network will continue to work if either one of the ports fails.

1. Choose Main Menu > System Settings > Network. The Network Connections dialog opens.
2. Click the Add Icon (plus sign).
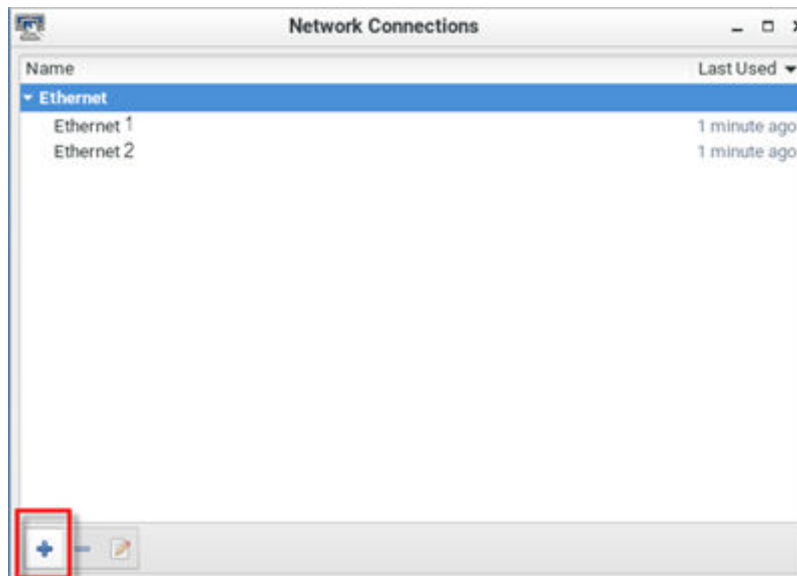
3. In the Choose a Connection Type dialog, select Bond, then click Create.
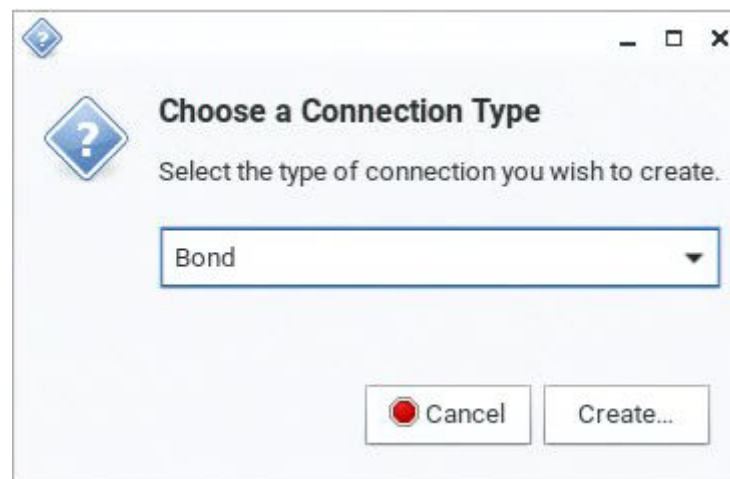
4. The Bond Connection dialog opens.

5. In the Bond tab, click Add.

6. Select the connection type you want to use for the bond connection, then click Create to create the first bond link for the first network interface.

7. In the bond link dialog, select the MAC address of the interface in the Device field. Click OK.

8. Click Add again to add the second bond link, which is automatically set as the same connection type.
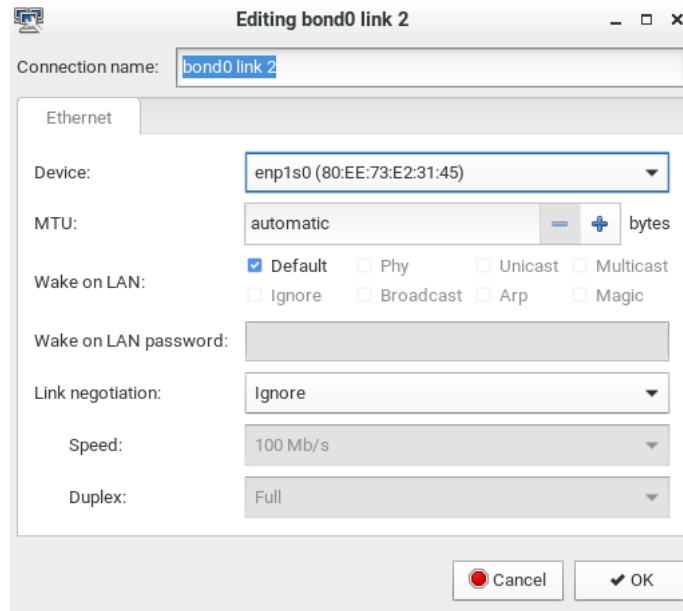
9. Click OK to save.
10. Return to the Main Menu > System Settings > Network page. Remove the old "Ethernet" entries, and keep the newly created "Bond Connection" entries.

OpenVPN Connections

An OpenVPN configuration can be uploaded to the Dominion User Station to use a VPN client for all connections. You must provide a valid config file including certificates server details as filetype .OVPN. Consult the OpenVPN documentation for details on creating the file. Once uploaded, if your configuration setup includes "connect automatically", the VPN will be connected when Dominion User Station reboots.

For CC-SG users to connect with VPN, the network setup must be done in advance by a local user.

► *To add OpenVPN connection:*

1. Choose Main Menu > System Settings > Network. The Network Connections dialog opens.
2. Click the Add Icon (plus sign).

Raritan.
A brand of legrand
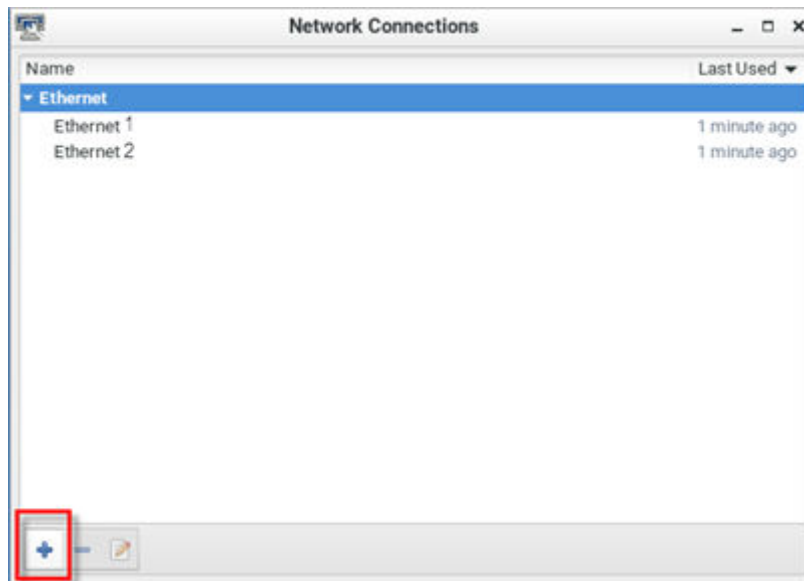
- In the Choose a Connection Type dialog, select "Import a saved VPN configuration..." then click Create.
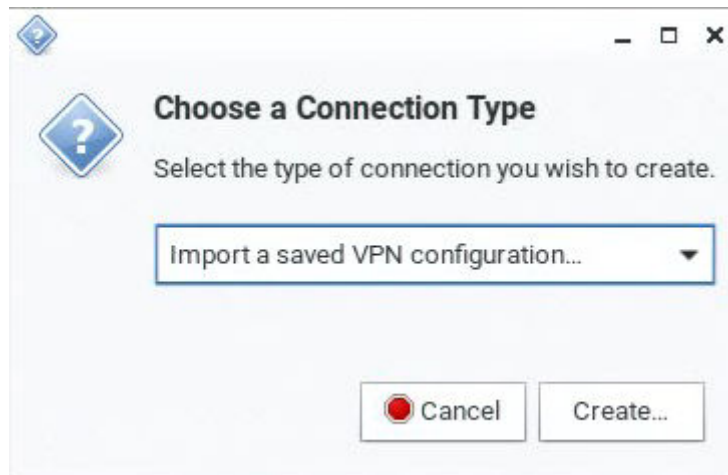
1. An upload dialog appears. Select the .ovpn config file, then click Open.
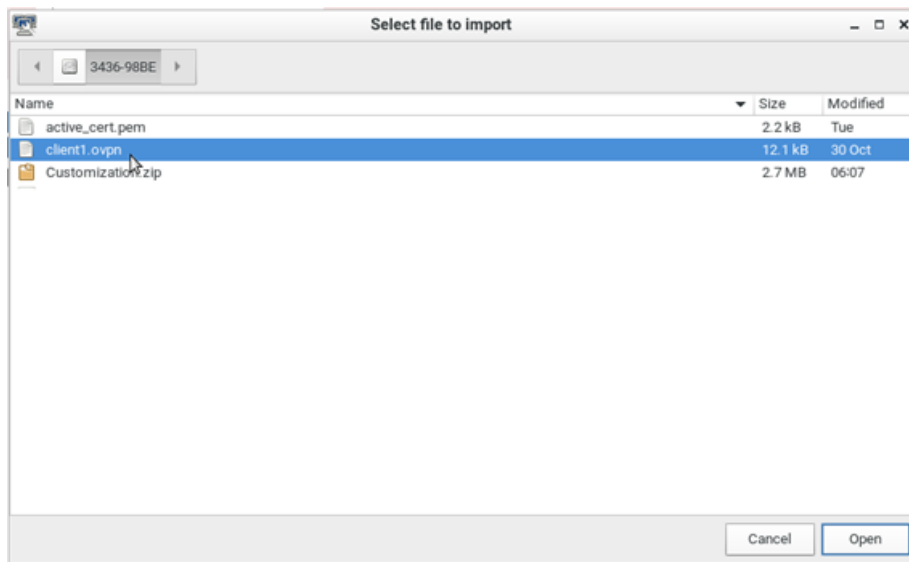
2. The VPN client is added. Select it and click the Edit icon.
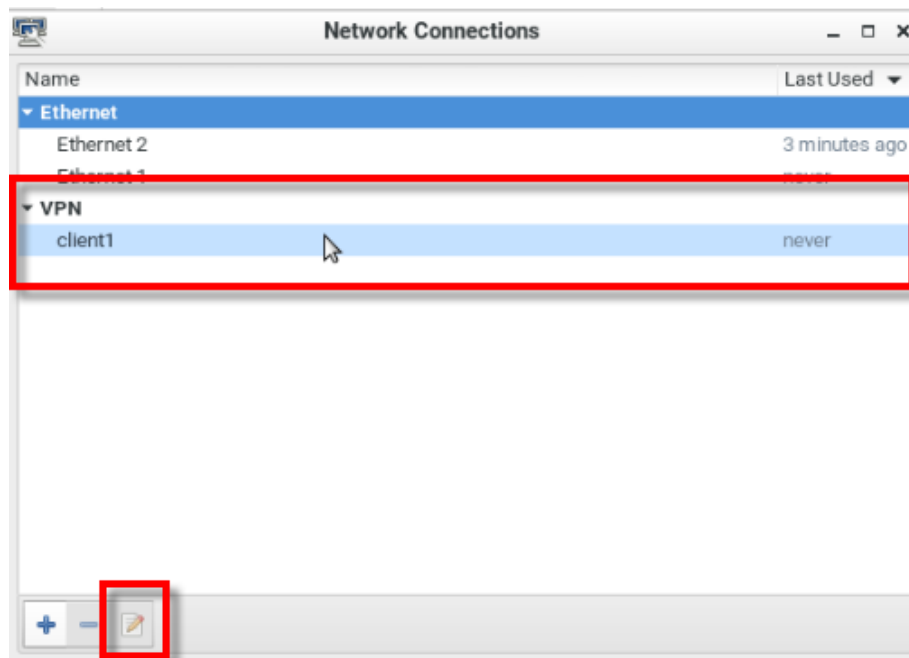
3. Edit the VPN Connection name and/or enter password.

Raritan.
A brand of legrand
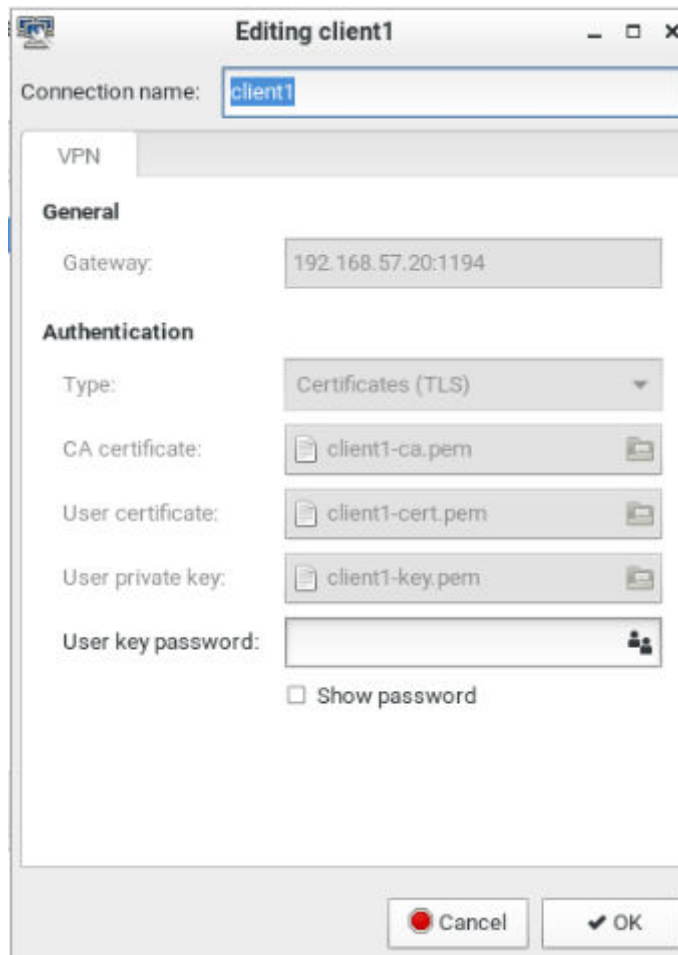
4. Click OK. When the VPN is connected, status bar will show that it is active. The "Lock" icon displays in the status bar when a user logs in with active VPN.
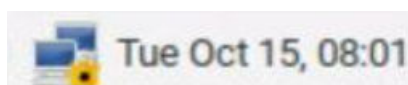
5. To automatically connect to VPN, edit the network connection, go to the Miscellaneous tab, and select "Automatically connect to VPN when using this connection". See Miscellaneous Settings (on page 40)

Default Shortcut Icons in the Main Toolbar

Shortcut icons in the Main Toolbar provides quick access to some system settings. For information on the Main Toolbar, see Main Menu, Port Navigator, Toolbar (on page 16).

This section introduces the following factory default icons.

Keyboard Layout Icon

► *Clicking the icon:*

The keyboard layout switches among available languages. By default, the following languages are available.

- *en* - English (US)
- *fr* - French
- *de* - German

► *Right-clicking the icon:*

A shortcut menu with these commands displays.

- *Layouts*: Changes the keyboard layout.
- *Keyboard Preferences*: Triggers the Keyboard Preferences dialog. See Keyboard (on page 24).
- *Show Current Layout*: Shows a keyboard image to indicate the current layout.

Volume Icon

► *Clicking the icon:*

A slider bar displays for you to adjust the volume.

► *Right-clicking the icon:*

A shortcut menu with this command displays.

- *Mute*: Mutes the sound.

Network Icon

► *Clicking the icon:*

A list of available Ethernet networks and connections displays.

- Only one network connection is shown if only one LAN port is connected to the network.
- Two network connections are listed if both LAN ports are connected to the network.
- By default, *Ethernet 1* is for LAN port 1, and *Ethernet 2* is for the other.
- You must have the System permission to make changes to network settings.

An "active" network connection is highlighted in bold, with a Disconnect command following it. To disable any active connection, select Disconnect.

- The formatting of that connection's name turns from bold to normal, indicating that it becomes inactive.

To activate any disabled network connection shown in the list, click it.

- The formatting of that connection's name turns from normal to bold, indicating that it becomes active.

► *Right-clicking the icon:*

A shortcut menu with these commands displays.

- *Enable Networking*: Enables or disables the networking capability. The default is to enable it.
- *Connection Information*: This command shows the networking information of the User Station, including IPv4 and IPv6 addresses.
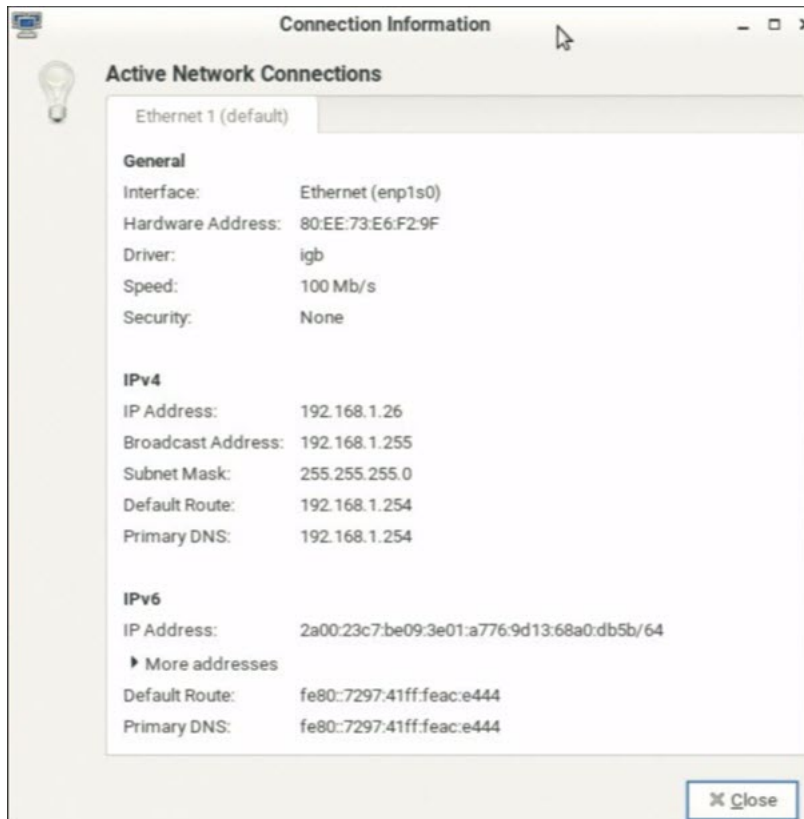
- When only one network connection is active, this dialog shows one tab.
- When both network connections are active, this dialog shows two tabs.
- The default connection has the word "default" shown on its tab.
- *Edit Connections*: This triggers the Network Connections dialog. See Network Connections - Ethernet (on page 30).

Clock Icon

► *Clicking the icon:*

A calendar with Locations section displays.

Click Locations to:

- Determine the location and time zone of the User Station.
- Change the time format of the clock shown in the Main Toolbar.

For details, see Location and Clock Time Format (on page 53).

To close the calendar, click the clock icon in the Main Toolbar again.

► *Right-clicking the icon:*

A shortcut menu with this command displays. You must have the System permission to change Date/Time settings.

- *Adjust Date & Time*: This triggers the date/time dialog. You must have Systems permissions to change the date and time. See Date/Time (on page 22).

Location and Clock Time Format

After expanding the Locations section, click Edit.

The Clock Preferences dialog appears. Click the desired tab or button to configure settings.
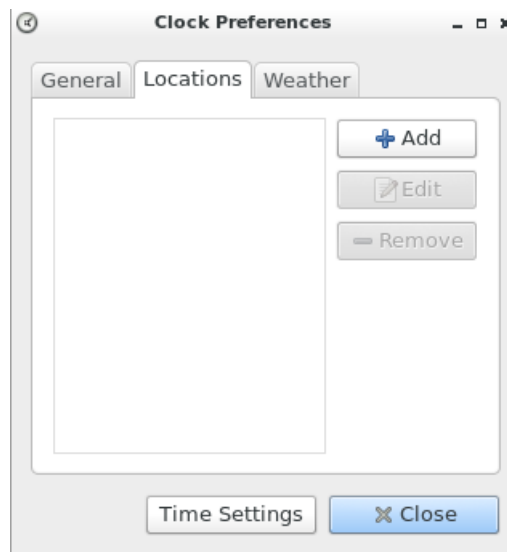
► *Time Settings:*

- See [Date/Time](#) (on page 22).

► *Locations:*

- Click Add to specify your city or country.
  - You can simply type the city or country name in the Location Name field and then select the correct one from the list that appears.
  - If your city's or country's name is not available in the list, you can manually specify the Timezone, Latitude and Longitude.
- To modify or delete any existing location in the Locations tab, select it and click Edit or Remove.

► *General:*

- *Clock Format*: Select the desired clock format to be shown in the Main Toolbar - 12 or 24 hour format.
- *Panel Display*: Select the information that is shown or available via the Main Toolbar - date, seconds, week numbers, weather and temperature.
  - Date and seconds, if selected, are shown in the clock on the Main Toolbar.
  - Week numbers, if selected, are shown in the calendar. A week number is the week's sequential number in a year.

- Weather and temperature, if selected, are shown in the following two positions:
- ▪ The Main Toolbar
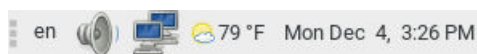
- ▪ The Locations section: When you hover your mouse pointer over the weather icon below the location name, more information is displayed, including the weather, temperature, wind speed and the time for sunrise/sunset.

Tip: If the system's time zone setting is different from the selected location's and you have the System Administration privilege, a "Set" button appears to the right of the location name when hovering the mouse pointer around it. You can click the button to set the location's time zone as the system's time zone.

► *Weather:*

- Determine the temperature unit: C (degree Celsius), F (degree Fahrenheit) or K (degree Kelvin).
- Determine the wind speed unit: m/s, km/h, mph, knots, or Beaufort scale.

Window Layouts (Create)

The window layouts feature allows you to save layouts of running access client windows so that the specific layout can be restored upon selection. The window layout data that is saved includes the visual attributes of each access client session, such as size, position, and displaying monitor, as well as the connection information for each.

Layouts are saved on a per user basis. The layouts saved by one user are not available to other users. There is a maximum of 16 named layouts per user.

You can access Window Layouts in the Port Navigator or the Main Menu.

Raritan.
A brand of Legrand
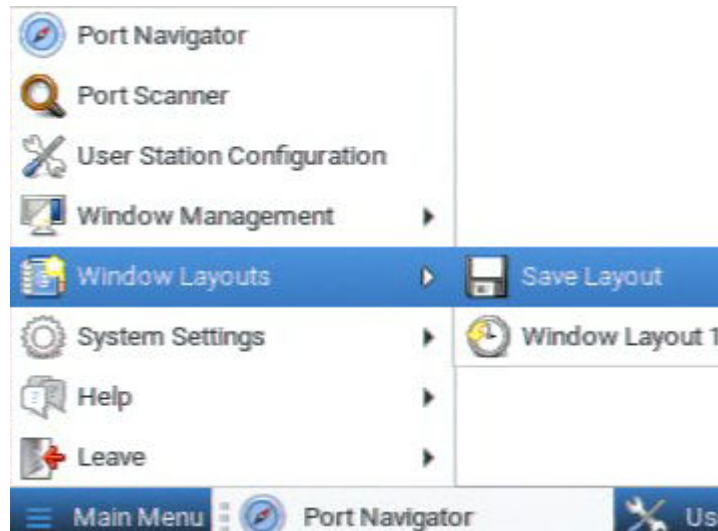
► *To save a layout:*

1. Arrange your client windows as desired. They can be freely sized and positioned across all monitors.
2. In Main Menu: Click Window Layouts > Save Layout. If previously saved layouts exist, the menu also includes an option to save as new, or overwrite a named layouts, such as Save Layout (current layout name). New layouts are automatically assigned names.
3. A desktop notification pops up to confirm the layout is saved and to display the name.

► *To restore a layout:*

• In Main Menu: Click Window Layouts, then click the named layout you want to restore.

When the layout is selected, all currently open clients are closed, and the selected layout is restored. Upon restoring a layout, some targets may not be available. The clients for those targets are restored anyway with their visual attributes and an error message that their target cannot be connected.

Port Scanner (Launch)

The Port Scanner displays an assortment of ports that you select, by scanning through each connection for a specified period of time. You can launch a KVM connection to any port shown in the scanner. The Port Scanner can also save target snapshots to an external USB device or network storage, when enabled. This is useful for forensic or surveillance purposes. See Port Scanner Settings (on page 188) for details on configuration and user privilege.

• Launch the Port Scanner from the Main Menu.
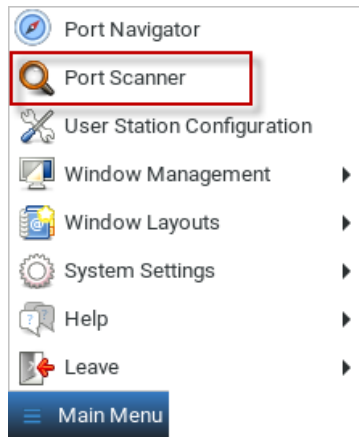
Window Management

Window Management helps you organize open sessions. All client types are included. Other User Station windows, such as Port Navigator and the Port Scanner, are not included in window management. If two monitors are connected to the User Station, the feature works separately on each monitor. Windows are not moved from one monitor to another.

For information about saving and restoring window layouts, see Window Layouts (on page 187).
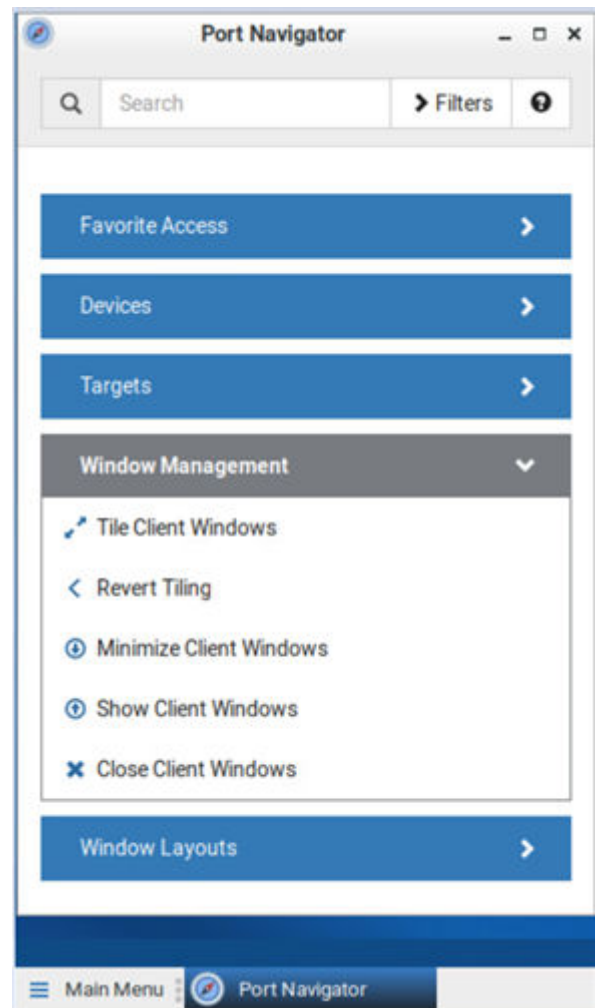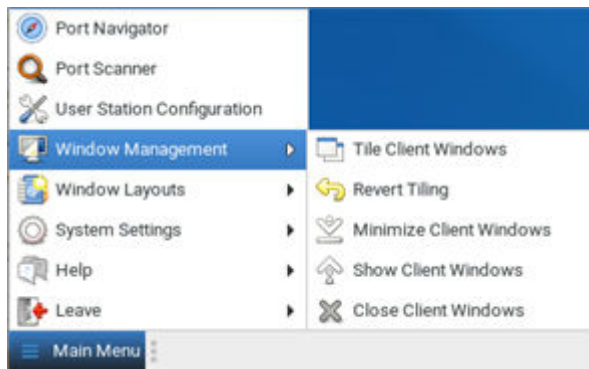
► *To use Window Management:*

1. Choose Main Menu > Window Management, then select an option.

OR

2. Open the Port Navigator, then open the Window Management panel to select an option.

- Tile Client Windows: arranges all client windows in a tiled layout on desktop. Minimized windows will be unminimized.

- Revert Tiling: Undo last tiling operation and restore previous window sizes. Previously minimized windows will be minimized again.

- Minimize Client Windows: Minimizes all client windows from desktop to task bar.

- Show Client windows: Restores all client windows from task bar and to desktop

- Close Client Windows: Closes all client windows.
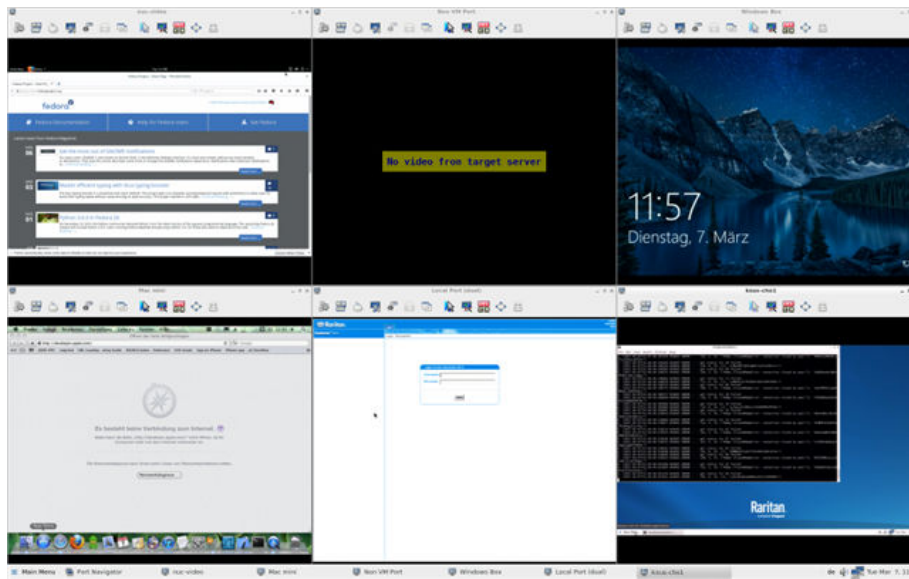
Logout or Shutdown

Logout, restart and shutdown commands are available under Leave in the Main Menu.

- *Log Out*: Logs the user out of the User Station.
- Restart: Restart the User Station

  Shut Down: Powers off the User Station. You should always use the software command as the only method to power off your User Station. For detailed information, see .

Warning: Do NOT turn the Dominion User Station off by holding down the Power button or unplugging the power cord because such operations may damage it. A short press of the Power button initiates a graceful shutdown that does not save open sessions.

Getting Started

This chapter introduces the basic installation and configuration.

In This Chapter

Installation and Configuration

Connect the Equipment

Step 1: Connect the DKX3/DKX4-UST and DKX3-EUST

Only the basic hardware installation is described. For additional connection information, see Overview (on page 9).

► *To make a basic connection:*

1. Disconnect all devices from power.
2. Connect a USB keyboard and mouse to the front or rear USB ports.
3. Optional. Connect a microphone and speakers to the front panel.
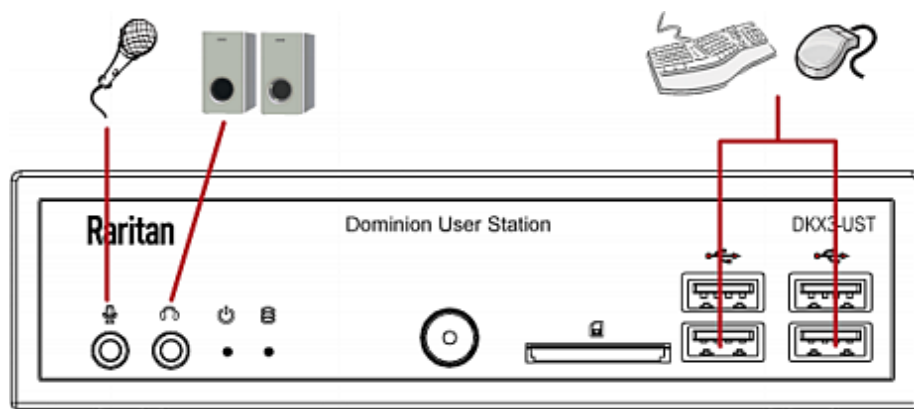
4. Connect the User Station to the network using either or both LAN ports on the rear panel.
5. Connect one or two or three monitors using either or both DisplayPort ports, or the HDMI port.
6. Power ON all devices.

DisplayPort and HDMI transmit both video and audio signals. Your monitors must support the audio transmission if audio is intended.

![Raritan. A brand of Legrand]

► *DKX4-UST:*
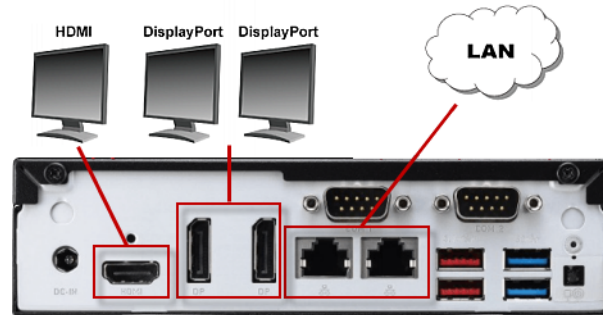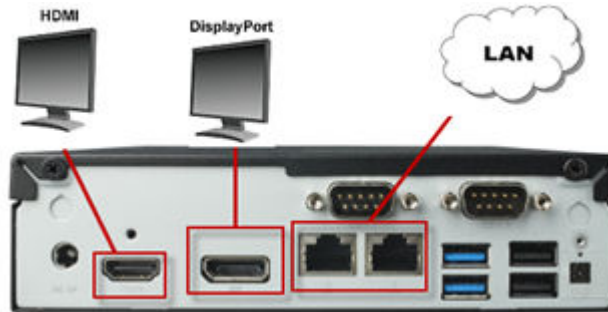
► *DKX3-UST Version 2:*

► *DKX3-UST Version 1:*
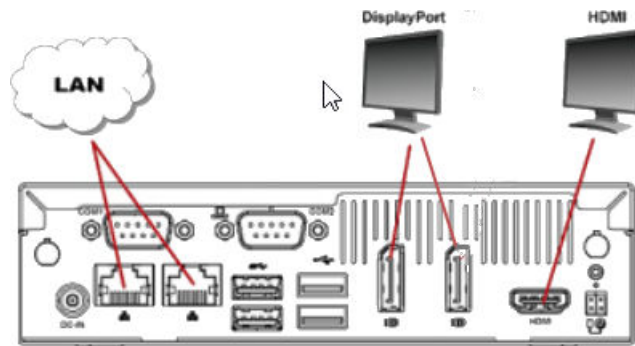
► *DKX3-EUST:*
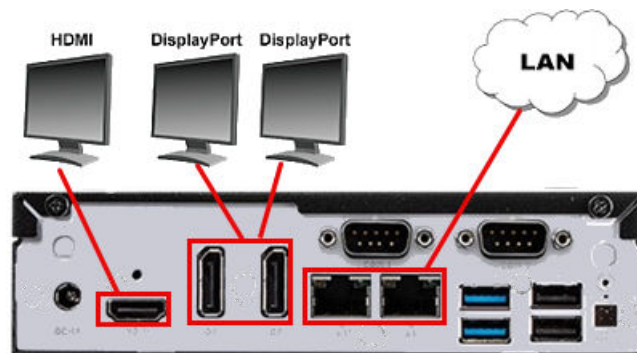
Step 1: Connect the DKX4-EUST

Only the basic hardware installation is described. For additional connection information, see Overview (on page 9).

► *To make a basic connection:*

1. Disconnect all devices from power.
2. Connect a USB keyboard and mouse to the front or rear USB ports.
3. Optional. Connect a speakers to the front panel.
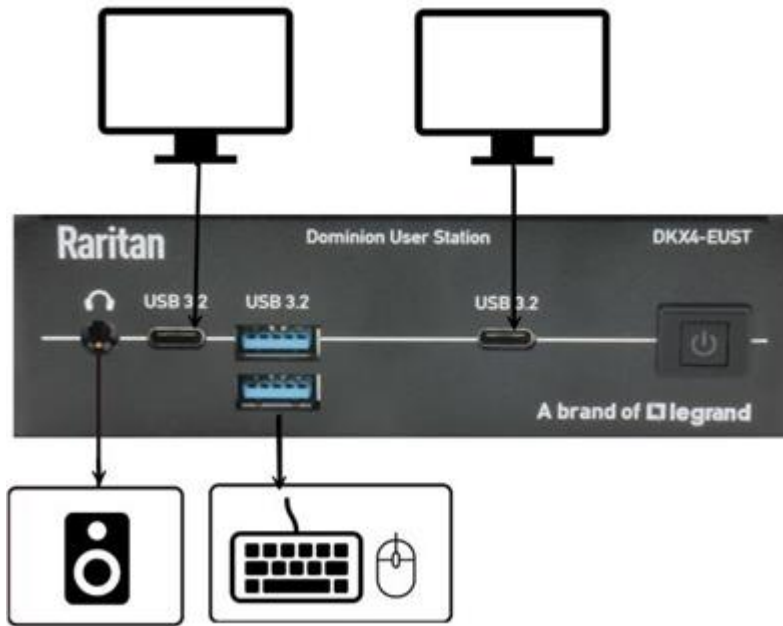
4. Connect the User Station to the network using either or both LAN ports on the rear panel.
5. Connect monitor(s) to HDMI, DisplayPort and USB-C ports.
6. Power ON all devices.

DisplayPort, HDMI and USB-C transmit both video and audio signals. Your monitors must support the audio transmission if audio is intended.

Note: Dominion Enhanced UserStation supports up to 4 monitors:

► *To make monitor connection:*

On a DKX4-EUST you can connect up to four monitors. Two in the front and two in the back.

Front:
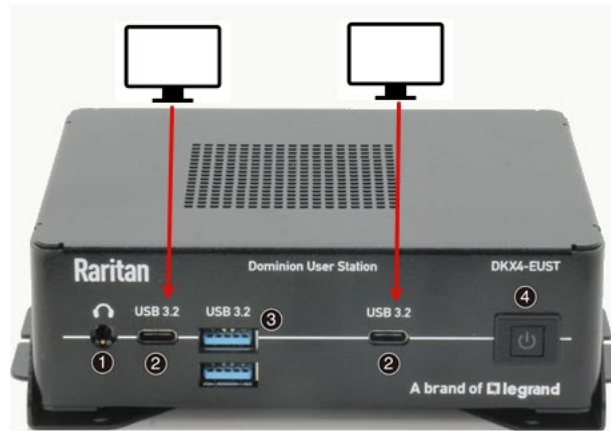
Back:

Step 2: Initial Log in to the Dominion User Station

Use the factory default user credentials for initial login. User credentials are case sensitive.

- User name: admin
- Password: raritan

Changing the default password to strong password is enforced at first login. For details on password changes, see Change Password (on page 193).

Step 3: Add KX/SX Devices (without CC-SG integration)

If you are not integrating your User Station with CC-SG, proceed with this step. If you want to integrate CC-SG, see CommandCenter Secure Gateway Integration (on page 215).

If the User Station is connected to a non-DHCP network, you must manually configure the network settings prior to adding KX and SX Devices. See Basic Network Settings (on page 74).

When you are not using CC-SG integration, KX and SX Devices are added in the User Station Configuration window.

► *To add KX/SX Devices:*

1. Launch the User Station Configuration window using either method below.
   - Press *Ctrl+Alt+C*.
   - Choose Main Menu > User Station Configuration. For the Main Menu's location, see Main Menu, Port Navigator, Toolbar (on page 16).
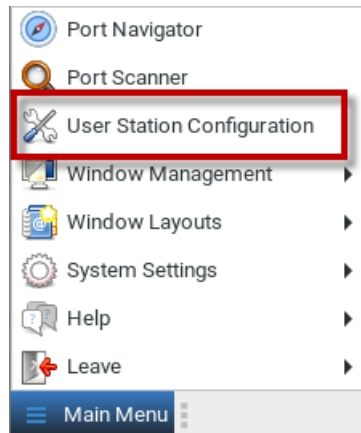
2. Click New.

You must enter IP address or Hostname of the device.

The default Discovery Port and HTTPS Port can be customized if needed.

Select the authentication method.

- Normal: You must enter login credentials for the KVM/Serial switch.
- Allow LDAP single sign-on: When users, KVM/Serial switches, and the Dominion User Station have the same LDAP environment, single sign-on can be used.

User credentials on the KVM/Serial switch are required for querying this KVM/Serial switch's port information.

The user credentials may or may not be the same as your user credentials for the User Station. See Authentication of User Stations and KVM/Serial Switches (on page 293).

Note: If you enter incorrect user credentials for a KVM/Serial switch, you may be blocked if User Blocking has been enabled on that KVM/Serial switch and too many incorrect attempts are made. When this occurs, contact the KVM/Serial switch's system administrator for help.

---

1. Click Save.

Important: If "Allow LDAP Single Sign-on" is enabled, LDAP users can omit entering credentials in favor of their LDAP credentials being used. Otherwise, user credentials for a KVM/Serial switch are saved on a per-user basis. Other users must enter and save their own user credentials for the KVM/Serial switches you added. See **Editing KVM and Serial Switches** (on page 84).

Step 4: Access KVM/Serial Switches and Ports (without CC-SG integration)

You access the computer devices connected to a device's ports and your other targets through the Port Navigator window, which contains 3 panels:

- Favorite Access shows the access you have configured as favorites. See Configuring KVM and Serial Ports (on page 88).
- Devices shows all added devices and their ports.
- Targets shows all added KVM, Serial, SSH, RDP and VNC Web ESXi targets.

This window is displayed by default. If not, launch it by pressing *Ctrl+Alt+N* or choosing Main Menu > Port Navigator.

Note: The User Station CANNOT access a KVM port that is connected to a tiered KVM switch or a blade chassis server.

► *To access a KVM/Serial switch's ports:*

1. Click a KVM/Serial switch in the Devices panel.

Favorite Access	❯
Devices (2)	⌄
❯ 192.168.2.103	
❯ 192.168.2.10	
Targets	❯
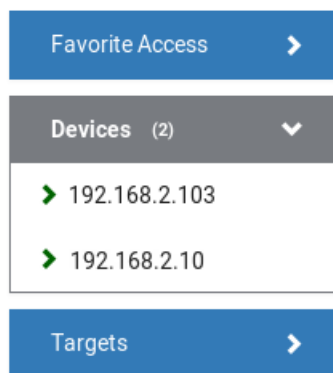
2. Per default, only a list of "up" ports is displayed under the selected KVM/Serial switch. For dual port video, only the primary port must be "up" to be displayed.
   - Numbers in parentheses are the physical port numbers on the KVM/Serial switch.
   - Dual port video shows the primary then secondary physical port numbers in parentheses.

Note: To show KVM/Serial ports whose status is down, see *Using Filters (on page 120)*.
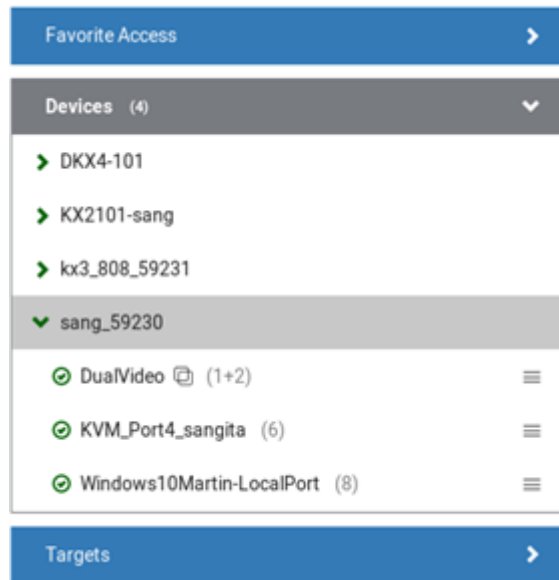
- Click the desired KVM/Serial port's icon ☰ , and select *Open in new KVM/Serial client or* or *Open in current KVM client.* Or, click the port name: single-click opens it in the current KVM Client window, double-click opens it in a new KVM Client window, right-click shows the KVM Client options.
- Number of sessions connected are seen next to the device. For example: if total of available channels are 8 and 4 are in use, It will be seen as "<device name> (4/8)"
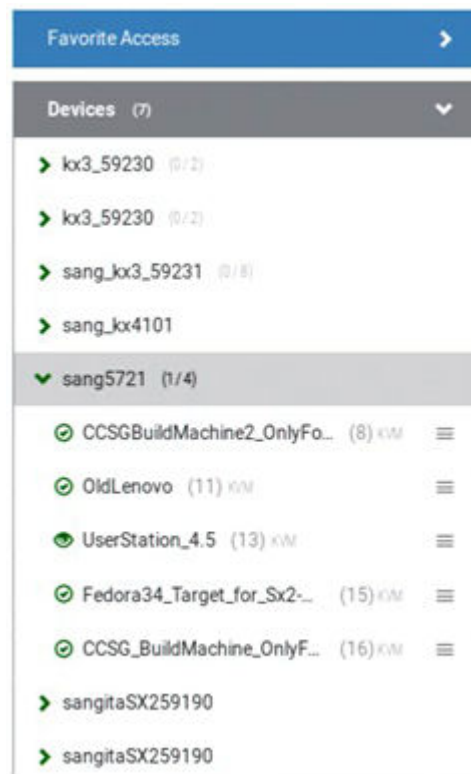
Raritan.
A brand of 🔲 legrand

Step 5: Use the KVM Client

The KVM Client window opens after accessing a port. The video of the target server that is connected to the port is displayed in the KVM Client. You can use the attached keyboard and mouse to control the target server.
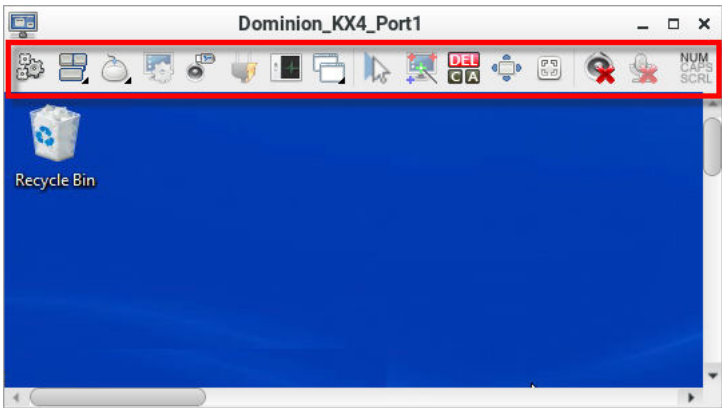
The toolbar is split into two groups.

The left group comprises the following buttons that you can use to change settings and properties.

Button	Function
	Connection Properties:
	Manages streaming video performance over *your* connection to the target server.
	Show information like FPS and video resolution.
	The factory default settings are ideal for most connections so it is not recommended to change the settings unless required.
	Keyboard:
	Shows a list of available hot key macros and sends the selected macro to the target server.
	Mouse:
	Switches between single mouse and various dual mouse modes, or synchronizes two mouse pointers onscreen.
	Video Settings:
	Adjusts video sensing and color calibration settings.

Button	Function
	Connect Audio, Mass Storage and SmartCard Devices:
	Connects or disconnects a virtual media drive or a SmartCard reader from the target server, if the target supports virtual media.
	For example, you can mount a CD-ROM or USB flash drive onto the target server.
	In addition, you can configure the audio connection to the target server.
	Power Operations:
	Turns on, off or power cycles the target server, if a PDU is connected.
	External Device Settings:
	Access the settings for operating an external device..
	View:
	Shows several display options, such as Scale Video and Full-Screen Mode.

The right group comprises the following shortcut buttons for frequently-used functions. These functions are also available in the left group, but the shortcut buttons allow quick access with a click.

Button	Function
	Synchronize Mouse:
	Forces the target server's mouse pointer to align with the User Station's in the dual mouse modes.
	Auto-sense Video:
	Forces the video re-sensing to adjust the video display.
	Send Ctrl+Alt+Del:
	Sends the hot key *Ctrl+Alt+Del* to the target server to ensure it is interpreted by that server.
	Full-Screen Mode:
	Displays the target server's video in full screen.
	Press *Ctrl+Alt+F* to quit the Full-Screen mode.
	Fit window to Target:
	Resizes the KVM Client window to the target server's desktop video.

Raritan.
A brand of ∎legrand

Button	Function
	Mute audio Mute or unmute audio.
	Mute microphone Mute or unmute microphone.
	Num Caps Scroll: Displays the status of Num Lock, Caps Lock, and Scroll. Active functions are in bold text

For detailed information on the toolbar buttons, see Using the KVM Client (on page 126).

Automatic Reconnection

If your connection to the KVM targets fails, an automatic reconnection will be attempted in most cases after a 30 second interval. This interval increases from 30 seconds to 1 minute, 2, 5, 10, 15 minutes if reconnect is not successful.

A message appears when the connection drops with information about reconnection timing and options to cancel or quit.

Automatic reconnection is not attempted when the connection failure is due to:

- Configuration error detected. Certificate must be uploaded.
- User authentication failed.
- User authorization failed.
- User has been actively disconnected by an administrator.
- KX device version not supported by the client.

Note: In FIPS mode, the User Station CANNOT connect to any KVM target on a KX3 or login to CC-SG if the security settings on the device are TLS 1.3 only and also fails to connect with RDP access clients.

Step 6: Use the Serial Client

The Serial Client window opens after accessing a port. The serial console output of the target server that is connected to the port is displayed in the Raritan HTML Serial Console (RHSC). You can use the attached keyboard and mouse to communicate with the target server.

You can use tool bar menu to access sub menu options to perform certain tasks on the target server.

Menu Option	Sub Menu Options
Emulator	Emulator provides access to settings, Get History, Clear History, Get Write Access, Get Write Lock, Write Unlock, Send Break, Reset Port, Connected Users and Exit options.
Edit	The Edit menu is disabled.
Tools	The Tools menu is disabled.
Power	Power provides access to Power Status, Power On, Power Off, and Power Cycle options.
Help	Help provides access to About option.

For detailed information on the toolbar buttons, see Using the Serial Client (on page 164)

Basic Network Settings

The Dominion User Station default network configuration is set to Automatic (DHCP) for both IPv4 and IPv6 settings.

This section describes basic network configuration only. For details, see Network Connections - Ethernet (on page 30).

► *To configure basic network settings:*

1. Choose Main Menu > System Settings > Network.
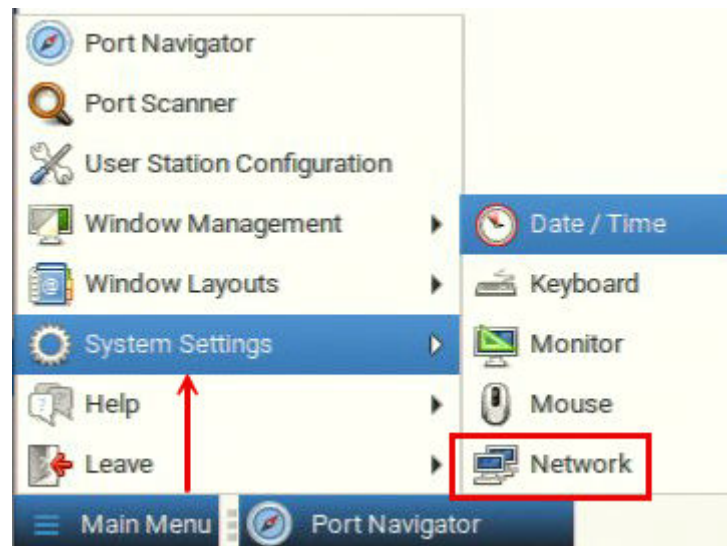
2. In the Network Connections dialog, two default network connections are available for two LAN ports. *Ethernet 1* is for LAN port 1, and *Ethernet 2* is for the other.

Select the desired one and click "Edit the selected connection" icon.
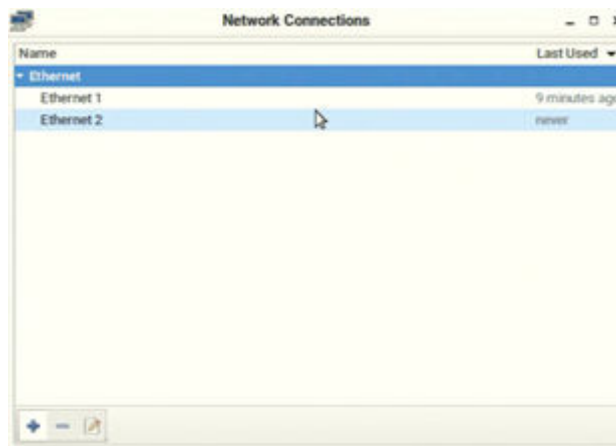
3. Click the IPv4 Settings tab.
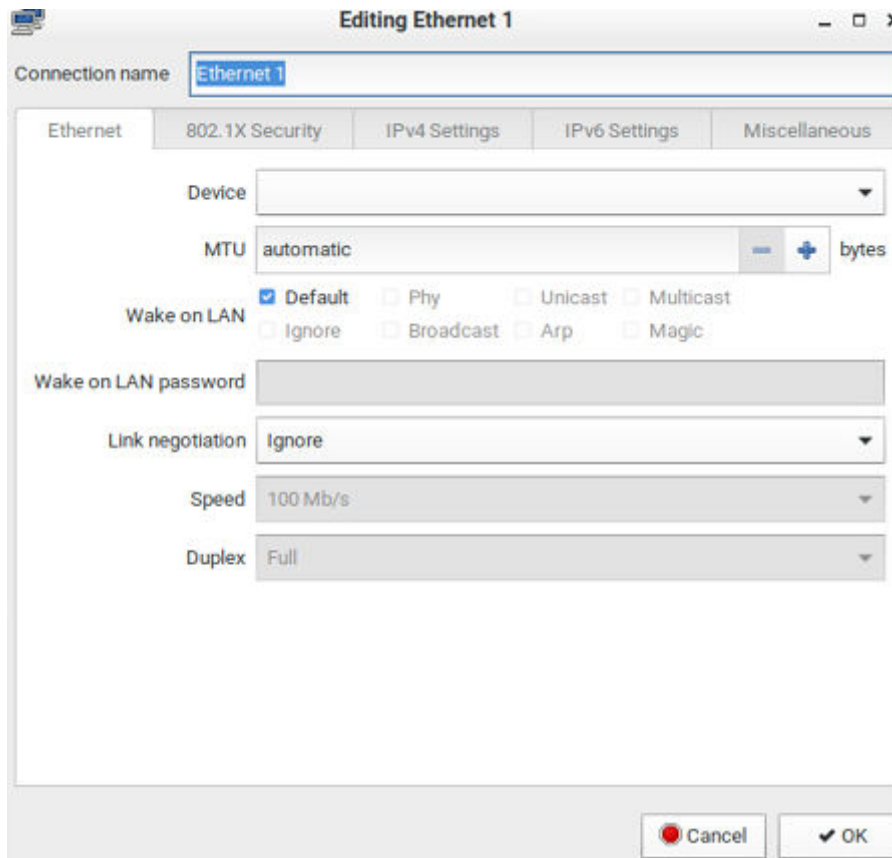
4. In the Method field, select one of the following options:

- *Automatic (DHCP)*: The DHCP server automatically assigns an IPv4 address. This is the default.
- *Automatic (DHCP) addresses only*: The DHCP server automatically assigns the IP address only. DNS comes from manual input.
- *Manual*: This option configures static addressing. Click Add to specify at least one IPv4 address, netmask and gateway.
- *Disabled*: IPv4 networking is disabled.

For details, see IPv4 Settings (on page 34).

5. If your network supports IPv6, click the IPv6 Settings tab, and repeat the above step for configuring IPv6 settings. Note that IPv6 provides the "Ignore" option instead of the "Disabled" option to disable the IPv6 networking. See IPv6 Settings (on page 36).

6. For additional settings, click the Ethernet tab. See Ethernet Settings (on page 33).

7. Click OK. The new network settings apply now.

VESA Mount

You can mount the Dominion User Station onto the back of a monitor with 75 or 100 mm VESA standards.

Mount DKX3/DKX4-UST and DKX3-EUST

► *VESA mount procedure:*

1. Turn OFF and disconnect all devices from the power sources, including the monitor.
2. Attach the VESA mount securely to the back of your monitor using four appropriate screws.
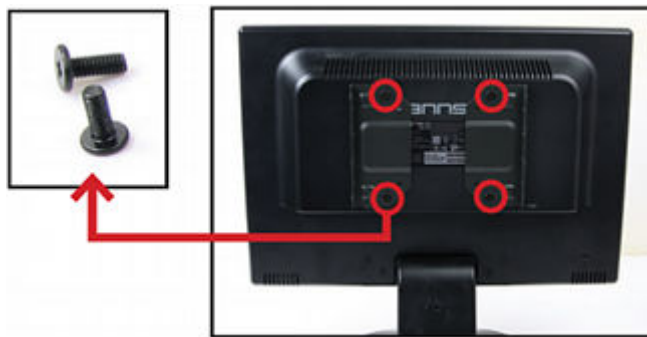
3. Align two screw holes on each side of the User Station with those on the VESA mount.

4. Tighten two sides securely using four appropriate screws.
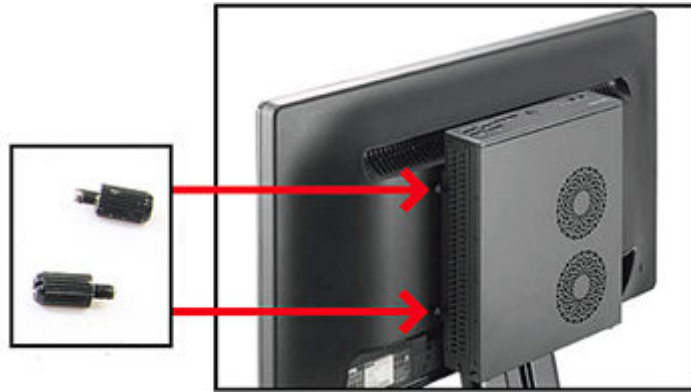
5. The Dominion User Station is now securely attached to the monitor.

Mount DKX4-EUST

► *VESA mount procedure:*

1. Turn OFF and disconnect all devices from the power sources, including the monitor.
2. Attach the VESA mount securely to the back of your monitor using four appropriate screws.

3. Align two screw holes on each side of the User Station with those on the VESA mount.
4. Tighten two sides securely using four appropriate screws.
5. The Dominion User Station is now securely attached to the monitor.
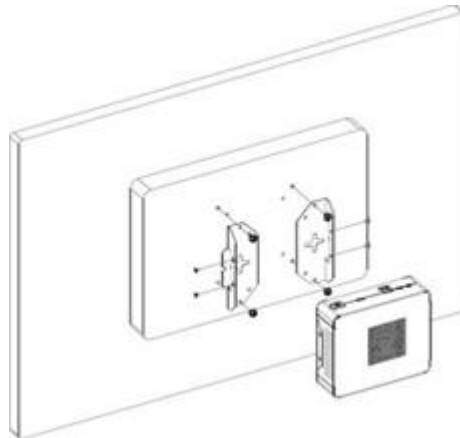
Managing KVM and Serial Switches and Ports

KVM, Serial switches and their ports are managed in the User Station Configuration window.

Note: If you are using CC-SG integration, you do not need to add KVM and Serial switches in this way. See CommandCenter Secure Gateway Integration (on page 215).

In This Chapter

User Station Configuration

► *To launch the User Station Configuration window:*

- Press *Ctrl+Alt+C*.
- OR choose Main Menu > User Station Configuration.
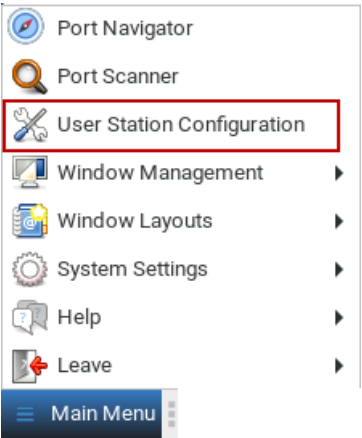
The User Station Configuration window opens.
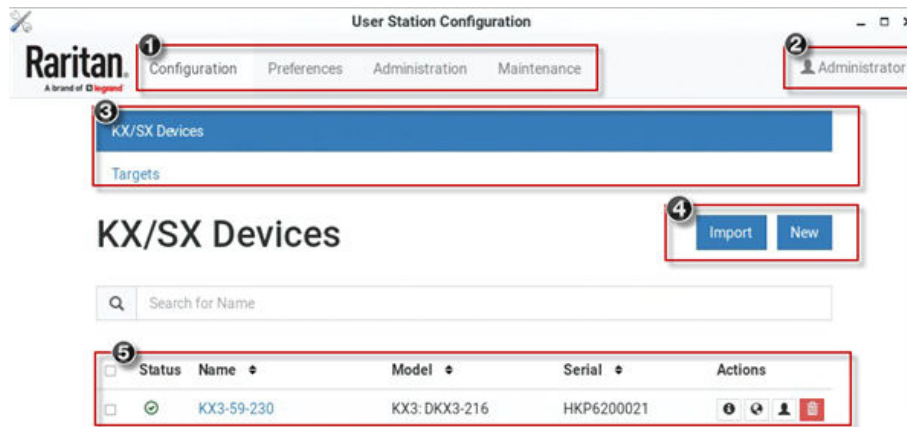
1. Configuration tabs:
   - *Configuration*: Manage KX/SX Devices and Targets. See the other sections in this chapter.
   - *Preferences*: Set personal preferences, such as audio settings. See Setting User Preferences (on page 171).
   - *Administration*: Manage administration tasks. See Administration Features (on page 194).
   - *Maintenance*: Manage maintenance tasks. See Maintenance Features (on page 258).
2. Your user account:

Click to view your user account settings.

3. KX/SX Devices and Targets options:
   - *KX/SX Devices*: Add or Import KX/SX devices and manage them.
   - *Targets*: Add and manage Targets. See Managing Targets and Access Methods (on page 95).
4. Import button and New button:
   - By default, the KX/SX Devices option is selected, and you can use the Import and New buttons to add or import KVM/Serial switches. See Adding KVM and Serial Switches (on page 81) See Importing KVM and Serial Switches (on page 86).
   - When the Targets option is selected, you can use the New button to add targets and access. Import is not available.
5. A list of added KVM/Serial switches:
   - When the KX/SX Devices option is selected, view the list of KVM/Serial switches here, and click the desired KVM/Serial switch to show all of its KVM/Serial ports and details.
   - When the Targets option is selected, view the list of Targets here, and click a Target to show its access methods and details.

Adding KVM and Serial Switches

All users can see the KX/SX devices added to this User Station, but they can only access those switches if they have provided valid user credentials. To add multiple devices that share an IP address, such as in a port-forwarding configuration, you must use different discovery and https ports. If users, KX/SX devices, and the Dominion User Station exist in the same LDAP environment, you can add your KVM or Serial switches with single sign-on capability.

Note: To add a KX/SX device that is under CC-SG management, make sure "Allow direct access" is checked for the device in CC-SG, then add the KX/SX device to the Dominion User Station using an admin-level account that is different from the one used to authenticate the device on CC-SG. Or, you can use CC-SG integration. See CommandCenter Secure Gateway Integration (on page 215)

► *To add a KVM/Serial switch:*

1. Click New in the User Station Configuration window. See User Station Configuration (on page 80).
2. The following page opens, and the user must enter the required information. See Step 3: Add KX/SX Devices (without CC-SG integration) (on page 66).

- Click Save, and the new KVM/Serial switch's content is shown.

Important: If "Allow LDAP Single Sign-on" is enabled, LDAP users can omit entering credentials in favor of their LDAP credentials being used. Otherwise, user

credentials for a KVM/Serial switch are saved on a per-user basis. Other users must enter and save their own user credentials for the KVM/Serial switches you added. See [Editing KVM and Serial Switches](#) (on page 84).

Editing KVM and Serial Switches

Added KVM/Serial switches are listed in the User Station Configuration window.

Each KVM/Serial switch has three icons in the Actions column. You must have Device Administration privileges to delete, edit or add KVM/Serial switches.

If you are not the one who added new KVM/Serial switches to the User Station, you must follow the procedure below to enter user credentials for newly-added KVM/Serial switches.

Note: For the difference between a KVM/Serial switch's and the User Station's user credentials, see Authentication of User Stations and KVM/Serial Switches (on page 293).

▶ *To view the KVM/Serial switch's ports:*

- Click the desired KVM/Serial switch. The ports list opens. See Configuring KVM and Serial Ports (on page 88).

▶ *To change the KVM/Serial switch's IP address/host name or authentication method:*

1. Click the desired KVM/Serial switch's ⓘ button.
2. Click Edit to open the Edit KX/SX Device page.
3. Modify the IP address or host name, discovery and HTTPs ports, or change the authentication method. See Adding KVM and Serial Switches (on page 81).
4. Click Save.

Raritan.
A brand of 🔲legrand

► *To open the KVM/Serial switch's administration page:*

1. Click the desired KVM switch's [icon] button.
2. The administration page launches. Login to access.

► *To enter new user credentials for a KVM switch:*

1. Click the [icon] button of the desired KVM switch.
2. Enter new user credentials.
3. Click Save.

Note: If you enter incorrect user credentials for a KVM/Serial switch, you may be blocked if User Blocking has been enabled on that KVM/Serial switch and too many incorrect attempts are made. When this occurs, contact the KVM/Serial switch's system administrator for help.

Deleting KVM and Serial Switches

The final button in the Actions column is used to delete this KVM/Serial switch.

► *To delete a KVM switch:*

1. Click the desired KVM/Serial switch's [icon] button.
2. Click OK on the confirmation message.

► *To delete multiple KVM/Serial switches:*
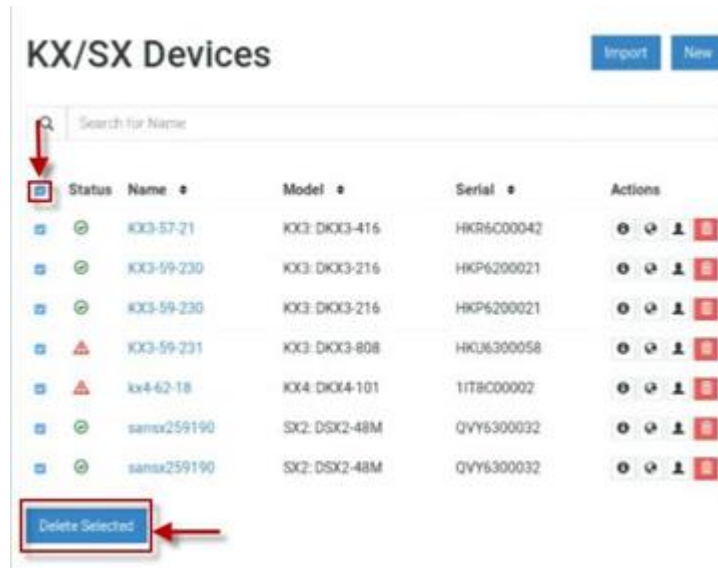
Importing KVM and Serial Switches

Bulk Import and Update allows you to add or update multiple KVM/Serial switches at once using a CSV file found in the root folder of a connected USB storage device.

When you import, Dominion User Station adds devices detected as new by their IP address/hostname. Dominion User Station uses the credentials given in the CSV file. If credentials are blank in the file, none are added. When Dominion User Station detects that a device identified in the CSV file already exists in the system, the import updates the credentials as given in the CSV. You can also optionally specify customized Discovery port and HTTPS port for each device.

► *CSV file format:*

The CSV file contains 5 columns: "ip address or hostname","user name","password", "discovery port", "HTTPs port"

Note: User name and password are optional. If not imported, user must enter them later. Discovery port and HTTPS port are optional. If they are not specified,the default ports 5000 and 443 are used.

See Bulk Import Examples (on page 88) for more details and limitations.

► *To import KVM switches:*

1. Click Import in the User Station Configuration window. See User Station Configuration (on page 80). The Bulk Import/Update KX / SX Devices page opens.
2. The Storage list displays all CSV files found in the root folder of connected USB and mounted Network Storages.

Raritan.
A brand of 🔲legrand

Bulk Import / Update KX/SX Devices
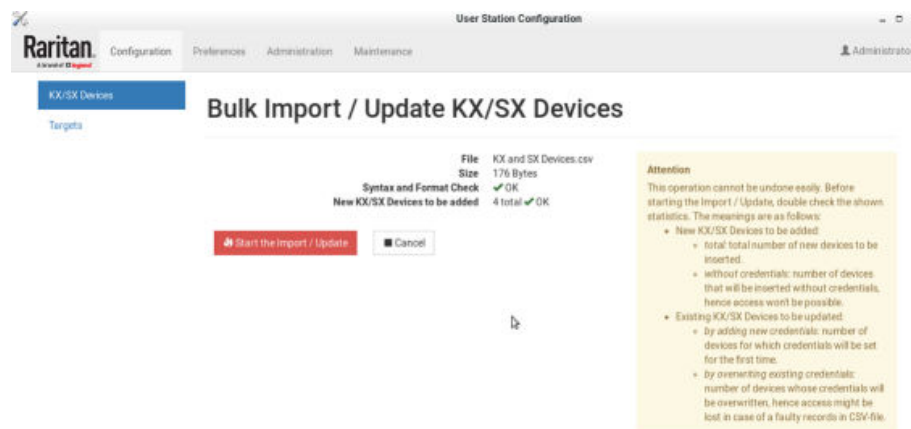
This dialog supports adding and updating many KX/SX Devices at once via CSV-file.

On adding, devices are inserted into the system's database with their IP-address / hostname and optionally with credentials for the user who initiates the operation.

On updating, credentials of the initiating user can be updated or added for devices which are already part of the system.

The CSV-record format is as follows:

`<hostname>,<username>,<password>,<discovery port>,<https port>`

Example:

`mydevice,admin,pass123,5000,443`

Note: The credentials and port numbers are optional.

USB or Network Storage	File Name	Size
4664-9FEF	KXwithspecialcharacters.csv	157 Bytes

Cancel

3. Click the file you want to import. The Bulk Import page opens to display the file details:

- File name and size
- Errors, if any, with line number, syntax, or format if appropriate
- Total number of KX/SX Devices to be added
- Number of KX/SX Devices to be added without credentials
- Number of KX/SX Devices to be updated with new credentials
- Number of KX/SX Devices to be updated by overwriting existing credentials

Note: If errors are listed, the import button is disabled. Correct the file and try again.

4. Click Start the Import/Update in the details dialog. Import progress shows in the dialog. When complete, a success message appears in the main page.

Bulk Import Examples

► *Import / update listed KX / SX switches:*

```
192.168.2.104,admin,raritan
192.168.2.103,thomas,thomas,5000,443
192.168.3.30,admin,raritan
192.168.5.52,user,password
```

► *Special characters and escaping*

Line 1 is an example of using comma in a value.

Line 2 is an example for escaping ", the resulting password string is "password"

```
192.168.2.104,admin,"rar,itan"
192.168.5.52,user,"""password"""
```

Note: If you create the CSV file using Microsoft Excel or similar tools, you do not need to escape special characters. These tools handle the special characters automatically when creating the CSV file. Check the resulting CSV file if you are not sure.

► *Commenting out*

Use the hashtag character (#) in the first position of a line to comment out the line. Hostnames are not allowed to contain #.

```
192.168.2.104,admin,raritan
#192.168.2.103,thomas,thomas
#192.168.3.30,admin,raritan
192.168.5.52,user,password
```

Configuring KVM and Serial Ports

A KVM/Serial switch's ports are shown after a KVM/Serial switch is selected.

► *To configure a KVM or Serial port:*

1. Click the desired KVM/Serial switch, and all of its KVM/Serial ports are listed on the screen. Serial switch ports are seen as serial type and can be connected and configured just like KVM ports.
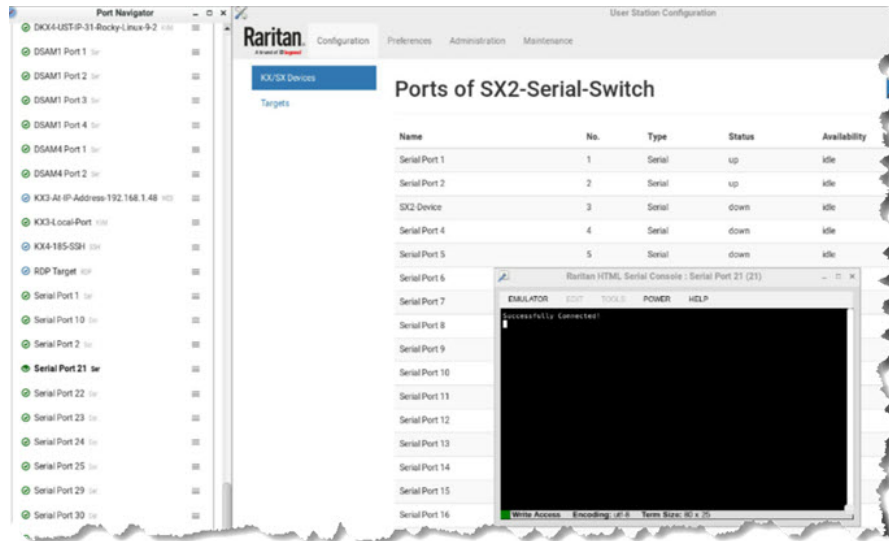
Note, to return to the devices view, click the Back to all KX/SX Devices link

General Settings Icons:

- ✳ The KVM or Serial port has been configured as a favorite port.

- 🔍 The KVM port is included in Port Scanner.

- 🔊 The KVM port is configured to automatically connect a speaker when the connection launches.

- 🎤 The KVM port is configured to automatically connect a microphone when the connection launches.

- The icon shown in the top-right corner of the Ports section indicates the KVM/Serial port information retrieval status. In this example, there is a green checkmark. See Port Data Retrieval Status (on page 92).
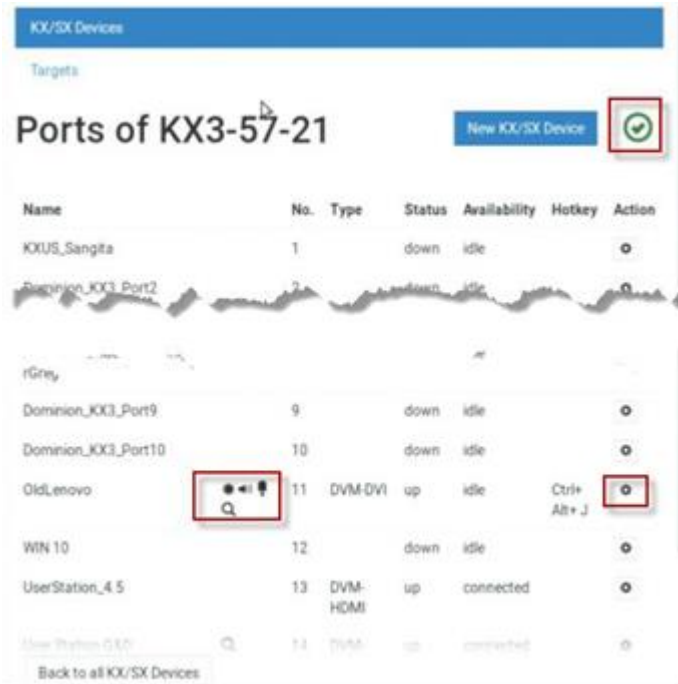
1. Click ⚙ in the Action column of the port that you want to configure. A settings page opens.
2. Configure the General Settings:

Checkbox	Function
Hotkey	Assign a hotkey combination for quickly accessing this KVM/Serial port. Available options include: • *Ctrl + Shift* + <character> • *Ctrl + Alt* + <character> • *Shift + Alt* + <character> • *Ctrl + Shift + Alt* + <character> <character> is an alphanumeric character or function key. Some hotkey combinations cannot be used for port access and thus are not available. See Unavailable Hotkeys for Port Access (on page 92).

Raritan.
A brand of **legrand**

Favorite	If this checkbox is selected, this KVM/Serial port is shown in the Favorite Access panel. See Port Navigator (on page 114).
Automatically connect Speaker	Speaker will automatically be connected to this KVM port at target launch.
Automatically connect Microphone	Microphone will automatically be connected to this KVM port at target launch.
Include in Port Scanner	Add the port to the port scanner. See Port Scanner (on page 122).

3. Configure the Target Window Settings if you want to override default settings.

- To view your default target window settings, click the Access Client Settings button. See Access Client Settings (on page 172) for details on each.
- If you want to override any of those settings for the port you are configuring, select the "Use port specific Access Client Settings" checkbox to enable the list.
- Select the checkbox for each setting that should override the default setting.

KVM Target:

Serial Target:

Target Window Settings

By default, Dominion User Station uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.
Adjust the default settings via the Access Client Settings dialog:

Access Client Settings

Notes:
 • These setting don't apply to already active target sessions.
 • The Full-Screen hotkey is always F11.

☐ Use specific Target Window Settings

☑ Window Decorations

Full-Screen Mode

Console Size

80 x 24 ▾

1. Click Save.

Unavailable Hotkeys for Port Access

The following hotkey combinations are not available for accessing KVM/Serial ports.

Unavailable hot keys	Notes
Ctrl + Shift + <number>	
Ctrl + Shift + Alt + <number>	<number> = 0 to 9
Shift + Alt + <number>	
Ctrl + Alt + <function_key>	<function_key> = F1 to F12
Ctrl + Alt + C Ctrl + Alt + F Ctrl + Alt + L Ctrl + Alt + M Ctrl + Alt + N	These hotkeys can be used if you first disable them as User Station hotkeys.

Port Data Retrieval Status

An icon is displayed in the top-right corner of the Ports section in the User Station Configuration window. This icon indicates the data retrieval status of the KVM/Serial ports on the selected KVM/Serial switch.

Raritan.
A brand of 🔲legrand

Click this icon to view additional information.

The icon changes depending on the current retrieval status of KVM port information.

Icon	Port data retrieval state
	Port information on the selected KVM/Serial switch is accessible.
	Port information on the selected KVM/Serial switch is NOT accessible. Possible causes may include: • Incorrect user credentials are entered for the KVM/Serial switch. • The presented certificate of the device cannot be verified, when certificate checking is enabled • Network connectivity issues. For example, the selected KVM/Serial switch is not connected to the network.
	Port information on the selected KVM/Serial switch is NOT accessible because NO user credentials have been entered for this KVM/Serial switch. See Editing KVM and Serial Switches (on page 84).

The port data retrieval status will affect the device and port status shown in the Port Navigator window. See Identifying States of KVM/Serial Switches and Ports (on page 117).

Dominion Serial Access Module (DSAM) Ports

Dominion User Station supports serial targets through direct serial connection of SX2 devices or via Dominion Serial Access Modules (DSAM) connected to the KX III or KX IV switch. DSAM ports appear on the User Station when the KX device is added, similar to KVM ports.

Your serial ports are labeled "Ser" to show the port type. The number label of a DSAM port is a combination of the DSAM-module-number and the serial port-number. For example, serial port 2 on DSAM-module 3 is shown as 3.2.

Serial ports appear in the Devices tab and the Targets tab. You can launch a serial session from either tab.

Managing Targets and Access Methods

Targets and Access methods are managed in the User Station Configuration window. See User Station Configuration (on page 80).

The Targets and Access methods feature offers different ways to view, manage, and connect to targets, using KVM/Serial port access, RDP, SSH, and VNC. You can also add access to a Web applications or ESXi virtual machines. These methods provide access to any KVM/Serial, non-KVM serial targets such as server, network switch, HVAC or other devices connected to your network.

Dominion User Station Multi KVM access (M-KVM) method makes it possible to configure two or more Dominion KX4-101 KVM ports into a virtual Multi Monitor KVM target.

When a KVM/Serial switch is added, Dominion User Station automatically detects ports and creates a Target with a KVM/Serial access method for each port. The Targets section of the User Station Configuration and the Device section of Ports Navigator populates with this information and available to access. KVM/Serial access cannot be added manually, it is always based on access to the KVM/Serial switches .

The Dominion User Station provides full capability of RDP software which captures the mouse and keyboard inputs from the local computer and sends them to the remote target. The RDP client has a "grab keyboard" feature which is available by default but you can turn it off. This feature allows you to grab all keyboard inputs including the power button and other keyboard shortcuts from the local Operating System, which are processed by the target and not by the Dominion User Station. RDP gives uninterrupted access to the video and audio of target applications as well.

Note: If you're working in CC-SG mode, your user experience is different. See Navigator with CC-SG Integration (on page 217).

In This Chapter

Adding Targets and Access Methods

► *To add targets and access methods:*

1. In Main Menu, open the User Station Configuration window, then click Targets.
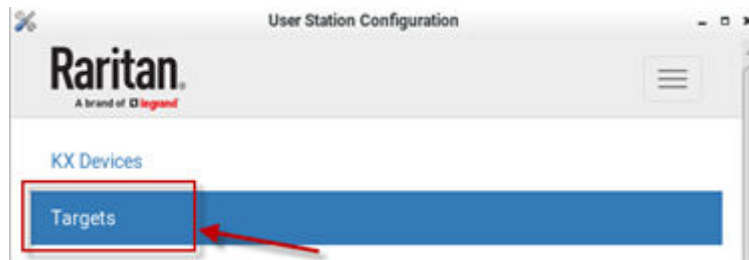
2. The Targets list appears. Click New.
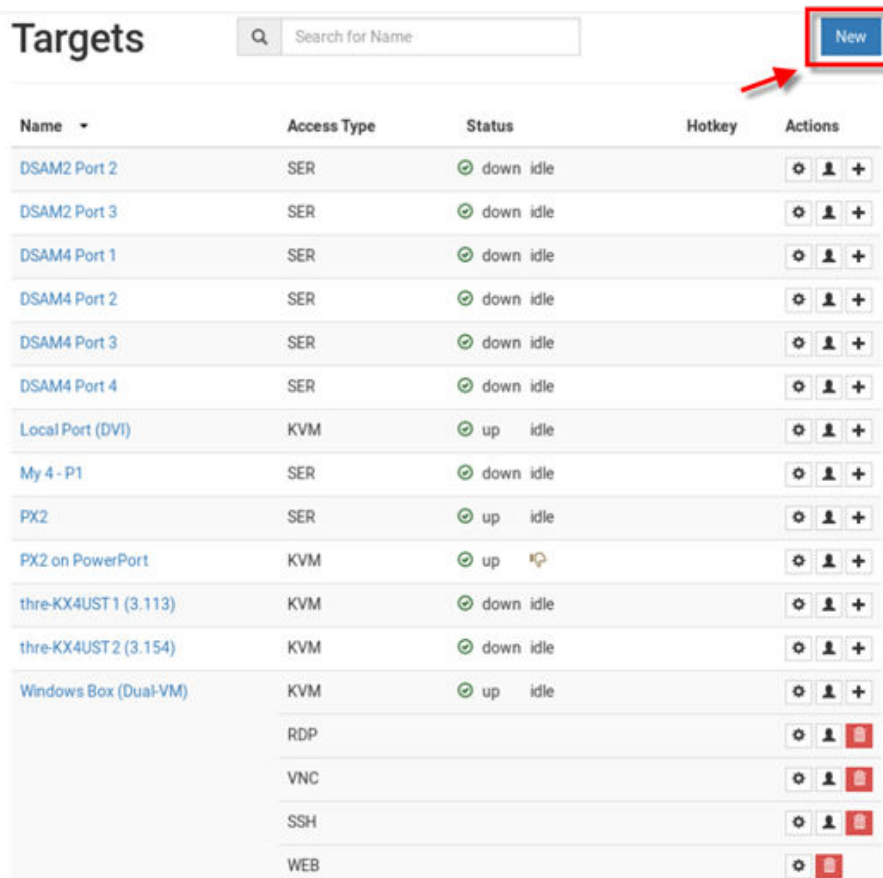
3. In the Add Access page, you will name the Target, and add the first access method.
   - Name: Enter a name for the target.
   - Type: Select the type of access method.
     - SSH
     - VNC
     - RDP
     - WEB
     - ESXi
     - Multi KVM

4. Next steps vary based on Access Type.
    - SSH, VNC, and RDP Access (on page 99)
    - WEB Access (on page 100)
    - ESXi Access (on page 101)
    - Multi KVM Access with Dominion KX4-101 devices (on page 103)

► *To add targets and access methods to an existing target:*

1. In Main Menu, open the User Station Configuration window, then click Targets.

2. The Targets list appears. Click ✚ button in front of the target.

3. Fill out access details and click Save.

Add Access to !@WindowsPC

Access

* Type

SSH	▾
SSH	
VNC	
RDP	
WEB	
ESXi	
Multi KVM	

* Port Number

22

User Credentials

Name

Password

[Save] [Cancel]

4.   Click Add Access to add multiple access methods to the target.

Raritan.
A brand of ☐ legrand
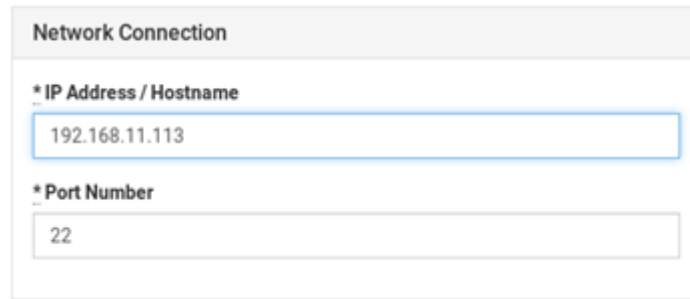
5. All Access Types list appears.

SSH, VNC, and RDP Access

1. Add a target, then add the access method: Adding Targets and Access Methods (on page 95).
2. When Type is selected as: SSH, VNC, or RDP, the similar information is required.
   - IP Address/Hostname: Enter the IP or hostname for the target.
   - Port Number: The default port number for the access type is populated automatically, but can be changed.

Network Connection

* IP Address / Hostname

192.168.11.113

* Port Number

22

- User Credentials: Enter the user name and password as required for the access type. *VNC requires password only.

User Credentials

Username

admin

Password

••••••••

Save   Cancel

3. Click Save. SSH/VNC/RDP access is added to the target and a list of all current access methods with options for editing displayed.

WEB Access

The WEB access method allows you to launch a web application in the Dominion User Station's own web client. This can be used to launch the Remote Control feature to control another User Station, or to access the web user interface of another KVM device.

See Remote Control via Web Browser (on page 244). The web client offers simple navigation only, and does not support Java, plugins, file upload/download, audio/video, webcams/microphones, opening new windows or tabs, or other advanced features. Single sign-on is not supported, so you must enter credentials each time you launch the WEB interface.

To launch WEB access, you must have the WEB Access privilege. To configure WEB access, you must have Device Administration or System Administration privilege.

1. Add a target, then add the access method: Adding Targets and Access Methods (on page 95).
2. Select WEB as the Access Type.
3. Enter the URL following this format: <schema>://<host>[: <port>]/<path>

For example: https://www.example.com/test

Raritan.
A brand of 🔲legrand

4. Click Save. WEB access is added to the target and a list of all current access methods with options for editing displays.
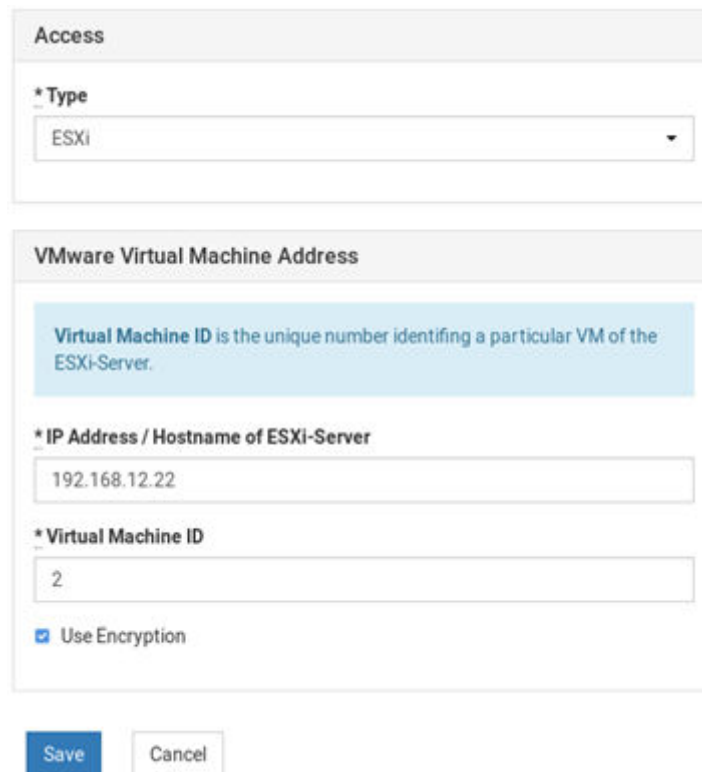
ESXi Access

The ESXi access method allows you to access and control VMware ESXi virtual machines from the User Station Navigator using the VMware "ESXi Embedded Host Client." The ESXi server must support the ESXi Embedded Host Client and must be version 6.0 or higher. Upon launching, the Remote Console of the virtual machine is shown. Single sign-on is not supported, so you must enter credentials each time you launch the interface.

To launch ESXi Access, you must have the ESXi Access privilege. To configure ESXi access, you must have Device Administration or System Administration privilege.

Note: These instructions apply to standalone mode. If you're working in CC-SG mode, your user experience is different. See Navigator with CC-SG Integration (on page 217).

Standalone ESXi connections not currently supported to ESXi version 6.5 or later.

1. Add a target, then add the access method: Adding Targets and Access Methods (on page 95)
2. Select ESXi as the Access Type.

3. Enter the IP Address or Hostname of the ESXi Server.
4. Enter the Virtual Machine ID. The ID can be found in the address bar of a browser where the URL to the virtual machine is displayed. The ID is the last component in the URL. See example images in host view and remote console view.

5. Select Use Encryption if you want to HTTPS as protocol for accessing the ESXi Remote Console.
6. Click Save. ESXi access is added to the target and a list of all access methods is displayed.

Raritan.
A brand of Llegrand

ESXi Access

IP Address / Hostname:
192.168.12.22
Virtual Machine ID:
2
Encrypted:
☑

Edit   🗑 Delete

Multi KVM Access with Dominion KX4-101 devices

You can configure two or more KVM ports as a virtual multi-monitor KVM target. The Dominion User Station supports up to six displays connected to the same target, with each display having its own dedicated KX4-101. Each KX4-101 is added to the Dominion User Station and then a new M-KVM target is created from the KVM ports of the KX4-101s. These independent ports are treated as a multi-monitor port group.

Important: Only Dominion KX4-101 ports connected to the same target PC are supported. The screen configuration on the target PC must match the configuration selected in the Dominion User Station.

To configure the Multi KVM access method, select the KVM ports that you want to group virtually, and set one of the supported orientations. Once Multi KVM access is created, these multi-monitor access points will be marked as "M-KVM" in the Navigator. The KVM ports included will still also be listed as separate ports in the Navigator. It is possible to connect to the single ports independently, but not recommended as functionality of mouse control is limited to the primary port. The Multi KVM targets cannot be added to the Port Scanner, but you can still add the single ports.

NOTE: It is important that the orientation, number of ports, and KVM port selection on the Dominion User Station match the display configuration. The following example image shows the Dominion User Station and target operation system. Display configuration for a Windows Server with 4 displays positioned horizontally. Use the Identify button on the Windows operating system to confirm that the display positioning on the target and Dominion User Station match.

Supported Orientations:

- Horizontal Dual
- Vertical Dual
- Horizontal Triple
- Vertical Triple
- Horizontal Quad
- Vertical Quad
- Quad 2x2
- Horizontal 5 Ports
- Vertical 5 Ports
- Horizontal 6 Ports
- Vertical 6 Ports
- 2x3 - 6 Ports
- 3x2 - 6 Ports
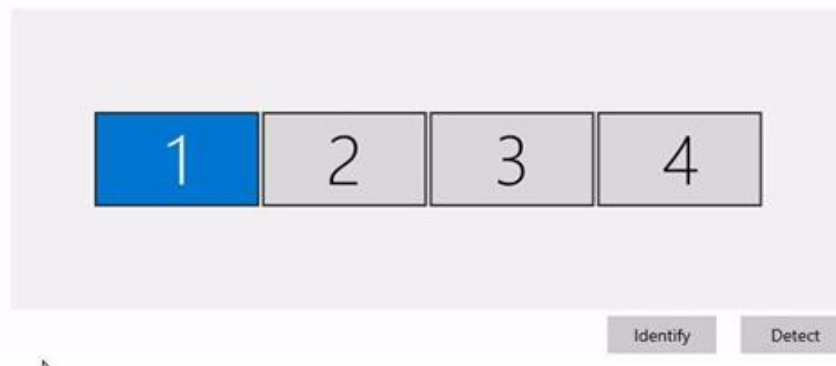
► *To configure Multi KVM Access:*

1. Add KX4-101s for target, then add the access method: Adding Targets and Access Methods (on page 95).
2. Select Multi KVM as th Access Type.
3. Select the orientation for the port group.
4. In the Primary Port and Secondary Port fields, you must select the KVM ports as follows:

- Primary Port: The KVM port located in the top left of the orientation of ports.
- Secondary Port: The KVM port located directly to the right of the primary, or directly below the primary.
- Then, for configurations with more than 2 ports, select Ports 3, 4, 5, and 6. Fields open as needed for each orientation.

5. Click Save. The new M-KVM target/access is added to the Targets list.

Adding Multi KVM to a Node Profile of CCSG

If the Dominion User Station is configured for CC-SG login, then the KX4-101s ports should be added to the same node and positioned to match the display configuration on the target server. Refer to the CC-SG Administrators Guide for detailed information.
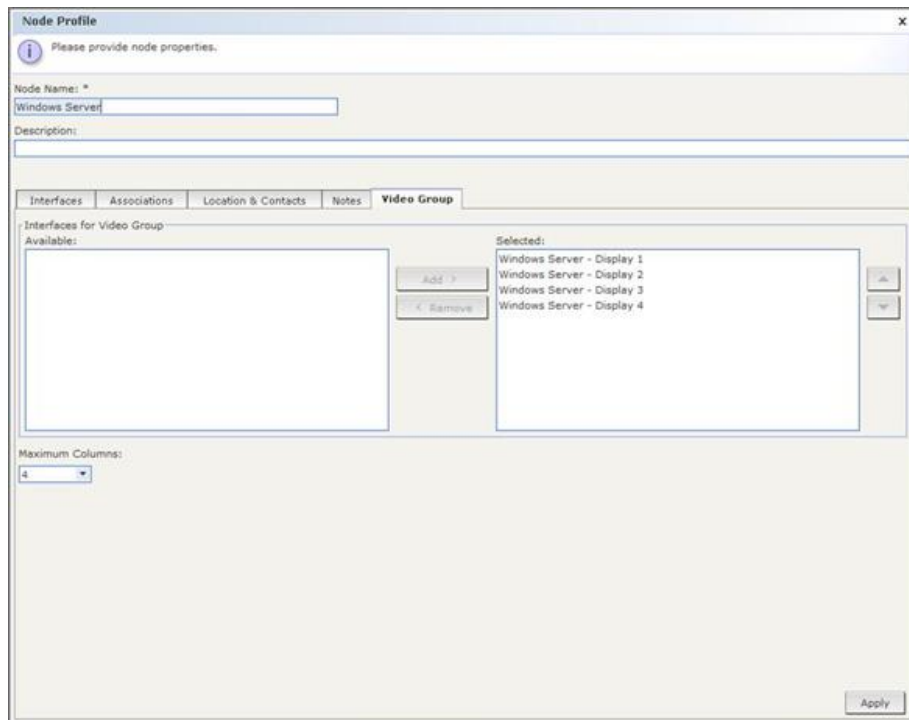
Note: Set the appropriate mouse mode to get best mouse response. Mouse Mode Support for Dual
Video Port Groups and M-KVM Targets (on page 295)

Editing and Deleting Targets and Access Methods

Targets and Access methods are listed in the User Station Configuration window.

You cannot delete KVM/Serial access, but all other access methods can be deleted. A Target must have
at least one access method, or the target is deleted.

► *To edit targets and access methods:*

1. In Main Menu, open the User Station Configuration window, then click Targets.

2. The Targets list appears. Use the Actions icons to edit as needed.

Name ▾	Access Type	Status	Hotkey	Actions
DSAM2 Port 2	SER	⊘ down idle		⚙ 👤 ✚
DSAM2 Port 3	SER	⊘ down idle		⚙ 👤 ✚
DSAM4 Port 1	SER	⊘ down idle		⚙ 👤 ✚
DSAM4 Port 2	SER	⊘ down idle		⚙ 👤 ✚
DSAM4 Port 3	SER	⊘ down idle		⚙ 👤 ✚
DSAM4 Port 4	SER	⊘ down idle		⚙ 👤 ✚
Local Port (DVI)	KVM	⊘ up idle		⚙ 👤 ✚
My 4 - P1	SER	⊘ down idle		⚙ 👤 ✚
PX2	SER	⊘ up idle		⚙ 👤 ✚
PX2 on PowerPort	KVM	⊘ up 🕹		⚙ 👤 ✚
thre-KX4UST 1 (3.113)	KVM	⊘ down idle		⚙ 👤 ✚
thre-KX4UST 2 (3.154)	KVM	⊘ down idle		⚙ 👤 ✚
Windows Box (Dual-VM)	KVM	⊘ up idle		⚙ 👤 ✚
	RDP			⚙ 👤 🗑
	VNC			⚙ 👤 🗑
	SSH			⚙ 👤 🗑
	WEB			⚙ 🗑

⚙	Edit settings for a port or access point. See Configuring KVM and Serial Ports (on page 88) for details on KVM port settings.
	See Configuring Access Settings (on page 107) for all other types.
👤	Edit user credentials for any access method.
🗑	Delete an access method. You cannot delete KVM or SER access. Deleting the last access method deletes the target.
✚	Add an access method to the target.

Configuring Access Settings

For each access type, you can configure General and Target Window Settings. Most settings are shared among all types of targets, but there are some unique settings in each category. Unique settings for each access type are outlined in the examples below.

By default, Dominion User Station uses Target Window Settings that are valid for all ports and access points. You can override these settings for a specific port/access point by selecting the "Use Specific Target Window Settings". For details on all settings, and to set defaults, see Access Client Settings (on page 172)

► *RDP Access Settings:*

Edit Settings for RDP Access to RDP_53111

General Settings

☐ Hotkey Ctrl+Alt ▼ + A ▼

☐ Favorite

☐ Automatically connect Speaker

☐ Automatically connect Microphone

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.

Note: Keypad keys are not recognized. Please use regular number keys only.

Target Window Settings

☐ Use specific Target Window Settings

　☑ Window Decorations

　☐ Full-Screen Mode

Resizing Behavior

Fixed Size ▼

Transmission Quality

Medium ▼

Preferred Resolution

1024 x 768 ▼

Display as Multi-Monitor Target

Use 2 monitors ▼

Desktop Scaling

100% ▼

By default, Dominion User Station uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

Access Client Settings

Notes:
- These setting don't apply to already active target sessions.
- The Full-Screen hotkey is always *Ctrl+Alt+Enter*.
- Multi-Monitor RDP targets are always launched in Full-Screen mode.

RDP Certificate

Fingerprint:
f6:17:d8:59:ef:90:9f:fb:2f:89:f0:f7:30:60:67:97:e9:43:0b:52:9c:4d:3d:4 c:b1:1a:91:f5:b4:af:55:70

Notes:
An RDP certificate is a cryptographic certificate used for identifying computers in the RDP protocol. Depending on the

Save　Cancel

► *VNC Access Settings:*

Raritan.
A brand of 🔲 legrand

Edit Settings for VNC Access to Dominion_KX3_Port13

General Settings

☐ Hotkey   Ctrl+Alt   ▾   +   A   ▾

☐ Favorite

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.

Note: Keypad keys are not recognized. Please use regular number keys only.

Target Window Settings

☐ Use specific Target Window Settings

☐ Scale Video

☑ Window Decorations

☑ Show Tool Bar

☐ Full-Screen Mode

☐ Allow Input if focused only

Cursor Shape (in Double Cursor Mode)

Default ▾

☐ Disable Banner Messages

By default, Dominion User Station uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

[Access Client Settings]

Notes:
- These setting don't apply to already active target sessions.
- To leave Full-Screen Mode, press the Full-Screen hotkey (*Ctrl+Alt+F* by default) in the Client.
- To launch the session in Full-Screen mode, an according hotkey must be configured, or the Tool Bar must be activated. Otherwise, users would be locked in into Full-Screen.

[Save]   [Cancel]

► *SSH Access Settings:*

Edit Settings for SSH Access to Dominion_KX3_Port6

General Settings

☐ Hotkey   Ctrl+Alt   ▾   +   A   ▾

☐ Favorite

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.

Note: Keypad keys are not recognized. Please use regular number keys only.

Target Window Settings

☐ Use specific Target Window Settings

☑ Window Decorations

☑ Show Menu Bar

☐ Full-Screen Mode

Console Size

80 x 24 ▾

By default, Dominion User Station uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

[Access Client Settings]

Notes:
- These setting don't apply to already active target sessions.
- The Full-Screen hotkey is always *F11*.

SSH Host Key

There is no SSH Host key saved for this access.

Notes:

An SSH host key is a cryptographic key used for authenticating computers in the SSH protocol. Depending on the Security Settings, it may be possible to connect to known hosts via SSH only.

If there is a host key saved for this access, you can see its fingerprint here and you can delete it.

[Save]   [Cancel]

► *WEB Access Settings:*

Edit Settings for WEB Access to Windows Box (Dual-VM)

General Settings

☐ Hotkey   Ctrl+Alt   ▼   +   A   ▼

☐ Favorite

> You can assign a Hotkey for quickly accessing this KVM Port or Access Point.
>
> **Note:** Keypad keys are not recognized. Please use regular number keys only.

Target Window Settings

☐ Use specific Target Window Settings
   ☑ Window Decorations
   ☑ Show Tool Bar
   ☐ Full-Screen Mode

> By default, Dominion User Station uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**. Adjust the default settings via the Access Client Settings dialog:
>
> [Access Client Settings]
>
> **Notes:**
> - These setting don't apply to already active target sessions.
> - The Full-Screen hotkey is always *F11*.

► *ESXi Access Settings:*

Raritan.
A brand of 🔲legrand

Edit Settings for ESXi Access to Windows Box (Dual-VM)

Known Limitations on Targets

There are some known limitations on how Target access sessions function compared to typical KVM Client sessions.

- When opening a session, "Open in new / Open in current" is available for KVM and VNC, RDP and SSH only support "Open in new".
- VNC: Only RFB protocol versions 3.3 to 3.8 are supported. Proprietary extensions and versions are not supported, for example:
  - RealVNC protocol version 4.x and 5.x
  - TightVNC tight authentication
  - UltraVNC authentication
  - Connections over TLS, which is proprietary for some VNC servers
- If RDP connections to Windows targets fail, check these settings. Open the Edit Group Policy tool from Control Panel or use the Windows Search dialog (Windows Key + R, then type in gpedit.msc). Browse to: Local Computer Policy>Computer Configuration>Administrative Templates>Windows Components>Remote Desktop Services>Remote Desktop Session Host>Remote Session Environment. Disable "Use the hardware default graphics adapter for all Remote Desktop Services sessions."
- The Dominion User Station embedded browser does not support:

- Java applets or Flash

- Pop-ups

- Auto-Fill

- Remember passwords

- Long-term cookies

- The RDP client does not support virtual media, SmartCard authentication, and other USB devices.

- When RDP target is in focus the Dominion User Station can not be powered off from short press of power button. You need to either minimize the RDP client or move it in background to power off the Dominion User Station. However, if option "Grab all Keyboard and Power Button events" in Access Client settings is unchecked, this changes this behavior.

Navigation and Access
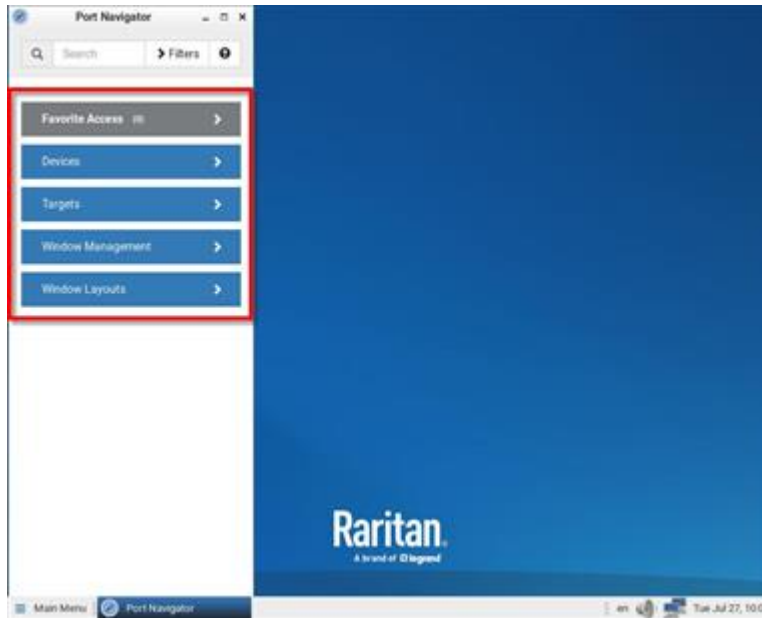
The Port Navigator contains three panels for accessing your ports and other targets:

- *Favorite Access*
- *Devices*
- *Targets*

And two panels for managing client windows:

- *Window Management*
- *Window Layouts*

The Navigator remembers the last-opened panel and returns to it when Navigator is opened again.

Note: When you are logged in as a CC-SG user, your user experience is different. See Navigator with CC-SG Integration (on page 217).

► *To access a KVM/Serial port in the Devices panel:*

1. Open the Devices panel. Once opened, the panel color turns gray.
2. Click a KVM/Serial switch.
3. Click a KVM or Serial port.

Note: The User Station CANNOT access a KVM port that is connected to a tiered KVM switch or a blade chassis server.

► *To access using the Targets panel:*

1. Open the Targets panel.
2. Click a target to access it by the default access method. See <u>Port Navigator</u> (on page 114) for details on multiple access methods and so on.

► *To use Window Management:*

1. Open the Window Management panel.
2. Click an option for arranging your open client windows. See <u>Window Management</u> (on page 58) for more details.

► *To use Window Layouts:*

1. Open the Window Layouts panel.
2. Click a window layout to open it. You must setup and save layouts before you can select them here. See <u>Window Layouts</u> (on page 187) for more details and configuration.

In This Chapter

Port Navigator

The Port Navigator window is displayed by default.

Note: When you are logged in as a CC-SG user, your user experience is different. See <u>Navigator with CC-SG Integration</u> (on page 217).

► *To launch Port Navigator:*

- Press *Ctrl+Alt+N*.
- OR choose Main Menu > Port Navigator.
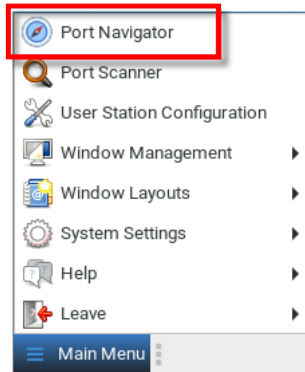
The Port Navigator window opens.
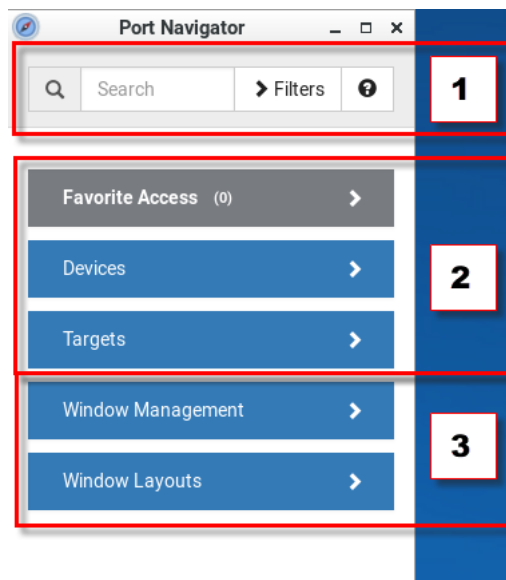
- Search, Filters, and Help:

    Search:

    Searches for ports, switches, or targets and access points containing the search word(s). See Using Search (on page 119).

Additional Filters:

   Determines which items are displayed in this window based on connectivity and availability. See Using Filters (on page 120).

Help ❓ :

   Shows the colors and icons denoting KVM/Serial switch and port states. See Identifying States of KVM/Serial Switches and Ports (on page 117).

- Favorite Access, Devices, and Targets:

    Favorite Access panel:

    Shows a list of favorite targets you have configured. See Configuring KVM and Serial Ports (on page 88).

Devices panel:

- Shows a list of all KVM/Serial switches and ports, plus DSAM serial ports.
- Left-click on port opens the KVM or Serial client.
- Right-click on port opens the context menu.
- The default is to show switches whose status is Normal or Unknown. See Using Filters (on page 120).

Targets panel:

- Shows a list of all Targets. Targets with KVM/Serial access also show port status.
- Left-click on the Target opens the appropriate client. If there is more than one Access Point defined, the following hierarchy applies for which type of Access to use:
  - M-KVM
  - KVM
  - SER
  - RDP
  - VNC
  - SSH
  - WEB
  - ESXi
- Next to the Target name, all configured access methods are listed. Click the access method directly to open the appropriate client. If there are multiple Access Points of the same type defined then the most recently added Access Point is opened.

- Right-click on the Target, or click the hamburger menu to list all access methods defined for the Target.

- If a second or third monitor is available for KVM or VNC targets, you can choose to open the target in the second or third monitor. Also on the right-click menu, choose Open Port Settings to jump to configuration.
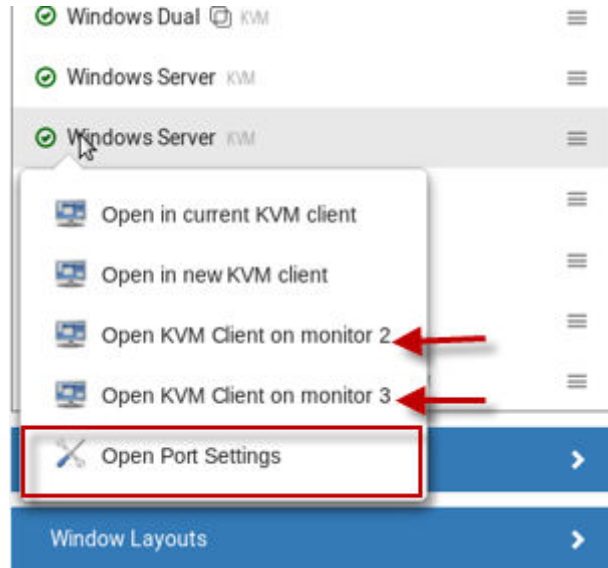
- The default is to show items whose status is Up. See Using Filters (on page 120).
- For dual port video, the name of the dual port video group is displayed instead of the port names. Dual port video groups whose primary port is Up will show in the list.
- Window Management and Window Layouts:
- Window Management: Manage open sessions with window management tools. See Window Management (on page 58).
- Window Layouts: Access saved layouts. See Window Layouts (on page 187).

Identifying States of KVM/Serial Switches and Ports

In the Port Navigator window, different icons and colors are applied to indicate current states of the added KVM/Serial switches and ports.

Icon and color information is available by clicking the question mark icon ❓ .
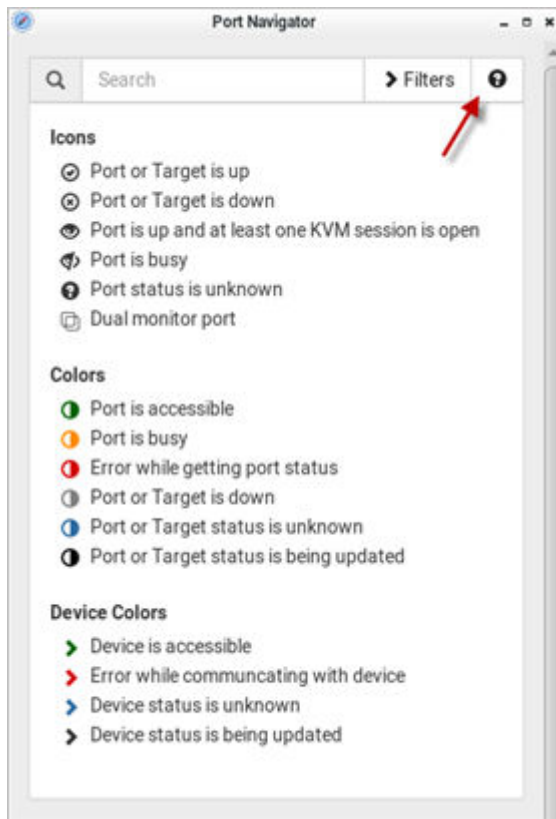
Identifying External Media

When external media are connected to a port via virtual media, the media icons display after the port name/number.
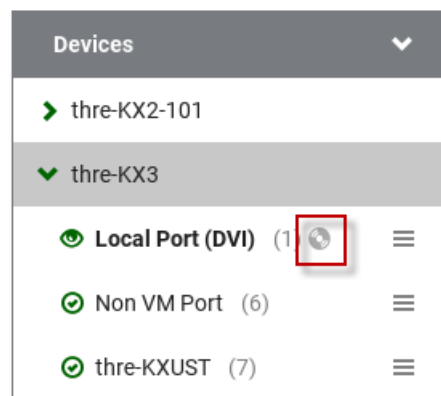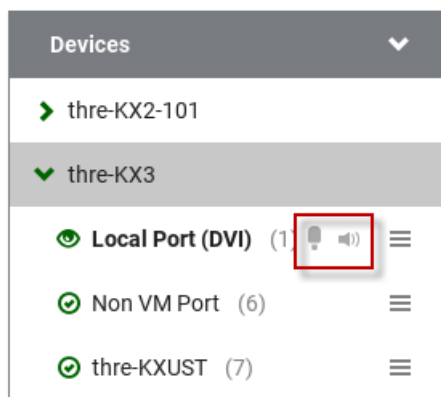
Icon	Port state
	Mass Storage

⊚	ISO/CD device
⬤	Microphone
◀))	Speaker
▭	SmartCard Reader

Dual Video Port Status

The primary port must have Status=Up to make a connection to both ports. The secondary port cannot be connected to directly, so its status is not reflected in the Navigator.

If the secondary port has Status=Down, there is still a dual monitor connection to both ports. There is either a "No Video" message or an error message such as "Cannot switch to port" on the secondary client. In this case, User Station acts differently from KX3, because User Station allows the user to connect to any target, independent of the status, using Filters. See Using Filters (on page 120).

Using Search

The search box allows you to search for the KVM/Serial ports or switches that match the user's search words.

► *To search for KVM/Serial ports or switches:*

1. Open the panel where you want to perform the search function.
   - To search for a KVM/Serial switch, click the Devices panel.
     - To search KVM/Serial ports of a specific KVM/Serial switch in addition to KVM/Serial switches, you can click the desired KVM/Serial switch to have its KVM/Serial ports displayed prior to using the Search function.

       Note: The User Station will NOT search the KVM/Serial ports of those unselected KVM/Serial switches in the Devices panel.

   - To search for a KVM/Serial port only, click the Targets panel.
   - To search for a "favorite" KVM/Serial port, click the Favorite Access panel.
2. Type the search word(s) in the Search box. Words are not case sensitive.
3. The currently opened panel immediately shows the search result.

Using Filters

By default, the Port Navigator window only shows devices that can be communicated with properly, and the ports and targets that are up. You can change the display criteria by using filters.

► *To change the filter:*

1. Click Filters, and the following checkboxes will appear.
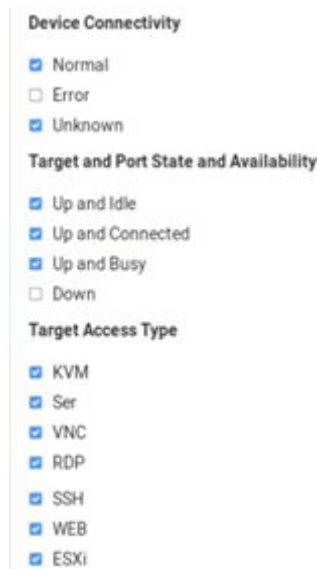
2. Select or deselect any checkboxes to determine what is shown.

Checkbox	KVM/Serial switch's state
Normal	The KVM/Serial switch can communicate with the User Station, and the device state is normal.
Error	The KVM/Serial switch cannot communicate with the User Station.
Unknown	The KVM/Serial switch can communicate with the User Station but cannot determine its device state.

Checkbox	KVM/Serial ports or target state and availability
Up and Idle	The port is up, accessible and no KVM/Serial sessions are active.

Raritan.

A brand of Llegrand

Up and Connected	The port or target is up, and at least one KVM/ Serial session is active.
Up and Busy	The port or target is up, but busy because an exclusive KVM/Serial session is active.
Down	The port is down.

1. For Target Access Type, select the access types you want to include.
2. When completed, click Filters again to hide the options.

Port Scanner

The Port Scanner displays an assortment of ports that you select, by scanning through each connection for a specified period of time. You can launch a KVM connection to any port shown in the scanner. The Port Scanner can also save target snapshots to an external USB device, when enabled. This is useful for forensic or surveillance purposes. See Port Scanner Settings (on page 188) for details on configuration and user privilege.

- Launch the Port Scanner from the Main Menu. See: Port Scanner (Launch) (on page 57)
- Ports are included by selecting the setting "Include in Port Scanner" when configuring the port. Go to User Station Configuration > Port Configuration settings. See Configuring KVM and Serial Ports (on page 88) for detailed instructions.
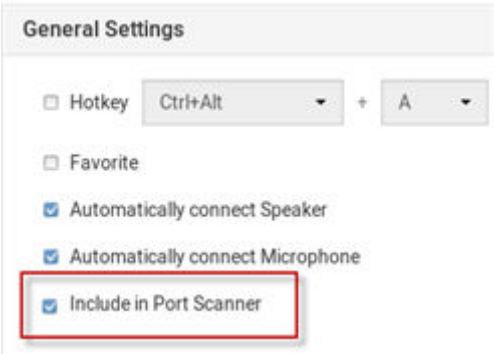
- The scanner allows you to pause and restart the scanning, open KVM sessions, show and hide thumbnails of each port, and set the scan options. See Operating the Port Scanner (on page 122).
- Audit log entries are created for each individual scanned port when you scan KX2-101/KX4-101 ports. When scanning KX3 ports, an audit log entry is created at the start and end of the scan session.
- The Port Scanner functions in both CC-SG mode and non-CC-SG mode.
- Window Management functions do not apply to the Port Scanner window.

In This Chapter

Operating the Port Scanner

1. The main toolbar at the top of the Port Scanner has 4 buttons:
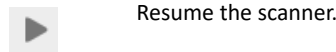
    ▶   Resume the scanner.

![pause icon]	Pause the scanner.
![thumbnails icon]	Show or hide the thumbnails.
![live preview icon]	Show or hide Live Preview image.
![scanner options icon]	Configure the scanner options. See Scanner Options (on page 124).
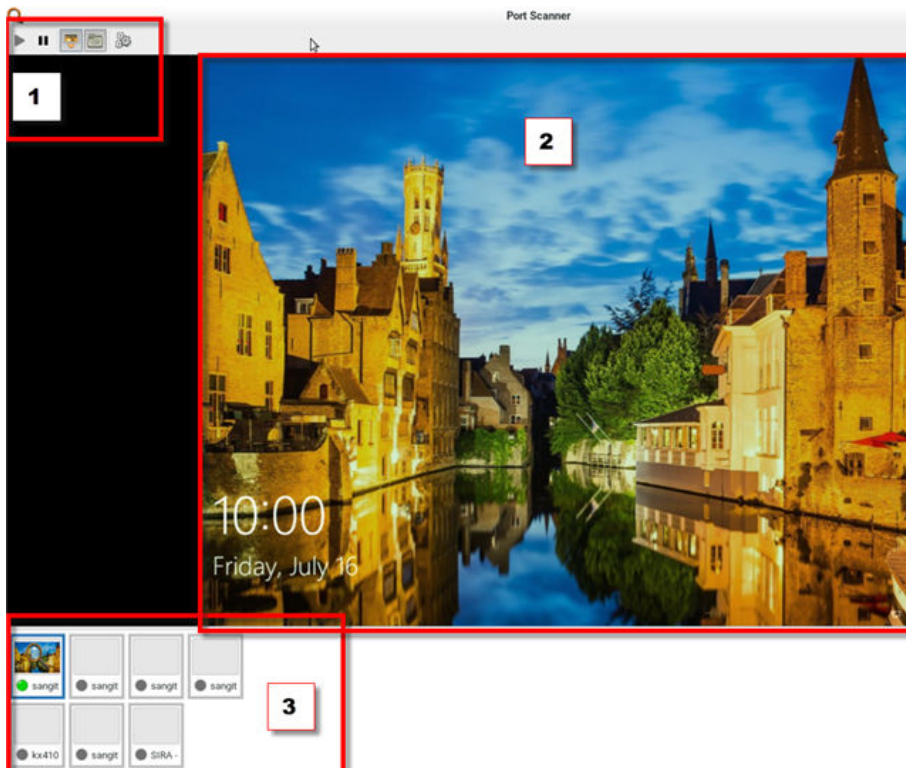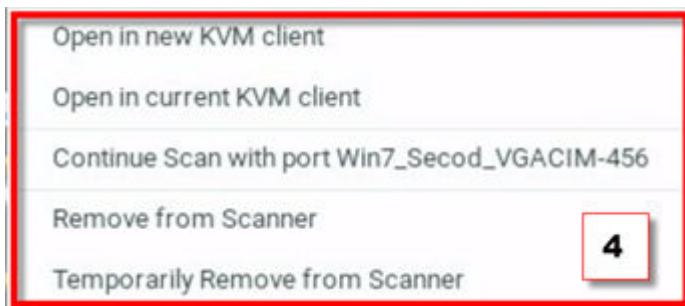
2. The thumbnail preview shows all included ports. Choose vertical or horizontal placement in the scanner options.

3. The currently displayed port is highlighted in the thumbnails preview. Click the thumbnail once to view the port in the scanner. Double-click the thumbnail to open a KVM session to the port. Note that the default action of a double-click can be configured in Launch Settings. See Access Client Settings (on page 172)

4. Right-click a thumbnail to open a pop-up menu with more options:

- Open in new KVM client: launch a KVM session to the port in a new window.

- Open in current KVM client: launch a KVM session to the port in the currrent window.

- Continue Scan with port "port name": Start scanning the selected port.

- Remove from scanner: Turns off the "Include in Port Scanner" setting for the port.

- Temporarily Remove from Scanner: The port is removed from this scanner session, but it is included the next time the scanner is started.

Scanner Options

The port scanner can be configured to set intervals and delays, thumbnail orientation, and pause behavior.

See Port Scanner Settings (on page 188) to configure recording scanner snapshots.

► *To set scanner options:*

1. In the Main Menu, click Port Scanner to open the port scanning window.

2. Click the Scan Settings icon to open the options.

3. Configure intervals and delays:

    a. Port Display Interval: Select the number of seconds to display each port before switching to next

    b. Interval between Ports: Select the number of seconds to pause after Port Display Interval ends.

4. Configure settings:

    a. Thumbnails orientation: Select Vertical or Horizontal to position thumbnails in relation to scan window.

    b. Use Grid View for Thumbnails: Select this checkbox to enable grid view. See Port Scanner Grid View (on page 125).

    c. Pause Scanner when opening KVM Sessions : Select this checkbox if the scanning should stop when you open a port into a full KVM session.

5. Click OK.
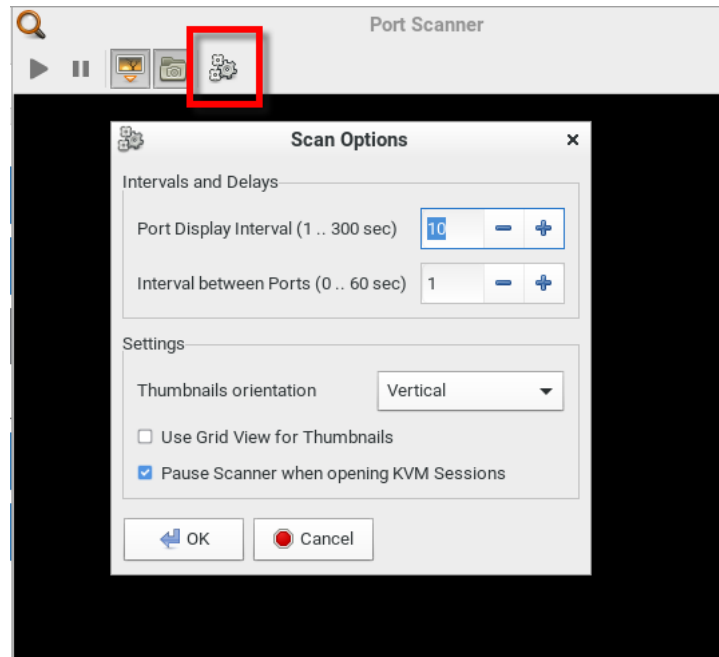
Port Scanner Grid View

The User Station port scanner offers a "grid" or "matrix" view option of ports from different Dominion devices. The grid view shows multiple thumbnails in a row/column view, all at the same time, and without scrolling. The number of ports is unlimited, varies as needed, and all ports are visible in the grid view. The grid view works for both CC-SG and non-CC-SG.

The port scanner grid view can show ports from more than one KX. Thumbnails can be arranged in a view, as a grid, without scroll bars. The thumbnails are automatically resized and arranged so that all ports in the port scanner are visible.

Note: The thumbnail views in the grid view are periodically updated. Due to technical limitations in the processor and video resources, the grid view does not allow live-updates.

► *How the Grid View Works*

- The thumbnails section can optionally be a grid view, showing all the thumbnails at once without scrollbars.
- The size and position of the thumbnails automatically adapt to the size of the thumbnails section, or the best fit.
- The thumbnails section fills the entire space; if preferred, the live preview section can be hidden.

Using the KVM Client

A KVM Client window opens after launching a KVM port where a server is physically connected. When dual video ports are configured, connecting to the dual video port group opens two KVM client windows that are bound together. See Dual Video Port Connections (on page 163).

The server or PC connected to a KVM port is called the *target server*.

The Dominion User Station's KVM Client settings are configured through the toolbar only. No menu bar is available.
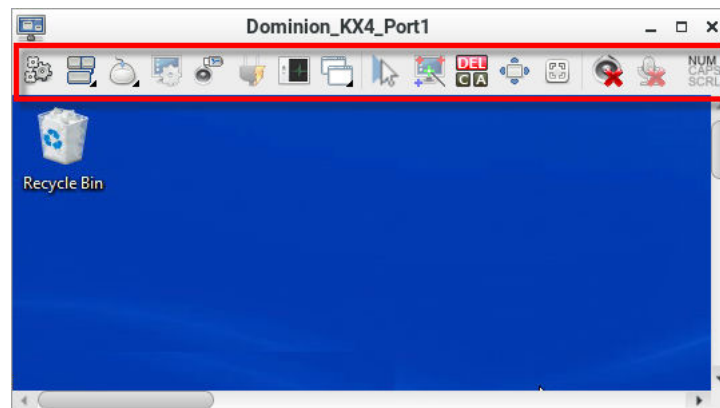
In This Chapter

Connection Properties

Connection properties manage streaming video performance over connections to target servers. The properties are applied only to your connection, not the connection of other users accessing the same target server.

► *To configure connection properties:*

1. Click ⚙ to open the Connection Properties dialog.
   - KX3 Target Server Connection Properties:
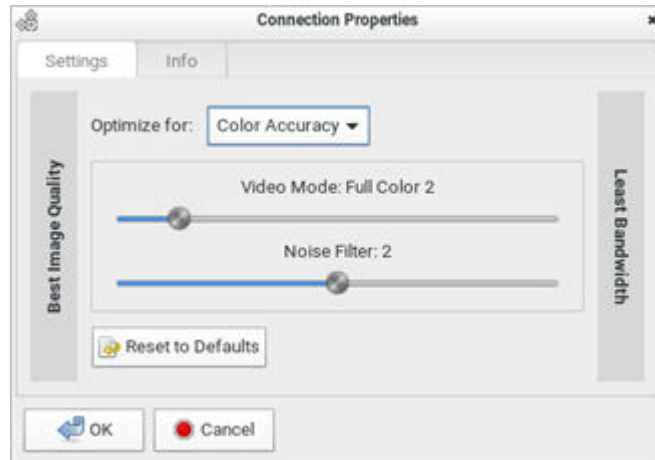
   - KX4-101 Target Server Connection Properties:
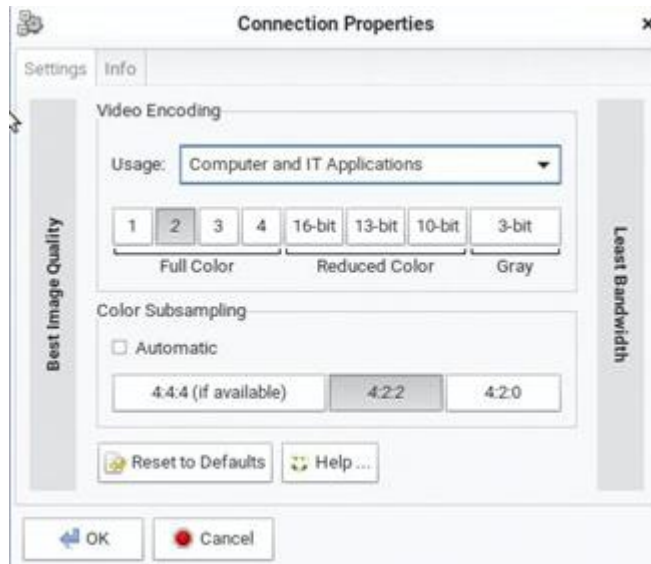
2. The default connection settings are the optimal settings for video performance most of the time. Do NOT make changes unless required. See .

Devices Settings and Description

KX3	
Setting	**Description**
Optimize for	Determine which aspect of video data is optimized for. There are two options: • Text Readability (on page) • Color Accuracy (on page)
Video Mode	This slider controls the video quality as well as the bandwidth. • Left: higher quality with higher bandwidth consumed. • Right: lower quality with less bandwidth consumed. This is useful for low-bandwidth connections. See Video Mode (on page 132).
Noise Filter	This slider controls the noise filter threshold. • Left: higher threshold. • Right: lower threshold. See Noise Filter (on page 132).
Reset to Defaults	Reset connection properties to the factory defaults.

KX4-101	
Setting	**Description**
Usage	Specifies general application area. There are two options: • General Purpose Video • Computer IT Applications
Video Encoding	This controls the video encoding algorithm and quality setting. • Left: higher image quality with higher bandwidth consumed. • Right: lower quality with less bandwidth consumed. This is useful for low-bandwidth connections.
Color Subsampling	This reduces the color information in the encoded video stream. There are four options: • Automatic: The optimal color subsampling mode. • 4:4:4: Highest quality at significant bandwidth cost. • 4:2:2: Good blend of image quality and bandwidth. • 4:2:0: Maximum savings of network bandwidth and client load.
Reset to Defaults	Reset connection properties to the factory defaults.
Help	This provides connection properties help .

1. Click OK to save any changes made. The settings are stored persistently for the accessed port.

► *To view connection information:*

•   Click the Info tab in the same dialog.
    •   KX3:
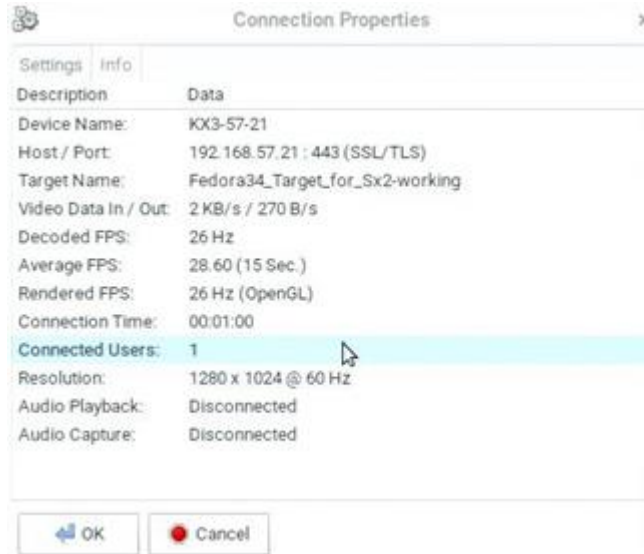
- KX4-101:
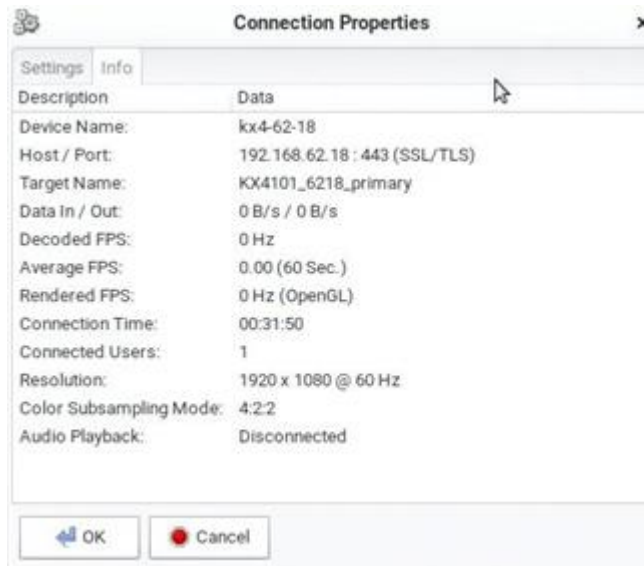
Item	Description
Device Name	The KVM switch's name.
Host / Port	The KVM switch's IP address, and the TCP/IP port used to access the KVM switch.
Target Name	The accessed KVM port's name.
Data In / Out	Rate of data received and sent out to the KVM switch in bytes per second.

Raritan.
A brand of ◻legrand

Item	Description
Decoded FPS	Number of frames per second that were received and decoded by the KVM Client.
Average FPS	Average number of frames per second
Rendered FPS	Number of frames per second that were displayed onscreen. Usually this number is similar to "Decoded FPS", but it may be lower on high graphics demand.
Connection Time	Duration of the current connection.
Connected Users	Number of connected users.
Resolution	Video resolution of the target server connected to this KVM port.
Color Subsampling Mode	The selected color subsampling mode. (KX4-101 only)
Audio Playback	Active, Disconnected or Muted.
Audio Capture	Active, Disconnected or Muted.

Default Connection Properties

The Dominion User Station comes configured to provide optimal performance for the majority of video streaming conditions.

▶ *KX3 default connection settings:*

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

► *KX4-101 default connection settings:*

- Usage: General Purpose Video
  - This video content emphasizes smooth color reproduction. The default video mode is always "Full Color 2", which is a high-quality mode and works well for most uses in LAN environments.
- Color Subsampling:
  - Reduces the color information in the encoded video stream.It is set to Automatic with 4:2:2 settings.

Video Mode

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

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

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

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

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

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

Noise Filter

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

The Noise Filter controls how much interframe noise is absorbed by the Dominion User Station.

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

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

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

Video Encoding (KX4-101 only)

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 Sampling (KX4-101 only)

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. In KX4-101 releases prior to 4.4.0 not supported for resolutions above 1920x1200, so for those resolutions color sub-sampling will automatically drop down to 4:2:2. In KX4-101 4.4.0 and above supported for all resolutions.
- 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.

Keyboard Macros

Click to select one of the pre-programmed hotkey macros.
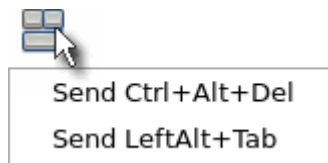
Note: If you have manually created any hotkey macros and have them enabled, these macros are displayed below "Send LeftAlt+Tab." See Managing Keyboard Macros (on page 177).

► *Send Ctrl+Alt+Del:*

To send this key sequence to the target server you are accessing:

- Click [icon] > Send Ctrl+Alt+Del.

- OR click [icon] .

► *Send LeftAlt+Tab:*

This hotkey macro switches between open windows on the target server you are accessing.

Warning: If you physically press *Ctrl+Alt+Del* or *Left Alt+Tab* using the KEYBOARD, these key sequences are processed on the User Station by default, instead of being transferred to the target server. To change the default behaviors so that they are processed on the target servers after being pressed on the keyboard, see Desktop Settings.

Mouse Settings

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

Single mouse mode displays only one mouse pointer while dual mouse mode displays two.

In any mouse mode, when the mouse pointer lies within the KVM Client's target server window, mouse movements and clicks are directly transmitted to the target server.

Click [icon] to select one mouse command or mode.
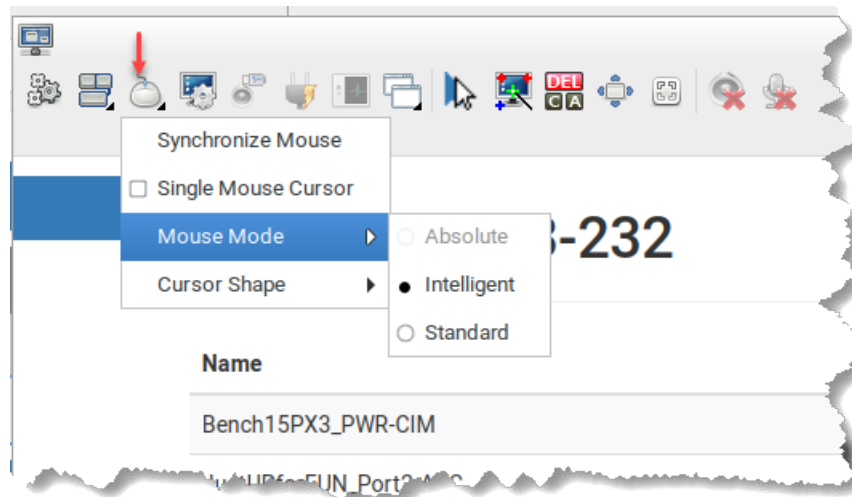
Single Mouse Cursor is for single mouse mode. Absolute, Intelligent and Standard are the dual mouse modes.

Important: Make sure you have configured mouse settings on the target servers properly. For information on configuring mouse settings of target servers, refer to the KX III KVM switch's user documentation from its application or the Dominion KX III section of the Raritan website's Support page.

Synchronize Mouse

In the dual mouse mode, the Synchronize Mouse command forces realignment of the target server's mouse cursor with the User Station's. See Dual Mouse Modes (on page 136).

► *To synchronize the mouse cursors:*

- Click [icon] > Synchronize Mouse.

- OR click [icon] .

Note: This option is available in Intelligent and Standard mouse modes only. However, mouse synchronization may not always be successful with this option. When this occurs, first check Mouse Synchronization Tips (on page 138). If the mouse synchronization issue still cannot be resolved, enter the Absolute or single mouse mode. See Single Mouse Cursor (on page 135) and Absolute Mouse Mode (on page 136).

Single Mouse Cursor

In single mouse mode, you only use the target server's mouse cursor, and the User Station's mouse cursor no longer appears on the screen.

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

► *To enter the single mouse mode:*

1. Click [icon] > Single Mouse Cursor.
2. Click OK on the confirmation message.

Single Cursor Mode ✕

You are about to enter Single Cursor mode. While you are in this mode, this software will have exclusive control over the mouse and keyboard.

To temporarily leave single cursor mode, press Ctrl+Alt+M.
To completely deactivate single cursor mode, use the menu item afterwards.

↵ OK   🔴 Cancel
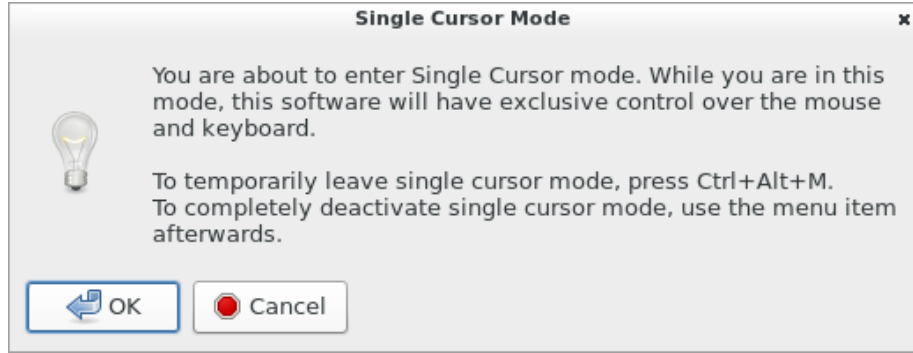
► *To temporarily exit the single mouse mode and then return to this mode:*

1. Press Ctrl+Alt+M on your keyboard. A message appears, indicating that the single mouse mode is temporarily suspended.

Now you can use the mouse to control the User Station.

2. To return to the single mouse mode, click anywhere on the target server's image in the KVM Client.

Dual Mouse Modes

In the dual mouse modes, two cursors appear onscreen. They are:

- The mouse cursor of the User Station.
- The mouse cursor of the target server connected to the KVM port you are accessing.

Two mouse cursors align if properly configured.

While in motion, the User Station's mouse pointer slightly leads the target server's mouse pointer.

Absolute Mouse Mode

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

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

Use of virtual media CIMs on target servers is required for this mouse mode. See Virtual Media CIMs.

Most modern operating systems on the target servers shall support the Absolute mouse mode.

Note: Some Linux, UNIX, Solaris or very "unusual" operating systems as well as some USB profiles may not support the Absolute mouse mode. In this case, use other mouse modes. For detailed information of each USB profile, see the section titled "Available USB Profiles" in the KX III KVM switch's user documentation, which is accessible from the KVM switch application or the Raritan website's Support page.

Raritan.
A brand of 🔲**legrand**

► *To enter the Absolute mouse mode:*

- Click ![icon] >Mouse Mode > Absolute.

Intelligent Mouse Mode

In this mode, the target server's mouse settings are detected and the mouse cursors synchronized accordingly, allowing mouse acceleration on the target server.

This mode is the default for non-VM target servers.

Note: A non-VM target server is the target server using a CIM that does not support virtual media.

► *To enter the Intelligent mouse mode:*

- Click ![icon] >Mouse Mode >Intelligent.

► *Intelligent mouse synchronization requirements:*

The Synchronize Mouse command automatically synchronizes mouse cursors during moments of inactivity in the Intelligent mouse mode. See *Synchronize Mouse* (on page 135).

For this to work properly, the following conditions must be met:
- No windows should appear in the top-left corner of the target server's page.
- There should not be an animated background in the top-left corner of the target server's page.
- The target server's mouse cursor shape should be normal and not animated.
- The target server's mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as "Enhanced pointer precision" or "Snap mouse to default button in dialogs" should be disabled on the target servers.
- Choose "Best Possible Video Mode" in the Video Settings dialog of the KVM Client.
- The edges of the target server's video should be clearly visible (that is, a black border should be visible between the target server's desktop and the KVM Client window when you scroll to an edge of the target video image).

After autosensing the target server's video, manually perform the Synchronize Mouse command. This also applies when the resolution of the target server 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. See *Standard Mouse Mode* (on page 138).

Note that mouse configurations will vary on different target servers' operating systems. Consult your OS guidelines for further details.

Note: Intelligent mouse synchronization does not work with UNIX target servers.

Standard Mouse Mode

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

In order for the User Station's and target server's mouse cursors to stay in sync, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

► *To enter the Standard mouse mode:*

• Click >Mouse Mode > 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 your User Station.

The KVM Client's Connection Properties dialog displays the actual values the User Station is seeing.

2. Force a video auto-sense by clicking the KVM Client's Auto-sense Video button .
3. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris target servers):
    a. Open a terminal window.
    b. Enter this command: `xset mouse 1 1`
    c. Close the terminal window.

4. Click the KVM Client's mouse synchronization button .

Note: If the mouse synchronization issue still cannot be resolved, enter the Absolute or single mouse mode. See Single Mouse Cursor (on page 135) and Absolute Mouse Mode (on page 136).

Cursor Shape

Select a Cursor Shape to customize the visible cursor, or use a transparent cursor to hide the Dominion User Station's mouse cursor in the video area of the screen. The transparent mouse cursor is still visible in the toolbar area of the screen.

• Click > Cursor Shape, then select from the list.

- Default arrow
- Dot
- Crosshair
- Transparent

Video Settings

Video Settings are available for KX3 targets, but they are not available for KX4 targets.

Click [icon] to open the Video Settings dialog.
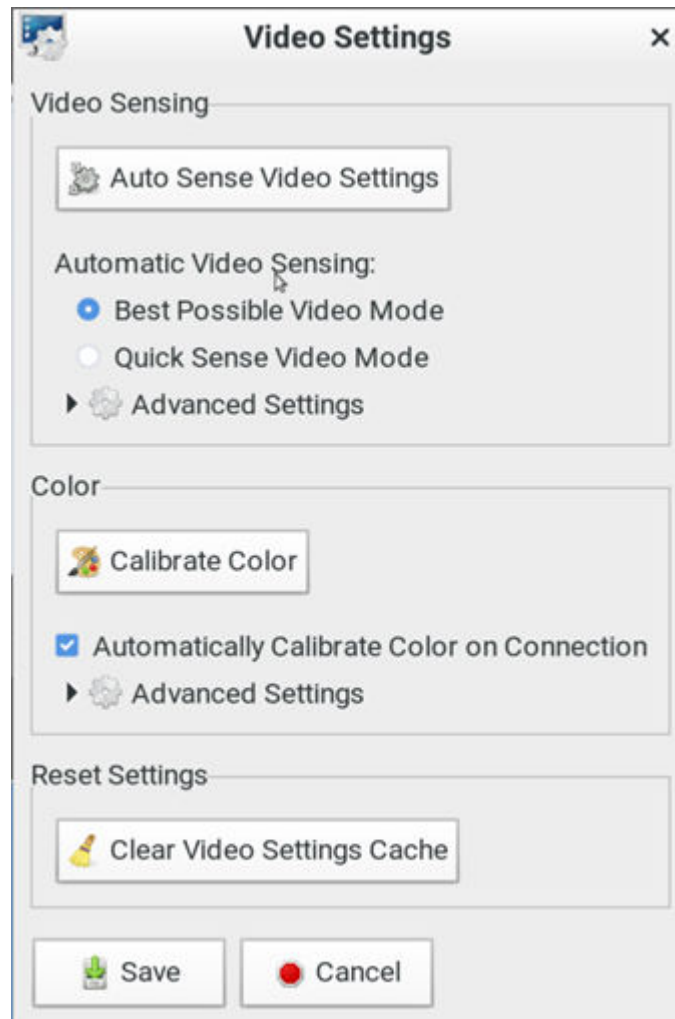
► *Video Sensing settings:*

Setting	Description
Auto Sense Video Settings	*Automatically detects the target server's video settings (resolution, refresh rate) and redraws the video screen.* *Clicking* *in the toolbar results in the same video re-sensing function.*
Best Possible Video Mode	*The User Station will perform the full Auto Sense process when switching target servers or target resolutions. Selecting this option calibrates the video for the best image quality.*
Quick Sense Video Mode	*Uses a quick video Auto Sense to show the target server's video sooner.* *This option is especially useful for entering a target server's BIOS configuration right after a reboot.*
Advanced Settings	*Adjusts the clock, phase, horizontal and vertical offset. See Advanced Video Settings (on page 141).*

Note: Some background screens, such as screens with very dark borders, may not center precisely. Use a different background or place a lighter colored icon in the upper-left corner of the screen.

► *Color settings:*

Setting	Description
Calibrate Color	*Optimizes the color levels (hue, brightness, saturation) of the transmitted video images. The color settings are on a target server-basis.* *Note that this command applies to the current connection only.*
Automatically Calibrate Color on Connection	*Causes the User Station to automatically update the color calibration once connected to a target server.*
Advanced Settings	*Adjusts brightness and contrast levels of red, green and blue colors. See Advanced Color Settings (on page 143).*

► *Reset Settings:*

The Clear Video Settings Cache button resets the cache where video settings are stored, which is useful when old video settings no longer apply, such as when a target server is replaced.

After calibrating the colors for a target server, color values are cached and reused whenever accessing that server. Changing resolutions resets the video to the cached values again.

Note that changes to the brightness and contrast levels are NOT cached.

When resetting the video settings cache, the User Station automatically does a video auto-sense and color calibration. New values are cached and reused for accessing that target server next time.

Advanced Video Settings

In the Video Settings dialog, click Advanced Settings in the Video Sensing section to show additional settings.
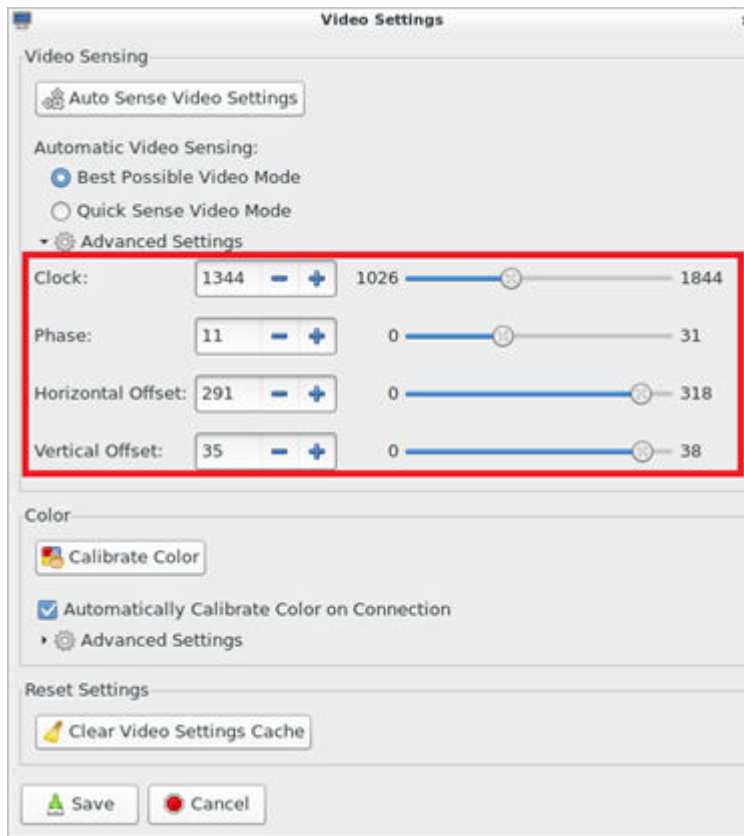
Click ⊟ or ➕ , drag sliders, or type a new numeric value in the text box to adjust corresponding settings.

Setting	Description
Clock	Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Under most circumstances, this setting should not be changed because the autodetect is usually quite accurate. Odd number settings are recommended.
Phase	Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.
Horizontal Offset	Controls the horizontal positioning of the target server display on your monitor.
Vertical Offset	Controls the vertical positioning of the target server display on your monitor.

Raritan.
A brand of 🔲 legrand

Advanced Color Settings

In the Video Settings dialog, click Advanced Settings in the Color section to show additional color settings.

Click ![minus button] or ![plus button] , drag sliders, or type a new numeric value in the text box to adjust corresponding settings.

Setting	Description
Brightness Red	Controls the brightness of the target server's display for the red signal.
Brightness Green	Controls the brightness of the green signal.
Brightness Blue	Controls the brightness of the blue signal.
Contrast Red	Controls the red signal contrast.

Setting	Description
Contrast Green	Controls the green signal contrast.
Contrast Blue	Controls the blue signal contrast.

Peripheral Devices and USB Settings

Click to open the "Audio, Mass Storage and SmartCard Devices" dialog, where you can virtually connect up to two devices of different types to a target server.

Important: It is strongly recommended to mount virtual media or audio devices onto the target server prior to the SmartCard reader. If the sequence is reversed, you will be logged out of the target's operating system as the card reader will be temporarily disconnected while connecting the audio or virtual media device.

Raritan.
A brand of 🔲 legrand

Section	Description
Connect New Device	• *Audio Device ...* Click this button to virtually connect an audio device to the target server. See Audio Device (on page 145). • *Mass Storage Device ...* Click this button to mount a USB drive or image file onto the target server. • *CD-ROM Device / ISO File ...* This button mounts a DVD drive, CD-ROM drive, or an ISO image onto the target server. See Virtual Media (on page 147). • *SmartCard Reader...* This button connects a SmartCard reader to the target server. See SmartCard Reader (on page 152).
Connected Devices	This section lists all devices which have been "virtually" connected to the target server. See Disconnecting a Virtual Device (on page 156).
USB Profiles	Click it to select a USB configuration profile that best applies to the target server. See USB Profiles (on page 157).

Note: For detailed information of each USB profile, see the section titled "Available USB Profiles" in the KX III KVM switch's user documentation, which is accessible from the KVM switch application or the Raritan website's Support page.

Audio Device

The User Station supports end-to-end, bidirectional, digital audio connections with a target server for digital audio playback and capture devices.

One of the following CIMs must be used:

- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Connecting Audio Devices

If an audio device is physically connected to the User Station, you can virtually connect it to one or multiple target servers simultaneously.

Note: Prior to connecting the audio devices to the target server, you may have to specify the audio devices you want to use. Per default, the front-panel analog speakers and microphone are used. See Audio Settings (on page 180).

► *To connect an audio device to the target server:*

1. Click [icon] to open the "Audio, Mass Storage and SmartCard Devices" dialog.

2. Click the "Audio Device ..." button. The Connect Audio Device dialog appears.
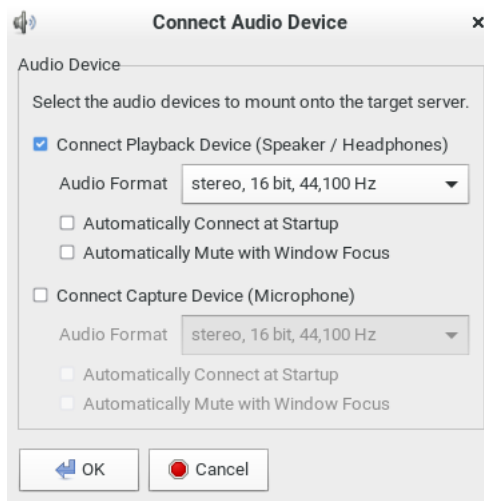
Note: KX4-101 does not support capture devices (Microphone).

Checkbox	Description
Connect Playback Device (Speaker / Headphones)	To manually connect an available audio playback device to the target server, select this checkbox. • Set the playback audio format in the Audio Format field. • Automatically Connect at Startup: The selected playback device will automatically be connected to the current target server whenever that target is accessed. • Automatically Mute with Window Focus: The selected device will automatically mute/unmute as window is active/inactive. • Mute/Unmute buttons are also available in the client toolbar for manual control.
Connect Capture Device (Microphone)	KX3 only: To manually connect an available audio recording device to the target server, select this checkbox. • Set the recorded audio format in the Audio Format field. • Automatically Connect at Startup: The selected microphone will automatically be connected to the current target server whenever that target is accessed. • Automatically Mute with Window Focus: The selected device will automatically mute/unmute as the window is active/inactive. • Mute/Unmute buttons are also available in the client toolbar for manual control.

1. Click OK.

► *To disconnect the audio device from the target server:*

• See Disconnecting a Virtual Device (on page 156).

Virtual Media

The Dominion User Station supports virtual media (VM). Virtual media extends KVM capabilities by enabling target servers to remotely access media from the User Station and network file servers.

With this feature, media mounted onto the User Station and network file servers are essentially "mounted virtually" by the KVM client to target servers. The target server can then read from and write to that media as if it were physically connected to the target server itself.

VM sessions are only encrypted when "Apply Encryption Mode to KVM and Virtual Media" is checked in KX security settings. They are secured using 128 or 256 bit AES encryption.

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

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

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

For the VM types supported by the Dominion User Station, see Supported Virtual Media Types (on page 148).

Prerequisites for Using Virtual Media

► *KVM switch requirements:*

- If you want to access virtual media, your "KVM switch" permissions must be set to allow access to the relevant KVM ports, as well as virtual media access (VM Access port permission) for those ports.

  KVM switch permissions are determined according to the user credentials you entered for the KVM switches. See Editing KVM and Serial Switches (on page 84).
- A USB connection through the virtual media CIM must exist between the KVM switch and the target server.

► *Target server requirements:*

- You must choose the correct USB profile for the target server. See Peripheral Devices and USB Settings (on page 144).
- KVM target servers must support USB connected drives.

Supported Virtual Media Types

- External hard drives
- USB-mounted CD/DVD drives
- USB mass storage devices
- ISO images (disk images)

  ISO9660 is the standard supported by Raritan. However, other ISO standards can be used.

Note: Connecting digital audio devices onto the target server is also supported. See Audio Device (on page 145).

Connecting Local USB Drives and Local Disk Images

This option mounts an entire USB drive virtually onto the target server when you select the Local USB Drive option. Use this option for external drives only. It does not include CD-ROM, or DVD-ROM drives.

You can connect to a local disk image with the .img or .dmg extension. Apple DMG files must not be encrypted or compressed. The disk images should be in the root folder of an attached USB drive or network storage.

► *To mount a local USB drive:*

1. Click to open the "Audio, Mass Storage and SmartCard Devices" dialog.
2. Click the "Mass Storage Device ..." button. The Connect Mass Storage Device/Image File dialog appears.

3. Choose the drive from the Local USB Drive drop-down list.
4. If you want Read and Write capabilities, select the Read-Write checkbox.
   - This option is not configurable in some scenarios. See Scenarios When Read/Write is Unavailable (on page 150).
   - When selected, you will be able to read or write to the connected USB drive.

   Note: Improper unmounting of the USB drive from the target server may result in data corruption. See Disconnecting a Virtual Device (on page 156). Therefore, if you do not require Write access, leave this option unselected.

5. Click OK.

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

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

Scenarios When Read/Write is Unavailable

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

- The drive is write-protected.
- The user credentials you entered for the KVM switch does not allow Read/Write permission on the KVM port you are accessing.

  For information on how to enter user credentials for KVM switches, see Editing KVM and Serial Switches (on page 84).

► *To connect to a Local Disk Image:*

1. Click [icon] to open the "Audio, Mass Storage and SmartCard Devices" dialog.
2. Click the "Mass Storage Device ..." button. The Connect Mass Storage Device/Image File dialog appears.

3. Click Select to choose local disk image. The Select button opens a dialog with a list of all local disk images found. Select the one you want to use and close the dialog with OK.

Mounting CD-ROM/DVD-ROM/ISO Images

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

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

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

1. Click [icon] to open the "Audio, Mass Storage and SmartCard Devices" dialog.
2. Click the "CD-ROM Device / ISO File ..." button. The Connect CD-ROM Drive / ISO Image dialog appears.
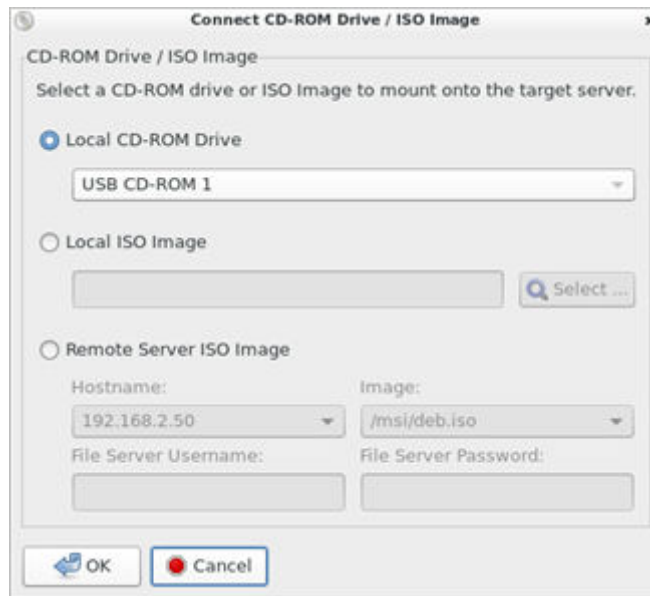
3. For USB CD-ROM/DVD-ROM drives:

   a. Select the Local CD-ROM Drive option.

   b. Choose the drive from the Local CD-ROM Drive drop-down list, which shows all available CD-ROM/DVD-ROM drive names.

4. For Local ISO Images: The ISO images must be on the root-folder of USB drive or Network Storage.

   a. Connect the USB drive or mount the network storage to the User Station.

   b. Select the Local ISO Image option. The Select button opens a dialog with a list of all ISO images found. Select the one you want to use and close the dialog with OK.

5. For remote ISO images on a file server:

Remote ISO images must be setup in KX3/KX4 to be available for selection by the KVM-Client. See Virtual Media File Server Setup in KX III's online help. (https://help.raritan.com/kx-iii/v3.6.0/en/#33617.htm)

   a. Select the Remote Server ISO Image option.

   b. Select Hostname and Image from the drop-down list.

   The hostnames (file servers) and image paths available in the list are those that you configured using the KX III KVM switch's File Server Setup page. See the KVM switch's user documentation for further information.

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

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

6. Click OK.

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

► *To disconnect the CD-ROM , DVD-ROM or ISO image from the target server:*

- See [Disconnecting a Virtual Device](#) (on page 156).

Number of Supported Virtual Media Drives

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

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

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

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

SmartCard Reader

If any target server requires a SmartCard for authentication, you can mount a SmartCard reader onto it.

If additional virtual devices are also required, *it is strongly recommended to connect them prior to the card reader*. Otherwise, a USB reconfiguration is triggered, which requires the user to log in again.

Note: SmartCard is supported in KX3 only.

Make sure you meet the following requirements for mounting a card reader to a target server.

► *CIMs required for mounting a SmartCard reader:*

- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

► *Supported card readers:*

- Refer to the topic titled "Supported and Unsupported SmartCard Readers" in the KX III KVM switch's user documentation, which is accessible from its application or the Dominion KX III section of the Raritan website's [Support page](#).

► *Target server requirements:*

- Refer to the topic titled "Target Server Requirements" in the KX III KVM switch's user documentation.

Mounting a Card Reader

You can physically connect multiple SmartCard readers to the User Station, but only one SmartCard reader can be virtually mounted onto a target server at a time.

► *To mount a SmartCard reader:*

1. Make sure a *supported* SmartCard reader has been physically connected to the User Station.

2. Click ⬤ to open the "Audio, Mass Storage and SmartCard Devices" dialog.

3. Click the "SmartCard Reader ..." button. The Connect SmartCard Reader dialog appears.
   - If this button is disabled, it may be impacted by the KX III KVM switch's settings. See Card Reader Restriction Caused by KX III KVM Switch Settings.
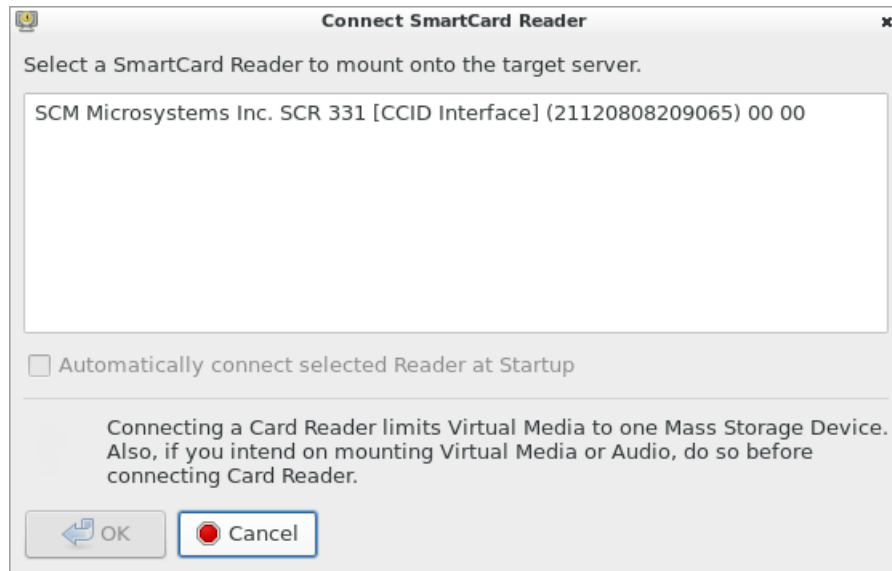
4. Select the desired card reader from the list shown in the dialog.

   - To automatically connect the selected card reader to the current target server whenever that target server is accessed, select the "Automatically connect selected Reader at Startup" checkbox.

5. Click OK to connect it.

6. When the card reader is listed as a virtual device in the "Audio, Mass Storage and SmartCard Devices" dialog, you can insert the card.

Raritan.
A brand of ∎legrand
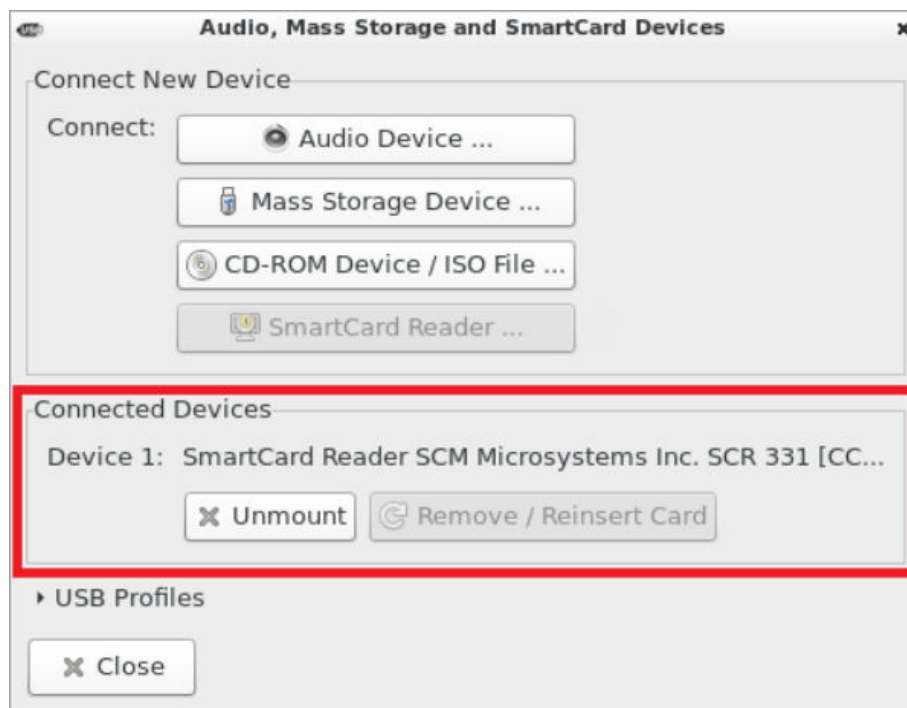
► *To disconnect the card reader from the target server:*

- Click the Unmount button in the "Audio, Mass Storage and SmartCard Devices" dialog. For details, see Disconnecting a Virtual Device (on page 156).

Emulating the Card Reinsertion

If the authentication on the target server fails while the card is being properly inserted into the card reader, you can attempt to solve the issue by removing and reinserting the card.

The User Station is able to emulate the card reinsertion without physically removing and reinserting the card.

► *To emulate the card removal and reinsertion:*

1. Click ⬚ to open the "Audio, Mass Storage and SmartCard Devices" dialog.

2. Click [Remove / Reinsert Card] .

Card Reinsertion Scenarios

The card is not detected in one of the following scenarios, you must reinsert the card or emulate the card reinsertion to solve the issue.

► *The scenario where you must physically remove and reinsert the card:*

a. The SmartCard reader with a card inserted is physically connected to the User Station and is configured to automatically connected to a specific target server at startup.

b. You establish and close the connections to that target server for several times.

c. When the card is no longer detected, PHYSICALLY remove and reinsert the card.

► *The scenario where you need to emulate the card reinsertion:*

a. Both the SmartCard reader and audio device are configured to automatically connected to a specific target server at startup.

b. You establish a connection to that target server, and the audio device and card reader with a card inserted are automatically connected to the target.

c. The card is not detected. You can emulate the card reinsertion to re-detect it. See <u>Emulating the Card Reinsertion</u> (on page 155).

Disconnecting a Virtual Device

When the KVM Client is closed, the virtual media connection to the target server is closed. Devices are also disconnected when switching the KVM Client to a different port or KX.

You can also use the Disconnect or Unmount button without closing the current KVM Client.

► *To disconnect the virtual peripheral device(s):*

1. It is highly recommended to first "safely remove" or "eject" the virtual media drive that you want to disconnect from the target server. If you have enabled the read/write mode, it may result in data loss when you do not perform this operation.

   • Refer to the user documentation of the target server's operating system for how to "safely remove" or "eject" a drive.

2. Click to open the "Audio, Mass Storage and SmartCard Devices" dialog.

Existing virtual devices are listed in the Connected Devices section.

Raritan.
A brand of ⬛legrand
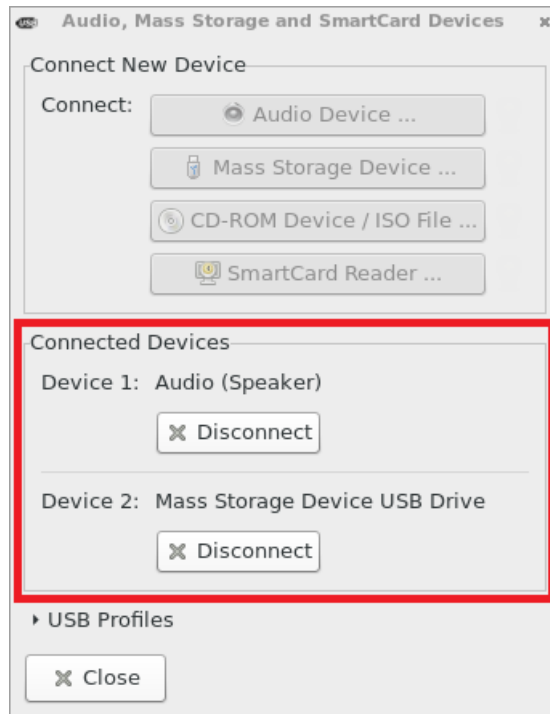
The devices that you can no longer mount onto the target server are disabled. Hover your mouse for a tooltip showing reasons.

3. Click the Disconnect button for the device you want to disconnect.
   - Click the Unmount button if you are disconnecting the SmartCard reader.
4. Click Yes on the confirmation message.

USB Profiles

Usually the "Generic" USB profile works fine for most target servers. In case any of your target servers requires a special USB profile to have the remote audio devices, virtual media and card reader work properly, select a different USB profile for it.

Note: USB Profiles are only available in KXIII.

► *To apply an appropriate USB profile to the target server:*

1. Click [icon] to open the "Audio, Mass Storage and SmartCard Devices" dialog.
2. Click USB Profiles to expand it.
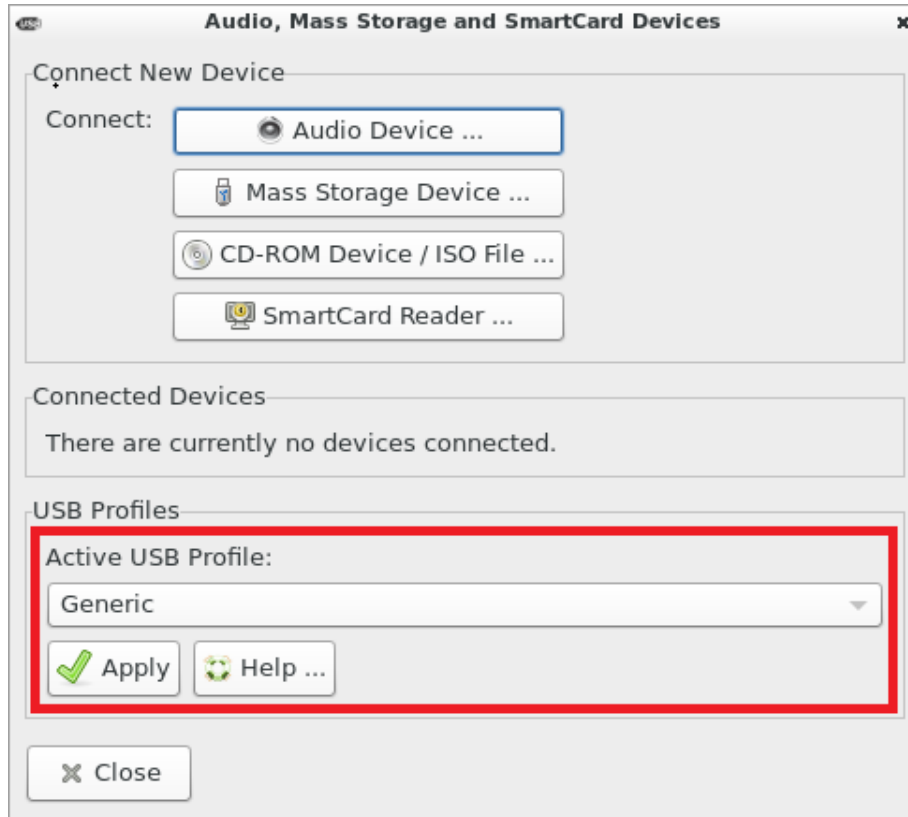
3. Select the desired USB profile from the Active USB Profile drop-down list, and click Apply.

- If intended, click the Help button to view information similar to USB Profile Overview (on page 158).
- For detailed information of each USB profile, see the section titled "Available USB Profiles" in the KX III KVM switch's user documentation, which is accessible from the KVM switch application or the Raritan website's Support page.

USB Profile Overview

Audio and mass storage devices are connected to the target server via USB ports of the CIM. Most of the time, this works without any problems. However, if you encounter any compatibility issues, you may have to change the USB configuration of the CIM.

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

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

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

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

Administrators configure the KVM port with the USB profiles that best meet the needs of the user, and the target server configuration.

A user connecting to a target server chooses among these preselected profiles in the KVM Client, depending on the operational state of the target server.

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

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

If none of the standard USB profiles provided by Raritan work with a provided target server, contact Raritan Technical Support for assistance.

For detailed information of available USB profiles, refer to the user documentation of the Dominion KX III KVM switch.

Power Control

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

This power control button is enabled only when the power control requirements are met.

► *Power control requirements:*

- On the KX III KVM switch, a PDU's outlet(s) must be associated with the selected KVM port.
- The user credentials you entered for the KVM switch grant you the power control permission.

See the KVM switch's user documentation for more information.

► *To power on, off or power cycle the target server:*

1. Click to select a power control option.
   - Power On: Turns ON the server.
   - Power Off: Turns OFF the server.
   - Power Cycle: Turns OFF and then turns ON the server.

2. Click Yes on the confirmation message.
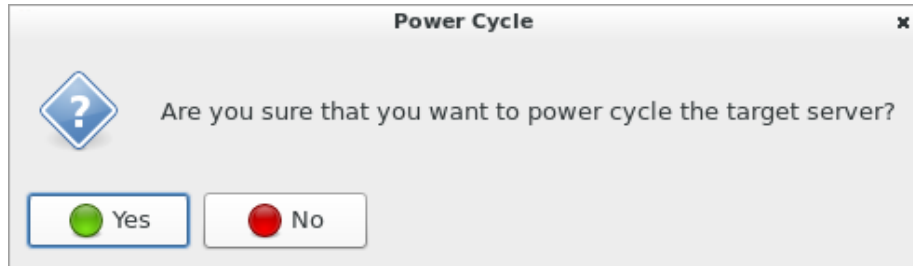
External Device Control

KX4-101 targets may have connected external devices that can be controlled.

1. Click the External Device icon in the toolbar to open the settings:
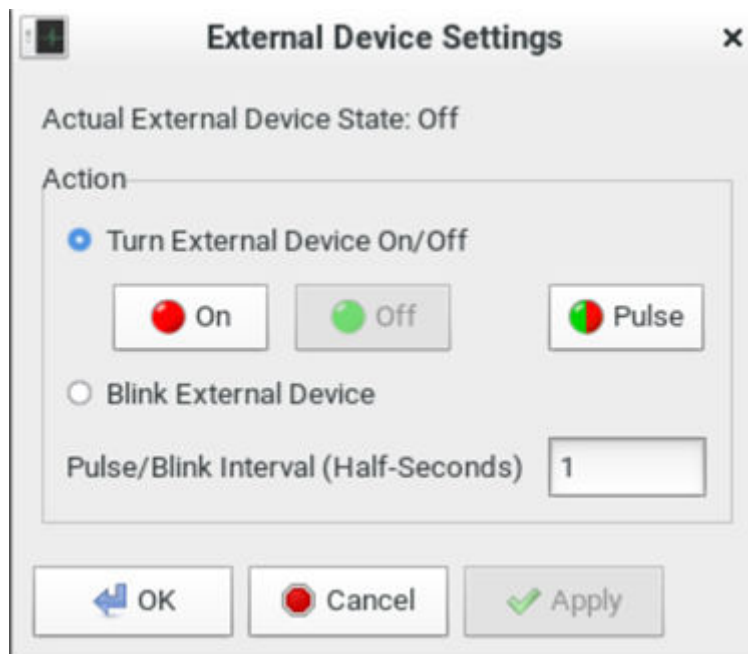
2. The device state is listed.
3. Enabled devices can be controlled using the Actions options.
    - Turn External Device On/Off: Click On or Off to control terminal output relay.
    - Pulse External Device: Sends a pulse to the device, either off to on, or on to off. Initial state of pulse can be changed by clicking button "On" and "Off".
    - Blink External Device: Enter the half-second interval to control blinking of the external device.
4. Click OK.

View Settings

Click to show available view options.
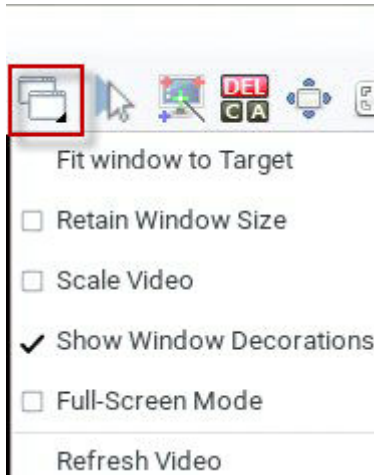
Fit window to Target

The "Fit window to Target" command enlarges or shrinks the size of the KVM Client window to the target server's video resolution.

The KVM Client's scroll bars may or may not appear, depending on whether the target server's resolution is small enough for the KVM Client window to show the target server's entire desktop video.

► *To fit the KVM Client window to the target server:*

- Click ⬛ > Fit window to Target.

- OR click ⬛ .

Retain Window Size

The Retain Window Size setting prevents changes made to the resolution of the target from affecting the KVM client's window size. The KVM client will display scroll bars or black borders when window size is retained.

Scale Video

Selecting the Scale Video checkbox increases or reduces the size of the target server's video to fit the KVM Client window size.

This feature maintains the aspect ratio so that you see the entire target server's desktop without using the scroll bars.

Tip: You can have this display option automatically enabled or disabled by setting your preferences on the KVM Client Settings page. See Access Client Settings (on page 172).

► *To toggle video scaling:*

- Click [icon] > Scale Video.

Show Window Decorations

You can use the KVM Client with or without the window decorations, including the window title and scroll bars.

Tip: You can have this display option automatically enabled or disabled by setting your preferences on the KVM Client Settings page. See Access Client Settings (on page 172).

► *To toggle the display of the window decorations:*

- Click [icon] > Show Window Decorations.

Full-Screen Mode

When you enter full screen mode, the target server's video displays in the full screen and acquires the same resolution as the target server.

In full screen mode, the KVM Client's scroll bars are invisible, and its toolbar displays for several seconds only before disappearing from the screen.

► *To enter full screen mode:*

1. Click [icon] > Full-Screen Mode, or click [icon] .
2. A message indicating that the toolbar will be hidden and the key combination to trigger it temporarily displays on the screen and then disappears.

► *To display the toolbar in this mode:*

- Move your mouse to the top of the screen.

► *To exit full screen mode:*

- Press Ctrl+Alt+F on your keyboard.

- OR click [icon] in the toolbar.

- OR click [icon] > Full-Screen Mode.

Dual Video Port Connections

When connecting to a Dual Video port, two KVM client windows are opened. The two client windows are bound to each other.

Window title: [<group_name>] port_name.

When one window is closed, the other one is closed automatically

Switching to and from Dual Video ports is not possible. When switching from a single port to a Dual Video port, the old connection is closed prior to connecting. When switching from a Dual Video port to another port, the connections are closed prior to connecting to the new port.
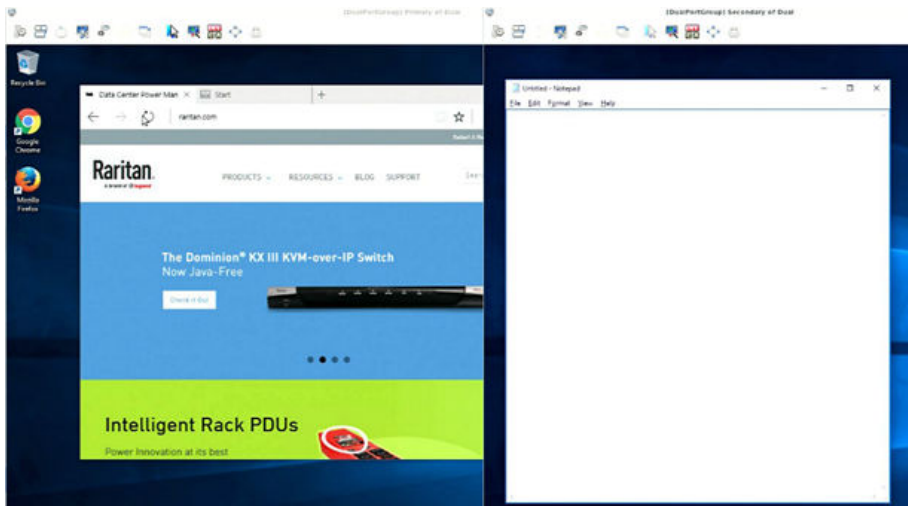
Using the Serial Client

A Serial Client window opens after connecting to a device with a serial target connected. The Raritan HTML Serial client provides tools for viewing and managing serial targets.

In This Chapter

Emulator

► *Access Emulator Options*

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

► *Settings*

- Select Settings from the Emulator drop down menu. The Terminal Properties dialog displays the default settings.

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

► *Get History*

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

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

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

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

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

► *Clear History*

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

► *Get Write Access*

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

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

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

► *Get Write Lock*

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

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

► *Write Unlock*

To get Write Unlock, choose Emulator > Write Unlock.

► *Send Break*

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

Only users with Write Access privileges can send a break.

To send an intentional "break" to a Sun Solaris server:

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

► *Reset Port*

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

► *Connected Users*

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

- Choose Emulator > Connected Users.
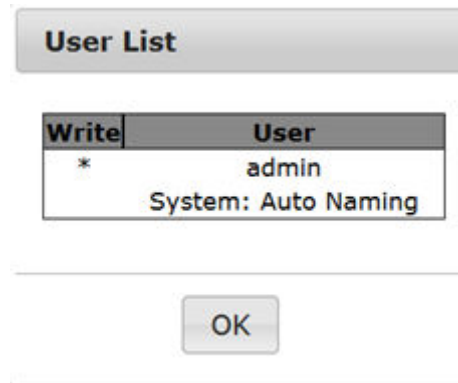
- A star appears in the Write column for the User who has Write Access to the console.

► *Exit*

1. Choose Emulator > Exit to close the RHSC.

Edit

Note: Edit menu is not enabled on serial client.

Tools

Note: Tools menu is not enabled on serial client.

Power

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

► *To view power status:*

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

Notification

Outlet 2 Power Status : On

OK

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

Notification

Port has no associated outlets, or user does not have power permission on this port.

OK

► *To perform power operations:*

- Choose an option from the Power menu to control the serial target's power.
  - Power On
  - Power Off
  - Power Cycle
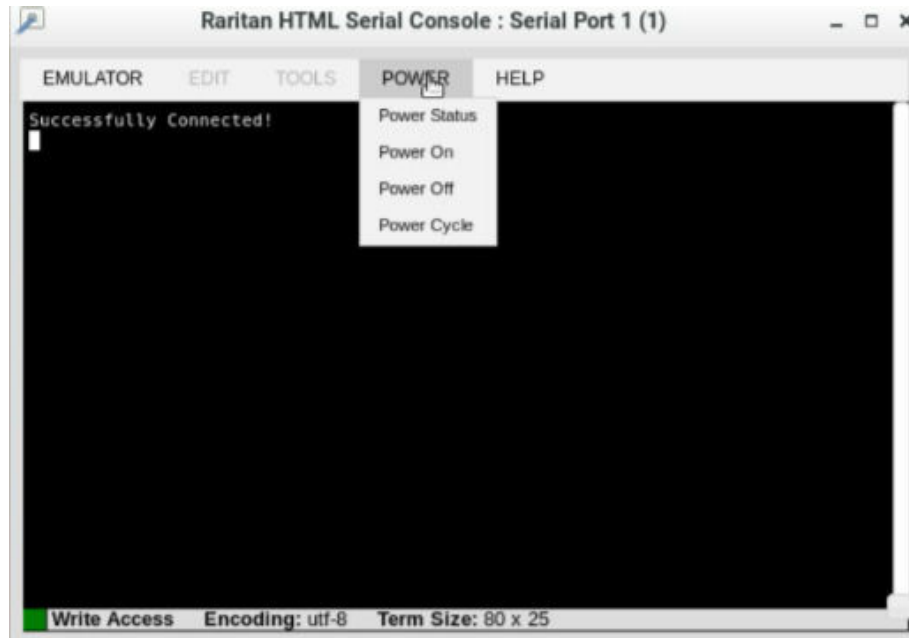
- Click OK in the success message.
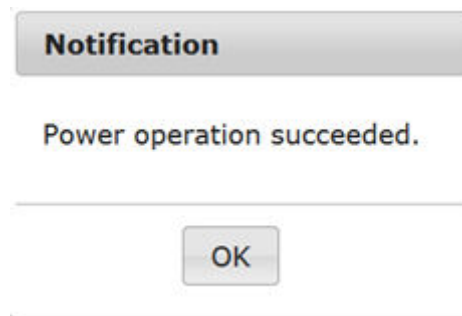
Setting User Preferences

In the User Station Configuration window, click Preferences to customize the following user settings.
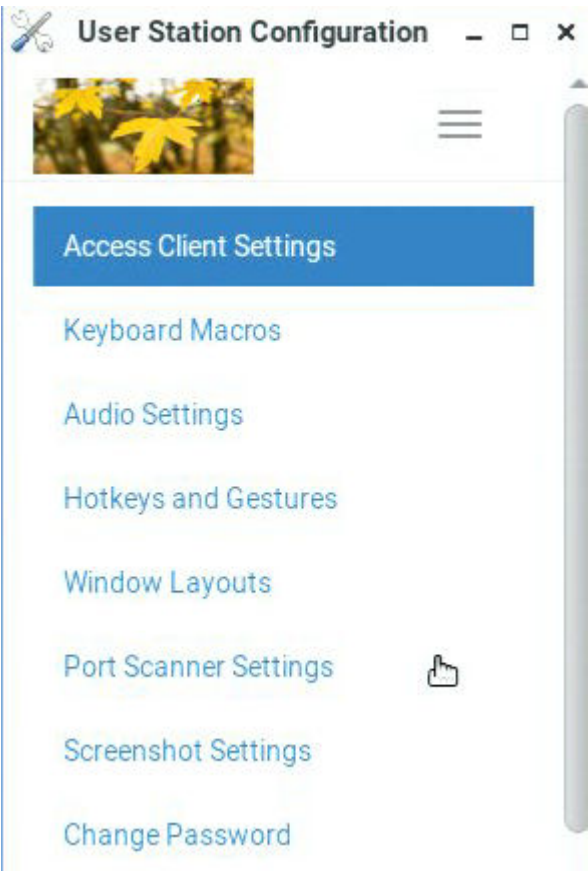
In This Chapter

Access Client Settings

You can configure settings for all access types, as well as general launch and connection settings. Users with the System Admin privilege can configure the default Access Client Settings for all new users.

- Video Target Window Settings
- Console Target Window Settings
- Web Target Window Settings
- Launch Settings
- Connection Settings

► *To set your Access Client preferences:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Preferences > Access Client Settings. The Access Client Settings page opens, showing the current preferences.

   - ☑ indicates the setting is enabled.

   - ☐ indicates the setting is disabled.

Video Target Window Settings		
Scale Video	☐	(KVM, M-KVM, VNC)
Positioning	Automatic	(KVM, VNC)
Window Decorations	☑	(KVM, M-KVM, VNC, RDP, ESXi)
Show Tool Bar	☑	(KVM, M-KVM, VNC)
Full-Screen Mode	☐	(KVM, M-KVM, VNC, RDP, ESXi)
Single Mouse Cursor Mode	☐	(KVM, M-KVM)
Synchronize Mouse	☐	(KVM, M-KVM)
Auto Sense Video Settings	☐	(KVM, M-KVM)
Allow Input if focused only	☐	(KVM, M-KVM, VNC)
Grab all Keyboard and Power Button ev…	☑	(RDP)
Limit to current Monitor	☐	(KVM, M-KVM, VNC)
Cursor Shape	Default	(KVM, M-KVM, VNC)
Disable Banner Messages	☐	(KVM, M-KVM, VNC)
Resizing Behavior	Fixed Size	(RDP)
Transmission Quality	Medium	(RDP)
Preferred Resolution	1024 x 768	(RDP)
Display as Multi-Monitor Target	Disabled	(RDP)
Desktop Scaling	100%	(RDP)

3. Click Edit to make changes.
   - Video Target Window Settings: These selections determine the initial settings applied to the video targets with the Access Client.

Scale Video	Enable or disable the Scale Video function.
	For details on Scale Video, see Scale Video (on page 161).

Raritan.
A brand of 🔲legrand

Positioning	Determines where the Access Client shows up on the screen: • Automatic: The positioning of the Client is not restricted. For example, the first Client that appears may align with the top-left corner of the screen, but the second Client may align with the bottom-right corner of the screen. • Left Upper Corner • Right Upper Corner Note: For dual or multi-KVM targets, if more than two windows are involved, all windows will be launched in the Left Upper Corner.
Window Decorations	Show or hide the window decorations. For details on window decorations, see Show Window Decorations (on page 162).
Show Tool Bar	Show or hide the client tool bar.
Full-Screen Mode	Enable or disable full-screen mode for KVM, M-KVM, VNC, RDP and ESXi sessions.
Single Mouse Cursor Mode	Enable or disable starting in single mouse mode. Note: When this setting is enabled, you must click into the KVM window to locate the mouse when you begin the session. For details on this mouse mode, see Single Mouse Cursor (on page 135). For details on how this works with dual monitor targets, see Single Mouse Mode for Dual Monitor Targets (on page 177).
Synchronize mouse	Enable or disable synchronize mouse after connecting. If enabled the mouse is automatically synced on connecting to KVM and M-KVM targets if the mouse mode is set to Intelligent or Standard Note: When entering Single Mouse Mode via the menu button, there is an option to "Synchronize Mouse after leaving Single Cursor mode", applicable to KVM and M-KVM targets using Intelligent or Standard mouse mode.
Auto Sense Video Settings	Enable or disable auto sense video settings. If enabled, the KVM target performs an auto sense automatically once the KVM client connects.

Allow Input if focused only	Enable or disable allow input if focused only. If enabled, mouse input only allowed on KVM, M-KVM and VNC targets when the client window is in focus.
Grab all Keyboard and Power Button events	Select to grab all keyboard input (including the power button and other keyboard shortcuts) from the local OS.
Limit to current Monitor	Select to limit the KVM, M-KVM and VNC targets to the current monitor.
Cursor Shape (in Double Cursor Mode)	Select customized cursor shape. • Default, Dot, Crosshair, Transparent • Use the Transparent option to hide the mouse cursor.
Disable Banner Messages	Select to remove banner messages from KVM, M-KVM and VNC sessions.
Resizing Behavior	Select resize preference for RDP sessions: • Fixed size, Dynamic Resolution Change, Scale
Transmission Quality	Select preferred transmission quality for RDP sessions: • Best Quality (Slowest), Medium, Fastest (Lowest Quality)
Preferred Resolution	Select preferred resolution for RDP sessions.
Display as Multi-Monitor Target	Select multi-monitor preferences for RDP sessions: • Disabled, Use 2 monitors, Use 3 monitors, Use 4 monitors and Use all monitors
Desktop Scaling	• Select a desktop scaling percentage for RDP sessions.

- Console Target Window Settings: These options apply to SSH and Serial access.

Console Target Window Settings

Window Decorations	Show or hide the window decorations. For details on window decorations, see Show Window Decorations (on page 162).
Show Menu Bar	Show or hide the menu bar.
Start in Full-Screen Mode	Enable or disable full-screen mode for console sessions. For SSH and Serial, the hot key for full screen is F11.
Console Size	Select the preferred console size. Serial Client size may not be accurate.

- Web Target Window Settings:

Web Target Window Settings

Window Decorations	Show or hide the window decorations. For details on window decorations, see Show Window Decorations (on page 162).
Show Tool Bar	Show or hide the tool bar.

Start in Full-Screen Mode	Enable or disable full-screen mode for web sessions.
	For web sessions, the full screen hot key is F11.
	To exit full-screen mode, press Ctrl + Alt + F in the KVM Client.

- Launch Settings: These options configure the mouse button click behavior at the Port Navigator, the default action for the Port Hotkeys, and the launching of multiple KVM sessions to one target (when PC share is enabled). Options apply to KVM and VNC Access Clients only.
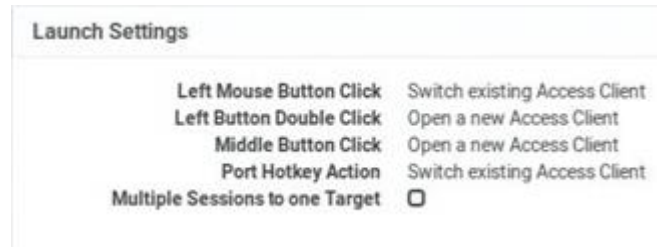
Switch existing Access Client	Switches the last active Access Client to the selected port or access point, if possible. Otherwise a new Access Client is opened.
Open a new Access Client	Always launches a new Access Client.
Open a new Access Client on secondary monitor	Always launches a new Access Client on the secondary monitor, if available.
Multiple Sessions to One Target: Enabled	Opens a second window to the target if: (1) Open a New Access Client is selected and (2) PC Share is enabled for device.
Disabled	Disables the left button double click or middle button click

- Connection Settings: Selecting the "Warn if a Virtual Media Connection is about to be disconnected" checkbox will cause a warning message to display if this event occurs.

Raritan.
A brand of ▢legrand

Connection Settings

If a KVM Client is switched to another port while a Virtual Media Connection is established, then the Virtual Media Connection is terminated. With this option you can choose whether you want to see a warning in this case.

☐ Warn if a Virtual Media Connection is about to be disconnected

1. Click Save. Note additional options when settings have been configured:
   - To save these settings as the default for all new users and existing users who have not changed their settings, click Set as Default. System Administration privilege required.
   - To delete all target/port-specific access client settings for the current user, click Reset all Target Specific.

[Edit] [Set as Default] [Reset all Target Specific]

Single Mouse Mode for Dual Monitor Targets

When Start in Single Mouse Cursor Mode is enabled for a dual monitor target:

- The top-left display KVM client is brought to front (instead of the primary) because this one controls the mouse.

Managing Keyboard Macros

Keyboard macros can be created to use instead of physical keystroke combinations, so that the actions intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by the User Station itself.

Keyboard macros are stored on the User Station, and only the user who created them can see and use these macros.

► *To create a keyboard/hotkey macro:*

1. If not displayed, launch the User Station Configuration window. See <u>User Station Configuration</u> (on page 80).
2. Click Preferences > Keyboard Macros > New Keyboard Macro. The New Keyboard Macro page opens.

Raritan.
A brand of ⬛legrand

New Keyboard Macro

☑ Enabled

* **Name**

[   ]

* **Sequence**

Key Sets: [All Keys   ⌄]

Keys:
```
Left Ctrl
Right Ctrl
Left Alt
Right Alt
Left Shift
Right Shift
Scroll Lock
Caps Lock
Num Lock
Left Windows Kev
```
▶ ▲ ▼ ◀

[Save] [Cancel]

3. Enter information for the new keyboard macro. The fields marked with the symbol * are mandatory.

Field/ option	Description
Enabled	Select this checkbox so that the new macro can appear in the KVM Client of this User Station. See Executing Macros (on page 179).
Name	Type a name for the new macro.
Key Sets	Select the key set containing the desired keys. See Available Key Sets. All keys that the selected key set contains are listed in the Keys box.
Keys	Select each desired key from the list and click ▶ to add it to the right box. Double-click also adds. • Select the keys in the order by which they are to be pressed. • A `Release` key command is automatically added for each key added to the right box. See Keyboard Macro Example (on page 180).

Raritan.
A brand of 🔲legrand

4. If needed, make changes to the keys shown in the right box.

   - To resort the key commands, select a key command and click ▲ or ▼ to move it up or down.

   - To remove a key command, select it and click ◀ .

5. Click Save, and the new macro's content is shown.

6. Click one of these buttons according to your needs.

   - Back: Return to the Keyboard Macro page.

   - Edit: Modify this macro.

   - Delete: Remove this macro.

Executing Macros

Manually-created keyboard macros, if they are enabled, appear following the pre-programmed keyboard macros in the keyboard pull-down list of the KVM Client. See Using the KVM Client (on page 126).

Click [icon] to show the keyboard macro list, and select the desired macro to send it to the target server.
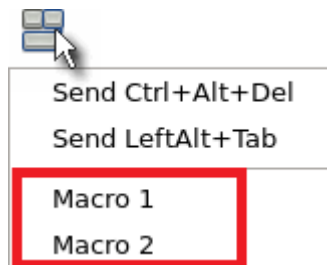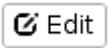
Editing or Deleting Macros

To view all manually-created keyboard macros in the User Station Configuration window, click Preferences > Keyboard Macros.

- Click the Name column header to sort the list.

- An enabled macro shows ☑ in the Enabled column.

- A disabled macro shows ☐ .

► *To edit a keyboard macro:*

1. Click the desired macro's [Edit] button.
2. Make necessary changes to the information shown. See [Managing Keyboard Macros](#) (on page 177).

► *To delete a keyboard macro:*

1. Click the desired macro's [Delete] button.
2. Click OK on the confirmation message.

Keyboard Macro Example

For example, you can create a keyboard macro to close a window by selecting `Left Alt+F4`.

The macro's content looks like the following.

```
Press Left Alt

Press F4

Release F4

Release Left Alt
```

Audio Settings
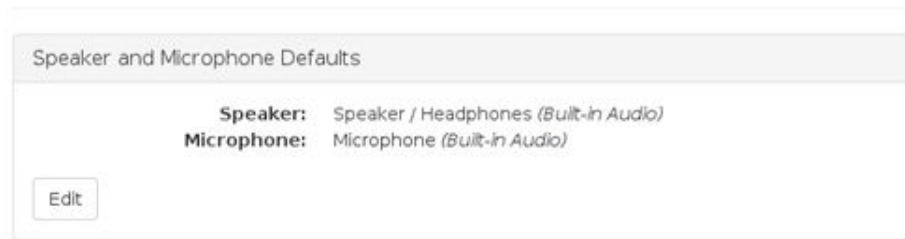
The default audio playback/capture devices used by the User Station are the front-panel analog speakers and microphone.

You can change this by setting other audio devices you prefer as the audio playback and/or capture devices. Note that the audio configuration changes made by any user apply on a User Station basis so the changes impact all users of this User Station.

► *To determine the audio appliances used by the User Station:*

1. If not displayed, launch the User Station Configuration window. See [User Station Configuration](#) (on page 80).
2. Click Preferences > Audio Settings. The Audio Settings page opens, indicating the current audio playback and capture devices being used.

Raritan.
A brand of legrand

Audio Settings
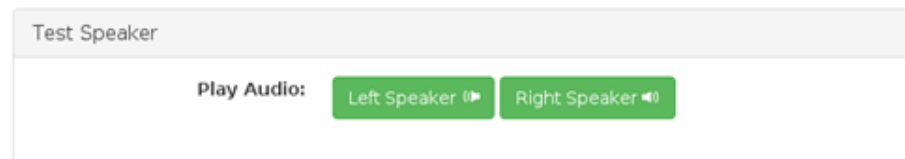
Speaker and Microphone Defaults

Speaker: Speaker / Headphones *(Built-in Audio)*
Microphone: Microphone *(Built-in Audio)*

Edit

3. Click Edit, if intending to make changes.
4. In the Speaker section, select the audio playback device you prefer.

   - The audio playback devices which are not available are marked with 🔇 .

5. In the Microphone section, select the audio capture device you prefer.
6. Click Save.
7. (Optional) To test whether the currently selected speaker works, click the Test Speaker buttons.

Test Speaker

Play Audio: Left Speaker ◖▶   Right Speaker ◀◗

Hotkeys and Gestures

You can enable, disable and customize hotkeys and gestures to control the User Station, manage windows, or control KVM Client functions. These hotkeys and gestures are executed on the User Station rather than being transmitted to any target servers you are operating. You can apply current user's settings to all new users or to the users who have not set their hot key preferences by clicking on "Set as Defaults".

Note: Many functions are programmed and enabled by default.

For a complete list of pre-programmed hotkeys of the User Station, go to Main Menu > Help > Help on Hotkeys, and see Help on Hotkeys (on page 18).

There are several categories of hotkeys and gestures:

- User Station Functions Hotkeys: Configure hotkeys that are always processed locally by the User Station desktop. They are not sent to a target server if you use them from within a KVM session. If you want to use any of these key combinations, such as Alt+Tab or Ctrl+Alt+Delete, in KVM sessions, you should make sure that key combination is not assigned in this category, or disable that function it is assigned to.

User Station Functions Hotkeys

Port Navigator	Ctrl+Alt+N
User Station Configuration	Ctrl+Alt+C
Port Scanner	Disabled
Tile Client Windows	Disabled
Revert Tiling	Disabled
Minimize Client Windows	Disabled
Show Client Windows	Disabled
Close Client Windows	Disabled
Screenshot of Desktop	Disabled
Screenshot of Active Window	Disabled
Lock Screen	Ctrl+Alt+L
Shutdown Dominion User Station	Ctrl+Alt+Delete
Save a new Window Layout	Disabled
Save the current Window Layout	Disabled
Restore Monitor Configuration	Disabled

- Window Management Hotkeys and Gestures: Configure hotkeys to close windows, switch between windows, or move them around on your desktop.

  - When Switch Keys is enabled, you can use Shift + Windows + Arrow to switch between open windows.

  - Move Keys are key combinations that move the foreground window around on the desktop. You can disable this function. See Move Keys (on page 185).

  - When Dragging with Alt Key is enabled, you can drag windows around on the Dominion User Station desktop using the mouse. Disable this feature if you want Alt Drag to apply to the target server.

  - Focus follows Mouse when enabled allows seamless mouse response on the hovered window session.

Window Management Hotkeys and Gestures

Close Window	Alt+F4
Next Window	Alt+Tab
Previous Window	Shift+Alt+Tab
Switch Keys	☑
Move Keys	☑
Dragging with Alt key	☑
Focus follows Mouse	☑

- KVM Client Hotkeys: Configure hotkeys for functions within the KVM Client. Note that if you disable the hotkey for single mouse mode, this function is disabled.

KVM Client Hotkeys

Single Mouse Cursor Mode	Ctrl+Alt+M
Full Screen Mode	Ctrl+Alt+F
Synchronize Mouse	Disabled
Auto Sense Video Settings	Disabled

- KVM and Serial Port Hotkeys: Hotkeys that have been configured for KVM and Serial ports launches appear here.
- Target Access Hotkeys: Hotkeys that have been configured for SSH, VNC, Web, ESXi, RDP and M-KVM target launches appear here.
- Window Layout Hotkeys: Configure hotkeys to manage your window layouts. See <u>Window Layouts</u> (on page 187).

KVM and Serial Port Hotkeys

Port Name	KX/SX Device	Hotkey	Actions
Serial Port 10	sansx259190	Ctrl+Alt+X	⚙
KX4-101 (192.168.59.89)	sansx259190	Ctrl+Alt+E	⚙
OldLenovo	KX3-57-21	Ctrl+Alt+J	⚙

Target Access Hotkeys

Access	Target	Hotkey	Actions
ESXi	1-vcenter6-5.raritan.com	Ctrl+Alt+7	⚙

Window Layout Hotkeys

Window Layout	Hotkey	Actions
Window Layout 1	Ctrl+Alt+A	⟲ Edit

► *To configure hotkeys and gestures:*

1. Launch the User Station Configuration window.
2. Click Preferences > Hotkeys and Gestures. The Hotkeys and Gestures page opens, showing the current settings for all categories.
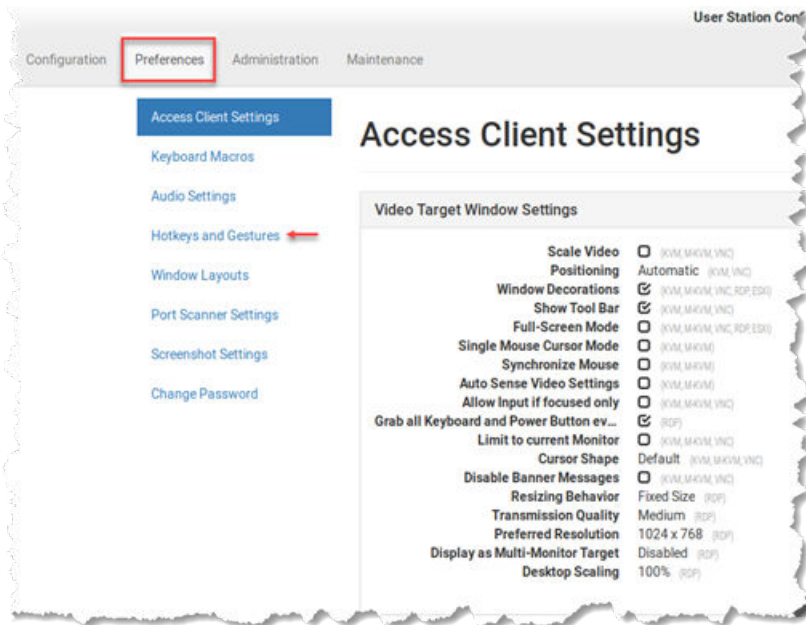
3. Scroll down and click Edit to make changes:
   - To enable, select a key combination for the function from its drop-down list.
   - To disable, select Disabled from its drop-down list.
4. Click Save.
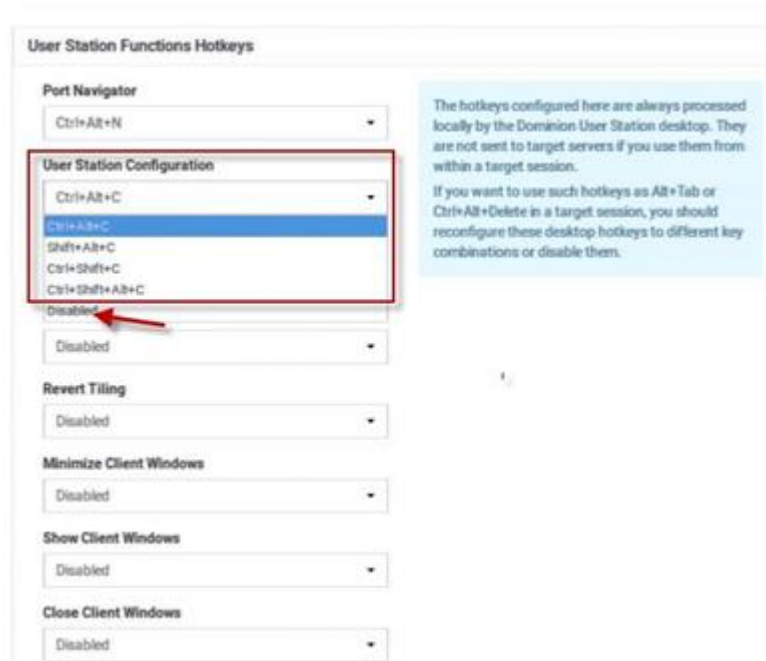
5. Click "Set as Default" to apply these new settings to all new users or to the users who have not setup their preferences.

Raritan.
A brand of 🔳legrand

Note: These settings will remain until the user customizes.

Hotkeys and Gestures

User Station Functions Hotkeys

Port Navigator	Ctrl+Alt+N
User Station Configuration	Ctrl+Alt+C
Port Scanner	Disabled
Tile Client Windows	Disabled
Revert Tiling	Disabled
Minimize Client Windows	Disabled
Show Client Windows	Disabled
Close Client Windows	Disabled
Screenshot of Desktop	Disabled
Screenshot of Active Window	Disabled
Lock Screen	Ctrl+Alt+L
Shutdown Dominion User Station	Ctrl+Alt+Delete
Save a new Window Layout	Disabled
Save the current Window Layout	Disabled
Restore Monitor Configuration	Disabled

Window Management Hotkeys and Gestures

Close Window	Alt+F4
Next Window	Alt+Tab
Previous Window	Shift+Alt+Tab
Switch Keys	☑

Edit   Set as Default

Move Keys

Move Keys are key combinations that move the foreground window around on the desktop. You can enable or disable these hotkeys using the "Move Keys" setting. See Hotkeys and Gestures (on page 181).

Hotkey	Function
Ctrl + Alt + Shift + ←	When there are two monitors connected, move the window to the other monitor.
Ctrl + Alt + Shift + →	

Hotkey	Function
Ctrl + Alt + ⬆	Move the window to the screen edge in the specified direction on the monitor.
Ctrl + Alt + ⬇	
Ctrl + Alt + ⬅	
Ctrl + Alt + ➡	
Ctrl + Alt + 1 (on the keypad)	Move the window to the screen corner in the specified direction on the monitor.
Ctrl + Alt + 3 (on the keypad)	
Ctrl + Alt + 7 (on the keypad)	
Ctrl + Alt + 9 (on the keypad)	
Ctrl + Shift + ⬆	Move the window, in the specified direction, to the nearest edge, which is one of the following: • Borders of another window • Monitor edges in the dual-monitor configuration • Desktop boundaries
Ctrl + Shift + ⬇	
Ctrl + Shift + ⬅	
Ctrl + Shift + ➡	
Ctrl + Windows + ⬆	Enlarge the window in the specified direction until its border touches the nearest edge, which is one of the following: • Borders of another window • Monitor edges in the dual-monitor configuration • Desktop boundaries *Note: If the window border already aligns with the screen edge, the window size shrinks instead.*
Ctrl + Windows + ⬇	
Ctrl + Windows + ⬅	
Ctrl + Windows + ➡	

Raritan.
A brand of legrand

Hotkey	Function
Alt + Windows + ↑	Shrink the window in the specified direction until its border touches the nearest edge, which is one of the following:
Alt + Windows + ↓	• Borders of another window • Monitor edges in the dual-monitor configuration
Alt + Windows + ←	• Desktop boundaries *Note: If no nearest edges are found in the specified direction, the window size is halved instead.*
Alt + Windows + →	

Switch Keys

Switch keys allow you to switch between open windows using Shift + Windows + Arrow keys.

To enable or disable switch keys, see Hotkeys and Gestures (on page 181).

Window Layouts

The window layouts feature allows you to save layouts of running access client windows so that the specific layout can be restored upon selection. The window layout data that is saved includes the visual attributes of each access client session, such as size, position, and displaying monitor, as well as the connection information for each.

Layouts are saved on a per user basis. The layouts saved by one user are not available to other users. There is a maximum of 16 named layouts per user.

You can access Window Layouts in the Port Navigator or the Main Menu. To create Window Layouts see: Window Layouts (Create) (on page 56)

► *To manage layouts:*

The tools for window layout management allow you to set a layout to be restored upon login, rename or delete layouts, and assign hotkeys to layouts.

- In User Station Configuration: Click Preferences > Window Layouts.
1. Login Window Layout: The layout that is restored on a user's login.
   - None: default, no layout is restored upon login.
   - As saved on last logout: Upon the next logout, the state of all clients is saved as a layout, and this layout is restored on the next login. This type of saved layout does not overwrite a named layout that is selected at the time of logout.

Note: The "logout" window layout is saved 30 seconds after login, then every 15 seconds.

- List of named layouts: Select a named layout from your list of saved layouts.
1. Saved Window Layouts: Lists all named layouts and provides options.
   - Each layout has options to Restore, Edit or Delete.
   - Click Restore to open the layout now. This option works the same as the Main Menu: Window Layouts selection.
   - Click Edit to change the name or hotkey. Names must be 4-32 characters. Hotkeys will be verified for availability.
   - Click Delete on a layout, or select multiple layouts and click Delete Selected to remove layouts. Click to confirm deletion.

Window Layouts

Login Window Layout

Window Layout to load on Login   None

Edit

Saved Window Layouts

☐	Name ◆	Hotkey ◆	Actions
☐	Window Layout 1	Ctrl+Alt+A	Restore · Edit · Delete

Delete Selected

Port Scanner Settings

You can configure the scanner intervals, delays, and orientation, and specify storage of snapshots from the scanner. Note that you can also configure intervals and orientation from the Port Scanner window. See Scanner Options (on page 124). However, snapshot settings only appear in the User Preferences > Port Scanner Settings page.

When enabled, snapshots are stored on an accessible USB device or mounted network storage. The image saved is the thumbnail image from the scanner. Sub-directories are created on the location per KX device, named after the device, port by number and name. Images are named by timestamp. Duplicate KX devices with the same name will all use the same directory.

You must have the "Record Scanner Snapshots" permission to capture snapshots from the scanner. See User Groups (on page 198).

► *To configure port scanner settings:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Preferences > Port Scanner Settings. The Port Scanner Settings page opens, showing the current preferences.

   - ☑ indicates the setting is enabled.

   - ☐ indicates the setting is disabled.

Port Scanner Settings

Intervals and Delays

Port Display Interval
10 Seconds
Interval between Ports
1 Second

Snapshot Recording

Enable Snapshot Recording
☐
Snapshot Recording Storage

Settings

Thumbnails Orientation
Vertical
Use Grid View for Thumbnails
☑
Pause Scanner when opening KVM Sessions
☑
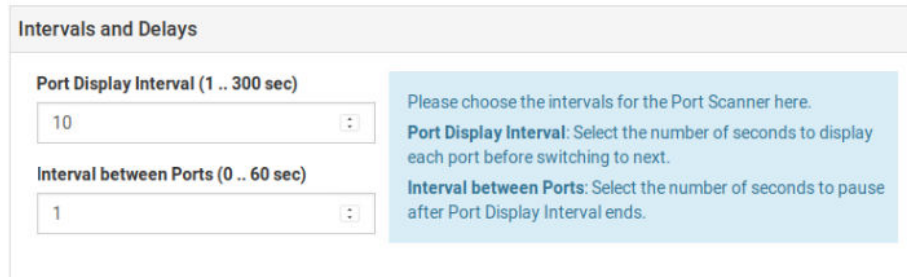
Edit

3. Click Edit to make changes.

4. To set Intervals and Delays:

- Port Display Interval (1..300 sec): Select the number of seconds to display each port before switching to next
- Interval between Ports (0..60 sec): Select the number of seconds to pause after Port Display Interval ends.

5. To set Snapshot Recording:

- Enable Snapshot Recording: Select the checkbox to turn the feature on.
- Make sure a USB drive or network storage is accessible.
- Make sure you have the Record Scanner Snapshots privilege.

6. To configure remaining preferences:

- Thumbnails Orientation: Select Vertical or Horizontal to position thumbnails in relation to scan window.
- Select the Use Grid View for Thumbnails checkbox for an optional grid view that shows all thumbnails at once without scroll bars.
- Select the Pause Scanner when opening KVM Sessions checkbox if the scanning should stop when you open a port into a full KVM session.

Settings

Please select some other settings here.

Thumbnails orientation: Select Vertical or Horizontal to position thumbnails in relation to scan window.

Select the **Pause Scanner when opening KVM Sessions** checkbox if the scanning should stop when you open a port into a full KVM session.

Thumbnails Orientation

Vertical ▾

☐ Use Grid View for Thumbnails

☑ Pause Scanner when opening KVM Sessions

7. Click Save.
8. To save these settings as the default for all new users and existing users who have not changed their settings, click Set as Default. System Administration privilege required.

Screenshot Settings

You have an option to set configured media to save screen shots, provided you have "System Administration" or "Take Screenshot" privilege. You can configure a Network storage or USB drive as your set configured media.

► *To configure Screenshot Settings:*

1. If not displayed, launch the User Station Configuration window. See .User Station Configuration (on page 80).
2. Click Preferences > Screenshot Settings. The Screenshot Settings page opens, showing the current preferences. By default no preferences are configured.

Raritan.
A brand of legrand
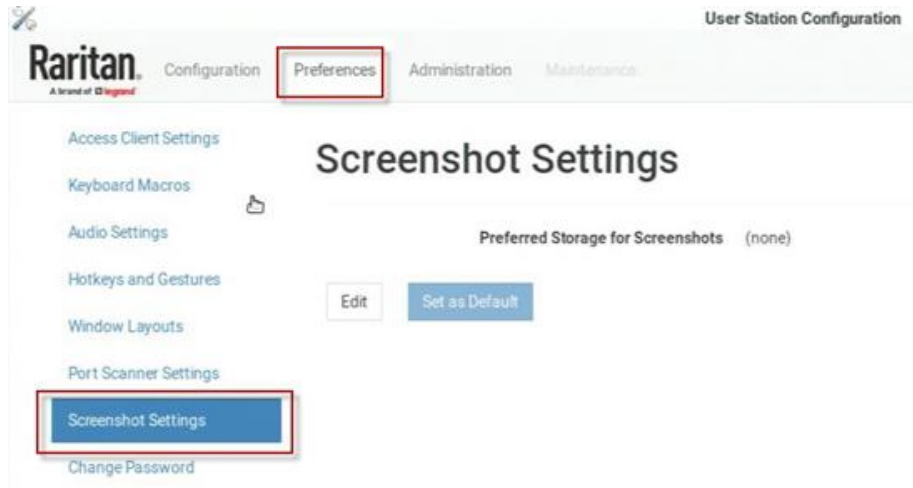
3. Connect USB drive or configure a network storage. See Network Storages (on page 253).
4. Click Edit. The Preferred Storage for Screenshots list becomes available.
5. Select the storage media and click Save.
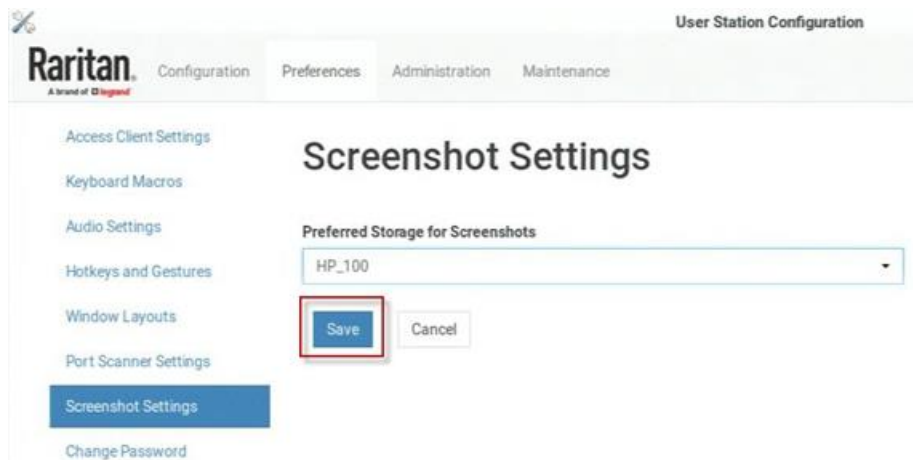
6. To save this Preferred Storage location as the default for all new users and existing users who have not changed their settings, click Set as Default. System Administration privilege required.
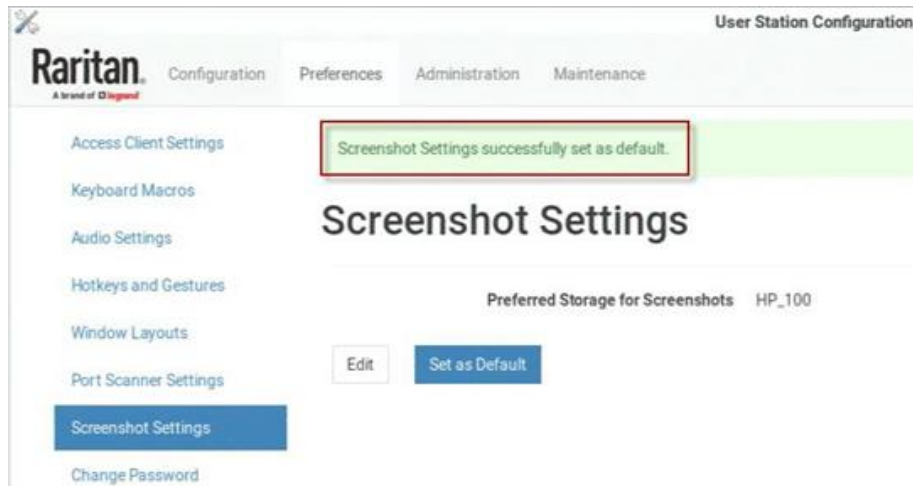
- Once screen shot is taken by the configured hot key, it is saved directly to the configured media, and you will see confirmation.

Change Password

You can change your own password.

► *To change your password:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Preferences > Change Password. The Change Password page opens, and you can enter new password.
3. Click Save.

Administration Features

In the User Station Configuration window, click Administration to perform the following User Station administration tasks.

In This Chapter

Users

The Dominion User Station provides a built-in administrator account, which is ideal for initial login and system administration.

You can add user profiles with configurable privileges for other users to operate and administer the User Station.

Note that the Dominion User Station's user profiles determine the permissions users are granted to have on the User Station instead of the KVM switches. See Authentication of User Stations and KVM/Serial Switches (on page 293).

► *To create a user profile:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).

2. In the User Station Configuration menu, click Administration > Users > New User. The New User page opens.

195

New User

* Login

[ ]

☐ Authenticate via LDAP

E-Mail

[ ]

Name

[ ]

* Password

[ ]

* Password confirmation

[ ]

* Selected User Groups   **Available User Groups**

[ ]   System Administrators
                      Devices Administrators
                      Restricted Users
                      testgroup1
                      newgroup
                      all
                      Devices Users
                      newgroup1
                      testgroup2
                      @singleuser

◄◄ ◄ ► ►►

[Save]   [Cancel]

3. Enter information for the new user. The fields marked with * are mandatory.

Field	Description
Login	User name for logging in to the User Station. • 2 to 255 characters • Restricted character: colon (:) :
Authenticate via LDAP	Select this checkbox if this user will be authenticated via LDAP. See LDAP (on page 202). If deselected, this user is authenticated via the local database of the User Station and you must store user passwords on the User Station.
Email	The email address to reach the user.
Name	Real name or nickname of the user.

Raritan.
A brand of ▢legrand

Field	Description
Password, Password confirmation	Password for logging in to the User Station. Minimum of 8 characters, at least 1 lowercase, 1 upper case and 1 numeric are required.
Selected User Groups	Assigning user groups determines the permissions granted to this user. See User Groups (on page 198). • Use the arrow buttons to move the user groups as needed. The user will be a member of the groups in the Selected User Groups list.

4. Click Save, and the new user profile's content is shown.

Editing or Deleting Users

To view existing user profiles in the User Station Configuration window, click Administration > Users.

Select an option in the Type field to show the desired user types. Note that this field is configurable only for users with the "System Administration" permission.
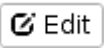
• Local: Shows local users only, who are authenticated via the User Station's local database.
• LDAP: Shows the users who are authenticated via LDAP.
• CC-SG: Shows the users who are authenticated using CC-SG.
• All: Shows all users, including Local, LDAP, and CC-SG. You must be the admin user to view all users.

Click each user's login name to view details.

Note that you cannot delete the built-in *admin* user, but you can modify its data other than the privileges (user groups).

► *To modify a user profile:*

1. Click the desired user's [Edit] button. The Edit User page opens.
2. Make necessary changes to the information shown. See Users (on page 195).
    - You cannot change the login name.
    - To change the user's password, type the new password in the "Password" and "Password confirmation" fields.
3. Click Save.

► *To delete a user profile:*

1. Click the desired user's [Delete] button, or select the check boxes for users you want to delete and click Delete Selected.
2. Click OK on the confirmation message.

User Groups

A user group determines the privileges its members can have.

There are several factory default user groups.

User groups	Default privileges
System Administrators	System Administration. See Privileges (on page 199).
Devices Administrators	Device Administration. Device Access.
Devices Users	Device Access. Change Preferences. Launch the Port Scanner
Restricted Users	Device Access

The Restricted Users group lacks the Change Preferences privilege, so this group can be used for access-only users.

You can create a new user group if the default user groups do not satisfy your needs.

► *To create a new user group:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Administration > User Groups > New User Group. The New User Group page opens.

Raritan.
A brand of **legrand**

New User Group

* Name

* Privileges

- ☐ Device Access
- ☐ ESXi Access
- ☐ WEB Access
- ☐ VNC Access
- ☐ RDP Access
- ☐ SSH Access
- ☐ Change Preferences
- ☐ Device Administration
- ☐ Launch the Port Scanner
- ☐ Record Scanner Snapshots
- ☐ Take Screenshots
- ☐ System Administration

[Save] [Cancel]

Device Access includes the permission to:
- Login
- Open KVM and serial sessions

VNC Access, RDP Access, SSH Access, WEB Access and **ESXi Access** include:
- Open VNC, RDP, SSH, Web and ESXi sessions

Change Preferences includes:
- Alter personal settings

Device Administration includes:
- Change Preferences permission
- Launch the Port Scanner permission
- Device Access permission
- VNC Access, RDP Access, SSH Access, WEB Access and ESXi Access permissions
- Addition and removal of KX/SX Devices
- Add, edit and remove VNC, RDP, SSH, Web and ESXi Access

Launch the Port Scanner includes:
- Launch the Port Scanner

Record Scanner Snapshots includes:
- Record snapshots from the Port Scanner
- Launch the Port Scanner

Take Screenshots includes:
- Take a screenshot and export it to a USB drive or Network Storage

System Administration permits everything

3. Enter information for the new user group.

Field	Description
Name	Type a name for the new user group.
Privileges	Assign one or multiple privileges to the new user group. See Privileges (on page 199).

4. Click Save, and the new user group's data is shown.

Privileges

Privilege	Operations permitted
Device Access	• Log in to the User Station. • Open KVM and serial sessions.
ESXi Access WEB Access	• Open ESXi or WEB sessions.
VNC Access RDP Access SSH Access	• Open VNC, RDP, and SSH sessions. • These permissions alone do not grant login privilege. User must also be a member of a group with System Administration, Device Administration or Device Access privileges.

Raritan.
A brand of legrand

Privilege	Operations permitted
Change Preferences	• Alter personal settings • Users who don't have this privilege cannot launch User Station Configuration, window layouts, or system settings
Device Administration	• Log in to the User Station. • Change Preferences permission. • Device Access permission. • Launch the Port Scanner. • ESXi Access, WEB Access, VNC Access, RDP Access and SSH Access permissions. • KX/SX device addition and removal. • Add, edit and remove ESXi, WEB, VNC, RDP and SSH access.
Launch the Port Scanner	• Launch the Port Scanner
Take Screenshots	• Take a screenshot and export it to a USB drive or network storage using the hotkey. • This permission alone does not grant login privileges. User must also be a member of a group with System Administration, Device Administration or Device Access privileges.
Record Scanner Snapshots	• Record snapshots from the Port Scanner. • Launch the Port Scanner.
System Administration	All operations on the User Station are permitted.

Editing or Deleting User Groups

To view all user groups in the User Station Configuration window, click Administration > User Groups.
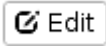
The Users column lists the names of all users who belong to this user group. If the real name is not available in the user profile, the user's login name is shown. See Users (on page 195).

Each user group shows a maximum of five users in this view.

Click each user group's name to view its details.

You can delete any user group even if it contains users.

► *To modify a user group:*

1. Click the desired user group's [**☑ Edit**] button.
2. Make necessary changes to the information shown. See User Groups (on page 198).
3. Click Save.

► *To delete a user group:*

1. Click the desired user group's [**🗑 Delete**] button.
2. A confirmation message appears.
   - If any user will not be able to log in after losing this user group, the confirmation message shows a warning similar to the following diagram. This is because the selected user group is the only user group that one or some of the group members have.

> Warning!   ✕
>
> This User Group has one member.
>
> One of them will not be able to login anymore once this User Group is deleted, because it's the only User Group the User belongs to.
>
> Are you sure you want to delete User Group "Managers"?
>
>   [Cancel] [**OK**]
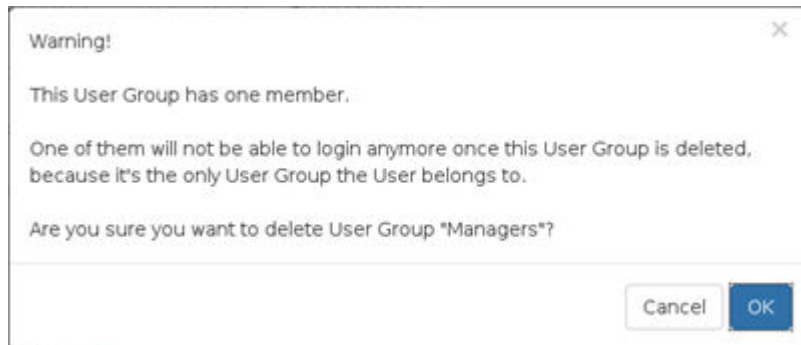
3. Click OK to confirm the deletion or Cancel to abort it.

Autologin

Enable the Autologin feature to allow a selected user to be automatically logged into the Dominion User Station when it boots up. To change users, log out, then re-login as the new user. Autologin is supported in both CC-SG integration mode and non-CC-SG integration mode.

Note: To configure Autologin for keyboard/mouse sharing setups, see Configuring Keyboard/Mouse Sharing (on page 251).

Raritan.
A brand of ☐legrand

► *To configure Autologin:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Administration > Autologin. The Autologin Settings page opens.
3. Click Edit to change the settings.
4. Select the Enabled checkbox to enable autologin, then select the user name in the list.
5. Click Save.

Edit Autologin Settings

☐ Enabled

User

admin ▾

This option enables an automatic login into the User Station for the selected user on boot up.

You have to specify the user's password here. It is stored in a secure way on the User Station.

Password

[Save] [Cancel]

LDAP

The external LDAP authentication has the following two modes:

- Authentication and authorization via LDAP
- Only authentication via LDAP

LDAP cannot be used when CC-SG Integration is enabled.

Note: For single sign-on capability in Dominion User Station, your KX devices, the Dominion User Station and your users must exist in the same LDAP environment, and the value of "login name attribute" should be the same as UID.

► *Authentication and authorization via LDAP:*

a. On the LDAP server(s), create both USERS AND USER GROUPS for the User Station.
b. On the User Station, create user groups whose group names are the same as those on the LDAP server(s). See User Groups (on page 198).
   - You can also import desired user groups from the LDAP server into the User Station after performing an LDAP search for user group objects. See Searching for LDAP Users and Groups (on page 211).
   - User names for this LDAP authentication mode are NOT needed on the User Station.

LDAP alias, which allows one user to have multiple logins, such as multiple common names, does NOT work in the LDAP authentication and authorization mode.

Raritan.
A brand of ∎legrand

► *Only authentication via LDAP:*

   a. On the LDAP server(s), create users for the User Station.
      - User groups are NOT needed on the LDAP server(s).
   b. On the User Station, create both USERS AND USER GROUPS. The user names must be the same as those on the LDAP server(s), but the user passwords are not stored on the User Station. See Users (on page 195) and User Groups (on page 198).
      - You can also import desired user names from the LDAP server into the User Station after performing an LDAP search for user objects. See Searching for LDAP Users and Groups (on page 211).

LDAP alias works fine in the LDAP authentication only mode.

► *User Station configuration required for either LDAP authentication mode:*

   - Add the LDAP server(s). See Adding LDAP Servers (on page 203).
   - Enable the LDAP authentication. See Enabling or Disabling the LDAP Authentication (on page 210) or Configuring the Maximum Search Results and Local Authentication Settings (on page 213).

TIP: When "admin" is entered as the user name and LDAP is enabled, an additional checkbox "Authenticate Locally" appears on the login page. You can select Authenticate Locally to authenticate using User Station's local database instead of the LDAP server(s) regardless of the LDAP authentication mode.

Adding LDAP Servers

To apply external LDAP authentication, at least one LDAP server must be added to the User Station. If you are not familiar with the LDAP settings, consult your LDAP administrator for help.

If there are multiple LDAP servers added, the order of the LDAP servers determines the authentication priority. The User Station first connects to the first LDAP server for user authentication, then the second if the first LDAP server fails, and so on until it successfully authenticates the user. If all LDAP servers fail the authentication, the user's access is denied.

► *To add LDAP servers:*

   1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).

   2. Click Administration > LDAP > [Add New Server] . The New LDAP Server page opens, with 5 groups of settings displayed.
   3. The General section determines general LDAP settings.

Setting	Description
Type	The type of the new LDAP server: • Active Directory Server: Microsoft Active Directory • LDAP server: OpenLDAP
Order	The order of this LDAP server, which determines the authentication priority when there are multiple LDAP servers. If adding more than one LDAP server, you can change the priority by selecting the sequential number of any existing LDAP server. That existing LDAP server and all servers that follow it will move down one position in the order.
Active	Leave this checkbox enabled unless you want to disable this LDAP server temporarily.

4. Enter the LDAP server's data in the Connection section.

Raritan.
A brand of Legrand

Setting	Description
Domain	Configurable when "Type" is set to "Active Directory Server." The Active Directory server's domain name. Usually the User Station can determine the Active Directory server's host name via its domain name and DNS. If you select the following Use Host checkbox, this behavior is replaced.
Use Host	Configurable when "Type" is set to "Active Directory Server." Enable this checkbox when intending to manually specify the host name or IP address of the Active Directory server.
Hostname/ IP-Address	The LDAP server's host name or IP address.
Use TLS/SSL	Select this checkbox if the security connection is required for the LDAP server.
Port	TCP port for the LDAP authentication, whose default is either of the following: • 389 (standard) • 636 (TLS/SSL)
Check Server Certificates	Configurable when the Use TLS/SSL checkbox is selected. Select this checkbox if it is required to validate the LDAP server's certificate by the list of accepted certificates on the User Station prior to the connection. If the certificate validation fails, the connection is refused.
Manage certificates	Click this link for installing a CA certificate as needed. See Trusted Certificates (on page 222).

Note: Currently, encrypted LDAP connections are not using the FIPS-accredited cryptographic code.

1. Enter the bind credentials in the Bind section.

Setting	Description
Base DN	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. Note that only relative distinguished names (RDNs) can be specified in this field. • Example: `cn`
Search Filter	Search criteria for finding LDAP user objects within the directory tree.
Search Scope	The depth to search for LDAP user objects, which starts at the directory level denoted by the "Base DN." • One: Searches one level below the base DN, with the base excluded. • Subtree: Searches all levels below the base DN, including the base.

Raritan.
A brand of 🟥legrand

Setting	Description
Search Credentials	If the authentication of a user requires the LDAP search, specify the search credentials for it: • no search: No LDAP search is performed. • anonymous: Enables the LDAP search without dedicated search credentials. • use admin credentials: Enables the LDAP search by entering the dedicated search credentials - a DN and password.
Admin DN, Admin Password	Configurable when "Search Credentials" is set to "use admin credentials." Distinguished Name and password of the administrator user who is permitted to perform the LDAP search.
Bind After Search	Configurable when "Search Credentials" is NOT set to "no search." Select this checkbox if the LDAP bind operation shall be performed with a DN derived from a search operation for the user who's trying to log in. Usually this checkbox is: • Deselected for the "Active Directory Server." • Selected for the "LDAP server."

2. To use LDAP groups for the authorization, configure the Groups section.

Setting	Description
Use Groups For Authorization	Select this checkbox if authorization via LDAP is intended. See LDAP (on page 202).
	When disabled, authorization is managed by the User Station, and this LDAP server only manages authentication.
Use Group Search DN	Select this checkbox when intending to search a dedicated base DN instead of the "Base DN" for user groups.
	When disabled, "Base DN" is used for group searches.
Group Search DN	Configurable when "Use Group Search DN" is enabled.
	The dedicated base DN for group searches.
Group ID Attribute	The attribute of the LDAP group class which denotes the ID of the group which is used to match local group names.

Setting	Description
Group Member Attribute	The attribute of the LDAP group class which denotes the users who belong to a group. Its value must be either one below: • A user's DN • Value of the "Login Name Attribute" *Note: If the value is not either one, the group member detection may not work as expected.*
Group Search Filter	Search criteria for finding LDAP group objects within the directory tree.
Group Search Scope	The depth to search for LDAP group objects, which starts at the directory level denoted by the "Base DN" or a group search base DN. • One: Searches one level below the base DN, with the base excluded. • Subtree: Searches all levels below the base DN, including the base.

3. To test whether the connection to the new LDAP server can be successfully established, type the LDAP user name and password in the Test Connection section and click Test.

4. Click Save.
5. Repeat the same steps to add more LDAP servers as needed.

Editing or Deleting LDAP Servers

To show a list of existing LDAP servers, click Administration > LDAP.

In the Active column:

- ☑ indicates that LDAP server is enabled.

- ☐ indicates that LDAP server is disabled.

► *To modify an LDAP server setting:*

1. Click the desired LDAP server's [⌧ Edit] button. The Edit LDAP Server page opens.
2. Make necessary changes to the information shown. For information on each field, see Adding LDAP Servers (on page 203).
3. Click Save.

► *To delete an LDAP server:*

1. Click the desired server's [🗑 Delete] button.
2. Click OK on the confirmation message.

Enabling or Disabling the LDAP Authentication

Click Administration > LDAP to open the LDAP Servers page. The right-most button indicates the current LDAP authentication setting.

When that page shows [LDAP is disabled], the LDAP authentication is currently disabled, which is the default. While disabled, all users are authenticated via the local database of the User Station so their user credentials must be available on the User Station. Therefore, only local users can log in. See Users (on page 195).

When that page shows **LDAP is enabled**, the LDAP authentication is currently enabled. While enabled, all users are authenticated via the LDAP servers so only LDAP users can log in. The only local user that can log in is the *admin* user.

▶ *To enable/disable the LDAP authentication:*

- To enable it, click **LDAP is disabled** .

- To disable it, click **LDAP is enabled** .

Tip 1: You can also enable or disable the LDAP authentication on the Edit LDAP Settings page. See Configuring the Maximum Search Results and Local Authentication Settings (on page 213).

Tip 2: To enable or disable a specific LDAP server only, select or deselect the desired LDAP server's Active checkbox. See Editing or Deleting LDAP Servers (on page 209).

Searching for LDAP Users and Groups

When LDAP authentication is enabled, you can manually search for LDAP users or user groups as needed.

▶ *To search for LDAP users and groups:*

1. Click Administration > LDAP > Search. The "Search for LDAP Users" page opens.
   - If the Search button is disabled, enable the LDAP authentication first. See Enabling or Disabling the LDAP Authentication (on page 210).

Search for LDAP Users

Authenticate

Server
192.168.5.153

* Search Credentials
specify below

Bind DN

Password

Search

Type
Users

Base DN
dc=testlab,dc=nix

Search Filter
(objectClass=user)

Search Scope
Subtree

Search   Cancel

2. In the Server field, select the desired LDAP server from the list of *active* LDAP servers.

3. The following settings on this page are pre-populated with the values of the selected LDAP server, but you can adjust them to match your search needs. If you are not familiar with the LDAP settings, consult your LDAP administrator for help.

Setting	Description
Search Credentials	One or two options are available, depending on the selected LDAP server's configuration. • stored admin credentials: Use the admin credentials stored in the LDAP server's configuration. • specify below: Use the search credentials specified in the following two fields.
Bind DN, Password	With "specify below" selected, you must specify the search credentials in the two fields.
Type	The type of user data to search - User or User Group.
Base DN	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search.
Search Filter	Search criteria for finding LDAP user objects within the directory tree.
Search Scope	The depth to search for LDAP user or group objects, which starts at the directory level denoted by the "Base DN." • Base: Searches the base DN only. • One: Searches one level below the base DN, with the base excluded. • Subtree: Searches all levels below the base DN, including the base.

4. Click Search.

5. From the search result, you can select desired LDAP users or groups and add them to the User Station by clicking the buttons below.

Raritan.
A brand of **Llegrand**

- *Add as local user*:

  This button is displayed for those users who are not added to the User Station yet. Click this button to add the LDAP user as a local user who can also be authenticated via LDAP in the "LDAP authentication only" mode. Its authorization is managed by the User Station so ensure this user is a member of at least one user group in the local database. See Editing or Deleting Users (on page 197).

- *Add this group*:

  This button is displayed for those groups that are not added on the User Station yet. Click this button to add the LDAP group as a user group with the "Device Access", "Change Preferences"and "Launch the Port Scanner" privilege assigned. "Record Scanner Snapshots" permission can be added by admin. To modify the privileges, see Editing or Deleting User Groups (on page 200).

- *Add selected*:

  To select multiple LDAP users or groups at a time, select their checkboxes and then click this button.

Warning: You MUST NOT add the LDAP users whose login names do NOT meet the User Station's login name requirements. These LDAP users, if added, will fail to log in to the User Station. For login name requirements, see Users (on page 195).

Configuring the Maximum Search Results and Local Authentication Settings

In the LDAP settings, you can set parameters for maximum search results and allow access for local users.

By default, these options are disabled.

- Max Search Results: The default limitation is 1000. If the found result entries are more than the upper limit you set, those result entries exceeding the maximum are not displayed but a message shows up to remind you to specify a more accurate search filter.

- Allow access to local users: When this setting is enabled, an option is added to the login screen to allow users to select local authentication instead of LDAP authentication.

▶ *To configure the maximum LDAP search results:*

1. Click Administration > LDAP, then click the Settings button.
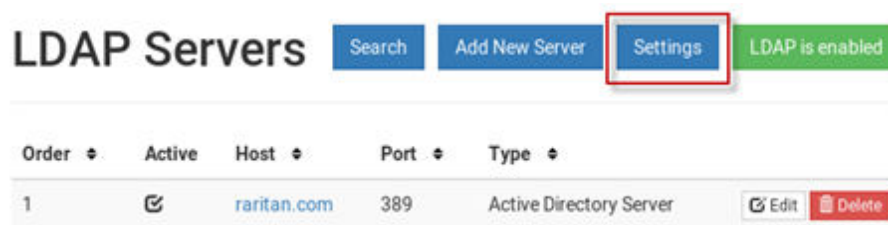
2. The Edit LDAP Settings page opens.
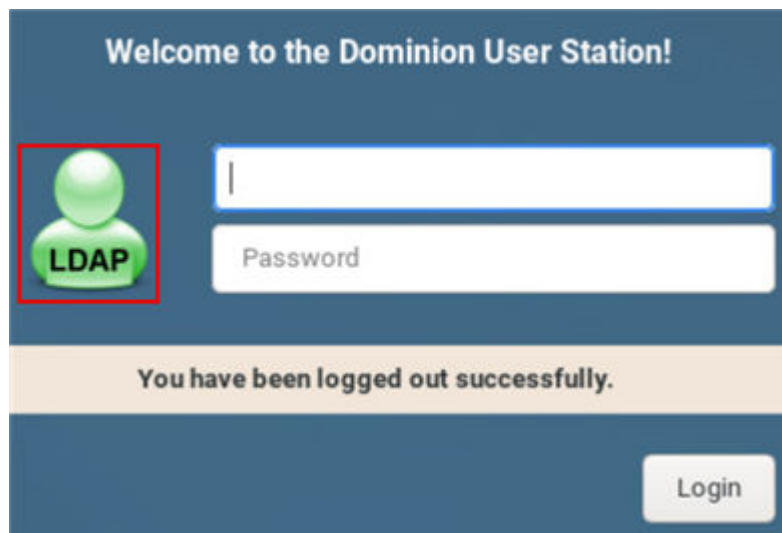
3. LDAP authentication must be enabled to set the upper limit for the LDAP search results. To enable, select the Enabled checkbox.

4. Select the desired value in the Max Search Results field: *10, 100, 1000* or *10000*.

5. Select "Allow access for local users" to enable the login screen checkbox for local authentication.

6. Click Save.

Logging in with LDAP

When LDAP is enabled, Dominion User Station presents a different login page. The login icon indicates the authentication type being used: Local, LDAP, or CC-SG.

When local users are allowed, an extra checkbox is also available for users to "Authenticate locally". See Configuring the Maximum Search Results and Local Authentication Settings (on page 213) for help with this setting.

LDAP Login Failure Message

LDAP user login attempt may fail with the event log message:

- Login of 'name' failed with hostname "IP Address" does not match the certificate at LDAPs://<IP address>

► *To resolve:*

- Update the LDAP server configuration. You may add the hostname, or disable TLS/SSL:
1. Open the User Station Configuration page. Choose Administration > LDAP.
   - Click the LDAP server's Edit button. Enter the hostname in the Hostname/IP-Address field, instead of the IP address.
   - OR, if you prefer, disable Use TLS/SSL for LDAP server.
2. Click Save.

CommandCenter Secure Gateway Integration

Raritan's CommandCenter® Secure Gateway (CC-SG) is an easy to deploy, plug-and-play appliance that provides IT administrators and lab managers with a secure, single point of remote access and control. Raritan's CC-SG consolidates multiple remote access technologies, including Dominion® KVM-over-IP switches and serial console servers, Raritan PX PDUs, service processors, and in-band methods such as RDP, SSH and VNC.

CC-SG integration in Dominion User Station allows you to access and control KX3, KX4-101, and SX2 nodes as well as any nodes with SSH, VNC, RDP,Web, or ESXi (VMW Viewer) interfaces without explicitly adding them directly to Dominion User Station. When CC-SG integration is setup, you can login to Dominion User Station with your CC-SG user name and password. Dominion User Station uses your CC-SG authorization information to automatically show the nodes you have access to in the Dominion User Station Navigator. Your permissions to view, access, and control are the same as in CC-SG because the same authentication and authorization are used.

The login page and the Navigator show a CC-SG label when integration is in effect:

- See Logging in with CC-SG Integration (on page 216)
- See Navigator with CC-SG Integration (on page 217)

Launching KVM/Serial sessions for ports works exactly the same as your usual Dominion User Station experience, using the KVM or Serial Client. See Using the KVM Client (on page 126), Using the Serial Client (on page 164)

SSH, VNC, RDP, and ESXi sessions are also launched by clicking the target, and the appropriate tool opens for the session type.

CC-SG Integration Requirements
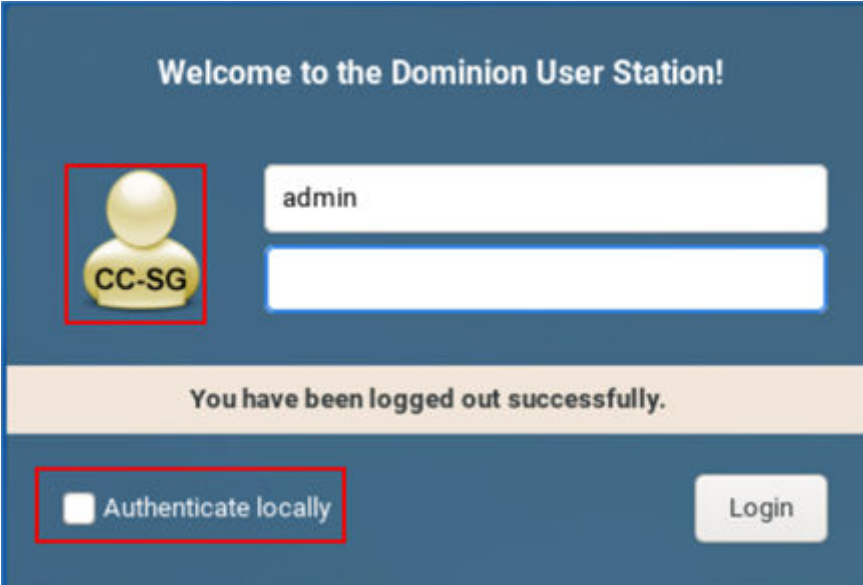
- Compatible CC-SG version: check the Dominion User Station Release Notes for latest compatible versions.
- LDAP cannot be enabled on Dominion User Station when CC-SG integration is enabled.

Logging in with CC-SG Integration

When CC-SG integration is enabled, the login page includes a CC-SG icon. Login with your CC-SG user name and password to access the targets you have permissions for on CC-SG.

Depending on your setting, you may see an extra checkbox for local users.

- Authenticate locally checkbox: This checkbox appears when the user name "admin" is entered so you can login with the standard Dominion User Station "admin" user. Users who need to use locally added KVM targets should select this checkbox, and enter local Dominion User Station login credentials. Authenticating locally means that CC-SG integration will be temporarily disabled for the current session.
- LDAP cannot be enabled when CC-SG integration is enabled.

CC-SG Authentication via SmartCard

When Authentication via SmartCard Certificate is enabled you can use your PIV SmartCard to log in to the User Station. You must configure the CC-SG to Enable Client Certificate Authentication, but it must not be set to Require Client Certificate Authentication.

Note: Remote Control and the Remote API do not work with Certificate Authentication.

Authenticate via SmartCard

► *To configure SmartCard integration:*

1. Click Administration > CC-SG.
2. Click Edit and select Authentication via SmartCard Certificate.
3. Click Save and Logout.

► *To log in via SmartCard:*

1. On the login screen, Use SmartCard for Authentication is checked by default.
2. Enter the SmartCard PIN instead of user name/password.

Note: SmartCard must be present during the login and for the screen saver unlock. The login with SmartCard only works with PIV cards and the certificate must be present on the card in the "Certificate for PIV Authentication" slot. The maximum of 8 characters PIN length is supported.

If SmartCard is configured, you can still login to the Dominion User Station manually with your user name and password, but you cannot use a SmartCard for auto-login. You can configure auto login using a user name and password.

SmartCard login is supported for all the KXUSTs where Keyboard and Mouse sharing is setup and the Controller and the Clients have the option "Automatically log in /out users" selected.

Navigator with CC-SG Integration

When CC-SG integration is enabled, the Navigator is optimized to show your Favorite Access items and CC-SG Targets. The CC-SG Targets section includes nodes that the user is authorized to view, including KVM, Serial, SSH, VNC, RDP, Web and ESXi interfaces. Ports of KVM and Serial switches that are configured locally on the Dominion User Station do not appear when you are logged in with a CC-SG user account.

Your nodes and interfaces are detected automatically. Each supported interface that is detected serves as an access method for the target. VMW Viewer interfaces are imported as ESXi access points. Only nodes already created on CC-SG are visible in Dominion User Station, and you cannot add, edit or delete nodes in Dominion User Station.

Your Dominion User Station supports the default interface feature of CC-SG. If you click the node (target) of a CC-SG, the default interface opens as follows

1. If a video group is defined, then the video group is launched as default (M-KVM).
2. If not, then the default interface as configured in CC-SG is launched.
3. If the default interface is not supported on the Dominion User Station, then the target is launched as per the pre-defined order of access points as in non CC-SG mode.
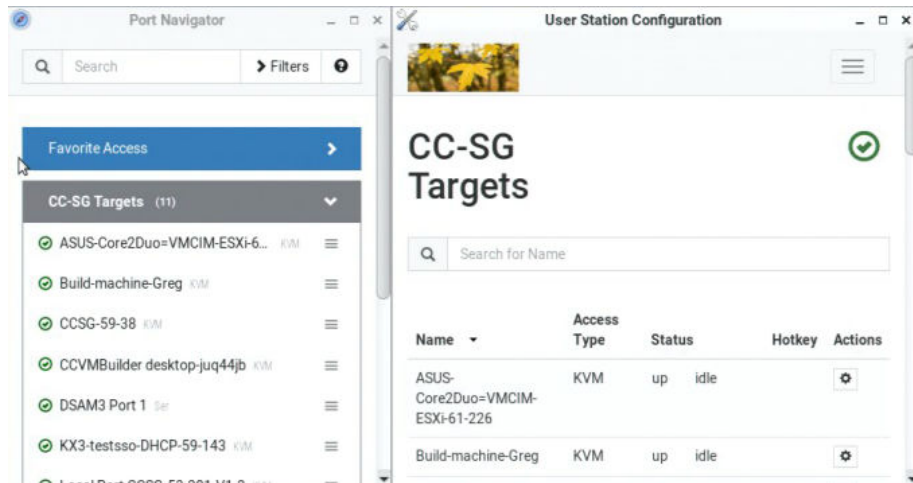
The Port Navigator window is displayed by default.

► *To launch Port Navigator:*

- Press Ctrl+Alt+N. OR choose Main Menu > Port Navigator.
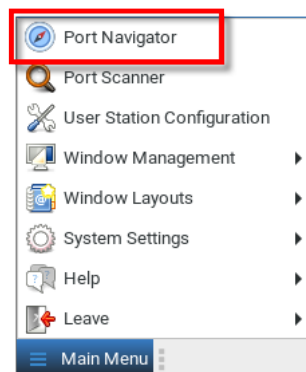
- The Port Navigator window opens.
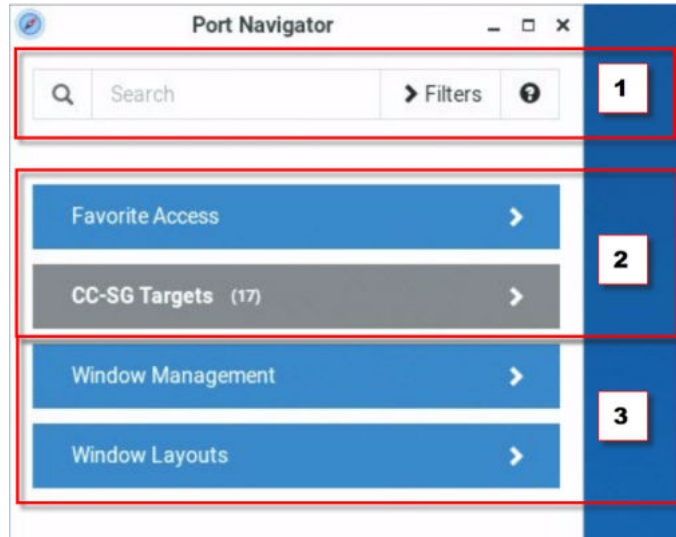
1. Search, Filters, and Help:

   • Search:

Searches for ports, or targets, containing the search word(s). See Using Search (on page 119).

   • Additional Filters:

Determines which items are displayed in this window based on connectivity and availability. See Using Filters (on page 120).

   • Help ❓ :

Shows the colors and icons denoting states. See Identifying States of KVM/Serial Switches and Ports (on page 117).

2. Favorite Access and CC-SG Targets:

   Favorite Access panel: When you first log in as a CC-SG user to the Dominion User Station, your list of favorites as configured in the CC-SG is shown. You can also customize the favorite access via edit settings of existing CC-SG targets in User Station Configuration.
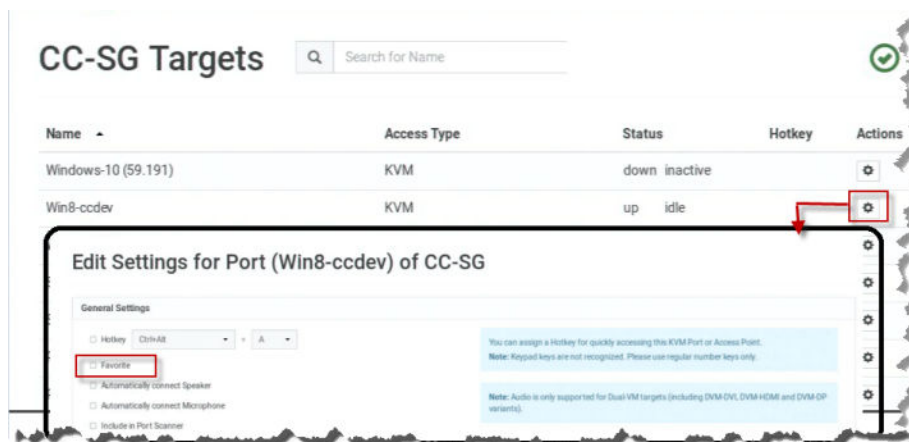
Note: Once changes are made to port settings in Dominion User Station, no new updates to favorites from CC-SG will be made. CC-SG will not overwrite preferences you have set in the Dominion User Station.

CC-SG Targets panel:

- Shows a list of all CC-SG Targets. Targets with KVM/Serial access also show port status.
- Video groups open all the configured ports for the group. "M-KVM" access method is assigned to video groups.
- Left-click on the Target opens the appropriate client. If there is more than one access method defined, the following hierarchy applies for which type of Access to use:
  - M-KVM
  - Default Interface

Note: If a video group is defined, then the video group is launched as default (M-KVM), otherwise the default interface as configured in CC-SG is launched. If the default interface is not supported on the Dominion User Station, then the target is launched as per the pre-defined order of access points as in non CC-SG mode.

- Next to the Target name, all configured access methods are listed. Click the access method directly to open the appropriate client. If there are multiple Access Points of the same type defined then the most recently added Access Point is opened.

- Right-click on the Target, or click the hamburger menu to list all access methods defined for the Target.
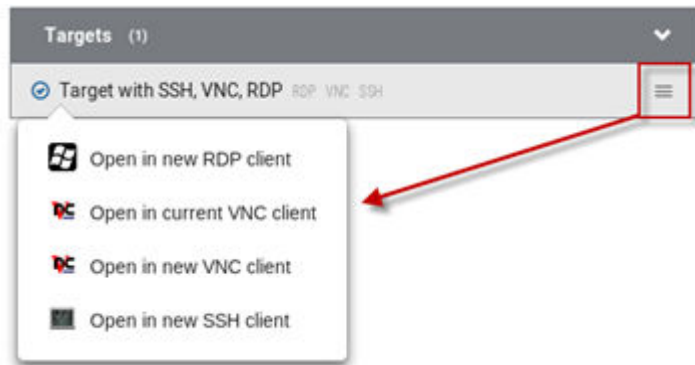
- The default is to show items whose status is Up. See Using Filters (on page 120).
- For dual port video, the name of the primary port is displayed instead of the port names. Dual port video groups whose primary port is Up will show in the list.

1. Window Management and Window Layouts:

- Window Management: Manage open sessions with window management tools. See Window Management (on page 58).
- Window Layouts: Access saved layouts. See Window Layouts (on page 187).

ESXi Access Requirements

You can access your VMW Viewer interfaces in the Navigator using the VMware "ESXi Embedded Host Client." The ESXi server must support the ESXi Embedded Host Client and must be version 6.0 or higher. Upon launching, the Remote Console of the virtual machine is shown. Single sign-on is not supported, so you must enter credentials each time you launch the interface.

To launch ESXi access, you must have the ESXi Access privilege

CC-SG Authentication Fallback

CC-SG has a fall-back authentication mechanism. CC-SG maintains an ordered list of authentication methods and if one authentication method fails CC-SG tries authentication with the next mechanism in the list.

For the best results with CC-SG integration, make sure users have the same access privileges in each authentication server that may be used.

Trusted Certificates

You must install trusted certificates on the User Station in these scenarios:

- A valid CA certificate is required to establish the LDAP connection. Then you must:
    a. Consult your LDAP server administrator to get the CA certificate file.
    b. Install this CA certificate onto the User Station.

- When FIPS mode is enabled, all encrypted connections to KVM/Serial switches are processed using the FIPS accredited cryptographic code and the authenticity of those KVM/Serial switches is checked via their certificate chain. When Check KX/SX Device Certificate is enabled, authenticity of KVM/Serial switches is checked via their certificate chain. You must install the trusted device or root-certificate of each KVM/Serial switch on the User Station, or the connection to the KVM/Serial switches fails.

When CC-SG integration in enabled, and FIPS mode or Check KX/SX Device Certificate is enabled as well, you must install the CC-SG certificate. Also, if the CC-SG and the KX/SX managed by the CC-SG have certificates signed by different CAs, then the certificates from both the CC-SG and the KX/SX devices should be added to the KX User Station , or the connection fails. A connection error message appears. See Certificate Failure Messages (on page 223). Certificates using RSA or DSA algorithm with key-sizes smaller than 1024 bit are not accepted by Dominion User Station.

For more details about creating certificates that are accepted, see Certificate Requirements.

► *To install the CA Certificates on the User Station:*

1. Plug a USB drive or mount a network storage containing the appropriate certificate file into the User Station.
2. Click Administration > Trusted Certificates, then click the Import Certificate button.

    ⬆ Import Certificate   The Import Trusted Certificate page opens with a list of detected certificates.
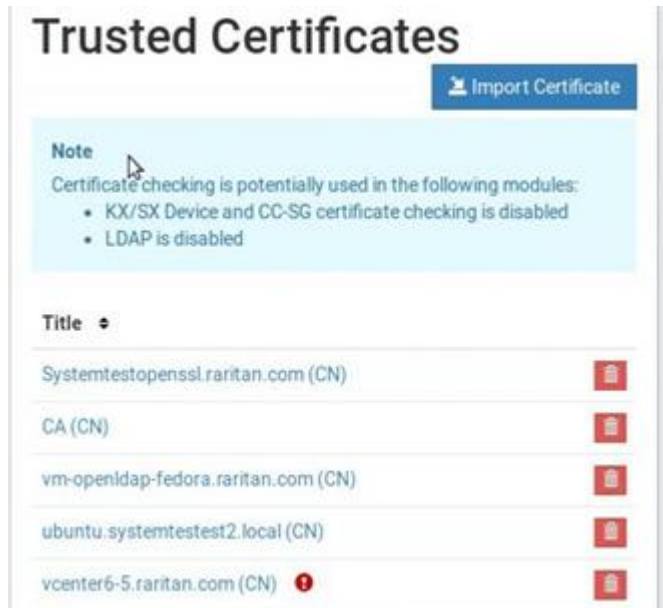
3. Click Import to install the desired certificate onto the User Station. Certificate files must be one of the following types: PEM, DER, TXT, CER, or CRT and must contain a PEM or DER encoded certificate.
4. The content of the installed certificate is displayed.
   - To show a list of installed certificates, click Back to all Certificates.
   - To remove this certificate, click Remove and then OK.
5. If multiple certificates are needed, repeat the same steps to install more.

Removing an Installed Certificate

If any installed certificate is outdated, invalid or no longer required, you can remove it.

▶ *To remove a certificate from the User Station:*

1. Click Administration > Trusted Certificates. A list of installed certificates is displayed.
2. Click the red trash icon for the certificate you want to remove. Or, click the certificate that you want to remove to check the contents first, then click Remove.
3. Click OK on the confirmation message.

Certificate Failure Messages

In the FIPS mode and when Check KX/SX Device Certificates is enabled, if the KVM/Serial connection failure is resulted from the absence of a valid KVM/Serial switch certificate on the User Station, an error message similar to the following appears.

Could not connect to target server.

The SSL certificate of the KX could not be verified. Either the SSL certificate is invalid or expired, or it cannot be trusted by the KX III Userstation. Please make sure that the certificate or the CA certificate that was used to sign the certificate is correctly imported into the KX III Userstation.

OK   Close
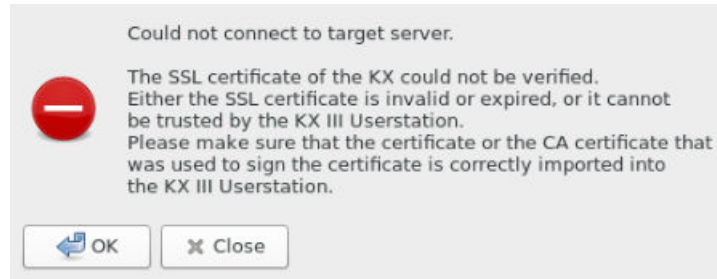
Server Certificate

Services that occur over network, such as remote control, are secured with TLS. This requires the installation of a TLS certificate on the Dominion User Station.

By default, the Dominion User Station has a demo certificate. You must have System Administrator privileges to view, download or change the certificate. A new certificate can be installed by:

- Uploading a new certificate and private key. See Import Private Key and Certificate (on page 225).
- Create a private key and a self-signed certificate in the Dominion User Station interface. See Create Self Signed (on page 226).

Note: It is strongly recommended to update the preinstalled demo server certificate if you want to use the Remote Control feature. See Remote Control via Web Browser (on page 244).

If the demo server certificate is not updated, a warning message is displayed: "You're still using the preinstalled server certificate. Please change it!"

▶ *To view the current server certificate:*

- Click Administration > Server Certificate. The summary information of the installed certification displays. Click Details for more.
- With a USB drive connected or a Network Storage mounted, you can export the file.

Import Private Key and Certificate

If you would like to use your own private key and certificate, you can import it from an attached USB drive or network storage.

Passphrase protected keys are not supported. The private key and certificate must be combined in one file. The following file types are supported:

- PEM format (.txt, .pem)
- PKCS12 (.p12, .pfx)

If the uploaded certificate is invalid, does not match the rules, or cannot be parsed otherwise, an error message displays.

► *To import private key and certificate:*

1. Plug a USB drive or mount a network storage containing the appropriate certificate file in the root directory into the User Station
2. Click Administration > Server Certificate.
3. Click the Import button.

4. The certificate filenames found on the USB flash drive or network storage appear in a list. Click Import for the correct file.

Import Private Key and Certificate

USB or Network Storage	Certificate Files	
Windows-Storage	Certificate_Key.txt	Import

Cancel

Note

In order to import a certificate insert a USB Storage, such as a USB flash drive, or mount a Network Storage containing the certificate file in its root directory.

The file must have a suffix of .pem, .txt, .p12 or .pfx (case insensitive).

The file has to contain the pair of key and certificate in one file. Passphrase protected keys are not supported.

5. The file is imported and validated. The certificate details are displayed.
6. Click Install New Certificate to use the imported certificate. Installing the certificate requires a reboot.

Create Self Signed

If you would like to use a self signed certificate, you can create the Private Key and the Certificate using Dominion User Station. After creating the certificate, you will install it.

► *To create a self signed certificate:*

1. Click Administration > Server Certificate.
2. Click the Create Self Signed button.

Server Certificate

Create Self Signed

Import

You're still using the preinstalled server certificate. Please change it!
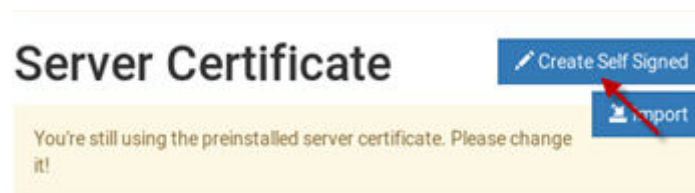
3. Enter certificate details and key parameters.
   - Country Code: Must be uppercase, 2-letter country code.
   - State or Province
   - Locality
   - Organization: Optional.
   - Organizational Unit: Optional.
   - Common Name: Must be a hostname.
   - Email address: Optional.
   - Key Length: 2048 or 4096.
   - Validity in days: 1 to 36525.
4. Click Create.

Raritan.
A brand of **Llegrand**

Create Self Signed Certificate

Subject

Country Code

* State or Province

* Locality

Organization

Organizational Unit

Common Name

Email Address

Key Creation Parameters

Key Length

2048

Validity in days

[Create]   [Cancel]

5. The certificate and key details display. If you approve, click Install to use this certificate. Installing the certificate requires a reboot.

New TLS Certificate Details

Issued To

Common Name	sangkxus.raritan.com
Organization Unit	Eng
Organization	DPC
Locality	Somerset
State or Province	NJ
Country Code	US

Issued By

Common Name	sangkxus.raritan.com
Organization Unit	Eng
Organization	DPC
Locality	Somerset
State or Province	NJ
Country Code	US

Validity Period

Issued on	2023-12-21 16:37:04 UTC
Expires On	2023-12-31 16:37:04 UTC

Miscellaneous

Version	3
Key Length	2048
Serial Number	AD:68:B0:DF:4F:3D:51:68
SHA1 Fingerprint	61:D5:53:B0:6B:E2:84:19:56:DD:11:18:D3:93:7C :A0:34:D8:2A:1A

[Install]   [Cancel]

Enable/Disable FIPS Mode and Device Certificate Settings

The User Station optionally uses a FIPS 140-2 encryption module that supports the Security Requirements for Cryptographic Modules of the Federal Information Processing Standards (FIPS), which is defined in the *FIPS PUB 140-2, Annex A: Approved Security Functions*. These standards are used to protect the Federal government's sensitive information with the cryptographic-based security systems in the U.S. and Canada.

The Check KX/SX Device/CC-SG Certificates option allows Dominion User Station to enforce SSL certificate checks in communication with the KX3/SX for both port information and KVM/Serial sessions.

When FIPS mode is enabled, all encrypted connections to KVM/Serial switches are processed using the FIPS accredited cryptographic code and the authenticity of those KVM/Serial switches is checked via their certificate chain. When Check KX/SX Device Certificate is enabled, authenticity of KVM/Serial switches is checked via their certificate chain. You must install the trusted device or root-certificate of each KVM/Serial switch on the User Station, or the connection to the KVM/Serial switches fails. See Trusted Certificates (on page 222).

Important: In the FIPS mode, the User Station CANNOT connect to any KVM target on a KX3 or login to CC-SG if the security settings on the device are TLS 1.3 only and also fails to connect with RDP access clients.

Note: Currently, encrypted LDAP connections are not using the FIPS-accredited cryptographic code.

► *To enable or disable the FIPS mode and configure device certificate settings:*

1. Click Administration > Security Settings. The Security Settings page opens.

   - ☑ indicates the setting is enabled.

   - ☐ indicates the setting is disabled.
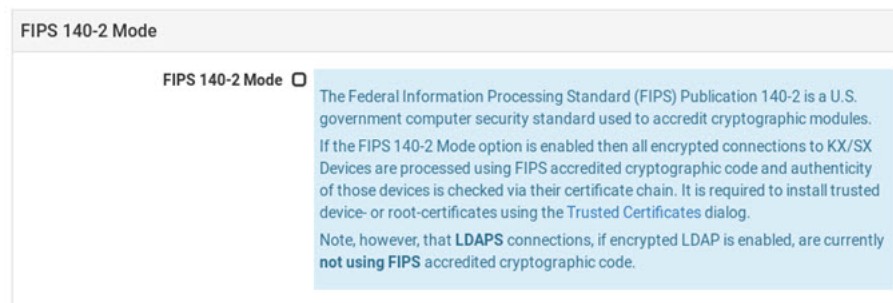
   Note: These options require certificates to be installed. Click Manage Certificates to check certificates or install more. See *Trusted Certificates (on page 222).*

2. Click Edit, and then select or deselect the checkboxes for FIPS, or KX/SX/CC-SG Certificate Settings.

Note: If certificates have not been installed yet, you will see a message. Click Manage Certificates to go to the import page. Certificate hostname verification is enforced.

3. Click Save.
4. Click OK on the confirmation message.
5. The User Station now reboots if FIPS mode was changed. Wait until the login page reappears.

Enable Keys and Certificates Check for SSH, RDP, Web and ESXi Clients

To strengthen security you can store SSH , RDP, WEB and ESXI keys and certificates. These keys and certificates are stored per target and per user.

Note: By default, verification of SSH keys and RDP, Web and ESXi certificates is ignored.

► *Configure SSH Keys Verification:*

1. Click Administration > Security Settings. The Security Settings page opens.
2. Click Edit.
3. In the Verify SSH Host Keys field, select an option.
   - Always ignore.
   - Accept on first connection.
   - Ask on first connection.
   - Always ask.
   - Deny unknown host keys.
4. Click Save.

The SSH key will upload to the SSH Host Key section of the Settings page on the SSH Client.
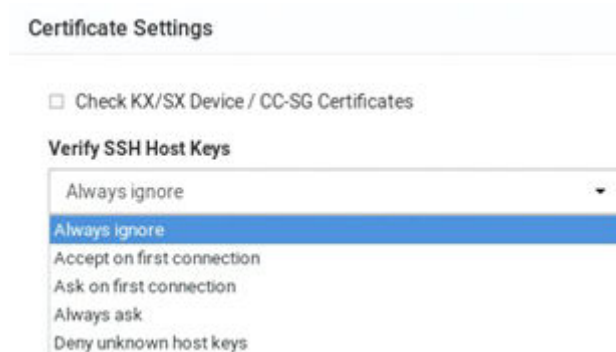
► *Delete SSH Key:*

1. Click Configuration >Targets > Click Edit Preferences of the target.
2. Scroll down to SSH Host Key Section.
3. Click Delete to remove the key.

SSH Host Key

Notes:

An SSH host key is a cryptographic key used for authenticating computers in the SSH protocol.
Depending on the Security Settings, it may be possible to connect to known hosts via SSH only.

If there is a host key saved for this access, you can see its fingerprint here and you can delete it.

Fingerprint:
192.168.59.48 RSA SHA256:Rn2i919h7vEqMb1Zed9k+9gvkCeQvM7AqxX0GKEhFPo

Delete

► *Configure RDP Certificate Verification:*

1. Click Administration > Security Settings. The Security Settings page opens.
2. Click Edit.
3. In the Verify RDP Certificates field, select an option.
   - Always ignore.
   - Accept on first connection.
   - Ask on first connection.
   - Deny unknown certificates.
4. Click Save.

The RDP Certificate will upload to the RDP Certificate section of the Settings page on the RDP
Client.

Certificate Settings

☐ Check KX/SX Device / CC-SG Certificates

Attention

KX/SX Device / CC-SG certificate checks cannot be performed because there are no certificates installed. All secure connection attempts will fail. Please install certificates.

Verify SSH Host Keys

Always ignore   ▼

Manage Certificates

Verify RDP Certificates

Ask on first connection   ▼

Always ignore
Accept on first connection
Ask on first connection
Deny unknown certificates

Note: RDP connections are not supported if FIPs mode is enabled.

► *Delete RDP Certificate:*

1. Click Configuration >Targets > Click Edit Preferences of the target.
2. Scroll down to RDP Certificate section.
3. Click Delete to remove the certificate.

Raritan.
A brand of ☐legrand

RDP Certificate

Fingerprint:
d8:64:d3:53:c5:70:e6:24:81:4f:65:22:a8:d7:c5:42:67:7f:28:85:2e:13:30
:bf:eb:9b:38:c6:ac:7a:e6:be

Notes:

An RDP certificate is a cryptographic certificate used for identifying computers in the RDP protocol. Depending on the Security Settings, it may be possible to connect to known hosts via RDP only.

If there is a certificate saved for this access, you can see its fingerprint here and you can delete it.

Delete

▶ *Configure Web and ESXi Certificate Check:*

Note: Web and ESXi certificates can be installed under Trusted Certificates.

---

1. Click Administration > Security Settings. The Security Settings page opens.

   - ☑ indicates the setting is enabled.

   - ☐ indicates the setting is disabled.

2. Scroll down and click Edit.
3. Select or de-select the Verify Certificates for Web and ESXi Targets check box.

4. Scroll down and click Save.
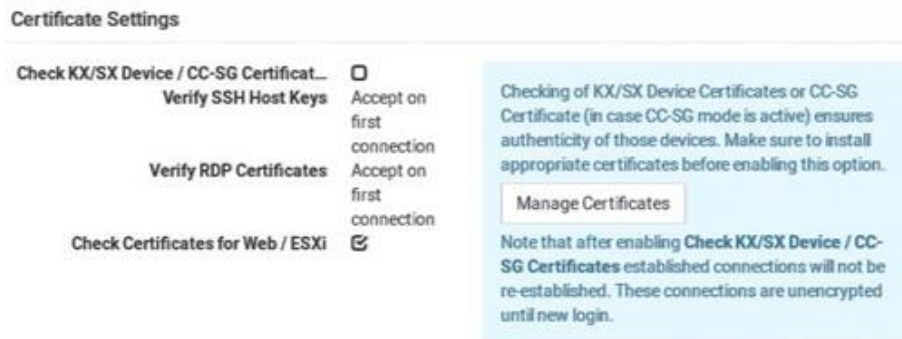
Note: Enabling Check Certificates for Web/ESXi forces HTTPS certificate checks.

Strong Password Settings

Password aging and strong passwords can be enabled to offer additional security. Password Aging forces users to change passwords regularly. Strong Passwords can be enabled to specify length and characters required, and limit reuse of old passwords.

Note: Strong Passwords is enabled by default.

► *To configure password settings:*

1. Click Administration > Security Settings. The Security Settings page opens.

   - ☑ indicates the setting is enabled.

   - ☐ indicates the setting is disabled.

Password Settings

In order to improve the system's security, you can set a password expiration interval, or you can enable strong passwords.

Notes:

- If Password Aging is enabled and a user has last changed his password with an old firmware release prior to Strong Passwords support, the user will be forced to change his password on the next login, regardless of the Password Aging Interval.
- The Strong Password setting only applies to newly set passwords. In case users have 'weak' passwords and strong passwords are enabled later, they will not be forced to change their password.

Password Aging
☐
Password Aging Interval
60 Days
Strong Passwords
☑
Minimum Password Length
8
Enforce Lower Case Character
☑
Enforce Upper Case Character
☑
Enforce Numeric Character
☑
Enforce Special Character
☐
Password History Size
5

Edit

2. Click Edit, then scroll down to the password options.
3. Specify options for Password Aging:
   - Select the Password Aging checkbox to enable the feature.
   - Password Aging Interval: All users are required to change their password at the selected interval.

☑ Password Aging

Password Aging Interval

60 Days	▾
7 Days	
14 Days	
30 Days	
60 Days	
90 Days	
180 Days	
365 Days	

4. Strong Passwords:

Raritan.
A brand of 🟥legrand

233

- Select the Strong Passwords checkbox to enable the feature. This requires users to create passwords that meet the additional criteria specified.
- Minimum Password Length: The minimum number of characters required in a password.
- Enforce characters: Users must include at least one of the specified characters, Lower Case, Upper Case, Numeric, Special.
- Select a Password History Size: The number specifies how many previous passwords are kept in the history and cannot be reused. For example, if Password History Size is set to 5, users cannot reuse any of their previous five passwords.

☑ Strong Passwords

Minimum Password Length

8	− +

☑ Enforce at least one Lower Case Character

☑ Enforce at least one Upper Case Character

☑ Enforce at least one Numeric Character

☐ Enforce at least one Special Character

Password History Size

5	− +

5. Scroll down to click Save.

User Blocking

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts.

The admin user is excluded from User Blocking.

If a blocked user tries to log in, "Authentication Failed" is displayed at the login screen. The user is not notified that they are blocked. An event log message is generated when a user is blocked.

► *Unblocking:*

Users are automatically unblocked after the specified amount of time, or a System Administrator user can unblock the user early in the Users configuration. The blocking status is shown on the Users list.

► *To configure user blocking:*

1. Click Administration > Security Settings. The Security Settings page opens.

- ☑ indicates the setting is enabled.

- ☐ indicates the setting is disabled.

Raritan.
A brand of ☐legrand

2. Click Edit, then scroll down to the user blocking options.
3. To enable user blocking, select the Block Users on Login Failures checkbox.
4. Block Timeout: The time period that the users with failed logins will be blocked from logging in.
5. Count of Failed Logins: The maximum number of failed logins before blocking a user.

6. Scroll down to click Save.

Links and Redirects

The Links and Redirects option allows you to redirect or link to external sites of Web and ESXi access clients. You can choose whether links or redirects to external pages are allowed. If you allow, you can also specify pages in the exception list to minimize the security risk.

Note: By default, links and redirects for Web and ESXi targets are forbidden.

Links and redirects

For Web and ESXi access points, a built-in web browser application is used. For security reasons, you can choose whether links or redirects to external pages are allowed, and if yes, which pages are listed in the exception list.

Note: It is strongly recommended to disable external links completely. If needed, limit the number of allowed pages to a minimum.

Allow links / redirects for Web Targets	Forbid all links and redirects
Allow links / redirects for ESXi Targets	Forbid all links and redirects

► *To Configure Links and Redirects:*

1. Click Administration > Security Settings. The Security Settings page opens.
2. Click Edit then scroll down to the Links and redirects section.
3. In the Allow links/redirect for Web Targets field, select an option:
   - Forbid all links and redirects.
   - Allow the listed links and redirects.
   - Allow all links and redirects.
4. If you selected "Allow the listed links and redirects", add the URLs. that should be allowed to the Allow list for Web Targets. Click the plus sign to add more links to the list.
5. In the Allow links/redirect for ESXi Targets field, select an option:
   - Forbid all links and redirects.
   - Allow the listed links and redirects.
   - Allow all links and redirects.
6. If you selected "Allow the listed links and redirects", add the URLs. that should be allowed to the Allow list for ESXi Targets. Click the plus sign to add more links to the list.

Note: There is no limitation on number of added links.

Raritan.
A brand of ☐ legrand

7. Scroll down to click Save.

Restricted Service Agreement

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed on the login screen. Users must select a checkbox to agree to the statement to login.

► *To configure the Restricted Service Agreement:*

1. Click Administration > Security Settings. The Security Settings page opens.

   - ☑ indicates the setting is enabled.
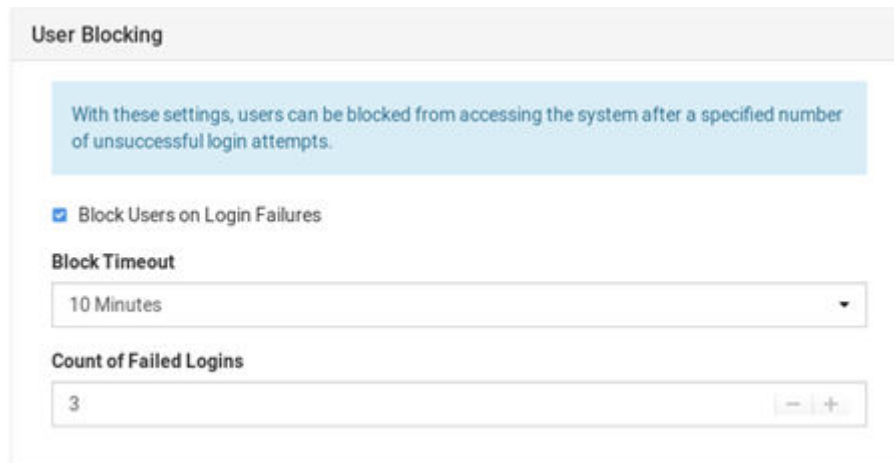
   - ☐ indicates the setting is disabled.

Restricted Service Agreement

Enforced
☐
Text
Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

2. Click Edit then scroll down to the Restricted Service Agreement options.
3. To enable the feature, select the Enforce Restricted Service Agreement checkbox.
4. A default agreement is provided. You can edit or replace the default text as needed.

Restricted Service Agreement

☑ Enforce Restricted Service Agreement

Restricted Service Agreement Text

Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

5. Click Save.

Display Settings

The User Station display can be configured to lock the screen or turn off the monitor in certain conditions.

Display settings include screen locking and scaling. The settings are applied to all users.

You must have "System Administrators" privileges to configure display settings.

Note: Port Scanning sessions and KVM sessions do not prevent monitor turn-off and/or screen locking when those options are configured.

► *To edit the display settings:*

1. Click Administration > Display Settings.
2. Click Edit.
3. To turn off the monitor after an idle timeout period, select the time period:
   - Select Never to keep monitor on.
   - Select 1, 2, 3, 5, 10, 15, 30 or 60 Minutes to enable the monitor turn off after the specified idle time period.
4. To lock the screen when idle, check the Lock Screen when idle checkbox. Lock Screen can only be enabled with Turn off Monitor after idle timeout. The screen is locked during the idle time period.
5. In the Scaling Settings, select the Desktop Scaling that works best for your monitor: 100% or 200%. If you are using a 4k HD monitor, 200% scaling may be preferable.
6. Click Save.

Edit Display Settings

Screen Locking Settings

Turn off Monitor after idle timeout

Never ▼

☐ Lock Screen when idle

Scaling Settings

Desktop Scaling

100% ▼

[Save] [Cancel]

Customization

To customize your Dominion User Station GUI appearance, you can replace the default Raritan desktop background, application logo, and login screen with your own images and messaging. System Administration privilege is required.

Customizations are applied for all users. Changes are logged to the event log with image name and user who performed the change. Customization's are included in backups and restore, while a factory reset restores the original default images. You can also restore the defaults at anytime.

Raritan.
A brand of ⬛legrand

Image files must be saved to the root directory of a USB stick or mounted network storage for upload.

Note: If the desktop does not show the new background image, it is likely the image file is broken. Replace with a different image file.

► *Image requirements:*

- Desktop background image: JPG, PNG, or SVG images up to 128 MB. Solid background color that is not transparent
- Application logo: Appears in the Configuration application in the top-left corner. JPG, PNG, or SVG images up to 512KB. Application logo images are automatically scaled to 110 x 48 pixels, or 220 x 96 pixels when 200% desktop scaling is used.
- Logo on the login screen: JPG, PNG, or SVG images up to 512 KB. Logo images are automatically scaled to 80 x 80 pixels, or 160 x 160 pixels when 200% desktop scaling is used.

► *To customize the Dominion User Station:*

1. Save the desired image files to a USB flash drive, and connect the USB flash drive to the Dominion User Station.
2. Click Administration > Customization and click Edit for the section you want to change.
   - Desktop Background: background image only
   - Application: logo image only
   - Login screen: logo image, plus Header and Message text options

Customization

Desktop Background

Current Background:
[Default]

Edit

Application

Logo:
[Default]

Edit

Login Screen

Logo:
[Default]
Heading:
[Default]
Message:
[Default]

Edit

3. If an custom image is currently in use, the file name is listed, while non-customized sections will show "Default". Image files found on the USB device or mounted network storage are listed as options. Click the Apply button for the image file you want to use.

Or, to restore the default image, click Install Default. This option is disabled when a custom file is not in use.

Once the image is set, click Back to return to the options.

Desktop Background

Current Background: [Default] [Install Default]

USB or Network Storage	Background Image	Size	
965A-C540	IMG_7298.jpg	3.65 MB	[Apply]

Note

In order to update the desktop background, insert a USB Storage, such as a USB flash drive, or mount a Network Storage containing the image file in its root directory.

The image file must have a suffix of .jpg, .png or .svg (case insensitive) and only files with a maximum size of 128 MB are allowed.

The background image will apply to all users and the default background can be restored via 'Install Default' button.

[Back]

- In this example, the current desktop background is the default Raritan branding, and there are 2 image files found on the connected USB device. Both listed images meet the requirements for a background image as JPG files under 128MB.

4. For Login Screen customization, you can also enter a custom Heading and Message, then click Save.

Heading

[   ]

Message

[   ]

[Save] [Cancel]

5. Desktop background image changes take effect immediately. Log out to see the login screen changes on your next login attempt.

Customization Examples

► *Customized "ABC" logo on User Station Configuration:*

In this example, the customized "application logo" was just saved.

Raritan.
A brand of ☐legrand
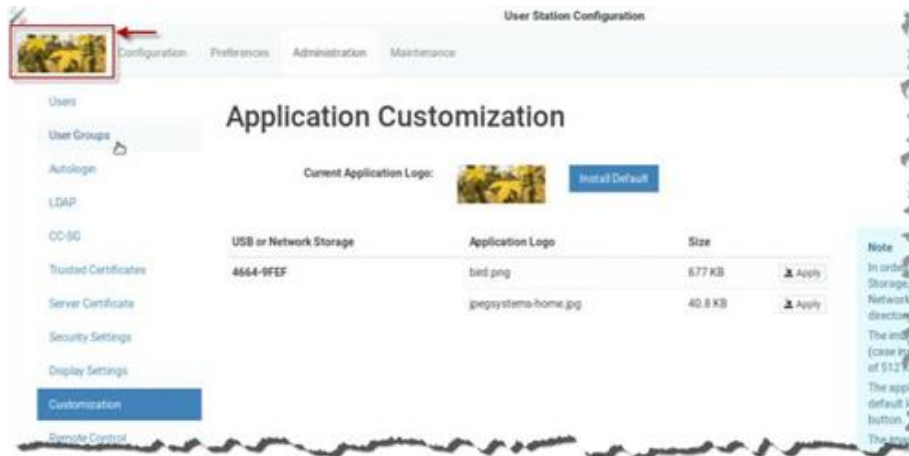
► *Customized login screen:*

In this example, a customized login screen was configured. The login screen contains the customized "sunshine" logo image, and the customized message "Welcome to the Dominion User Station!".

Remote Control

One common use case for remote control is to connect the controlled user station to a wall monitor and remotely control the display of various target servers on monitor via web browser.

Using a web browser, connect to the Remote Control interface of the Dominion User Station using the IP address or hostname as the URL. Login as usual. Upon successful login, the Dominion User Station presents the Port Navigator just as it appears in the local console. Selecting and opening ports works the same as in the local console, but the KVM clients open in full screen mode at the Dominion User Station that is being remotely controlled. If "Unrestricted Navigator" is enabled, you can also use window management and window layout features, launch multiple sesions, and use non-full-screen view.

Remote Control can also be accomplished via the RESTful API (HTTPS & JSON) to control Dominion User Station programmatically from customer applications. There are two main use cases: to launch sessions or window layouts and/or to perform administrative tasks.

Raritan.
A brand of legrand

Remote Control via Web Browser

The remote control via web browser configuration allows the Dominion User Station to be controlled via web browser accessed by a smart phone or PC that can reach the Dominion User Station on the network.

By default, Remote Control via web browser offers full-screen sessions only, without access to Window Layouts or Window Management. Enable the Unrestricted Navigator setting to add those features to remote control sessions.

► *Supported browsers:*

- Chrome 60+
- Firefox 52+
- Safari 11+
- Edge 42+

► *To configure remote control:*

You must have the System Administration privilege.

1. Click Administration > Remote Control.
2. Click the Edit button to enable the options.
3. Select Enable Remote Control via HTTPS to enable the feature.
4. Allow HTTP:
   - If "Allow HTTP" is checked, Remote Control is available via both HTTP and HTTPS. There is no redirect.
   - If "Allow HTTP" is not checked, HTTP is redirected to HTTPS.
5. Unrestricted Navigator: Enable Unrestricted Navigator to allow additional features:
   - The Unrestricted Navigator can launch sessions in non-full-screen mode, and show multiple sessions at the same time.
   - Windows Layout and Window Management functions can be used from Remote Control.
6. Click Save.

Raritan.
A brand of legrand

Remote Control via API

The Dominion User Station supports a remote RESTful API via HTTPS, allowing programmed remote control to:

- Launch Access Client sessions or Windows Layouts.
- Perform certain administrative tasks.
- See API (on page 278) for API documentation.

► *API Overview*

- The API can be enabled independently from the regular remote control setting.
- The API uses HTTPS (HTTP is not an option), listening on port 8443.
- If remote control is enabled, the API is available only on port 8443.
- Regular remote control cannot be used on port 8443.
- The API is not available on regular remote control ports 80 and 443.
- The API uses JSON documents for both POST request data (method parameters) and responses.
- One checkbox on the Remote Control page enables/disables the API access, which is disabled by default.
- The API Description document (in OpenAPI format) can be exported to a USB drive or a network storage.
- The TLS certificate can be configured using the Server Certification setting of the Configuration tool.

► *To configure Remote Control via API:*

1. Click Administration > Remote Control.
2. Click the Edit button to enable the options.
3. Select the Enable Remote Control via HTTPS checkbox.
4. Select the Remote Control via API checkbox.
   - Export the API file to a connected USB drive or configured network storage. Choose a file format and click "Export the API file".
5. Click Save.

Edit Remote Control Settings

Remote Control via Web Browser

☑ Enable Remote Control via HTTPS

☐ Allow HTTP

☐ Unrestricted Navigator

This option enables Remote Control of the User Station via HTTPS.

HTTP access is possible but not recommended.

By default, Remote Control is limited to one access client session in full-screen. If **Unrestricted Navigator** is enabled, then the remote Navigator allows to launch sessions in non-full-screen mode, and show multiple sessions at the same time. Also, in unrestricted mode, Window Layouts and Window Management functions can be used from Remote Control.

Remote Control via API

☑ Remote Control API

Export API description file to   AB9A-F1DC ▾

Remote Control is also available via an REST API (over HTTPS) on port 8433. You can export an OpenAPI specification file here.

For further documentation and examples, please contact Raritan support.

[Save] [Cancel]

Using the API

1. Create a login session to authenticate on further calls. There are API calls to create the login session.
2. The remote API session is bound to a local user session. If an API user logs in, the following will happen:

Raritan.
A brand of 🔲legrand

- If the API user is already logged in on the local console, the API will take over the session.
- If no user is logged in on the local console, the API user will be automatically logged in.
- If another user is logged in on the local console, then the user is logged off and the API user is logged in.

3. Once the session is created, the API uses HTTP cookies for authentication. When the session is created, the client receives cookies. These cookies must be sent back on further API requests.

4. When finished, the API user can log off the session. Logging off also terminates the session on the local console.

See API (on page 278) for details.

Access via iOS devices

You must install a CA-signed certificate on your Apple iOS devices (iPad/iPhone) before you can connect to the Dominion User Station. Access is prevented if only the default certificate is present. Depending on your browser, you may see an error such as "This Connection is Not Private".

When creating certificates, the certificate Common name should match the IP address/Hostname used to connect to the device. Install both the Dominion User Station certificate and the CA certificate used to sign the Dominion User Station certificate.

Keyboard/Mouse Sharing

Keyboard and Mouse Sharing allows you to control several Dominion User Stations by one keyboard and mouse that is connected to one of the Dominion User Stations. This can be useful in a control room setting with multiple monitors connected to multiple Dominion User Stations.

Note: The Keyboard/Mouse Sharing feature does not support Caps, Num and Scroll Lock.

▶ *KX4 User Station 6 Monitor Vertical Configuration Example:*
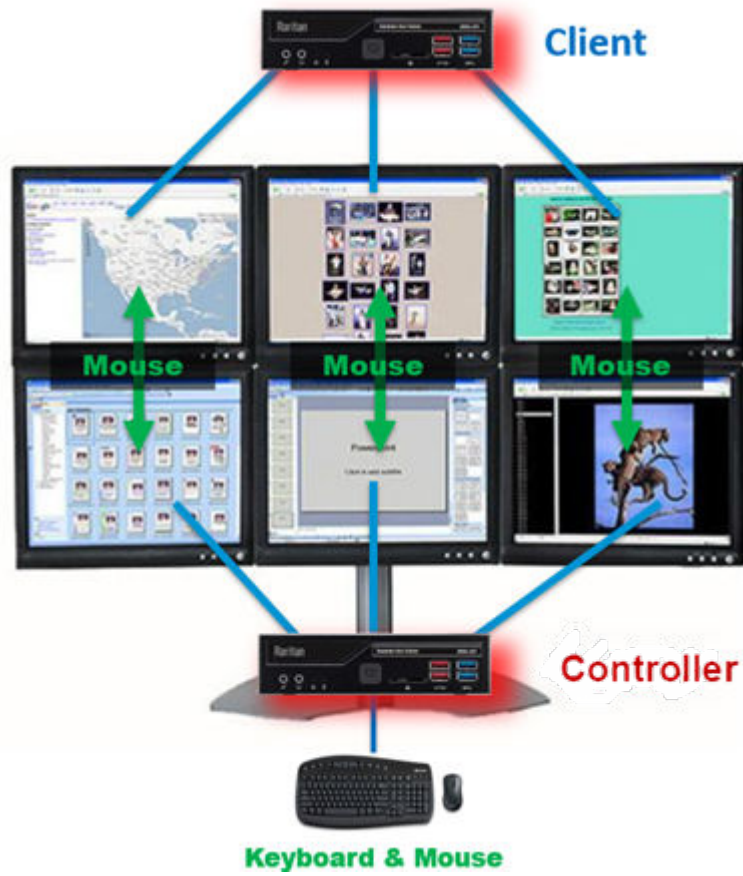
► *KX3 User Station 4 Monitor Vertical Configuration Example:*
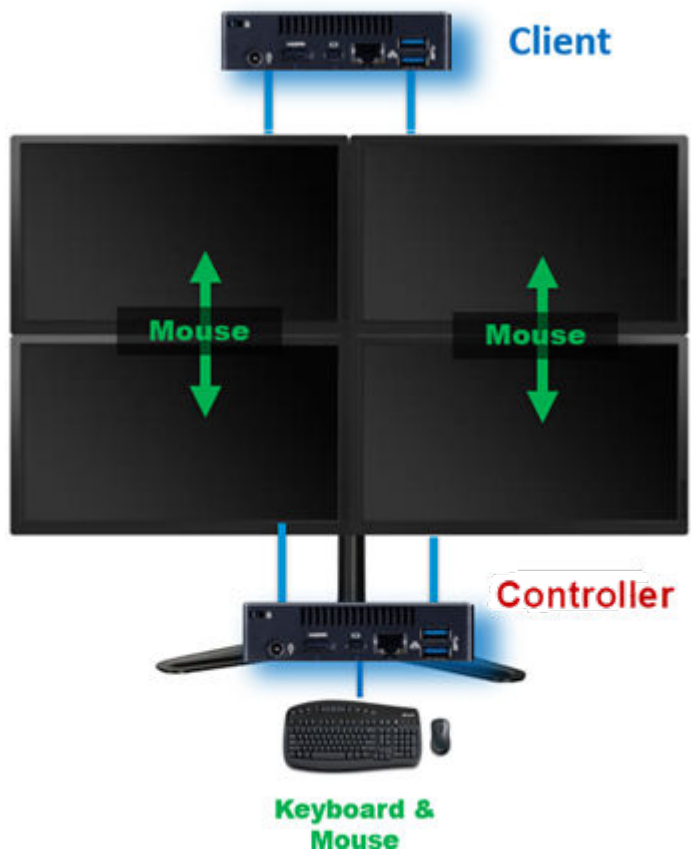
► *KX4-EUST 6 Monitors Vertical Configuration Example:*
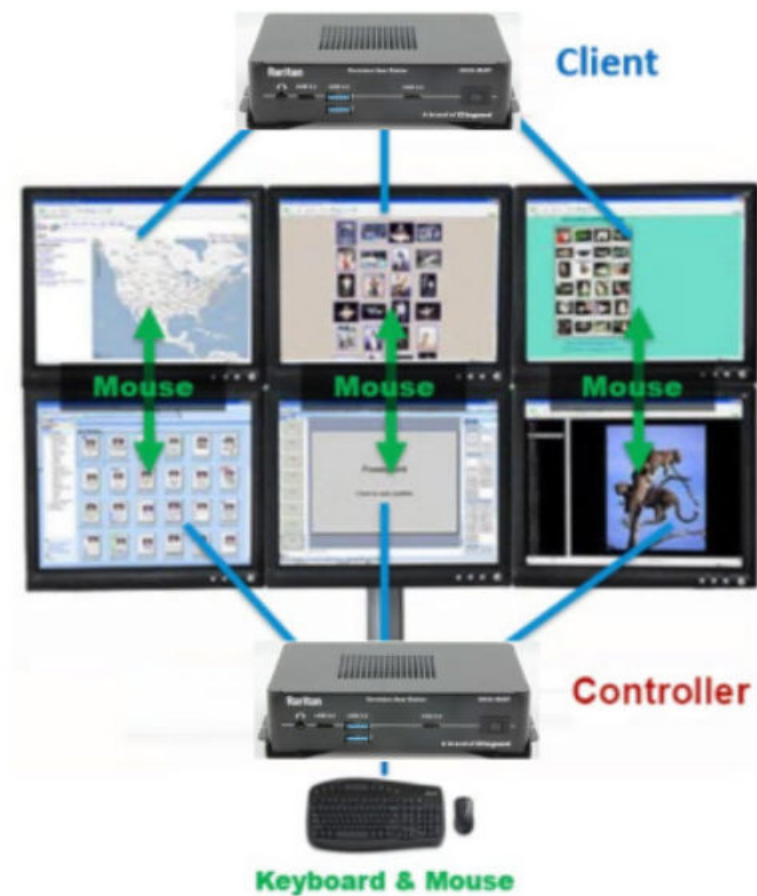
To configure, designate the Dominion User Station with the keyboard and mouse connected as "Controller". The Dominion User Stations you intend to share the keyboard and mouse with are designated as "client". For the initial configuration, connect a keyboard and mouse to each client Dominion User Station--You can remove these when the configuration is complete. Login to each client Dominion User Station to enter the controller's IP address/hostname and assign the client a unique screen name. In the controller setup, add the unique client names to the Arrangement of Screens, a grid representing the physical screen location. Screens can be added in any formation up to a 5 by 3 grid, as long as each screen has a neighbor on at least one edge. See Configuring Keyboard/Mouse Sharing (on page 251) for detailed instructions.

Once configured, the Mouse will move either horizontally or vertically from screen to screen. Each Dominion User Station can have its own extended desktop with multiple monitors, so the Mouse will move from the ends of each extended desktop. Each Dominion User Station is still independent--you cannot drag KVM Windows from one Dominion User Station to another.

► *Example Arrangement of Screens:*

The Arrangement of Screens is used to define how the mouse and keyboard moves between the screens of the Controller and Client User Stations. The mouse can move either horizontally or vertically as shown.

- Moving the Mouse to the right edge of Client5 will move to the left edge of Client1
- Moving the Mouse to the left edge of Client2 will move to the right edge of KXUS4
- Moving the Mouse to the bottom edge of Client3 will move to the top edge of Client4

Configuring Keyboard/Mouse Sharing

If you need to configure your monitors first, see Monitor (on page 28).

Controller is the Dominion User Station where the keyboard and mouse are physically connected. Clients are Dominion User Stations that will share the Controller's keyboard and mouse.

► *To configure client screens:*

1. Login to a client Dominion User Station.
2. Click Administration > Keyboard/Mouse Sharing.

3. Click Edit, then select Enabled.

4. Select Client in the Mode field.

5. Select the Share Window Layouts option to allow saved layouts to be shared among all clients in the keyboard/mouse sharing configuration.

   - Window Layouts must be created on all User Stations manually.

   - When you restore a layout on one User Station, all others restore the Window Layout with the same name.

6. Select the Automatically Log in/out Users option to automatically login/logout to all user stations connected by keyboard/mouse sharing while using the configuration.

7. In the Client Settings, enter a Screen Name to identify this client. All screens in the sharing formation must have unique names.

   - Up to 64 characters.

   - Alphanumeric characters allowed.

   - Hyphen and underscore allowed.

8. Enter the IP address/Hostname of the ControllerDominion User Station, which is where the keyboard and mouse are connected.

9. Click Save. Repeat this task for all client screens.

► *To configure the Controller:*

1. Login to the Controller Dominion User Station.

2. Click Administration > Keyboard/Mouse Sharing.

3. Click Edit, then select Enabled.

Raritan.
A brand of ☐legrand

4. Select Controller in the Mode field.

5. Select the Share Window Layouts option to allow saved layouts to be shared among all clients in the keyboard/mouse sharing configuration.

6. Select the Automatically Log in/out Users option to automatically login/logout to all user stations connected by keyboard/mouse sharing while using the configuration.

7. In the Controller Settings, enter a Screen Name to identify this Controller screen. All screens in the sharing formation must have unique names.

   - Up to 64 characters.

   - Alphanumeric characters allowed.

   - Hyphen and underscore allowed.

8. In the Arrangement of Screens fields, enter the names of this controller screen and all client screens in the position representing their location in the sharing formation.

   - Make sure the names entered here match the names in the "Screen Name" field in each client Dominion User Station's configuration exactly.

   - No duplicate names allowed.

   - Each screen must have at least one neighbor screen, either beside, above or below.

9. Click Save.

Network Storages

You can configure Network Storages in the Dominion User Station. These storages are used like USB storage to install updates, export diagnostics, or for Backup and Restore files.

Two type of storages are supported:

- NFS (Network File System)
- CIFS/SMB(Common Internet File System, Server Message Block)

You can enable the automatic mounting of the storage at the boot or can do it manually.

Note: When FIPs is enabled, the connection to CIFS/SMB shares will not work.

► *Important facts about Network Storage in Dominion User Station*

- Need administrative privileges to configure network storage.
- There are no limitations on the number of shares.
- The network share is available for all import/export operations and shows up next to the USB drive.
- Network shares are a global setting and may be used by all users.
- Event Log entries are created for creation, update, deletion of network shares

► *To configure Network Storage:*

1. Click Administration->Network Storages.
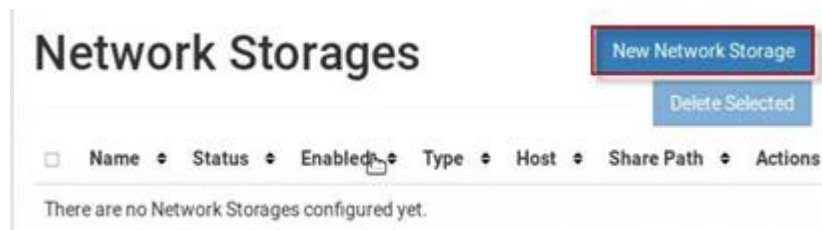
2. Click New Network Storage.

3. Enter details for New Network Storage.

- Name: Required
- Enabled: Select the checkbox to enable automatic mounting of the storage at boot, otherwise manual mounting will be set
- Type: NFS, CIFS/SMB
- Host: Required, HostName or IP Address
- Share Path: Required, /path to share
- Domain/User name/Password: These entries are optional for CIFS/SMB. These are not required for NFS

Note: For CIFS/SMB, authentication is optional. Anonymous/guest mount is used if nothing is provided.

1. Click Save.
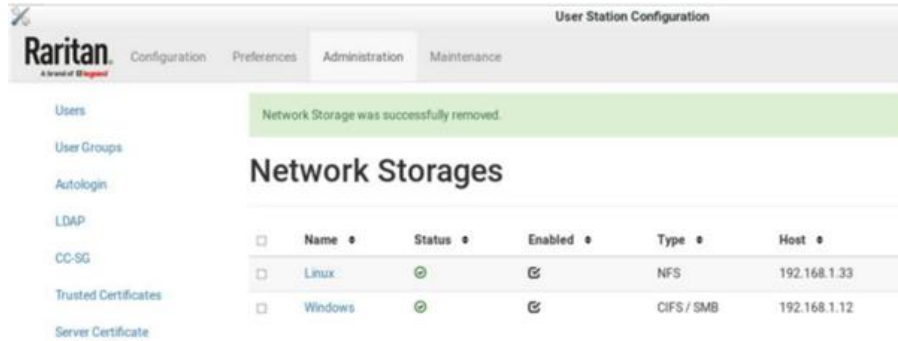
Language Settings

The Language Settings feature allows you to change the Dominion User Station GUI and system language.

- English
- French: Français
- German: Deutsch
- Chinese (Simplified): 中文(简体)
- Japanese: 日本語

After setting a new language, you must reboot to fully update the language in every area. Note that some text is not available in all languages. Language setting is part of backup and restore, but upon factory reset the language setting is English.

Chinese and Japanese input methods are not supported.

► *To change the language setting:*

1. Click Administration > Language Settings. The current language selection is listed.

2. Click Edit, then select the language from the list.

3. Click Save. You will see an immediate change in the GUI, but you must reboot the Dominion User Station to ensure a full language update.
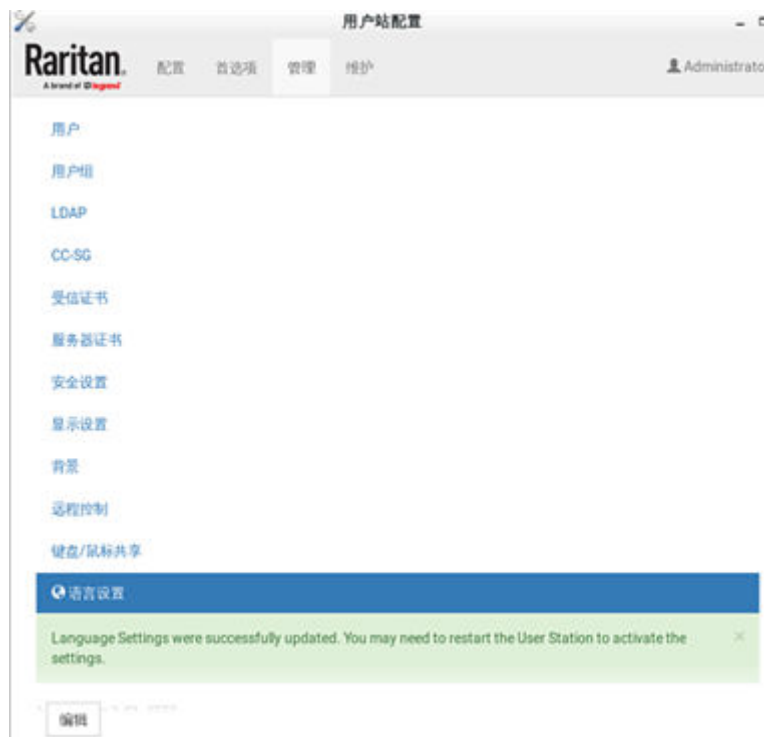
Maintenance Features

In the User Station Configuration window, click Maintenance to perform the following User Station maintenance tasks.
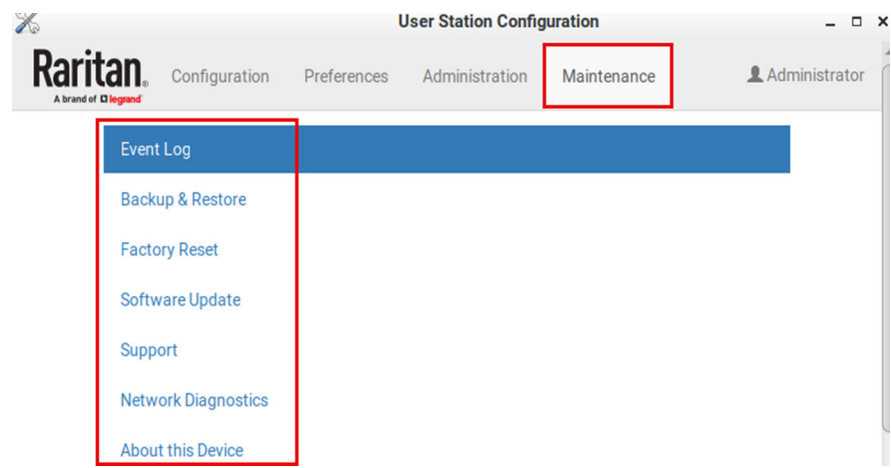
In This Chapter

Event Log

The Event Log is an application level log of activity taking place in the User Station. It records who did a certain task and when it was done. For example, login and logout, open connection to a KVM-port, updating the software and so on. The Event Log also records system incidents that cannot be shown otherwise, such as LDAP authentication and authorization processing and decisions.

The Event Log is different from the Diagnostic Log File that can be downloaded from the User Station, which contains the raw system logs that cannot be conveniently read or filtered.
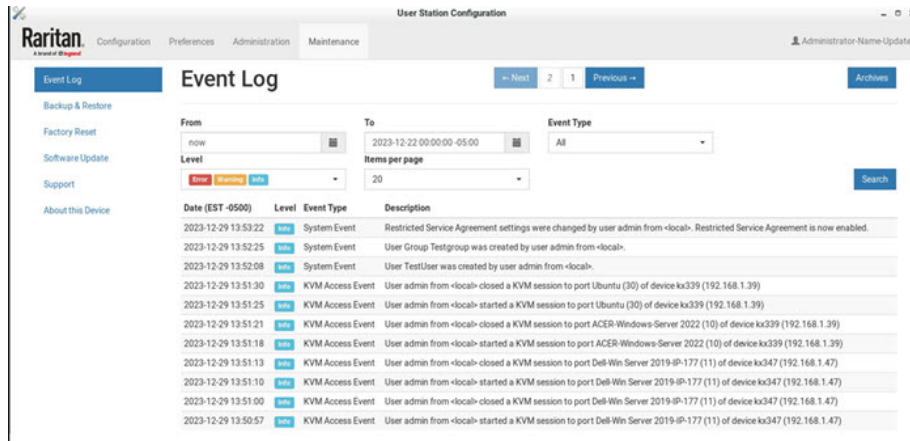
► *To search and view the Event Log:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Maintenance> Event Log. The Event Log page opens.
3. Search functions appear at the top of the screen. The most recent seven days of entries in the event log appear at the bottom of the screen.
   - Search by date: Select a date range in the From and To fields.
   - Search by Event Type: See Event Type and Description (on page 259). When Authentication is selected, you can select a user from the User field.
   - Search by Event Severity: Info, Warning, or Critical.
   - Items per Page: Select how many records to display per page of search results.
4. Click Search. The filtered list of events appears at the bottom of the search controls.

Event Type and Description

The Event Log includes the following events types.

- Authentication Events: Description includes user name, auth type (Local, LDAP or CC-SG) and from (Local or IP address).

- LDAP Events: Errors and information for LDAP authentication and authorization.

- CC-SG Events: Access of CC-SG, connections failures.

- KVM Access Events: Access of KVM ports. Description includes device, port, user name and from (Local or IP address).

- Serial Access Events: Access of Serial ports. Description includes device, port, user name and from (Local or IP address).

- RDP, SSH, VNC, Web, and ESXi Access Events: Access sessions opened and/or closed.

- System Events: Changes of the system such as adding users or KX devices.
  User and from is logged in description when applicable.

Event Log Archives

Event Log records can be archived to clear the database. Event Log archives are always created and stored inside the User Station. The file created is a compressed CSV file containing one line per record and all attributes of the record. Each record has a timestamp in UTC.

All stored archives are listed with the following details:

- date of creation
- filename: kxust-event-log-archive-<year>-<month>-<day>-<time>.gz
  - example: kxust-event-log-archive-2016-11-18-140000.gz
- size

```
Date,Level,Type,Description
2022-03-07 22:39:32 UTC,Info,System Event,System started
2022-03-07 22:40:40 UTC,Info,Auth Event,Local user admin logged in
2022-03-07 22:42:28 UTC,Info,System Event,Bulk import by user admin: 5 KX/SX Devices were imported
2022-03-07 22:45:23 UTC,Info,System Event,KX/SX Device csv line 4 (kx4185.systemtestest2.local) was updated by user admin.
2022-03-07 22:46:23 UTC,Info,System Event,CC-SG mode was enabled by user admin with CC-SG cc224.systemtestest2.local
```

You can create a manual archive at anytime. See Create an Archive (on page 260).

The Dominion User Station also automatically creates an archive if the total amount of event log records reaches a certain threshold. See Automatic Archives (on page 261).

Create an Archive

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Maintenance> Event Log. The Event Log page opens.
3. Click Archives. The Event Log Archives page opens.
4. Choose how records will be included in the archive: Age or Date
   - In the Age field: select a file age to include:
     - 1 week
     - 1 month
     - 2 months
     - 6 months
     - 1 year (default)

Raritan.
A brand of ⬛legrand

- 2 years
- 5 years
- 10 years
- Or, select "older than selected Date" to enable the Date field, and choose a specific Date in the calendar. To choose a specific time, use the clock icon on the calendar, as shown.
- All events logged older than the selected Age, or older than the selected Date will be archived.
5. Click Archive.
6. Click OK in the confirmation dialog.
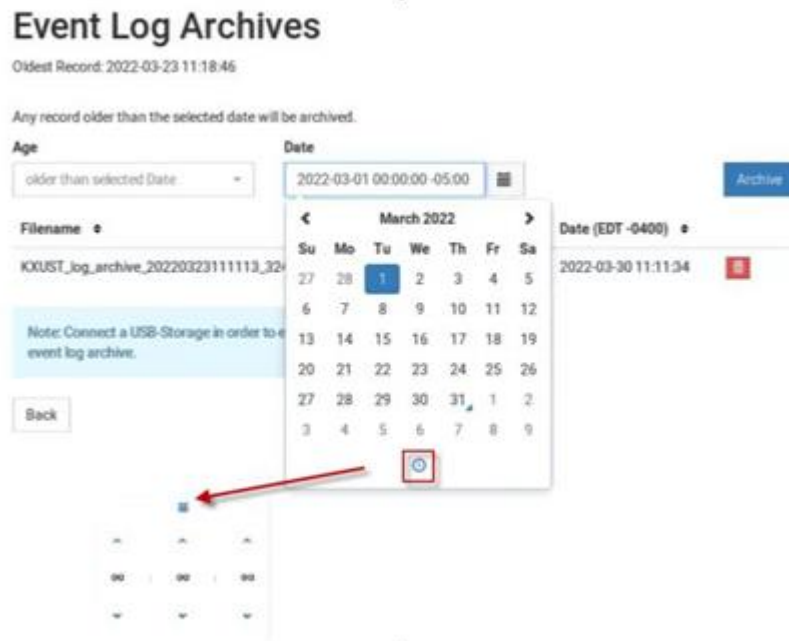
Automatic Archives

Dominion User Station will automatically create archives in cases where the database has become full of too many records.

Automatic archives are implemented with two thresholds, Warning and Critical. The thresholds are checked once per day. If thresholds are met, an error message appears in the event log. The archive is created automatically when the Critical threshold is met.

► *Warning threshold:*

A warning message displays in the Event Log page when 2 million records has been reached:

There are more than 2 Million entries in event log. Please archive event log entries or auto-archiving will be started once event log grows above 3 Million entries.

► *Critical threshold:*

The critical threshold is 3 million records. An automactic archive is created, including all log entries above the warning threshold of 2 million records. Automatic archiving doesn't trigger immediately upon reaching 3 million entries, but will run once per day

The automatic archive creation is logged in the Event Log with user name <system>

Exporting Archive Files

To export an archive file, you must connect a USB flash drive or mount a network storage to the User Station first. When the User Station detects the connected USB drive, or network storage the export button [icon] appears next to it.

1. Click the Export icon [icon] of the file you want to export to USB or network storage

Filename ⬥	Status ⬥	Size ⬥	Date (EST -0500) ⬥	
KXUST_log_archive_20230113095848_181942.zip	Done	11 KB	2023-01-20 09:58:54	[export] [delete]

2. The file is exported to the USB drive or network storage.

Deleting Archive Files

You can delete an archive file. If you want to save the file off the Dominion User Station before deleting it, see Exporting Archive Files (on page 262).

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Maintenance> Event Log. The Event Log page opens.
3. Click Archives. The Event Log Archives page opens.
4. All archive files are listed at the bottom of the page. Click the Delete icon next to the file you want to delete.

Filename ⬥	Status ⬥	Size ⬥	Date (EDT -0400) ⬥	
KXUST_log_archive_20220323111113_3248ab.zip	Done	11.2 KB	2022-03-30 11:11:34	[delete] ←

5. A confirmation message appears. Deleting cannot be undone. Click OK to delete the archive file.

Raritan.
A brand of 🔲legrand
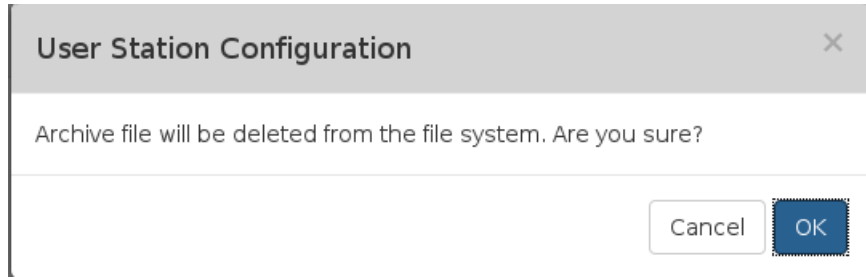
Archive File Storage

The amount of storage to keep Event Log archives inside Dominion User Station is limited. If no more storage is available, you will see an error message upon attempting to create a new archive.

The error message prompts you to delete old archive files.

You can export files to external storage before deleting, if needed. See Exporting Archive Files (on page 262).

You must delete archive files before you can create the new archive. See Deleting Archive Files (on page 262).

If the storage is full when an automatic archive must be created, the oldest archives are automatically deleted until there is enough space to write the new archive.

Deletion of each archive is logged into the Event Log

Backup and Restore

The User Station allows you to back up the latest settings and data with one click. By default, the backup files are stored in the User Station.

In case you have to restore to the previous settings and data, select the backup file you need and perform the restore command.

Note: Following system settings are NOT stored in the backup file so they CANNOT be restored.

- Network, see Network Connections - Ethernet (on page 30)
- Event Log Archives
- Backup Files

Tip: You can export or import backup files from a USB flash drive or network storage. See Exporting and Importing Backup Files (on page 265).

► *To back up the current settings and data:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Maintenance > Backup & Restore. The Backup & Restore page opens.
3. Click Create Backup.

4. Once completed, the Backup Archives page lists the backup file, with the filename, software version and file size shown on the screen.

► *To restore to the previous settings and data:*

1. If there are an existing backup files, the Backup Archives page lists all of them.
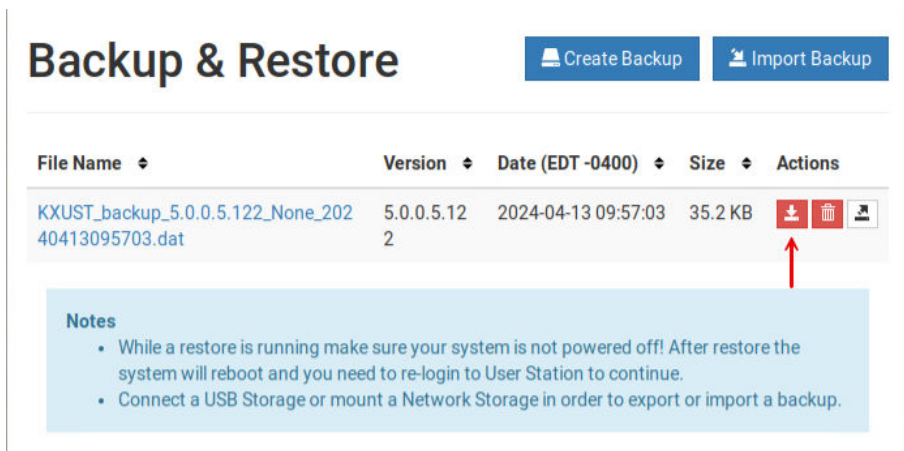
2. Determine the desired file and click the restore icon [icon] button.

Or, click the filename link to view details, and click the Restore button in the details page.

3. Click OK on the confirmation message.

4. A text screen appears to show restore progress. When restore is completed, Dominion User Station restarts and opens the login page.

Exporting and Importing Backup Files

To export or import a backup file, you must connect a USB flash drive to the User Station or configure network storage first.

► *To export backup files:*

1. Connect a USB drive formatted with any of the following file system or configure network storage.

- VFAT (FAT16, FAT32)
- NTFS
- EXT2, EXT3, EXT4
- XFS

2. Click Maintenance > Backup & Restore. The Backup & Restore page opens. When the User Station detects the connected USB drive or network storage, the export button ⬚ appears in the Actions column.

3. Click the ⬚ button of the desired backup file.

The selected file is exported to the connected USB drive/network storage and therefore listed in the "Import backup from USB or Network Storage" section.

► *To import backup files:*

 Make sure the connected USB drive or network storage contains backup files in its *root* directory.

1. Click Maintenance > Backup & Restore. The Backup & Restore page opens.
2. Click Import Backup. The Import Backup from USB or Network Storage page opens. All backup files detected are listed.

Import Backup from USB or Network Storage

Note

In order to import a backup, insert a USB Storage, such as a USB flash drive, or mount a Network Storage containing the backup file in its root directory.

USB or Network Storage	File Name	Size	Actions
Fedora	KXUST_backup_4.6.0.5.420_20230327072802.dat	139 KB	⬇

Back

3. Click the import button of the desired backup file.

The selected file is imported and shown in the Backup & Restore page.

Deleting Backup Files

To check the creation date of a backup file before removing it:

The creation date and time stamp is included as the last set of numbers in the filename, after software version and sometimes serial number. The date is expressed in 8 digits.

► *Examples:*

Backup filename with version number and date/time stamp:

`KXUST_backup_4.6.0.5.320_20240429155444.dat`

The software version is `4.6.0.5.320.` The date is `20240429`, April 29, 2024.

Backup filename with version number, serial number, and date/time stamp:

`KXUST_backup_4.6.0.5.320_22U9700018_20240429155444.dat`

► *To remove a backup file:*

1. To show existing backup files, click Administration > Backup & Restore.

2. Click the 🗑 button of the desired file.

3. Click OK on the confirmation message.

Factory Reset

The factory reset feature resets all of your User Station's settings to the factory defaults. All other customized data is removed simultaneously, including:

- All KVM switches added to the User Station
- User credentials entered for each KVM switch
- All Targets and Access Points
- Users and Groups
- "admin" user profile is recreated with factory default settings
- Built-in user groups reset to factory default settings
- All user preferences settings
- System settings
- Network storages
- Trusted certificates
- Server certificates
- Desktop background
- Backup files
- Log files

Note: To perform factory reset at startup instead of using the User Station Configuration window, see Factory Reset at Startup (on page 297).

► *To perform the factory reset:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Maintenance > Factory Reset. The factory reset page opens. Read this page before proceeding to the next step.
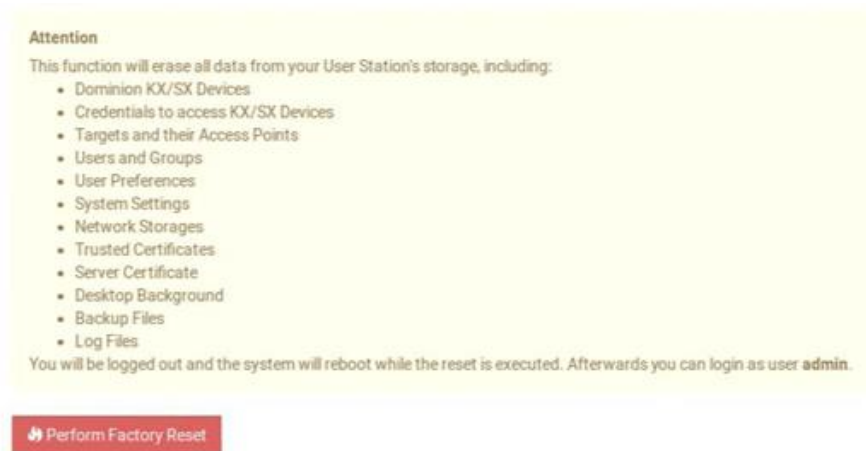
3. Click Perform Factory Reset. A confirmation message appears.
4. Click OK to confirm the operation or Cancel to abort it.

Software Update

The software update feature only permits software UPGRADE, not downgrade.

Note: To perform software downgrade, contact Raritan Technical Support for help.

To perform the software update, you must meet the following requirements:

5.0 GA is the minimum required version to upgrade to 5.1.

- You have a USB flash drive with one of the following formats, or a USB/CD-ROM/DVD-ROM drive or Network Storage containing the software update file. Supported drive formats are:
  - VFAT (FAT16, FAT32)
  - NTFS
  - EXT2, EXT3, EXT4
  - XFS
- The version of the software which you will install is equal to or higher than the software version currently running on your User Station. See About this Device (on page 275).

Important: It is strongly recommended to back up all data and settings and export to a USB drive or network storage prior to the software update. See Backup and Restore (on page 263).
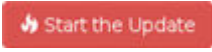
► *To perform the software UPGRADE:*

1. Use a computer to download the User Station software file from the Dominion User Station section of the Raritan website's Support page.
2. Connect the USB/CD/DVD drive or Mount the Network storage with the upgrade file.
3. On the User Station, log in as a user who has the System Administration privilege.
4. Launch the User Station Configuration window. See User Station Configuration (on page 80).

Click Maintenance > Software Update. The Software Updates page opens, with a list of software files found in the root directory of the USB/CD/DVD or Network Storage.

1. Click the desired file, and it will be analyzed. Verify the minimum required version and validity check results.
2. Click Start the Update [Start the Update] to perform the software upgrade.

Warning: Do NOT power off the User Station during the software upgrade.

3. Click OK on the confirmation message.

4. When the upgrade completes, the User Station reboots, and then the login screen is shown.

Support

The Support page provides two features that help Raritan Technical Support to troubleshoot your User Station issues.

- Support Login: This feature allows the Technical Support to remotely access your User Station.
- Log Level: This feature allows you to set the log level of the Diagnostic Log file. Note, this file is different from the Event Log.
- Diagnostic Log File: This feature downloads a diagnostic log file from your User Station, which is helpful for troubleshooting.

Support Login

The Support Login feature allows remote access from Raritan Technical Support.

By default, this feature is disabled for security.

You *MUST NOT* enable this feature unless you are instructed by Raritan Technical Support to do so.

► *To permit remote access from Raritan Technical Support:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).

2. Click Maintenance > Support. The Support page opens.

In the Support Login section:

- ☑ indicates the setting is enabled.

- ☐ indicates the setting is disabled.
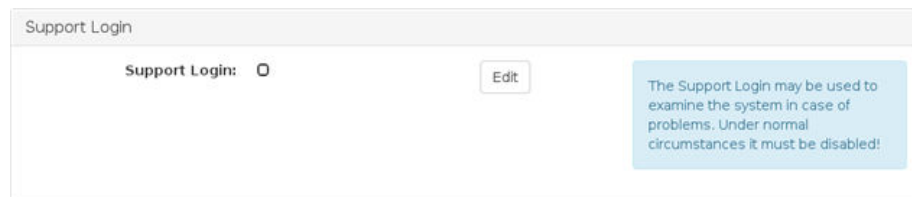
3. Click Edit.

4. Select the Support Login checkbox.

5. Click Save.

6. Provide your User Station's IP address to Raritan Technical Support.

   - To retrieve the IP address(es), right-click the network icon in the Main Toolbar to select Connection Information. See Network Icon (on page 50).

Important: Disable this feature immediately after Raritan Technical Support finishes the troubleshooting task.

Log Level for Diagnostic Log Files

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).

2. Click Maintenance > Support. The Support page opens.

3. Click Edit.

4. In the Log Level section, select which logs to include in the diagnostic log file.

Note: Selecting Debug may affect system performance.
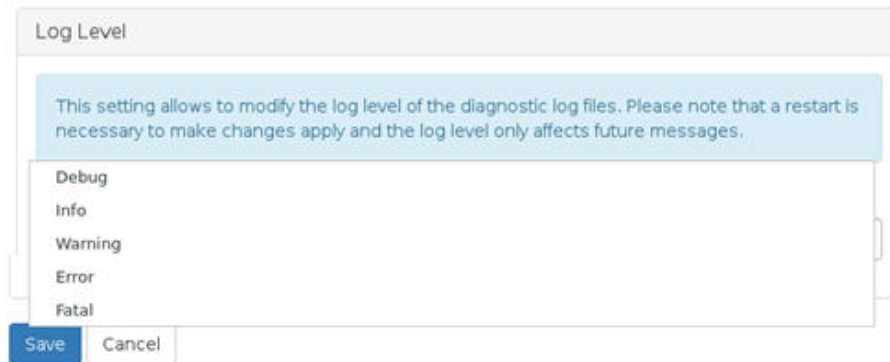
5. Click Save. Click OK in the confirmation message to set the level and restart the Dominion User Station.

Diagnostic Log File

When the User Station does not work properly, you can export the User Station's diagnostic log file to a connected USB flash drive or to a mounted network storage, and send the file to the Raritan Technical Support for troubleshooting.

You must have the System Administration permission to perform this operation.

Note: The Diagnostic Log File is different from the Event Log. See Event Log.

► *To download the diagnostic log from the User Station:*

1. Make sure your User Station has a USB drive connected or network storage mounted.

2. In the User Station Configuration window, click Maintenance > Support.

3. Select the USB drive or network storage from the drop-down list, and click "Export to" to export the diagnostic log.

Diagnostic Log File

This allows the export of diagnostic log files to a connected USB Storage or mounted Network Storage for sending to Raritan Support. Please do not remove the USB Storage during export!

Export to

4664-9FEF ▼

4. Wait until the User Station finishes the export, displaying the "Successfully finished" message as well as the filename of the diagnostic log.

Diagnostic Log File

This allows the export of diagnostic log files to a connected USB Storage or mounted Network Storage for sending to Raritan Support. Please do not remove the USB Storage during export!

Export to

4664-9FEF ▼

✔ Successfully finished:
KXUST_diagnostics_20230120101124.dat copied to external Storage 4664-9FEF.

5. Send the file to Raritan Technical Support.

Network Diagnostics

The Dominion User Station provides information about the status of your network interfaces. To get specifics of one of the interfaces you can ping, trace route or perform a DNS inquiry as follows:

► *To view information about your network interface:*

Ping Host:

1. Choose Maintenance > Network Diagnostics. The Network Diagnostics page opens.
2. Enter Host name or ipaddress.
3. Select "Use IPV6" option if want to use IPv6.
4. Click Run. The relevant information is displayed as shown below:

Raritan.
A brand of ⬛legrand

Ping Host

Host   192.168.62.89

Use IPv6   ☐

Run

PING 192.168.62.89 (192.168.62.89) 56(84) bytes of data.
64 bytes from 192.168.62.89: icmp_seq=1 ttl=128 time=16.1 ms
64 bytes from 192.168.62.89: icmp_seq=2 ttl=128 time=18.8 ms
64 bytes from 192.168.62.89: icmp_seq=3 ttl=128 time=22.7 ms
64 bytes from 192.168.62.89: icmp_seq=4 ttl=128 time=16.2 ms
64 bytes from 192.168.62.89: icmp_seq=5 ttl=128 time=15.1 ms

--- 192.168.62.89 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 15.076/17.776/22.714/2.753 ms

Trace Route to Host:

1. Choose Maintenance > Network Diagnostics. The Network Diagnostics page opens.

2. Enter Host name or ipaddress.

3. Select "Use IPV6" option if want to use IPv6.

4. Select "Use ICMP packets" if you want to see ICMP format.

5. Click Run. The relevant information is displayed as shown below:

Trace Route to Host

Host   192.168.62.89

Use IPv6   ☐
Use ICMP packets   ☑

Run

traceroute to 192.168.62.89 (192.168.62.89), 30 hops max, 60 byte packets
1 _gateway (192.168.75.2) 0.229 ms 0.153 ms 0.154 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *

DNS Lookup:

Raritan.
A brand of 🔲 legrand

1. Choose Maintenance > Network Diagnostics. The Network Diagnostics page opens.
2. Enter Host name or ipaddress.
3. Click Run. The relevant information is displayed as shown below:

DNS Lookup

Host   google.com

Run

Server: 192.168.75.2
Address: 192.168.75.2#53

Non-authoritative answer:
Name: google.com
Address: 142.250.72.174
Name: google.com
Address: 2607:f8b0:4007:819::200e

Network Diagnostics also list the current TCP connections and TCP/UDP listen Sockets, which can be refreshed by clicking the Refresh button.

List TCP Connections

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
ESTAB	0	0	192.168.75.128:53564	192.168.53.129:5000
ESTAB	0	0	192.168.75.128:48836	192.168.62.89:5000
ESTAB	0	0	192.168.75.128:53552	192.168.53.129:5000
ESTAB	0	0	192.168.75.128:48840	192.168.62.89:5000
ESTAB	0	0	[::1]:39448	[::1]:8000
ESTAB	0	0	[::1]:8000	[::1]:56644
ESTAB	0	0	[::1]:56644	[::1]:8000
ESTAB	0	0	[::1]:8000	[::1]:39448

Refresh

List TCP/UDP Listen Sockets					
Netid	**State**	**Recv-Q**	**Send-Q**	**Local Address:Port**	**Peer Address:Port**
udp	UNCONN	0	0	0.0.0.0:111	0.0.0.0:*
udp	UNCONN	0	0	[::]:111	[::]:*
tcp	LISTEN	0	500	127.0.0.1:41243	0.0.0.0:*
tcp	LISTEN	0	511	0.0.0.0:8000	0.0.0.0:*
tcp	LISTEN	0	511	[::]:8080	[::]:*
tcp	LISTEN	0	511	[::]:8000	[::]:*
tcp	LISTEN	0	244	[::1]:5432	[::]:*
tcp	LISTEN	0	4096	[::]:111	[::]:*
tcp	LISTEN	0	128	[::]:22	[::]:*

Refresh

About this Device

The "About this Device" page shows the firmware version i, Model number, and Mac Addresses. You can access this page from the Main Menu or the User Station Configuration window.

- In the User Station Configuration window, click Maintenance > About this Device.
- In the Main Menu, choose Help > About this Device.

Specification

Specification DKX3-UST, DKX4-UST, DKX3-EUST

Chassis design	Slim 1.3 liter metal chassis, black
Dimension (LxWxH)	190 x 165 x 43 mm
Operating temperature	0 to 40 degrees Celsius
Humidity	non-condensing: 10~90%
VESA mount	• 75 x 75 mm • 100 x 100 mm
Video	• 1 x HDMI • 2 x DisplayPort • Support video resolutions up to 3840 x 2160 up to 60 Hz
I/O ports	• 1 x SD card reader (available only on some devices. DKX3-EUST and some DKX3-UST devices have no SD card slot) • 2 x Audio (Line out, mic) • 4 x USB front and 4 x USB rear • 2 x Gigabit LAN (RJ-45), supports WOL, PXE • 2 x COM ports (RS-232 + RS-232/RS-422/RS-485)
Power supply	External 90W fanless power adapter

Specification DKX4-EUST:

Chassis design	Slim 0.6 liter metal chassis, black
Dimension (LxWxH)	130mm x 109.25mm x 40mm
Operating temperature	-4°F ~ 140°F (-20°C ~ 40°C), according to IEC68-2 with 0.5 m/s AirFlow (w/ Industrial wide Temp. SSD/RAM)
Humidity	5 ~ 95% @ 40C, non-condensing
VESA mount	• 75 x 75 mm • 100 x 100 mm
Video	• 1 x HDMI • 1 x DisplayPort • 2 x USB-C • Support video resolutions up to 3840 x 2160 up to 60 Hz

Raritan

A brand of Legrand

I/O ports	• 1 x Line out and can have USB and Monitor audio also Front: • 2 x USB 3.2 Gen2 (Type A) • 2 x USB 3.2 Gen2 (Type C, Supports DP1.2a display output) Back: • 2 x USB 2.0 • 1x 1 GBit and 1x 2.5 GBit Ethernet
Power supply	65W, ADAPTER

API

In This Chapter

Session Management

Session Creation and Login

In order to use the API, users need to authenticate and create a session. The first step is always a POST to /session/login with the user credentials.

Parameters

- user name: The login name of the user. Required.
- password: The user's password. Required.
- user type: The type of the user. Optional. May be one of
  - "local" (users existing in the User Station only)
  - "ldap" (LDAP authenticated users) or
  - "ccsg" (CC-SG users).
  - If not specified, local user is assumed.

Raritan.
A brand of ◻ legrand

Response

- result: The result of the authentication process. One of:
  - success: The authentication was successful and the user is logged in. The session can be used immediately for further operations.
  - failed: The authentication failed. Either the given credentials are incorrect, or the user type is incorrect (for example, ccsg is specified, but CC-SG mode is not enabled).
- in_progress: The authentication was successful, but the user is not logged in immediately. Instead, the login process is started and takes some time. There is another responsevalue "auth_id" which can be used to wait for the login process to finish. Use a POST to the URL /session/progress to query the login process's status.

NOTE: You cannot use this session for further requests until the login process is finished *and* you requested this finished state via /session/progress.

- auth_id: The ID of the login process. Only used if "result" is "in_progress" and needs to be used for /session/progress to query the login process's progress.

Login Progress

If the login proces is started asynchronously and the /session/login call returned "in_progress" and result, it is required to wait until the login process in finished before making any further API calls. It is required to request the status of the login process until it is signalled to be finished. Use the /session/progress call to get the status.

Parameters

- auth_id: The authentication ID returned by a call to /session/login.

Response

- progress: The current status/progress of the login process. One of:
  - unknown: The auth_id is invalid, or the login process was not able to start correctly.
  - initializing: The login process is about to start.
  - started: The login process has started, but is not finished yet.
  - done: The login process is finished. From now on, you may use this session for further API requests.

Session Close / Logout

When the remote API session is not needed anymore, it should be closed. When the session is closed, the user is logged out of the User Station. Use a request to `/session/logout` to achieve this.

Parameters

* none

Response

* result: A boolean value. True is the logout was successful, false otherwise (e.g. the user was already logged out of other reasons).
* error: Optional. An error if the result is false.

Example

* First, start the login process:

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "user name":"admin", "password":"raritan", "user_type": "local"}' https://192.168.3.175:8443/api/v1/session/login

{"result":"in_progress","auth_id":"4dc950f2-2f8b-424b-ba31-d6fb33f943b7"}

* Wait for the login process to end:

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{ "auth_id":"4dc950f2-2f8b-424b-ba31-d6fb33f943b7"}' https://192.168.3.175:8443/api/v1/session/
progress

{"progress":"started"}

* Now wait some seconds

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{ "auth_id":"4dc950f2-2f8b-424b-ba31-d6fb33f943b7"}' https://192.168.3.175:8443/api/v1/session/
progress

{"progress":"done"}

* Now, use the session for further request.
* Close the session and logout:

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/session/logout

```
{"result":true}
```

- The user is loged out, the session is closed.

Access Functionality

Get Devices and Targets

The User Station supports two views on target systems:

- Access Device centric view: There are access devices, each device has one or more ports to connect to the target systems.
- Targets view: There are targets, each of them has one or more ways (access points) to access it.

For both views, there are ways to enumerate the access methods.

Get Devices and Ports

In order to get all access devices with their ports, send a GET request to the /access/items URL. The result is an array of items (access devices) with all ports of the device. Some of the ports may not be accessible (either due to missing permissions, or if a port is unsupported). Also, a device may have multi-monitor port groups. In that case, the single ports are not accessible, but the port groups are.

Each of the items has the following members:

- id: The ID of the item.
- name: The name of the item.
- ports: An array of ports (see below)
- port_groups: An array of multi-monitor port groups (see below)

Each of the ports in the ports array has the following properties:

- id: The ID of the port
- name: The name of the port
- port_type: The type (KVM, Serial or unsupported port type)
- status: The port status of the port associated with this access point (KVM access points only)
- availability: The availability status s of the port associated with this access point (KVM access points only)
- access_id: The ID of the access point, belonging to this port. Use the ID to create an access session to this access point of this port. If this port is not accessible, the this property is missing.

Each of the port groups in the port_groups array has the following properties:

- id: The ID of the port group
- name: The name of the port group
- port_ids: an array of port IDs forming this port group
- access_id: The ID of the access point, belonging to this port group. Use the ID to create an access session to this access point of this port group. If this port group is not accessible, the this property is missing.

► *Example*

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/access/items
```

```
{

"items": [

{

"id":1,

"name":"thre-KX3",

"ports": [

{"id":6,"name":"thre-Mac-mini","status":"up","availability":"idle","port_type":"kvm","access_id":5},

{"id":1,"name":"Local Port (DVI)","status":"up","availability":"idle","port_type":"kvm","access_id":2},

{"id":2,"name":"Windows Box (Dual-
VM)","status":"up","availability":"idle","port_type":"kvm","access_id":777},

{"id":833,"name":"DSAM4 Port
1","status":"down","availability":"idle","port_type":"serial","access_id":1255},

{"id":834,"name":"DSAM4 Port
2","status":"down","availability":"idle","port_type":"serial","access_id":1256},

{"id":8,"name":"thre-KX3UST","status":"up","availability":"idle","port_type":"kvm","access_id":7},

{"id":7,"name":"thre-KX4UST","status":"up","availability":"idle","port_type":"kvm","access_id":6},

{"id":3,"name":"Windows Box Multi-Monitor 1","status":"up","availability":"idle","port_type":"kvm"},

{"id":4,"name":"Windows Box Multi-Monitor 2","status":"up","availability":"idle","port_type":"kvm"},

{"id":5,"name":"Windows Box PS/2","status":"up","availability":"idle","port_type":"kvm","access_id":4}

],

"port_groups": [

{"id":1,"name":"Windows Box Dual","port_ids":[3,4],"access_id":8}

]

},

{
```

```
"id":594,

"name":"DKX4-101",

"ports": [

{"id":472,"name":"Dominion_KX4_Port1","status":"up","availability":"idle","port_type":"kvm","access_id":770}

],

"port_groups": []

}

]

}
```

Get Targets and Access Points

In order to get all targets and their access points, send a GET request to the /access/targets URL. You will retrieve an array of targets. Each target has an ID, a name and an array of Access Points. Each of the Access Points have an access ID (required to launch a target connection to this access point) and a type (KVM, Serial, SSH, VNC, etc.). The KVM and Serial targets which represent a port of a access device also have a status (up or down?) and an availability setting.

The call returns an array of targets. Each target has the following members:

- id: The ID of the target.
- name: The name of the target.
- access: An array of access points to this target (see below).

Each of the access points has the following members:

- access_id: The ID of this access point. Use the ID to create an access session to this access point of this target.
- access_type: The type of this access point (KVM, Serial, RDP, VNC, etc.). The "multi_kvm" type refers to a pre-configured multi monitor target on the access device, "virt_multi_kvm" is a virtual multi monitor target configured on the User Station.
- status: The port status of the port associated with this access point (KVM access points only)
- availability: The availability status s of the port associated with this access point (KVM access points only)

► *Example*

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/access/targets

{

"targets": [

{"id":2,"name":"Local Port (DVI)","access":
[{"access_id":2,"access_type":"kvm","status":"up","availability":"idle"}]},

{

"id":3,

"name":"Windows Box (Dual-VM)",

"access":[

{"access_id":19,"access_type":"ssh"},

{"access_id":20,"access_type":"vnc"},

{"access_id":21,"access_type":"rdp"},

{"access_id":22,"access_type":"web"},

{"access_id":23,"access_type":"esxi"},

{"access_id":777,"access_type":"kvm","status":"up","availability":"idle"},

{"access_id":781,"access_type":"virt_multi_kvm","status":"up","availability":"idle"}

]

},

{"id":4,"name":"Windows Box PS/2","access":
[{"access_id":4,"access_type":"kvm","status":"up","availability":"idle"}]},

{"id":5,"name":"thre-Mac-mini","access":
[{"access_id":5,"access_type":"kvm","status":"up","availability":"idle"}]},

{"id":6,"name":"thre-KX4UST","access":
[{"access_id":6,"access_type":"kvm","status":"up","availability":"idle"}]},

{"id":7,"name":"thre-KX3UST","access":
[{"access_id":7,"access_type":"kvm","status":"up","availability":"idle"}]},

{"id":8,"name":"Windows Box Dual","access":
[{"access_id":8,"access_type":"multi_kvm","status":"up","availability":"idle"}]},

{"id":993,"name":"DSAM4 Port 1","access":
[{"access_id":1255,"access_type":"serial","status":"down","availability":"idle"}]},

{"id":994,"name":"DSAM4 Port 2","access":
[{"access_id":1256,"access_type":"serial","status":"down","availability":"idle"}]},

```
{"id":595,"name":"Dominion_KX4_Port1","access":
[{"access_id":770,"access_type":"kvm","status":"up","availability":"idle"}]},

]

}
```

Handling of Access Client Sessions

Create Access Client Sessions

Access Clients (KVM, VNC, RDP, SSH, etc.) can be opened and closed via API.

To open an Access Client session, POST to the /access/open_client URL. This call has the following parameters:

- access_id (required): The Access Poinjt ID. In order to get the ID, see above (Get Devices and Targets).
- options (optional): An array of key/value pairs to configure the session. See the API description for a list of available options.
- audit_message (optional): A message for the audit log. Currently used for CC-SG connections only.

► *Examples*

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "access_id": 2 }' https://
192.168.3.175:8443/api/v1/access/open_client

{"result":true}

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "access_id": 2, "options":
[ { "key": "current", "value": "true" } ] }' https://192.168.3.175:8443/api/v1/access/open_client

{"result":true}

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "access_id": 2, "options":
[ { "key": "fullscreen", "value": "false" }, { "key": "x", "value": "1200" }, { "key": "y", "value": "800" },
{ "key": "width", "value": "300" }, { "key": "height", "value": "200" }, { "key": "scale", "value": "true" } ] }'
https://192.168.3.175:8443/api/v1/access/open_client

{"result":true}
```

Close Access Client

In order to close an Access Client session, POST to the /access/close_client URL. This call has one parameter: the Access Point ID. In order to get the ID, see above (Get Devices and Targets).

► *Example*

```
curl -c cookies.txt -b cookies.txt --H "Content-Type: application/json" -d '{ "access_id": 2 }' https://
192.168.3.175:8443/api/v1/access/close_client
```

{"result":true}

Named Scenes (aka Window Layouts)

Named Scenes (or Window Layouts) are collections of Access Client windows which can saved and restored with all their positions and sizes. With the API, users can currently get a list of available scenes, and they can restore (or open) a scene. It is not possible to create new scenes or overwrite existing scenes currently.

► *Get a list of scenes*

To get a list of scenes, use a GET request to the /access/scenes URL. The API will return an array of scenes. Each scene has an ID (member "id") and a "name". One of the scenes may be the active one (the "is_active" member is true for this scene).

► *Example*

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/access/scenes

{"named_scenes":[{"id":22,"name":"Window Layout 1","is_active":false},{"id":23,"name":"Window Layout 2","is_active":true}]}

Restore a Named Scene

To restore a Named Scene, POST to the /access/open_scene URL. This request has 2 parameters:

● scene_id (required): The ID of the scene. To get the ID of a scene, see above (Get a list of scenes).
● audit_message (optional): A message for the audit log. Currently used for CC-SG connections only.

► *Example*

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "scene_id": 23 }' https://192.168.3.175:8443/api/v1/access/open_scene

{"result":true}

Window Management

The User Station API allows some special Window Management functions to arrange or close Access Client windows. To perform such an operation, POST to the /access/window_management URL. This call has one parameter: the operation to perform. This may be one of the following:

● tile: Arrange the windows in tiles.
● untile: Un-do the latest "tile" operation.
● minimize: Minimize all windows
● unminimize: Restore the windows
● close: Close all client windows

► *Example*

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "operation": "close" }' https://
192.168.3.175:8443/api/v1/access/window_management
```

```
{"result":true}
```

Maintenance

The User Station supports some basic maintenance functions via the API. It currently has functions for identity, firmware information and update and settings backup/restore.

Note: The firmware update and backup/restore functionality requires System Administration privileges.

Identity Information

In order to get some basic identity information, use a GET request to the /maintenance/identity URL. You will get the product code, the vendor, the device's serial number and the MAC addresses.

► *Example*

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/identity
```

```
{"product":"DKX4-UST","vendor":"Raritan Inc.","serial":"12345","mac":
["80:EE:73:E2:31:45","80:EE:73:E2:31:46"]}
```

Firmware Operations

► *Software Versions*

To retrieve some informations about the firmware versions, send a GET request to the /maintenance/firmware URL. The resulting object contains the versions of the installed firmware, the underlying operating system and the Linux kernel version.

► *Example*

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/firmware
```

```
{"firmware_version":"4.4.0.5.85.20210323123034","base_os_version":"CentOS Linux release 7.9.2009
(Core)","kernel_version":"Linux 3.10.0-1160.6.1.el7.x86_64"}
```

Firmware Update

To perform a software upgrade, use a POST request to the /firmware/upgrade URL. This request has one parameter: the URI of the firmware file. The User Station will download this firmware upgrade file and apply it, if it is a valid update image. This call returns a boolean result, whether the update was initiated successfully or not. In case of an error, an error string is also returned.

Raritan.
A brand of ❑legrand

Note: Importing the firmware upgrade is done synchronously. Especially the download, but also the unpacking, will take some seconds to complete. Also, this API call just initiates the upgrade. Once the import is complete and the upgrade file is valid, this API function returns and the actual upgrade is done in background. API users have no control over the actual upgrade process. When the upgrade process is done, the User Station will automatically reboot.

► *Example*

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "uri":"https://192.168.2.101/KXUST_4.4.0.1.50_update.bin" }' https://192.168.3.175:8443/api/v1/maintenance/firmware/upgrade

{"result":false,"error":"The provided software version is too old! It must be equal or newer than the current version."}

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "uri":"https://192.168.2.101/KXUST_4.4.0.1.98_update.bin" }' https://192.168.3.175:8443/api/v1/maintenance/firmware/upgrade

{"result":true}

Backup/Restore

With the User Station Remote API, you can access system backup files. You can list all backups available in the system, you can download or upload them, you can restore or delete backups.

► *Get all backups in the system*

In order to get a list of all backup files currently available in the system, use a GET request to the /maintenance/backups URL.

The response is an array "backups" with all backups in the system. Each entry has the following members:

- id: The ID of the backup.
- filename: The name of the file internally representing this backup.
- status: The current status of the update. Since updates are created asynchronously, the creation of a backup may not be finished yet when you retrieve it. The following values are possible:
- initialized: The backup has just been started. It is not created yet.
- working: The backup process has started, but is not finished yet.
- complete: The backup is finished and can be used.

► *Get one backup in the system (metadata only)*

If you are interested in one backup only (e.g. if you are waiting for the backup process to finish), you don't have to query the whole list of backups. When you know the ID of a backup, you can GET this backup's metadata only by sending a GET request to the /maintenance/backups/<id_of_the_backup> URL.

The response is similar to the list above, but only one backup is returned.

Raritan.
A brand of ▢legrand

► *Get the content of one backup file*

To get the binary file data of a backup file, use a GET request to the /maintenance/backups/ <id_of_the_backup>/content URL. this call returns the data in form of a Base64 encoded string (or an error in case something went wrong).

► *Delete a backup in the system*

To delete a backup in the system, use a GET request to the /maintenance/backups/ <id_of_the_backup>/destroy URL. The call returns the result of the operation and an error string in case there was an error.

► *Create a new backup*

If you want to create a new backup of the system at the state it is currently in, then use a GET request to the /maintenance/backups/new URL. This returns the result (success or fail), the ID of the new backup (if successful) or an error string if something went wrong.

You can use the ID returned by this call for later use of the backup, e.g. you can downlaod it later. Please note that the backup is created in the background and cannot be used immediately. Please request the details of this backup until the state property changes to "complete".

► *Import a backup file*

There is also the possibility to upload or import backups into the system. Use a POST request to the /api/v1/maintenance/backups/import URL.

You can either upload the file directly (using a Base64 encoded string) (use the "content" parameter), or an URL can be specified (use the "uri" parameter), where the User Station downloads the backup file from. This returns the result (success or fail), the ID of the new backup (if successful) or an error string if something went wrong.

Please note that you cannot have the same backup file more than once in the system. Uploading a backup which already exists will fail.

► *Restore a backup*

To restore a backup, use a GET request to the /maintenance/backups/<id_of_the_backup>/restore URL. This returns the result (success or fail) and an error message in case of failure.

Please note that this call only initiates the resrore process. The main work of restoring a backup is done in background, with shut down web services. It is not possible to see the progress or status of the restore process. When this call returns "success", this means the restore was successfully started. But it does not mean, the backup was successfully restored.

► *Example*

- First, get a list of all backups in the system.

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups

{

"backups": [

{ "id":11,"filename":"KXUST_backup_4.4.0.5.85.20210324092030_12345_20210325104406.dat","status":"complete" },

{ "id":10,"filename":"KXUST_backup_4.4.0.5.85.20210324092030_12345_20210325104402.dat","status":"complete" }

]

}

- Delete the existing backups.

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/10/destroy

{"result":true}

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/11/destroy

{"result":true}

- Get the list again, which is now empty.

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups

{"backups":[]}

- Create a new backup

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/new

{"result":true,"backup_id":12}

- Now query the state of this backup

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/12

```
{"backup":
{"id":12,"filename":"KXUST_backup_4.4.0.5.85.20210324092030_12345_20210325104912.dat","status":"working"}}
```

- The backup is not finished yet (status is "working"), wait some time and try again.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/12
```

```
{"backup":
{"id":12,"filename":"KXUST_backup_4.4.0.5.85.20210324092030_12345_20210325104912.dat","status":"complete"}}
```

- The backup is now complete. Download it to a file.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/12/content > backup.txt
```

```
{"content":{"[...]"}}
```

- Delete the backup.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/12/destroy
```

```
{"result":true}
```

- Upload the backup again.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d "@backup.txt" https://
192.168.3.175:8443/api/v1/maintenance/backups/import
```

```
{"result":true,"backup_id":13}
```

- Wait until the status of this backup is "complete".

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/13
```

```
{"backup":
{"id":12,"filename":"KXUST_backup_4.4.0.5.85.20210324092030_20210325104912.dat","status":"complete"}}
```

- Or: Import the backup using an URL.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "uri":"http://192.168.2.101/
backup.bin" }' https://192.168.3.175:8443/api/v1/maintenance/backups/import
```

```
{"result":true,"backup_id":13}
```

- Now restore this backup.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://
192.168.3.175:8443/api/v1/maintenance/backups/13/restore
```

{"result":true}

- The backup is restored in background. The User Station reboots when finished.

BIOS Settings

A reduced number of BIOS settings are available in Dominion User Station, compared to a regular PC. A few settings may be changed to allow for troubleshooting (boot order), power management, and security.

Entering the BIOS

► *To enter the BIOS:*

1. Reboot or Power On the Dominion User Station.
2. In the first Raritan screen, press the Del key.

BIOS Settings

► *Main*

Includes an overview about the installed hardware: Processor, RAM, BIOS version.

System date and time can be changed.

Advanced Settings

► *Power Management*

- Suspend Mode: Not Supported.
- Wake Up by USB: Not Supported.

- EuP Function: Enable automatic energy management.
  - Enabled: Maximum energy savings.
  - Disabled: Custom energy settings can be set.

The following settings can only be changed if EuP is disabled.

- Power-On after Power-Fail: Choose the power state to be applied after power loss (on, of, last state).
- Wake Up by Ring: Allow waking up the User Station via modem. Not supported on DKX4-UST models.
  - See https://en.wikipedia.org/wiki/Wake-on-ring for details.
- Wake Up by LAN: Allow waking up the User Station via LAN.
  - https://en.wikipedia.org/wiki/Wake-on-LAN
- PowerOn by RTC Alarm: Configure a time (hour, minute, second) at which the User Station is powered on automatically.

Raritan.

A brand of ▢legrand

► *Boot*

Boot Settings are used for troubleshooting only, such as if a new OS installation is required.

You can change the boot order, including hard drive priority and USB drive priority.

Default is to boot from the internal disk only

► *Security*

- Set or clear a BIOS password. This is useful to prevent users from entering the BIOS.

  _____
  It is recommended to set a BIOS password!
  _____

  _____
  Important: Do not forget the BIOS password!!!
  _____

- Flash Write Protection: Do not change this. Used for BIOS updates.

► *Save & Exit*

Save or discard the changed BIOS settings.

Load default BIOS values.

Authentication of User Stations and KVM/Serial Switches

User credentials you use to log in to the Dominion User Station can be different or identical to the user credentials you enter for accessing the port information of any KX III KVM or SX Serial switch.

► *User Station's user credentials:*

User credentials for logging in to the User Station determine the tasks/permissions you are allowed to perform on the User Station, but not the tasks/permissions you can perform on KVM/Serial switches and KVM/Serial ports.

For example, user credentials of the User Station determine whether you can add or remove the data of KVM/Serial switches, or whether you can back up and restore the User Station settings.

For detailed information on what you can do on a User Station, see .

► *KVM/Serial Switch's user credentials:*

User credentials entered for KVM/Serial switches determine the tasks/permissions you are allowed to perform while accessing computer devices connected to KVM ports (that is, target servers).

For example, user credentials for the KVM/Serial switch determine whether you can access all KVM/ Serial ports on this KVM/Serial switch, or whether you can perform the virtual media or power control function on a KVM/Serial port/target server.

This is why users of the User Station CANNOT share user credentials of KVM/Serial switches, and each user must enter and save his or her own user credentials for KVM/Serial switches respectively. See Editing KVM and Serial Switches (on page 84). However, if LDAP is enabled, and you can add your KVM/ Serial switches with a special setting that makes single sign-on possible. See Adding KVM and Serial Switches (on page 81), and also check the LDAP help for more details. See LDAP (on page 202).

For detailed information on what you can do with a KVM/Serial port/target server, see the user documentation for KX III KVM or SX Serial switches, which is accessible from the KVM/Serial switch's application or KX III/SX section of Raritan website's Support page.

► *Examples:*

The following table illustrates different combinations of user credentials for User Stations and KVM switches.

User account for the User Station	Tasks you can do on the User Station	User account for the KVM switch	Tasks you can do on a KVM port/ target server
admin	You can do anything, including: • System administration, such as backup or software update. • Device administration, such as adding KVM switches. • Device access, such as access to the data of all KVM switches and KVM ports.	user-A	Limited privileges are granted: • Port access permitted. • No virtual media access permitted. • No power control permitted.
user-1	Limited privileges are granted: • Device access permitted. • No device administration permitted. • No system administration permitted	admin	You can do anything, including: • Port access. • Virtual media access. • Power control permitted.
admin	You can do anything. See above.	admin	You can do anything. See above.

Raritan.
A brand of ⬛legrand

Appendix A Appendices

In This Chapter

Open Ports Recommendations

► *Listening Ports:*

By default, the User Station does not have any listening ports opened unless the following settings are enabled:

- 80 (HTTP) commonly used internet protocol
- 443 (HTTPS) if Remote Control is enabled
- 22 (SSH) if Support Login is enabled
- 24800 if Keyboard/Mouse sharing is enabled
- 8443 for Remote API

► *Outgoing TCP Ports:*

- 5000 and 443 for the communication to the KX4 (configurable)
- 5900 for VNC targets (configurable; some VNC clients may use other ports)
- 3389 for RDP targets (configurable)
- 22 for SSH targets (configurable)
- 80 and 443 for web targets (configurable)
- 24800 for Keyboard/Mouse sharing
- LDAP uses ports 389 or 636 (if TLS is used; both are configurable).
- Communication to CCSG uses port 443 (HTTPS).

Mouse Mode Support for Dual Video Port Groups and M-KVM Targets

Based on your operating system, choose the best mouse mode for Dual Video port group or M-KVM targets.

► *Mouse Mode behavior on different OS:*

Windows Operating Systems:

RECOMMENDATION: Intelligent Mode works best provided "Enhanced Pointer Precision" is unticked on the target (Control Panel/Mouse/Pointer Options) and mouse speed is 50%.

- Standard Mode also works provided "Enhanced Pointer Precision" is unticked and mouse speed is 50%.
- Mouse does not sync correctly in Absolute Mouse Mode on latest Windows Operating Systems. You will have two mice, one for the client and one for the operating system. They do not sync together and allow for one continuous display across all monitors.

Note: The display resolution must not be scaled or have black borders

Linux Operating Systems:
- Absolute mouse mode works best.

Apple Operating Systems:

RECOMMENDATION: Single Mouse mode should be used as the mouse does not sync on any mode for M-KVM/Dual Video Port Apple Mac targets.

Additional Features

Screen Unlocking

When the User Station screen is locked, no data is displayed onscreen.

Note: See Desktop Settings for details on screen locking.

When you attempt to unlock the screen, a password prompt appears. Only the user who locked the screen can unlock the User Station. Other users must log out and then log in to the User Station if intending to operate it.

Raritan.
A brand of legrand
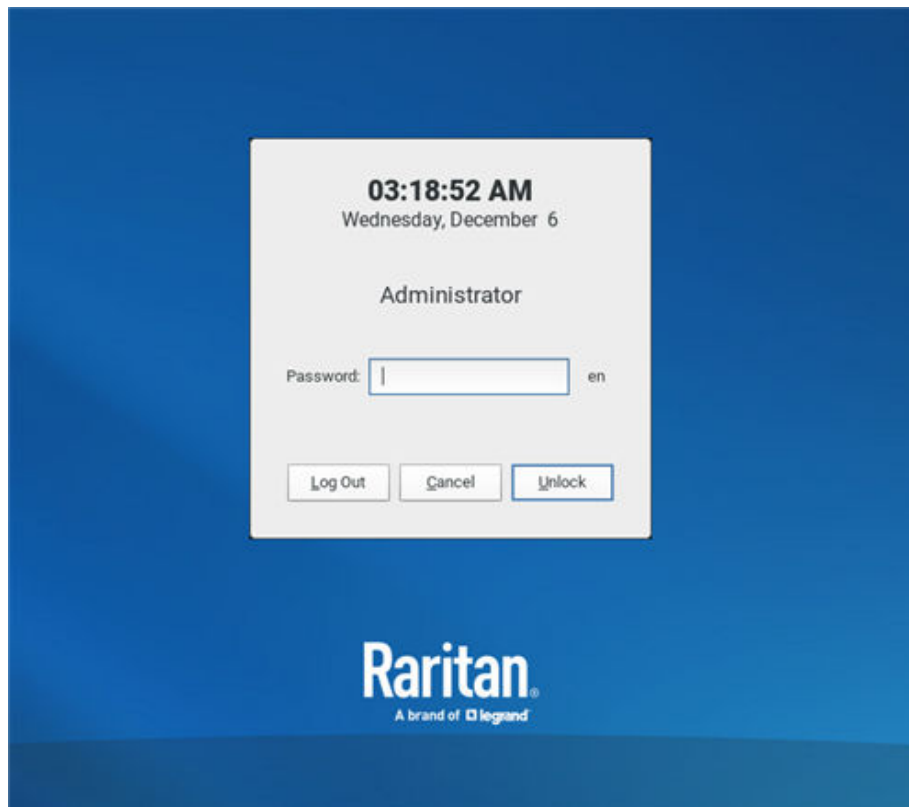
► *To unlock the User Station:*

1. Press any key on the keyboard.
2. A password prompt displays.
3. Enter the password of the user who triggered the screen-locking mode.
4. Click Unlock.

► *To log out of the User Station:*

1. At the password prompt, click Log Out. NO password is needed.
2. The Login Screen displays, and any user can log in.

Factory Reset at Startup

In addition to the factory reset feature in the User Station Configuration window, you can reset the User Station to factory defaults by performing the factory reset during the device boot.

Only the admin user can perform the factory reset at startup. Note that the factory reset removes all customized data. See Factory Reset (on page 267).

► *To perform factory reset when the device boots up:*

1. Restart or boot up the User Station.
2. When a blinking text cursor displays on the top-left corner of the screen after the initial BIOS image, press Esc within a second.
3. A menu with the two options below is shown.
   - `Boot Dominion User Station`
   - `Reset Dominion User Station to Factory Defaults`
4. Select `Reset Dominion User Station to Factory Defaults.`
   - To abandon the factory reset, select the other option.
5. When the system prompts you to enter user credentials, type the admin credentials -- "admin" user and the current admin password.
   - The default admin password is "raritan"
6. If the admin credentials are correct, the User Station performs the factory reset and then reboots. If the credentials are incorrect, the User Station returns back to the menu.

Take a Screenshot

To take a screenshot, you must be in a user group with the Take Screenshot privilege and a privilege such as Device Access that allows you to login. See Privileges (on page 199).

A hotkey must be configured for the function.

Your screenshot is saved to a connected USB storage device or mounted Network Storage. The preferred storage can be configured under Preferences > Screenshots. If more than one USB storage is detected, the first device by alphabetical device name is chosen.

Note: Active RDP sessions may affect the screenshot commands. When an RDP session is open, make sure to click in the Dominion User Station desktop before taking a screenshot.

► *To enable the hotkey for taking a screenshot:*

1. Open User Station Configuration, then choose Preferences > Hotkeys and Gestures.
2. Scroll down to "Screenshot of Desktop" and "Screenshot of Active Window". If the functions are enabled, use the hotkey displayed. If the functions are disabled, click Edit, then select a hotkey for the function and click Save.

See Hotkeys and Gestures (on page 181).
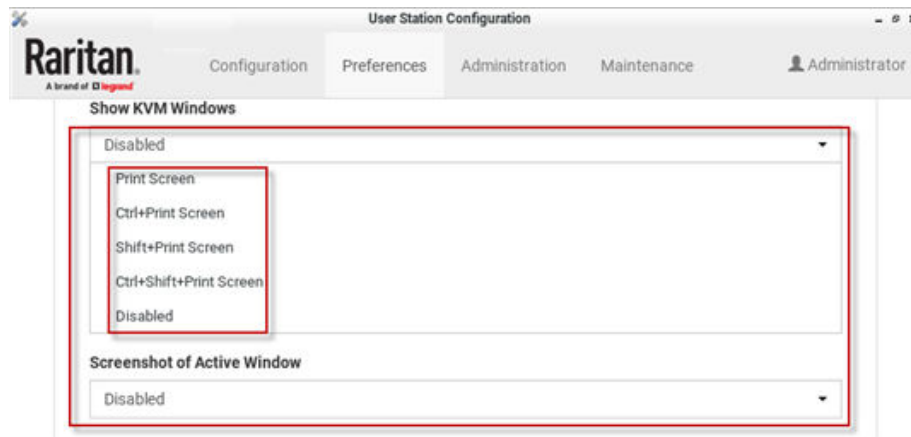
Enabling CC-SG Integration

Enable CC-SG integration in the Administration settings.

When the feature is enabled or disabled, you must logout of Dominion User Station, and then log back in so that the authentication can take effect.

If you have local users and CC-SG users, make sure "Allow access for local users" is checked. This setting adds a local users option to the login page, so that all of your users can access. Using a local login disables the CC-SG integration access for the current session. Local users will not see any CC-SG devices.

▶ *To enable CC-SG integration:*

1. If not displayed, launch the User Station Configuration window. See User Station Configuration (on page 80).
2. Click Administration > CC-SG.
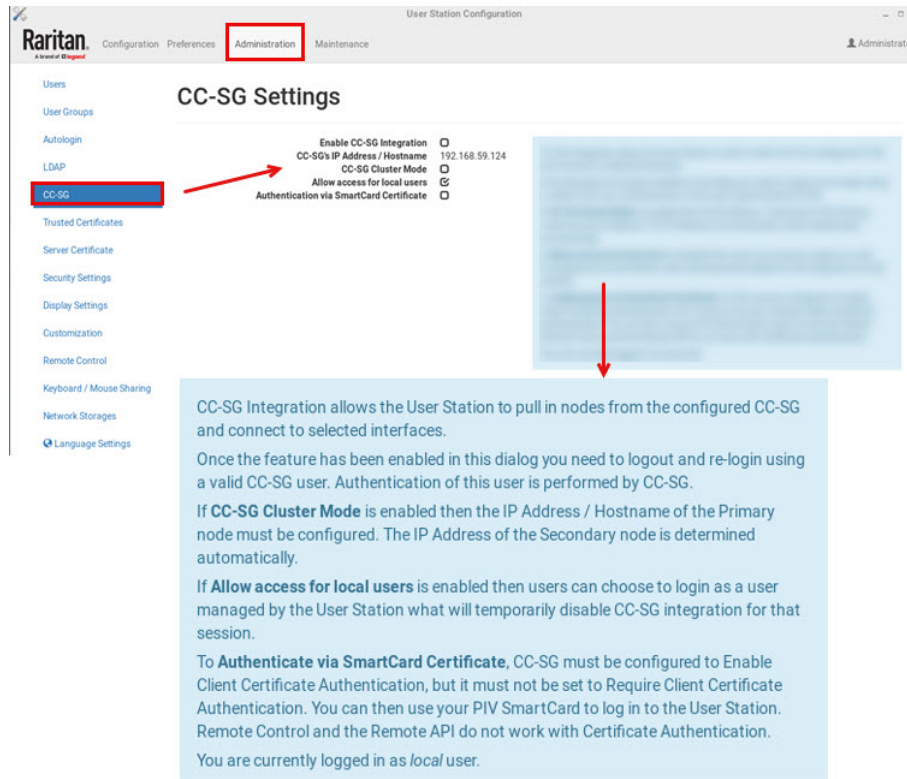
3. In the Edit CC-SG Settings page, select the options for your CC-SG integration:

   a. Enable CC-SG Integration: select the checkbox, then add the CC-SG IP Address/Hostname.

   b. Select CC-SG Cluster Mode if you have Primary and Secondary CC-SG units in a cluster configuration. Make sure the IP address of the Primary node is entered here.

   c. Allow access for local users: select this option to allow local users to access even when CC-SG integration is enabled. When enabled, an additional checkbox appears on the Dominion User Station login page for users to select when they need to login locally.

   d. Select Authentication via SmartCard Certificate to allow user to use SmartCard authentication method.

   e. Select Allow launch of CC-SG Admin Client to access the CC-SG Admin Client.

4. For the setting to take effect, you must log out of Dominion User Station, then login again with your CC-SG credentials. See Logging in with CC-SG Integration (on page 216).

5. The CC-SG user group by default has "Device Access, Change Preferences, and Launch the Port Scanner" permissions, but these can be modified by the admin user. "Take Screenshot" and "Record Scanner Snapshots" privileges can be added to this user group.

Index

Raritan.
A brand of legrand

Raritan.
A brand of legrand

Raritan.
A brand of ▢legrand