KVM and Serial Access Clients

User Guide

Active KVM Client, Virtual KVM Client, Multi-Platform Client, Raritan Remote Client and Raritan Serial Client

KVM_Serial_Clients-0P-E

July 2013

255-62-5223-00-0I

FCC Information

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

VCCI Information (Japan)

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

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

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

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

Contents

Chapter 4 Virtual Media 162

Chapter 5 Raritan Serial Console 176

Appendix A Informational Notes 199

Chapter 1 Introduction

In This Chapter

Overview

Raritan Multi-Platform Client (MPC), Raritan Remote Client (RRC), Virtual KVM Client (VKC), and the Active KVM Client (AKC) are graphical user interfaces for the Raritan Dominion and IP-Reach product lines, providing remote access to target servers connected to Raritan KVM over IP devices.

Non-Windows generation 2 users must use Raritan Multi-Platform Client, AKC or VKC. Windows users connecting to a generation 1 Raritan device must use RRC or MPC.

The standalone Raritan Serial Console (RSC) is used to make direct connections to a serial target without going through the device. The user specifies the device address and the port number (target), and is then connected.

KVM and Serial Access Client Help

This help provides information on using Raritan's KVM and serial clients. A PDF version of the help can be downloaded from Raritan's Firmware and Documentation page on the Raritan website (see www.raritan.com). Raritan recommends that you refer to the Raritan website for the most up-to-date user guides available.

Proxy Server Configuration for Use with MPC, VKC and AKC

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

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

To configure the SOCKS proxy:

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

a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.

b. Select 'Use a proxy server for your LAN'.

c. Click Advanced. The Proxy Settings dialog opens.

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

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

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

3. Next, configure the proxies for Java™ applets by selecting Control Panel > Java.

e. On the General tab, click Network Settings. The Network Settings dialog opens.

f. Select Use Proxy Server.

g. Click Advanced. The Advanced Network Settings dialog opens.

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

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

4. If you are using standalone MPC, you must also do the following:

i. Open the start.bat file in MPC directory with a text editor.

j. Insert the following parameters to the command line. Add them before "-classpath": -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port>

The parameters should look as follows:

start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70 -XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true -DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080 -classpath .\sdeploy.jar;.\sFoxtrot.jar;.\jaws.jar;.\sMpc.jar com.raritan.rrc.ui.RRCApplication %1

Client Uses with Raritan Products

The following table lists Raritan products and the client applications with which they work:

Product	Works with...				
	MPC	RRC	VKC	RSC	AKC
KX 1 G1	✓	✓			

Product	Works with...				
KX II G2	✓		✓		
KX II 2.2 (or later)	✓		✓		✓
KX II-101	✓		✓		
KX II-101-V2		✓			
KX 101 G1	✓	✓			
KSX G1	✓	✓			
KSX II G2	✓		✓	✓	✓
LX 2.4.5 (or later)	✓		✓		✓
SX				✓	
IP Reach G1	✓	✓			
UST-IP G1	✓	✓			

Legend:

G1	Generation 1
G2	Generation 2

Note: There are some differences in MPC when used with the Dominion KX I, Dominion KX II, and Dominion KSX II devices; these differences are noted in the respective device user guides.

Note: MPC and VKC are Java™ based. AKC is .NET based.

Chapter 2 Virtual KVM Client (VKC) and Active KVM Client (AKC)

In This Chapter

The Virtual KVM Client (VKC) and Active KVM Client (AKC) are interfaces used to access remote targets. AKC and VKC share similar features with the exception of the following:

- Minimum system requirements
- Supported operating systems and browsers
- Keyboard macros created in AKC cannot be used in VKC.
- Direct port access configuration (see **Enabling Direct Port Access via URL**)
- AKC server certification validation configuration (see **Prerequisites for Using AKC**)

About the Virtual KVM Client

Whenever you access a target server using the Remote Console, a Virtual KVM Client (VKC) window opens. There is one Virtual KVM Client for each target server connected. These windows can be accessed via the Windows® task bar.

Virtual KVM Client windows can be minimized, maximized, and moved around your computer desktop.

Note: Refreshing your HTML browser closes the Virtual KVM Client connection, so exercise caution.

Note: If you are using Firefox 3.0.3, you may experience problems launching the application. If this occurs, clear the browser cache and launch the application again.

Note: Some features, such as client launch settings and smart cards, are not supported by the LX and, as such, are not supported by AKC or VKC when used in conjunction with the LX.

Note: The KX II-101-V2 only supports a connection to one target at a time.

About the Active KVM Client

The Microsoft Windows .NET-based Active KVM Client (AKC) is available in the KX II 2.2 (and later) and LX 2.4.5 (and later). AKC can be used with all KX II and LX models. The KX2-101 and KX II-101-V2 is not supported.

AKC is based on Microsoft Windows .NET technology and allows you to run the client in Windows environments without the use of the Java Runtime Environment (JRE), which is required to run Raritan's Virtual KVM Client (VKC) and Multi-Platform Client (MPC). AKC also works with CC-SG.

Note: Some features, such as client launch settings and smart cards, are not supported by the LX and, as such, are not supported by AKC or VKC when used in conjunction with the LX.

Note: If you are using direct port access with AKC, you must open a new browser window or browser tab for each target you want to access. If you try to access another target by entering the DPA URL into the same browser window or browser tab you are currently accessing a target from, you will not be able to connect and may receive an error.

AKC Supported .NET Framework, Operating Systems and Browsers

.NET Framework

AKC requires Windows .NET® version 3.5 or 4.0. AKC works with both 3.5 and 4.0 installed.

Operating Systems

When launched from Internet Explorer®, AKC allows you to reach target servers via the KX II 2.2 (and later) and the LX 2.4.5 (and later). AKC is compatible with the following platforms running .NET Framework 3.5:

- Windows XP® operating system
- Windows Vista® operating system (up to 64 bit)
- Windows 7® operating system (up to 64 bit)

Note: You must be using Windows 7 if WINDOWS PC FIPs is turned on and you are accessing a target using AKC and a smartcard.

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

Note: Raritan recommends Windows XP® operating system users verify you have a working version of .NET 3.5 or 4.0 already installed before you launch AKC. If you do not verify your .NET version is working, you may be prompted to download a file versus receiving the default message to check your .NET version.

Browser

- Internet Explorer 6 or later

If you attempt to open AKC from a browser other than IE 6 or later, you will receive an error message instructing you to check your browser and to switch to Internet Explorer.

Prerequisites for Using AKC

In order to use AKC:

- Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.
- Windows Vista, Windows 7 and Windows 2008 server users should ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone and that Protected Mode is not on when accessing the device.

Enable AKC Download Server Certificate Validation

If the device (or CC-SG) administrator has enabled the Enable AKC Download Server Certificate Validation option:

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

When launching AKC from the CC-SG Admin Client, you must have JRE™ 1.6.0_10 or above.

Toolbar Buttons and Status Bar Icons

Button	Button name	Description	Product availability
	Connection Properties	Opens the Modify Connection Properties dialog from which you can manually adjust bandwidth options (such as connection speed, color depth, smoothing, and so forth).	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Video Settings	Opens the Video Settings dialog, allowing you to manually adjust video conversion parameters.	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Color Calibration	Adjusts color settings to reduce excess color noise. Same as choosing Video > Color Calibrate.	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ Not supported by the KX II-101-V2

Button	Button name	Description	Product availability
	Target Screenshot	Click to take a screenshot of the target server and save it to a file of your choosing.	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Audio	Opens a dialog that allows you to select from a list of audio devices connected to a client PC. Once audio devices have been connected to the target, select to disconnect the devices.	▪ KX II 2.4.0 (and later) ▪ KSX II 2.5.0 (and later) ▪ Not supported by LX or KX II-101-V2
	Synchronize Mouse	Dual-mouse mode forces the realignment of the target server mouse pointer with the mouse pointer. *Note: Not available if Absolute Mouse mode is selected.*	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Refresh Screen	Forces a refresh of the video screen.	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Auto-sense Video Settings	Forces a refresh of the video settings (resolution, refresh rate).	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Smart Card	Opens a dialog that allows you to select from a list of smart card readers connected to a client PC.	▪ KX II 2.1.0 (and later) ▪ KSX II 2.3.0 (and later) ▪ Not supported by the LX, KX II-101, or KX II-101-V2

Button	Button name	Description	Product availability
	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Del hot key combination to the target server.	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Single Cursor Mode	Starts Single Cursor mode in which the local mouse pointer no longer appears onscreen. Press Ctrl+Alt+O to exit this mode.	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Full Screen Mode	Maximizes the screen real estate to view the target server desktop.	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2
	Scaling	Increases or reduces the target video size so you can view the entire contents of the target server window without using the scroll bar.	▪ KX II ▪ KSX II ▪ LX ▪ KX II-101 ▪ KX II-101-V2

Audio is supported by KX II 2.4.0 (and later). Audio capture is supported by KX II 2.5.0 (and later).

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

Connection Properties

The dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. The devices optimize KVM output not only for LAN use, but also for WAN use. These devices can also control color depth and limit video output, offering an optimal balance between video quality and system responsiveness for any bandwidth.

The parameters in the Properties dialog can be optimized to suit your needs for different operating environments. Connection properties are saved across subsequent connections to generation 2 devices once they are set and saved.

To set the connection properties:

1. Choose Connection > Properties or click the Connection Properties button  in the toolbar. The Properties dialog appears.

2. Choose the Connection Speed from the drop-down list. The device can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to bandwidth limitations.
   - Auto
   - 1G Ethernet
   - 100 Mb Ethernet
   - 10 Mb Ethernet
   - 1.5 Mb (MAX DSL/T1)
   - 1 Mb (Fast DSL/T1)
   - 512 Kb (Medium DSL/T1)
   - 384 Kb (Slow DSL/T1)
   - 256 Kb (Cable)
   - 128 Kb (Dual ISDN)
   - 56 kb (ISP Modem)
   - 33 kb (Fast Modem)
   - 24 kb (Slow Modem)

   Note that these settings are an optimization for specific conditions rather than an exact speed. The client and server always attempt to deliver video as quickly as possible on the network regardless of the current network speed and encoding setting. But the system will be most responsive when the settings match the real world environment.
3. Choose the Color Depth from the drop-down list. The device can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths.
   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White

Important: For most administrative tasks (server monitoring, reconfiguring, and so on), the full 24-bit or 32-bit color spectrum made available by most modern video graphics cards is not necessary. Attempting to transmit such high color depths wastes network bandwidth.

4. Use the slider to select the desired level of Smoothing (15-bit color mode only). The level of smoothing determines how aggressively to blend screen regions with small color variation into a single smooth color. Smoothing improves the appearance of target video by reducing displayed video noise.
5. Click OK to set these properties.

Connection Information

To obtain information about your Virtual KVM Client connection:

- Choose Connection > Info... The Connection Info window opens.

The following information is displayed about the current connection:

- Device Name - The name of the device.
- IP Address - The IP address of the device.
- Port - The KVM communication TCP/IP port used to access the target device.
- Data In/Second - Data rate in.
- Data Out/Second - Data rate out.
- Connect Time - The duration of the connect time.
- FPS - The frames per second transmitted for video.
- Horizontal Resolution - The screen resolution horizontally.
- Vertical Resolution - The screen resolution vertically.
- Refresh Rate - How often the screen is refreshed.
- Protocol Version - RFB protocol version.

To copy this information:

- Click Copy to Clipboard. The information is available to be pasted into the program of your choice.

Keyboard Options

Keyboard Macros

Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by the computer on which the Virtual KVM Client is running (your client PC).

Macros are stored on the client PC and are PC-specific. Therefore, if you use another PC, you cannot see your macros. In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.

Keyboard macros created in the Virtual KVM Client are available in Multi-Platform Client (MPC) and vice versa. However, keyboard macros created in Active KVM Client (AKC) cannot be used in VKC or MPC, and vice versa.

Import/Export Keyboard Macros

Macros exported from Active KVM Client (AKC) cannot be imported into Multi-Platform Client (MPC) or Virtual KVM Client (VKC). Macros exported from MPC or VKC cannot be imported into AKC.

To import macros:

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

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

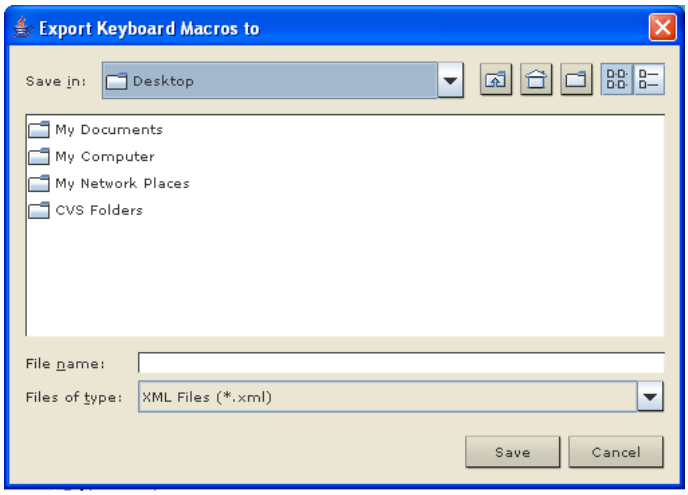
b. If during the import process the number of allowed, imported macros is exceeded, a dialog appears. Click OK to attempt to continue importing macros or click Cancel to stop the import process.

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

To export macros:

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

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



Building a Keyboard Macro

To build a macro:

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

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

Press Left Alt

Press F4

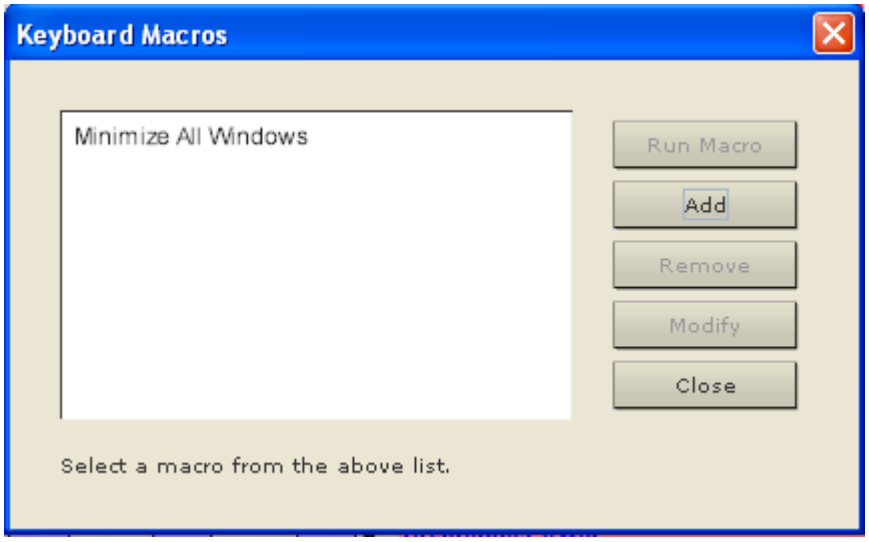
Esc

Release F4

Esc

Release Left Alt

6. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
   a. To remove a step in the sequence, select it and click Remove.
   b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.
7. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.
8. Click Close to close the Keyboard Macros dialog. The macro now appears on the Keyboard menu in the application. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.



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

1. Click the Keyboard > Sent Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target.

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

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

Running a Keyboard Macro

Once you have created a keyboard macro, execute it using the keyboard macro you assigned to it or by choosing it from the Keyboard menu.

Run a Macro from the Menu Bar

When you create a macro, it appears under the Keyboard menu. Execute the keyboard macro by clicking on it in the Keyboard menu.

Run a Macro Using a Keyboard Combination

If you assigned a keyboard combination to a macro when building it, you can execute the macro by pressing its assigned keystrokes. For example, press the keys Ctrl+Alt+0 simultaneously to minimize all windows on a Windows target server.

Modifying and Removing Keyboard Macros

To modify a macro:

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Choose the macro from among those listed.
3. Click Modify. The Add/Edit Macro dialog appears.
4. Make your changes.
5. Click OK.

To remove a macro:

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Choose the macro from among those listed.
3. Click Remove. The macro is deleted.

Ctrl+Alt+Del Macro

Due to its frequent use, a Ctrl+Alt+Delete macro is preprogrammed.

Clicking on the Ctrl+Alt+Delete button  in the toolbar sends this key sequence to the server or to the KVM switch to which you are currently connected.

In contrast, if you were to physically press the Ctrl+Alt+Del keys, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

Setting CIM Keyboard/Mouse Options

To access the DCIM-USBG2 setup menu:

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

Video Properties

Refreshing the Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

- The Refresh Screen command forces a refresh of the video screen.
- The Auto-sense Video Settings command automatically detects the target server's video settings.
- The Calibrate Color command calibrates the video to enhance the colors being displayed.

In addition, you can manually adjust the settings using the Video Settings command.

To refresh the video settings, do one of the following:

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

Auto-Sense Video Settings

The Auto-sense Video Settings command forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.

To automatically detect the video settings, do the following:

- Choose Video > Auto-sense Video Settings or click the Auto-Sense Video Settings button  in the toolbar. A message stating that the auto adjustment is in progress appears.

Calibrating Color

Use the Calibrate Color command to optimize the color levels (hue, brightness, saturation) of the transmitted video images. The color settings are on a target server-basis.

Note: The Calibrate Color command applies to the current connection only.

To calibrate the color, do the following:

- Choose Video > Calibrate Color or click the Calibrate Color button  in the toolbar. The target device screen updates its color calibration.

Adjusting Video Settings

Use the Video Settings command to manually adjust the video settings.

To change the video settings:

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar to open the Video Settings dialog.
2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:
   a. Noise Filter

      The device can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.
      Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

   b. PLL Settings

      Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances this setting should not be changed because the autodetect is usually quite accurate.

      Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

   c. Brightness: Use this setting to adjust the brightness of the target server display.

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

   e. Brightness Green - Controls the brightness of the green signal.

   f. Brightness Blue - Controls the brightness of the blue signal.

   g. Contrast Red - Controls the red signal contrast.

   h. Contrast Green - Controls the green signal.

   i. Contrast Blue - Controls the blue signal.

      If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

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

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

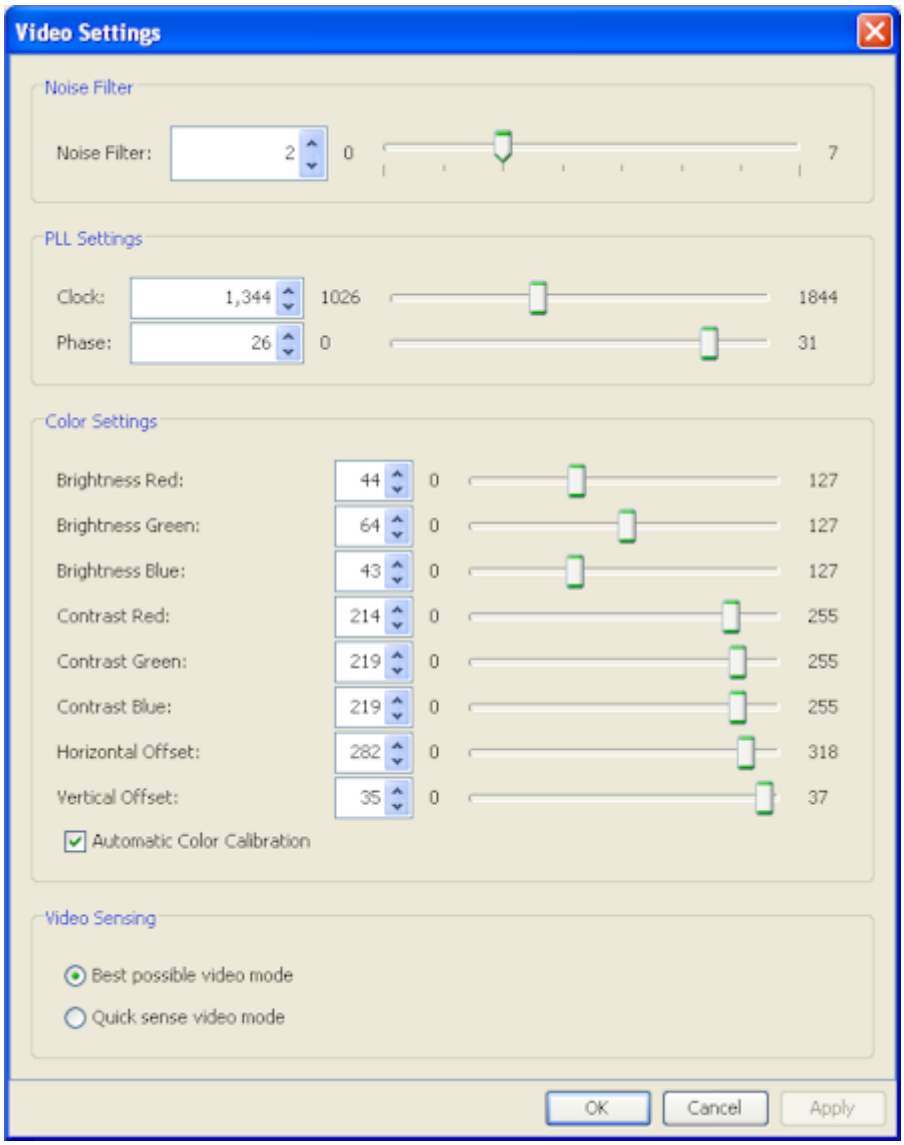
3. Select Automatic Color Calibration to enable this feature.
4. Select the video sensing mode:
   - Best possible video mode

   The device will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.

   - Quick sense video mode

   With this option, the device will use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
5. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.

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

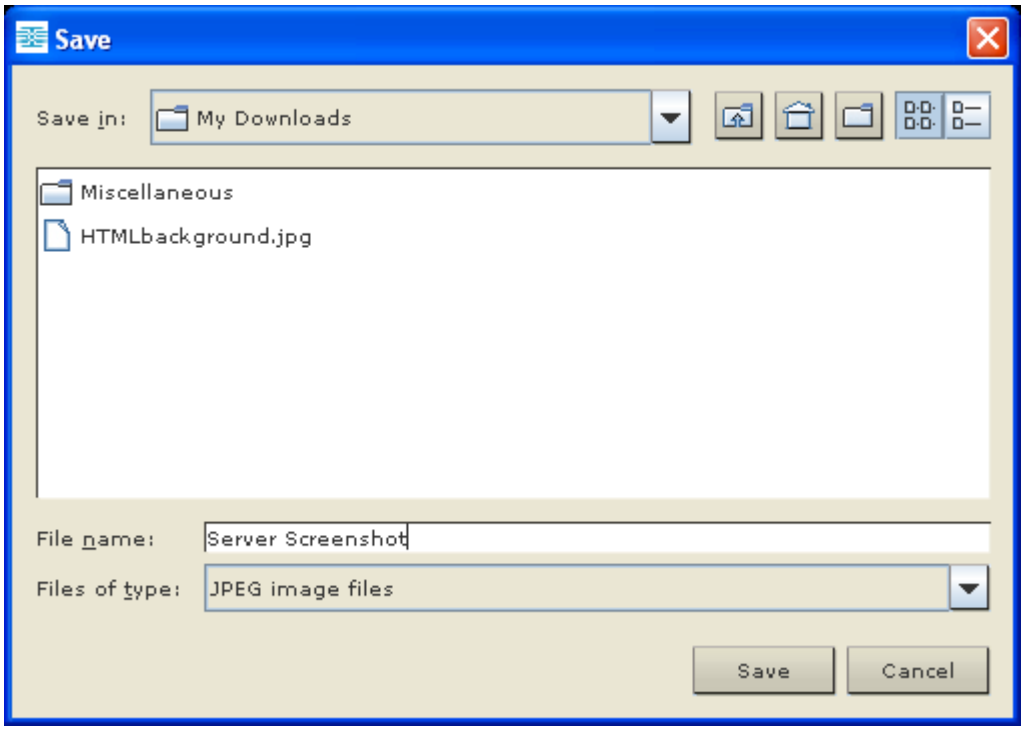


Using Screenshot from Target

You are able to take a screenshot of a target server using the Screenshot from Target server command. If needed, save this screenshot to a file location of your choosing as a bitmap, JPEG or PNG file.

To take a screenshot of the target server:

1. Select Video > Screenshot from Target or click the Screenshot from Target button  on the toolbar.
2. In the Save dialog, choose the location to save the file, name the file, and select a file format from the 'Files of type' drop-down.
3. Click Save to save the screenshot.



Changing the Maximum Refresh Rate

If the video card you are using on the target uses custom software and you are accessing the target through MPC or VKC, you may need to change the maximum refresh rate of the monitor in order for the refresh rate to take effect on the target.

To adjust the monitor refresh rate:

1. In Windows®, select Display Properties > Settings > Advanced to open the Plug and Play dialog.
2. Click on the Monitor tab.
3. Set the 'Screen refresh rate'.
4. Click OK and then OK again to apply the setting.

Mouse Options

When controlling a target server, the Remote Console displays two mouse cursors: one belonging to your client workstation and the other belonging to the target server.

You can operate in either single mouse mode or dual mouse mode. When in dual mouse mode, and provided the option is properly configured, the mouse cursors align.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

Mouse Pointer Synchronization

When remotely viewing a target server that uses a mouse, two mouse cursors are displayed: one belonging to your remote client workstation and the other belonging to the target server. When the mouse pointer lies within the Virtual KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server. While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

On fast LAN connections, you can disable the Virtual KVM Client mouse pointer and view only the target server's pointer. You can toggle between these two modes (single mouse and dual mouse).

Mouse Synchronization Tips

Be sure to follow these steps when configuring mouse synchronization:

1. Verify that the selected video resolution and refresh rate are among those supported by the device. The Virtual KVM Client Connection Info dialog displays the actual values that the device is seeing.
2. For KX II and LX devices, verify that the cable length is within the specified limits for the selected video resolution.
3. Verify that the mouse and video have been properly configured during the installation process.
4. Force an auto-sense by clicking the Virtual KVM Client auto-sense button.
5. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
   a. Open a terminal window.
   b. Enter the following command: `xset mouse 1 1`
   c. Close the terminal window.
6. Click the "Virtual KVM Client mouse synchronization" button  .

Additional Notes for Intelligent Mouse Mode

- Be sure that there are no icons or applications in the upper left section of the screen since that is where the synchronization routine takes place.
- Do not use an animated mouse.
- Disable active desktop on KVM target servers.

Synchronize Mouse

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse pointer with Virtual KVM Client mouse pointer.

To synchronize the mouse, do one of the following:

- Choose Mouse > Synchronize Mouse or click the Synchronize Mouse button  in the toolbar.

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

Standard Mouse Mode

Standard Mouse mode uses a standard mouse synchronization algorithm using relative mouse positions. Standard Mouse mode requires that mouse acceleration is disabled and other mouse parameters are set correctly in order for the client and server mouse to stay synchronized.

To enter Standard Mouse mode:

- Choose Mouse > Standard.

Intelligent Mouse Mode

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

During synchronization, the mouse cursor does a “dance” in the top left corner of the screen and calculates the acceleration. For this mode to work properly, certain conditions must be met.

To enter intelligent mouse mode:

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

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

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as “Enhanced pointer precision" or “Snap mouse to default button in dialogs” should be disabled.
- Choose “Best Possible Video Mode” in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, Raritan recommends you do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

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

Absolute Mouse Mode

In this mode, absolute coordinates are used to keep the client and target cursors in sync, even when the target mouse is set to a different acceleration or speed. This mode is supported on servers with USB ports and is the default mode for VM and dual VM targets.

To enter absolute mouse mode:

- Choose Mouse > Absolute.

Note: The absolute mouse setting requires a USB target system and is the recommended mouse setting for KX II-101.

Note: For KX II, Absolute Mouse Synchronization is available for use with the virtual media-enabled USB CIM (D2CIM-VUSB and D2CIM-DVUSB) only.

Single Mouse Mode

Single Mouse mode uses only the target server mouse cursor and the local mouse pointer no longer appears onscreen. While in single mouse mode, the Synchronize Mouse command is not available (there is no need to synchronize a single mouse cursor).

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

To enter single mouse mode, do the following:

1. Choose Mouse > Single Mouse Cursor.

2. Click the Single/Double Mouse Cursor button in the toolbar.

To exit single mouse mode:

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

Tool Options

General Settings

To set the tools options:

1. Click Tools > Options. The Options dialog appears.
2. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.
3. Choose the Keyboard Type from the drop-down list (if necessary). The options include:
   - US/International
   - French (France)
   - German (Germany)
   - Japanese
   - United Kingdom
   - Korean (Korea)
   - French (Belgium)
   - Norwegian (Norway)
   - Portuguese (Portugal)
   - Danish (Denmark)
   - Swedish (Sweden)

- German (Switzerland)
- Hungarian (Hungary)
- Spanish (Spain)
- Italian (Italy)
- Slovenian
- Translation: French - US
- Translation: French - US International

In AKC, the keyboard type defaults to the local client, so this option does not apply. Additionally, the KX II-101 and KX II-101-V2 do not support single cursor mode, so the Exit Single Cursor Mode function does not apply for those devices.

4. Configure hotkeys:
   - Exit Full Screen Mode - Hotkey. When you enter Full Screen mode, the display of the target server becomes full screen and acquires the same resolution as the target server. This is the hot key used for exiting this mode.
   - Exit Single Cursor Mode - Hotkey. When you enter single cursor mode, only the target server mouse cursor is visible. This is the hot key used to exit single cursor mode and bring back the client mouse cursor.
   - Disconnect from Target - Hotkey. Enable this hotkey to allow users to quickly disconnect from the target.

   For hotkey combinations, the application does not allow you to assign the same hotkey combination to more than one function. For example, if Q is already applied to the Disconnect from Target function, it won't be available for the Exit Full Screen Mode function. Further, if a hotkey is added to the application due to an upgrade and the default value for the key is already in use, the next available value is applied to the function instead.
5. Click OK.

Keyboard Limitations

Turkish Keyboards

If using a Turkish keyboard, you must connect to a target server through the Active KVM Client (AKC). It is not supported by other Raritan clients.

Slovenian Keyboards

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

Language Configuration on Linux

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

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

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

Client Launch Settings

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

Note: LX devices support this feature in MPC. LX does not support client launch setting in VKC and AKC.

To configure client launch settings:

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

Configure Scan Settings in VKC and AKC

The KX II and LX provide a port scanning feature that searches for selected targets and displays them in a slide show view, allowing you to monitor up to 32 targets at one time. You can connect to targets or focus on a specific target as needed. Scans can include standard targets, blade servers, tiered Dominion devices, and KVM switch ports. Configure scan settings from either the Virtual KVM Client (VKC) or Active KVM Client (AKC). See Configure Scan Settings in VKC and AKC for more information. See Scanning Ports. Use the Scan Settings tab to customize the scan interval and default display options.

To set scan settings:

1. Click Tools > Options. The Options dialog appears.
2. Select the Scan Settings tab.
3. In the "Display Interval (10-255 sec):" field, specify the number of seconds you want the target that is in focus to display in the center of the Port Scan window.
4. In the "Interval Between Ports (10 - 255 sec):" field, specify the interval at which the device should pause between ports.
5. In the Display section, change the default display options for the thumbnail size and split orientation of the Port Scan window.
6. Click OK.

View Options

View Toolbar

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

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

- Choose View > View Toolbar.

View Status Bar

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

To hide the status bar:

- Click View > Status Bar to deselect it.

To restore the status bar:

- Click View > Status Bar to select it.

Scaling

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

To toggle scaling (on and off):

- Choose View > Scaling.

Full Screen Mode

When you enter Full Screen mode, the target's full screen is displayed and acquires the same resolution as the target server. The hot key used for exiting this mode is specified in the Options dialog, see ***Tool Options*** (on page 29).

While in Full Screen mode, moving your mouse to the top of the screen will display the Full Screen mode menu bar. If you want the menu bar to remain visible while in Full Screen mode, enable the Pin Menu Toolbar option from the Tool Options dialog. See ***Tool Options*** (on page 29).

To enter full screen mode:

- Choose View > Full Screen.

To exit full screen mode:

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

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

To set Full Screen mode as the default mode:

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

Digital Audio

The KX II 2.4.0 (and later) supports end-to-end, bidirectional, digital audio connections for digital audio playback and capture devices from a remote client to a target server. The audio devices are accessed over a USB connection. A D2CIM-DVUSB and the current device firmware are required.

The digital audio feature supports:

- ***Saving Audio Settings*** (on page 37)
- ***Connecting to Multiple Targets from a Single Remote Client*** (on page 38)
- Connecting to a Single Target Server from Multiple Remote Clients
- Connecting and Disconnecting a Digital Audio Device
- ***Adjusting Capture and Playback Buffer Size (Audio Settings)*** (on page 41)

Windows®, Linux® and Mac® operating systems are supported. The Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC) support connections to audio devices.

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

Before you begin using the audio feature, Raritan recommends you review the audio related information documented in the following sections of Help:

- ***Supported Audio Device Formats*** (on page 109, on page 35)
- Recommendations for Dual Port Video
- Supported Mouse Modes
- CIMs Required for Dual Video Support
- ***Informational Notes*** **(on page 199),** ***Audio*** (see "***Audio Notes***" on page 205)

Supported Audio Device Formats

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

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

Audio Playback and Capture Recommendations and Requirements

Audio Level

Set the target audio level to a mid-range setting. For example, on a Windows® client, set the audio to 50 or lower. This setting must be configured through the playback or capture audio device, not from the client audio device control.

Recommendations for Audio Connections when PC Share Mode is Enabled

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

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

The interruption occurs because the USB device needs to be re-enumerated with the new device configuration. It may take some time for the target to install a driver for the new device. Audio applications may stop playback completely, go to the next track, or just continue playing. The exact behavior is dependent on how the audio application is designed to handle a disconnect/reconnect event.

Bandwidth Requirements

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

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

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

A general recommendation is to have at least a 1.5MB connection before running playback and capture. However, high video-content, full-color connections using high-target screen resolutions consume much more bandwidth and impact the quality of the audio considerably. To help mitigate quality degeneration, there are a number of recommended client settings that reduce the impact of video on audio quality at lower bandwidths:

- Connect audio playback at the lower quality formats. The impact of video consuming bandwidth is much less notable at 11k connections than at 44k
- Set the connection speed under Connection Properties to a value that best matches the client to server connection
- Under Connection Properties, set the color depth to as lowt value as possible. Reducing the color depth to 8 bit color considerably reduces the bandwidth consumed
- Set Smoothing, to High. This will improve the appearance of the target video by reducing displayed video noise
- Under Video settings, set the Noise Filter to its highest setting of 7 (highest value) so less bandwidth is used for target screen changes

Saving Audio Settings

Audio device settings are applied on a per device basis. Once the audio devices settings are configured and saved on the , the same settings are applied to it.

For example, you can configure a Windows® audio device to us a stereo, 16 bit, 44.1K format. When you connect to different targets and use that Windows audio device, the stereo, 16 bit, 44.1K format is applied to each target server.

For both playback and recording devices, the device type, device format, and the buffer settings applied to the device are saved.

See Connecting and Disconnecting a Digital Audio Device for information on connecting to and configuring an audio device, and ***Adjusting Capture and Playback Buffer Size (Audio Settings)*** (on page 41) for information on audio device buffer settings.

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

So, when a user joins an audio session, the target machine settings are used. See Connecting to a Single Target Server from Multiple Remote Clients.

Connecting to Multiple Targets from a Single Remote Client

2.5.0 (and later) allows you to listen to audio on up to four (4) target servers at the same time from a single, remote client. See Connecting and Disconnecting a Digital Audio Device for information on connecting to audio devices.

Note: When an audio session is underway, be sure to keep the session active or change the 's idle timeout time so the audio session does not time out.

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

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

A Speaker icon  is displayed in the status bar at the bottom of the client window. It is grayed out when no audio is being used. When the Speaker icon and Microphone icon  are displayed in the status bar, the session is being captured as it is streamed.

Connecting to Digital Audio

Audio device settings are applied on a per device basis. Once the audio devices settings are configured and saved on the , the same settings are applied to it. See ***Saving Audio Settings*** (on page 37) for more information.

Note: If you are using the audio feature while running PC Share mode and VM Share mode, see **Audio Playback and Capture Recommendations and Requirements** *(on page 36) for important information. See also* **Conducting Multiple Audio Sessions at Once** *(see "***Connecting to Multiple Targets from a Single Remote Client***" on page 38).*

To connect to an audio device:

1. Connect the audio device to the remote client PC prior to launching the browser connection to the KX II 2.4.0 (and later).
2. Connect to the target from the Port Access page.
3. Once connected, click the Audio icon  in the toolbar. The Connect Audio Device dialog appears. A list of available audio device connected to the remote client PC is displayed.

   Note: If there are no available audio devices connected to the remote client PC, the Audio icon is grayed out. .
4. Check Connect Playback Device if you are connecting to a playback device.
5. Select the device that you wish to connect from the drop-down list.
6. Select the audio format for the playback device from the Format: drop-down.

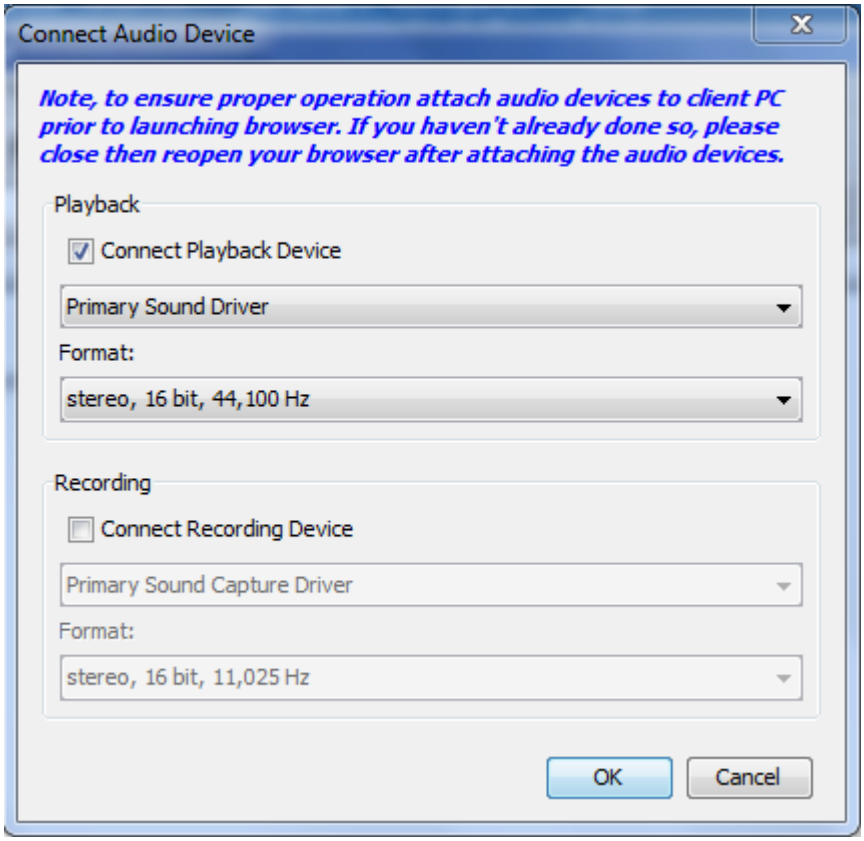
   Note: Select the format that you wish to use based on the available network bandwidth. Formats with lower sampling rates consume less bandwidth and may tolerate more network congestion.
7. Check Connect Recording Device if you are connecting a recording device.

   Note: The device names listed in the Connect Recording Device drop-down are truncated to a maximum of 30 characters for Java clients.
8. Select the device that you wish to connect from the drop-down list.
9. Select the audio format for the recording device from the Format: drop-down.
10. Click OK. If the audio connection is established, a confirmation message appears. Click OK.

If the connection was not established, an error message appears.

Once an audio connection is established, the Audio menu is changed to Disconnect Audio. Additionally, the settings for the audio device are saved and applied to the audio device.

A Speaker icon is displayed in the status bar at the bottom of the client window. It is grayed out when no audio is being used. When the Speaker icon and Microphone icon are displayed in the status bar, the session is being captured as it is streamed.



To disconnect from the audio device:

- Click the Audio icon in the toolbar and select OK when you are prompted to confirm the disconnect. A confirmation message appears. Click OK.

Adjusting Capture and Playback Buffer Size (Audio Settings)

Once an audio device is connected, the capture and playback buffer size can be adjusted as needed. This feature is useful for controlling the quality of the audio, which may be impacted by bandwidth limitations or network spikes.

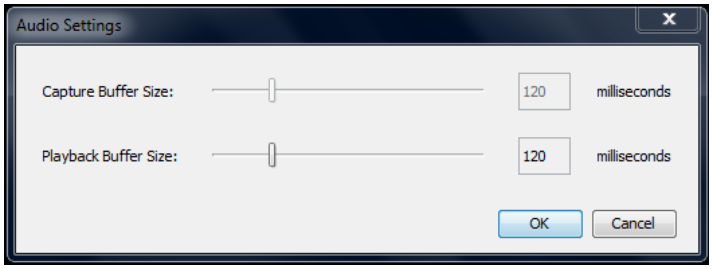
Increasing the buffer size improves the audio quality but may impact the delivery speed. The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

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

Audio settings are configured in the AKC, VKC or MPC clients.

To adjust audio settings:

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



Smart Cards (VKC, AKC and MPC)

Using the KX II 2.1.10 (and later) or KSX II 2.3.0 (and later), you are able to mount a smart card reader onto a target server to support smart card authentication and related applications. For a list of supported smart cards, smart card readers, and additional system requirements, see ***Supported and Unsupported Smart Card Readers*** (on page 44).

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

When accessing a server remotely, you can select an attached smart card reader and mount it onto the server. Smart card authentication is used with the target server, it is not used to log into the device. Therefore, changes to smart card PIN and credentials do not require updates to device accounts. When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached. Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS. When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

When PC-Share mode is enabled on the device, multiple users can share access to a target server. However, when a smart card reader is connected to a target, the device will enforce privacy regardless of the PC-Share mode setting. In addition, if you join a shared session on a target server, the smart card reader mounting will be disabled until exclusive access to the target server becomes available.

After a KVM session is established to the target server, a Smart Card menu and button are available in the Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC). Once the menu is opened or the Smart Card button is selected, the smart card readers that have been detected as attached to the remote client are displayed. From this dialog you can attach additional smart card readers, refresh the list of smart card readers attached to the target, and detach smart card readers. You are also able to remove or reinsert a smart card. This function can be used to provide notification to a target server OS that requires a removal/reinsertion in order to display the appropriate login dialog. Using this function allows the notification to be sent to a single target without affecting other active KVM sessions.

To mount a smart card reader:

1. Click the Smart Card menu and then select Smart Card Reader.

   Alternatively, click the Smart Card button  in the toolbar.
2. Select the smart card reader from the Select Smart Card Reader dialog.

3. Click Mount.
4. A progress dialog will open. Check the 'Mount selected card reader automatically on connection to targets' checkbox to mount the smart card reader automatically the next time you connect to a target. Click OK to begin the mounting process.

To update the smart card in the Select Smart Card Reader dialog:

- Click Refresh List if a new smart card reader has been attached to the client PC.

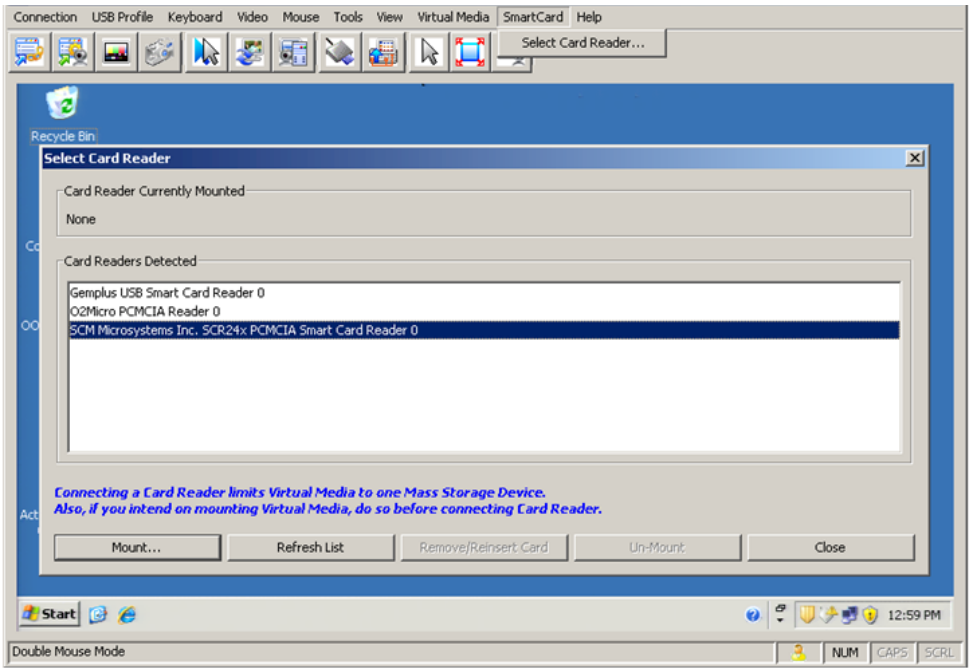
To send smart card remove and reinsert notifications to the target:

- Select the smart card reader that is currently mounted and click the Remove/Reinsert button.

To unmount a smart card reader:

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

Smart card reader mounting is also supported from the Local Console. See **Local Console Smart Card Access** in your Dominion device help.



Supported and Unsupported Smart Card Readers

External, USB smart card readers are supported.

Supported Smart Card Readers

Type	Vendor	Model	Verified
USB	SCM Microsystems	SCR331	Verified on local and remote
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	Verified on local and remote
USB	ActivIdentity	ActivIdentity USB Reader v3.0	Verified on local and remote
USB	Gemalto®	GemPC USB-SW	Verified on local and remote
USB Keyboard/Card reader Combo	Dell®	USB Smart Card Reader Keyboard	Verified on local and remote
USB Keyboard/Card reader Combo	Cherry GmbH	G83-6744 SmartBoard	Verified on local and remote
USB reader for SIM-sized cards	Omnikey	6121	Verified on local and remote
Integrated (Dell Latitude D620)	O2Micro	OZ776	Remote only
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	Remote only
PCMCIA	SCM Microsystems	SCR243	Remote only

Note: SCM Microsystems SCR331 smart card readers must be using SCM Microsystems firmware v5.25.

Unsupported Smart Card Readers

This table contains a list of readers that Raritan has tested and found not to work with the Raritan device, therefore they are unsupported. If a smart card reader does not appear in the supported smart card readers table or in the unsupported smart card readers table, Raritan cannot guarantee it will function with the device.

Type	Vendor	Model	Notes
USB Keyboard/Card	HP®	ED707A	No interrupt endpoint

Type	Vendor	Model	Notes
reader Combo			=> not compatible with Microsoft® driver
USB Keyboard/Card reader Combo	SCM Microsystems	SCR338	Proprietary card reader implementation (not CCID-compliant)
USB Token	Aladdin®	eToken PRO™	Proprietary implementation

Smart Card Minimum System Requirements

Local Port Requirements

The basic interoperability requirement for local port attachment to the is:

- All devices (smart card reader or token) that are locally attached must be USB CCID-compliant.

Target Server Requirements

When using smart card readers, the basic requirements for interoperability at the target server are:

- The IFD (smart card reader) Handler must be a standard USB CCID device driver (comparable to the generic Microsoft® USB CCID driver).
- A digital CIM or D2CIM-DVUSB (Dual-VM CIM) is required and must be using firmware version 3A6E or later.
- Blade chassis server connections, where a CIM per blade is used, are supported.
- Blade chassis server connections, where a CIM per chassis is used, is only supported for IBM® BladeCenter® models H and E with auto-discovery enabled.

Windows XP Targets

Windows XP® operating system targets must be running Windows XP SP3 in order to use smart cards with the . If you are working with .NET 3.5 in a Windows XP environment on the target server, you must be using SP1.

Linux Targets

If you are using a Linux® target, the following requirements must be met to use smart card readers with the Raritan device.

- CCID Requirements

  If the Raritan D2CIM-DVUSB VM/CCID is not recognized as a smart card reader by your Linux target, you may need to update the CCID driver version to 1.3.8 or above and update the driver configuration file (Info.plist).

Operating system	CCID requirements
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12
Fedora® Core 10	ccid-1.3.8-1.fc10.i386

Remote Client Requirements

The basic requirements for interoperability at the remote client are:

- The IFD (smart card reader) Handler must be a PC/SC compliant device driver.
- The ICC (smart card) Resource Manager must be available and be PC/SC compliant.
- The JRE™ 1.6.x with smart card API must be available for use by the Raritan client application.

Linux Clients

If you are using a Linux® client, the following requirements must be met to use smart card readers with the Raritan device.

Note: User login to client, on smart card insertion, may take longer when 1 or more KVM sessions are actively in place to targets. As the login process to these targets is also under way.

- PC/SC Requirements

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

- Create a Java™ Library Link

  A soft link must be created to the libpcsclite.so after upgrading RHEL 4, RHEL 5 and FC 10. For example, ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so, assuming installing the package places the libraries in /usr/lib or /user/local/lib.

- PC/SC Daemon

  When the pcsc daemon (resource manager in framework) is restarted, restart the browser and MPC, too.

Help Options

About Raritan Virtual KVM Client

This menu command provides version information about the Virtual KVM Client, in case you require assistance from Raritan Technical Support.

To obtain version information:

1. Choose Help > About Raritan Virtual KVM Client.
2. Use the Copy to Clipboard button to copy the information contained in the dialog to a clipboard file so it can be accessed later when dealing with support (if needed).

Chapter 3 Multi-Platform Client and Raritan Remote Client

In This Chapter

Overview

Raritan Multi-Platform Client (MPC) and Raritan Remote Console are graphical user interfaces for the Raritan product lines, providing remote access to target servers connected to Raritan KVM over IP devices. See ***Client Uses with Raritan Products*** (on page 2) for information on the clients that are compatible with specific Raritan devices.

Requirements and Installation

MPC Requirements and Installation Instructions

Note to CC-SG Users

If you are using Dominion KX II in a CC-SG configuration, do not use the CC-SG proxy mode if you are also planning to use the Multi-Platform Client (MPC).

MPC Minimum System Requirements

The minimum system requirements for the Multi-Platform Client are:

- CPU Speed: 1.0 GHz
- RAM: 512 Mbytes

Note: Running the client software on system configurations below either of these specifications may impact performance and result in errors.

MPC Supported Operating Systems and Browsers

Operating Systems

When launched as a web applet or as a standalone application, MPC allows you to reach target servers via different Raritan Dominion devices and IP Reach models.

Following are the operating systems and browsers supported for Generation 1 and Generation 2 Raritan devices using MPC.

Device generation	Operation system	Browsers
Generation 1	• Windows XP® operating system • Windows 2000® operating system SP4 • Windows Vista® operation system (32 bit only) • Red Hat Enterprise Workstation 3.0 and 4.0 • SUSE Linux Professional 9.2 and 10 • Fedora Core 5 and above • Mac OS 10.4.9 or later®* • Solaris™	• Internet Explorer® 6 and above** • Firefox® 1.0 or later • Safari® 2.0 or later • Netscape® 7.2 • Mozilla® 1.7
Generation 2	• Windows 7® (32 and 64 bit) • Windows XP operating system • Windows 2008 • Windows 2003 Windows 2000® operating system SP4 • Windows Vista operation system (32 and 64 bit) • Red Hat Enterprise Workstation 4.0 and 5.0 • Open SUSE Linux 10 and 11 • Fedora Core 8 -11 • Mac* OS 10.5 and above Solaris™	• Internet Explorer 6 and above** • Firefox 1.5, 2.0 and 3.0 (up to build 3.0.10) • Safari 3.0 or later

*** Important: Only Macs with an Intel® processor can run JRE 1.6 and, therefore, be used as a client. Mac 10.5.8 does not support MPC as a standalone client.**

*** Note: If you are using Internet Explorer® 7, you may run into permission issues when trying to connect to a target server. To avoid this, do the following:*

1. In Internet Explorer, click Tools > Internet Options to open the Internet Options dialog.

2. In the "Temporary Internet files" section, click Settings. The Settings dialog opens.

3. In the "Check for newer versions of stored pages" section, select Automatically.

4. Click OK to apply the settings.

JRE

- Generation 1 devices support JRE™ 1.4.2_05 and above
- Generation 2 devices support JRE 1.6.x and higher with the exception of 1.6.2

The JRE™ plug-in is available for the Windows® 32-bit and 64-bit operating systems. MPC and VKC can be launched only from a 32-bit browser, or 64-bit IE7 or IE8 browser.

Following are the Java™ 32-bit and 64-bit Windows operating system requirements.

Mode	Operating system	Browser
Windows x64 32-bit mode	Windows XP®	• Internet Explorer® 6.0 SP1+ or 7.0, IE 8 • Firefox® 1.06 - 4 or later
	Windows Server 2003®	• Internet Explorer 6.0 SP1++, IE 7, IE 8 • Firefox 1.06 - 3
	Windows Vista®	• Internet Explorer 7.0 or 8.0
	Windows 7®	• Internet Explorer 9.0 • Firefox 1.06 - 4 or later
Windows x64 64-bit mode	Windows XP	64bit OS, 32bit browsers:

Mode	Operating system	Browser
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

Note: If you are using Internet Explorer 8 to access MPC and do not have Java installed on your machine, an alert bar or a dialog opens asking you to download the latest version of Java. However, in some instances, only a blank window opens and you are prompted to perform the download. If this occurs, set Internet Explorer 8 to use Compatibility View. See Microsoft® Internet Explorer help for information on change IE to this view.

Note to IPv6 Users

Due to a browser limitation, MPC cannot be downloaded via the KX IPv6 address from Firefox® if Pop-up Manager is enabled. Do one of the following to avoid this issue:

- Use the hostname of the device for the MPC browser download.
- Set Firefox to not block Pop-up windows via edit\Preferences\Privacy and Security.
- Use IPV4 address.
- Use standalone MPC.
- Use the latest version of Firefox.

Special Characters in MPC

The following table identifies the special characters that can be used in MPC:

Character	Description	Character	Description
!	Exclamation point	:	Colon
"	Double quote	;	Semi-colon
#	Pound sign	=	Equal sign
$	Dollar sign	>	Greater than sign
%	Percent sign	?	Question mark
&	Ampersand	@	At sign

Character	Description	Character	Description
'	Single quote	[	Left bracket
(	Left parenthesis	\	Backward slash
)	Right parenthesis	]	Right bracket
*	Asterisk	^	Caret
+	Plus sign	_	Underscore
,	Comma	`	Grave accent
-	Dash	{	Left brace
.	Period	|	Pipe sign
/	Forward slash	}	Right brace
<	Less than sign	~	Tilde

Invalid MPC Username Characters

The following characters cannot be used in usernames for MPC.

Character	Description
:	Colon
"	Double quote
&	Ampersand
'	Single quote

Installing and Opening Standalone MPC

Raritan recommends that you open only one standalone MPC session at a time. Opening more than one standalone MPC session on the same client at the same time may cause performance problems and system errors.

Important: MPC modem connectivity is supported on the Windows® operating system. When working in Windows, use Standalone MPC.

Important: Only Macs with an Intel® processor can run JRE 1.6 and, therefore, be used as a client. Mac 10.5.8 does not support MPC as a standalone client.

You must have the MPC JAR file to install MPC for any of these operating systems.

To check for the MPC JAR file:

1. Download the installation file, MPC-installer.jar from the Raritan website (www.raritan.com) on the Support > Firmware and Documentation page.
2. Locate the Dominion product you are working with and click the Standalone Multi-Platform Client link.
3. If copying MPC-installer.jar from a known location, double-click the file to start installation.

Windows

To check the JRE version in Windows:

1. Do one of the following to check the JRE version in Windows:
   - Determine your version of the JRE from the Java website: http://www.java.com/en/download/help/testvm.xml.
   - Click the Windows Start button at the bottom left of your page and click Control Panel.

   Tip: In the upper left corner of the page, you may see a panel named Control Panel with the option Switch to Classic View or Switch to Category View. For easier viewing, opt for Classic View.

   a. Search the Control Panel files for a Java icon. When you locate the Java icon, double-click it to open the Java Control panel. Click the General tab and then click the About button to check the current Java Runtime Environment (JRE).

   b. If the JRE is version 1.6 or later, proceed with the MPC Installation. If the Java icon does not exist in the Control Panel or if the JRE version is prior to 1.6, go to the Sun Microsystems website at http://java.sun.com/products/ to download the latest version of JRE.
2. For future Java access and to automatically open it, set your path to the Java executable.

   a. Right-click the My Computer icon on your desktop and click Properties.

   b. Click the Advanced tab and then click "Environment variables".

   c. Edit the Path address so that it contains the path to the Java executable.
   For example, if Java is installed on C:\j2re1.6 and your path is currently set to C:\WINDOWS\SYSTEM32, then change the path to read C:\WINDOWS\SYSTEM32;C:\j2re1.6

To install MPC for Windows:

1. Download the MPC-installer.jar installation file or copy the file from a known location.
2. Double-click the jar file icon to open the installation dialog.
3. After the initial dialog appears, click Next.
4. Choose the directory where you want to install MPC and click Next. Click Browse to locate a non-default directory.

   Note: If you are using Windows 7, when User Access Control is turned on, you will need to manually create a folder to contain the MPC files. You will also need to assign the Admin user, at a minimum, Write permissions to the folder from Properties dialog > Security tab. Alternatively, you can turn off User Access Control.

5. Click Next.
6. In the Shortcut dialog, choose a shortcut location, determine who should have the shortcut, and determine whether you want the shortcut on the desktop. When finished, click Next.

   Once the installation is complete, the final dialog indicates where you will find an uninstaller program and provides an option for generating an automatic installation script. Click Done to close the Installation dialog.

To open MPC in Windows:

1. Click the Windows Start menu and then choose All Programs > Raritan Multi-Platform Client. Alternatively, double-click the MPC desktop shortcut icon if you created one.
2. Double-click the desired device in the Navigator to establish a connection.
3. Type your user name and password in the device dialog and then click OK to log on.

To disable Java caching and clear the cache (use these steps with Microsoft Windows XP and JRE 1.6.0):

1. From the Start menu, click Control Panel.
2. Double-click on the Java icon to launch it. The Java Control Panel dialog appears.
3. To disable Java caching:
   a. From the General tab, click the Settings button. The Temporary Files Settings dialog appears.
   b. Click the View Applets button. The Java Applet Cache Viewer opens.

c. Deselect the Enable Caching checkbox if it is already checked.

d. Click OK.

4. To clear the Java cache:

a. From the Temporary Files Settings dialog, click the Delete Files button. The Delete Temporary Files dialog appears.

b. Select the temporary files that you want to delete.

c. Click OK.

Linux®

Determine your version of the JRE from the Java website: http://www.java.com/en/download/help/testvm.xml.

You may need some configuration depending on your OS and browser. Configuration instructions are provided with the JRE download.

Important: When launching MPC from a browser, it is highly recommended that you disable the Java Applet caching.

Although no actual problems have occurred when Java caching is turned on, some non-impacting Java exceptions have occurred. Generation of these Java-exceptions can appear in the Java Applet Console window and may degrade performance.

For Linux/UNIX environments, the Java Control Panel is located in the JRE's bin directory; the location varies based on where JRE was installed by your Linux/UNIX administrator.

Tip: It is also recommended that you clear the Java cache.

To check the JRE version in Linux:

1. In a graphical environment, open a terminal dialog.
2. Type `java-version` in the command line and press Enter on your keyboard. The currently-installed version of Java Runtime Environment (JRE) is displayed.

   If your path variable is not set to where the java binaries have been installed, you may not be able to see the JRE version.
3. Set your path:

a. To set your path and assuming JRE 1.6 is installed in /usr/local/java: you must set your PATH variable.

b. To set the path for bash shell, export PATH=$PATH:/usr/local/java/j2re1.6/bin.

c. To set the path for tcsh or csh, set PATH = ($PATH /usr/local/java/j2re1.6/bin).

These commands can be typed at the terminal each time you login. Alternatively, you can add it to your .bashrc for bash shell, .cshrc for csh, or tcsh so that each time you login the PATH is already set.

See your shell documentation if you encounter problems.

4. If the JRE is version 1.6 or higher, proceed with the MPC installation. If the version is prior to 1.6, go to the Java website at http://java.sun.com/products/ to download the latest Runtime Environment.

To install MPC for Linux:

You must have Administrative privileges to install MPC.

1. Download the MPC-installer.jar file or copy it from a known location.
2. Open a terminal dialog and open the directory where the installer is saved.
3. Type *java -jar MPC-installer.jar* and press Enter to run the installer.
4. After the initial page loads, click Next.
5. Use the Browse function to select a directory to install MPC if the directory is different from the default path displayed in the "Select the installation path" field.
6. Click Next to open the Shortcut dialog.
7. On the Shortcut dialog:
   - Choose a shortcut location from the "Select a Program Group for the Shortcuts:" field.
   - Select either "current user" or "all users" to define who should have access to the shortcut.
   - Check the "Create shortcut on the desktop" checkbox if you want the shortcut to appear on the desktop.
8. When finished, click Next.

Note: Once MPC is installed successfully, a shortcut will be available on the desktop. However, for Linux users, you will need to log off of and then back into your session before the shortcut will be visible on the desktop.

Once the installation is complete, the final page indicates where you will find an uninstaller program and provides you with the option to generate an automatic installation script.

9. Click Done to close the Installation dialog.

To open MPC in Linux:

1. Open a terminal window and change directories to the directory where you installed MPC (default location: /usr/local/Raritan/Raritan MPC/*version number*).
2. Type ./start.sh and press Enter to open MPC.
3. Double-click the desired device to establish a connection, type your user name and password, and click OK to log on.

Solaris™

To check the JRE version for Sun Solaris:

1. Launch a terminal window on the Sun Solaris desktop.
2. Type `java-version` in the command line and press Enter. The currently-installed version of Java Runtime Environment (JRE) appears.

   If your path variable is not set to where the java binaries have been installed, you may not be able to see the JRE version.

   a. To set your path and assuming JRE 1.6 is installed in /usr/local/java, you must set your PATH variable.

   b. To set path for bash shell, export PATH=$PATH:/usr/local/java/j2re1.6/bin.

   c. To set path for tcsh or csh, set PATH = ($PATH /usr/local/java/j2re1.6/bin).
3. These commands can be typed at the terminal each time you login. Alternatively, you can add it to your .bashrc for bash shell, .cshrc for csh, or tcsh so that each time you login the PATH is already set. See your shell documentation if you encounter problems.
4. If the JRE is version 1.6 or higher, proceed with the MPC installation. If the version is prior to JRE 1.6, go to the Sun website at http://java.sun.com/products/ to download the latest Runtime Environment.

To install MPC for Sun Solaris:

You must have administrative privileges to install MPC.

1. Download the MPC-installer.jar file or copy it from a known location.
2. Open a terminal window and navigate to the directory where the installer is saved.
3. Type *java -jar MPC-installer.jar* and press Enter to run the installer.
4. After the initial page loads, click Next.
5. Use the Browse function to navigate to the directory you want to install MPC or select the default directory displayed in the "Select the installation path" field.

6. Click Next.
7. When installation is complete, click Next.
8. Click Next again.

   Once the installation is complete, the final dialog will indicate where you will find an uninstaller program and provides the option to generate an automatic installation script.
9. Click Done to close the Installation dialog.

To open MPC in Sun Solaris:

1. Open a terminal window and navigate to the directory where you installed MPC (the default location is /usr/local/Raritan/Raritan MPC/*version number*).
2. Type ./start.sh and press Enter to open MPC.
3. Double-click the desired device to establish a connection, type your user name and password, and click OK to log on.

Macintosh®

To check JRE on a Mac®:

1. Launch a terminal window on the Macintosh desktop.
2. Type `java-version` in the command line and press Enter. The currently-installed version of the Java Runtime Environment (JRE) is displayed.
3. If the JRE is version 1.6 or higher, proceed with the MPC installation. If the version is prior to 1.6, go to the Apple website to download the latest Runtime Environment.

To install MPC on a Mac:

You must have administrative privileges to install MPC.

1. Download the MPC-installer.jar file or copy it from a known location.
2. Open a Finder window and locate the installer.
3. Double click the MPC-installer.jar file to run the installer.
4. After the initial dialog appears, click Next.
5. Use the Browse function to select a directory to install MPC if the directory is different from the default path displayed in the "Select the installation path" field.
6. When installation is complete, click Next.

   Once the installation is complete, the final dialog indicates where you will find an uninstaller program and provides you with the option to generate an automatic installation script.

7. Click Done to close the Installation dialog.

To open MPC on a Mac:

1. Open a Finder window and navigate to the directory where you installed MPC (the default location is /Applications/Raritan/Raritan MPC/*version number*).
2. Double-click the desired device to establish a connection, type your user name and password, and click OK to log on.

Connecting to a Server via MPC when Alternate RADIUS Authentication is Enabled on the KX II-101

When Alternate RADIUS Authentication is enabled, you are authenticated exclusively against a remote authentication database. If the remote authentication database is inaccessible, you will be authenticated against a local authentication database and will be prompted to enter your local authentication username and password.

Remote authentication will be attempted again on the next login after you have successfully logged on and then logged out, or after the third unsuccessful attempt to log on with your local authentication database credentials.

See **User Authentication Process** in the Dominion KX II-101 Help for details about the Alternate RADIUS Authentication process and how it works with MPC.

Launching MPC from a Web Browser

Important: Regardless of the browser you use, you must allow pop-ups from the Dominion device's IP address in order to open MPC.

Important: Only Macs with an Intel® processor can run JRE 1.6 and, therefore, be used as a client. Mac 10.5.8 does not support MPC as a standalone client.

1. To open MPC from a client running any supported browser, type http://IP-ADDRESS/mpc into the address line, where IP-ADDRESS is the IP address of your Raritan device. MPC opens in a new window.

   Note: The Alt+Tab command toggles between windows only on the local system.

   When MPC opens, the Raritan devices that were automatically detected and which are found on your subnet are displayed in the Navigator in tree format.
2. If your device is not listed by name in the navigator, add it manually:
   a. Choose Connection > New Profile. The Add Connection window opens.

b. In the Add Connection window, type a device Description, specify a Connection Type, add the device IP address, and click OK. These specifications can be edited later.

3. In the Navigator panel on the left of the page, double-click the icon that corresponds to your Raritan device to connect to it.

Note: Depending on your browser and browser security settings, you may see various security and certificate check and warning messages. It is necessary to accept the options in order to open MPC.

Note: If you are using Firefox 3.0.3, you may experience problems launching the application. If this occurs, clear the browser cache and launch the application again.

Launching MPC on Mac Lion Clients

If you are using Mac® Lion on your client, Raritan's Multi-Platform Client (MPC) does not launch. Use the following workaround to launch MPC.

Delete the JavaApplicationStub from the install, and create a link from the correct JavaApplicationStub.

- rm /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub
- ln -s /System/Library/Frameworks/JavaVM.framework/Resources/MacOS/JavaApplicationStub /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub

To run, use:

- /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub

RRC Requirements and Installation Instructions

Important: RRC works only with Microsoft® Internet Explorer®. If you are using a different web browser, MPC loads automatically.

Most users access RRC via Internet Explorer, while other users, particularly those operating over a modem connection, access RRC standalone. Both options are detailed in this guide.

Note: Modem use is not supported with Raritan's Dominion KX101.

RRC Minimum System Requirements

The minimum system requirements for the Raritan Remote Client are:

- CPU Speed: 1.0 GHz
- RAM: 512 Mbytes

Note: Running the client software on system configurations below either of these specifications may impact performance and result in errors.

Installing and Opening Standalone RRC

Note: This step is optional. Devices can be accessed from a remote PC either by installing RRC software or by opening RRC via a web browser. Accessing Devices via a web browser does not require any software installation on a remote PC.

This section lists the steps required to invoke RRC using standalone software, which may be useful for accessing devices via modem or if you wish to close firewall access to ports 80 and/or 443.

1. Launch your web browser and go to Raritan's website (http://www.raritan.com/).
2. Click Support in the top navigation bar and then click Firmware Upgrades in the left navigation panel (or type the URL http://www.raritan.com/support/firmwareupgrades).
3. Scroll down the page until you see the appropriate product name and click on it.
4. Locate the version of the standalone RRC client you are using. The entry for the standalone RRC client is a .zip file which contains the release notes and the installer for standalone RRC. Check the release notes for the latest information.
5. Download the .zip file or simply click on the .zip file entry.
6. Double-click on the installer executable in the .zip file and follow the instructions in the InstallShield Wizard to complete the RRC installation. Be sure to check the release notes for the latest information and any release specific instructions.

   Depending upon the configuration of your PC, the RRC installation program may also automatically install DirectX® and Microsoft® Foundation Class libraries (if they are required). If they are installed, you are asked to restart your PC after the installation.
7. A Raritan Remote Client icon appears on your desktop after the installation is complete. Click on this icon to open the standalone RRC application.

   The standalone application can be uninstalled using the Add or Remove Programs function in the Windows® Control Panel.

Note: You must uninstall the application before installing a new version of standalone RRC.

Opening RRC from a Web Browser

Your device features web browser-access capabilities and can provide a connection from any Windows-based, remote PC running Microsoft® Internet Explorer® 6.0/7.0.

Security Settings

To access a device via the web, your web browser must be configured appropriately on the Internet Explorer security settings tab. Specifically:

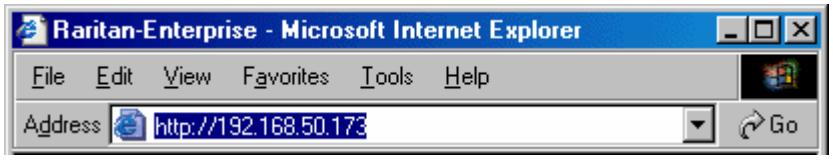
- "Download Signed ActiveX controls" should be set to either Enable or Prompt.
- "Run ActiveX controls and plug-ins" should be set to either Enable or Prompt.

Consult your Microsoft Internet Explorer documentation for additional information.

Note: Microsoft Windows 2000®, Windows XP®, and Windows 2003® operating systems restrict certain types of users from downloading and running ActiveX® controls and plug-ins regardless of the settings in Internet Explorer. Consult your Microsoft Windows documentation for more information.

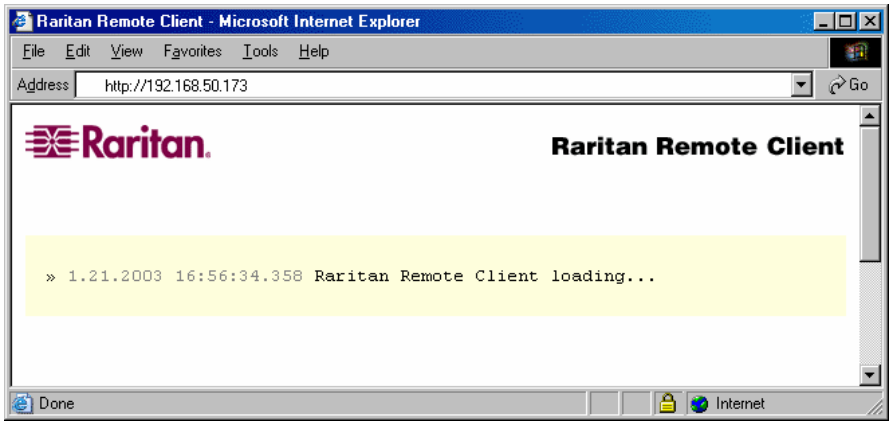
To open RRC:

1. Ensure that your browser security settings are configured appropriately and type the IP address assigned to your device in the URL field of your web browser.

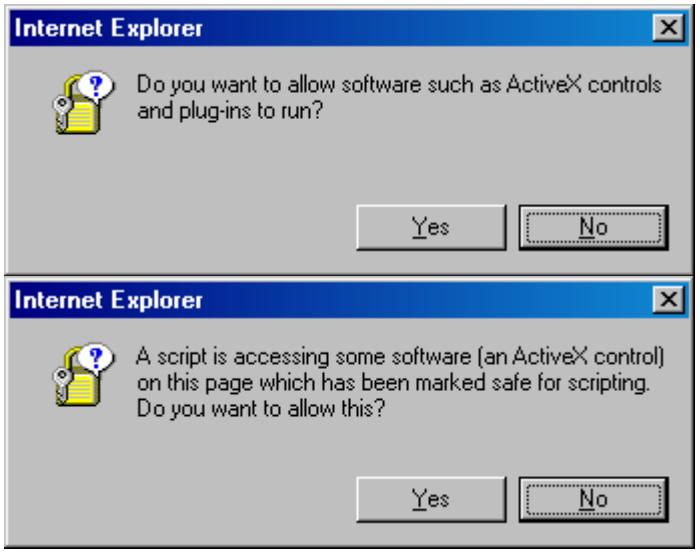


Note: Devices ship with the default IP address of 192.168.0.192. Note that an IP address must be used. Host names are not currently supported.

You are redirected to an HTTPS (128-bit) secure web page so you can open RRC.



2. Depending on your browser and its security configuration, you may see any or all of the following dialogs asking you to confirm you want to access and open an externally-provided application. Click Yes to accept these prompts.



Removing RRC from the Browser Cache

- To remove RRC from your browser cache for any reason, follow the standard procedure for your web browser software.

To remove cached files in Internet Explorer v6.0:

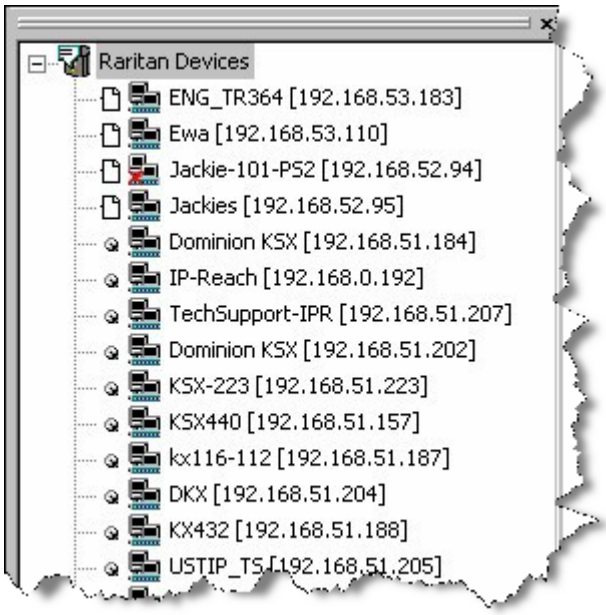
1. If you have used RRC recently, exit all instances of Internet Explorer and restart Internet Explorer.
2. On the Internet Explorer Tools menu, choose Internet Options.
3. When the Internet Options dialog appears, click on the General Settings tab and then click Delete Files.
4. Click on the Settings tab and then click View Objects.
5. Internet Explorer displays a list of cached objects. Select any entries named “TeleControl Class,” “Raritan Console,” or “Power Board” and delete them.

Operation

Navigator

The navigator provides a tree view of every known Raritan device. From this panel, access all Raritan networked devices for which a connection profile exists and/or all Raritan devices automatically identified on the network.

Note: Automatic Raritan device identification uses the UDP protocol and typically identifies all Raritan devices on your subnet. Network administrators rarely allow UDP broadcasts to function outside of a subnet. Automatic Raritan device identification finds only those Raritan devices that are configured to use the default TCP Port (5000) or another broadcast port, which is defined on the Advanced tab of the Options dialog (choose Tools > Options to access the Options dialog).



Device Naming in the MPC Navigator

In MPC, devices are named according to the Manager Name field on the Manager's Network Configuration page. Dominion devices are named according to the Device Name field on the Dominion Console Network Settings page.

Devices in the RRC Navigator

In RRC, profiled devices are listed in the Navigator according to the data in the Description field of the device's profile. Automatically-identified devices are identified according to the name assigned to them in that device's network configuration setting.

Device Ports in the Navigator

For each device to which you are connected, you are able to expand the tree associated with it to see each device port to which you have access. Ports with a green icon indicate that you are connected to that port. The port that is bolded in the Navigator indicates that it is the port currently displayed (active) in the remote desktop area of the application.

If no name is assigned to a port, by default it is listed in the Navigator as 'Unnamed' for Generation 1 devices and, for the KX II, as Dominion_KX2_PortN (N = port number).

Depending on the maximum number of KVM sessions the device can handle at once, if all device ports to which you are connecting are already occupied, an alert message appears and you must wait until one of the ports is available in order to connect.

Navigator Icons

Each device in the Navigator is assigned two icons. One icon represents the device's connection profile and the other icon represents its network status. A connection profile is generally created by a user in order to store personalized information about specific devices (see ***Connection Profiles*** (on page 84) for additional information). The connection status indicates the current status of the device.

Device Connection Profile Icons (Left Icon)

Icon	Description
	Profiled - A network connection profile exists for this device.
	Modem Profile - A modem connection profile exists for this device.
	Not Profiled - The device was found on the network but a connection profile does not exist for it.

Device Network Status Icons (Right Icon)

Icon	Description
	Connected (green) - You are currently authenticated and connected to this device.
	Available (black) - This device is currently available on the network but you are not currently connected to it.
	Unavailable - A profile exists for this device but it is not currently available on the network. (Note that all devices to which you *are not* currently connected and that have modem profiles use this icon.)

Port Connection Status Icons

For each server port listed in the Navigator, the following icons can be associated with it depending on its status:

Icon	Description
	Connected
	Available for connection.
	Unavailable (either no device is connected or access is blocked).
	In use by another user (may be unavailable depending on permissions).

Customizing the Navigator

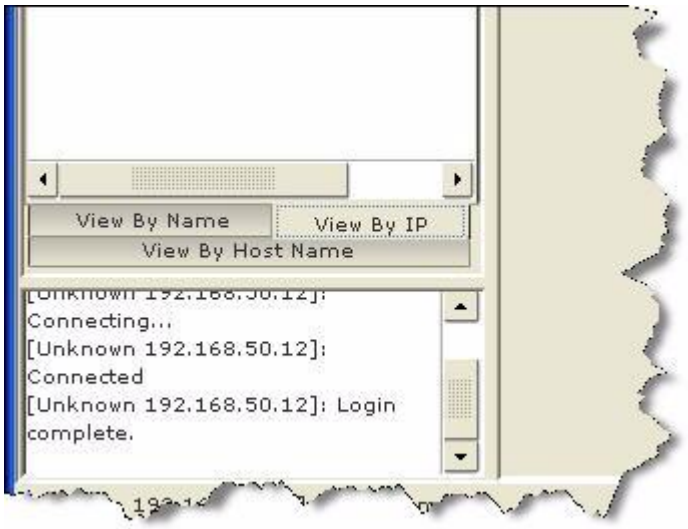
Use specific tools in the toolbar to customize some Navigator attributes:

Icon	Action	Description
	Display/Hide Navigator	Select Navigator in the View menu to toggle between displaying and hiding the Navigator.
	Refresh Navigator	Updates the device status information displayed in the Navigator.
	Browse Discovered Devices	When enabled, Show Discovered Devices displays devices that are “not profiled” but have been found on the network. This option can also be enabled by choosing View > Show > Discovered Devices. *Note: The Browse Discovered Devices*

Icon	Action	Description
		option is the only method of connecting to a Raritan device configured to use a DHCP IP address.

MPC Navigator Tabs

MPC tabs at the base of its Navigator pane. These tabs allow you to change how you display devices. Click the View By Name tab to sort the list alphabetically by name, click the View By IP tab to sort the list numerically by IP address, or click on the View by Host Name tab to sort the list alphabetically by display name.



These tabs are available only in the MPC interface.

Navigator Display and Sort Options

To better organize your view of all ports, use the Show and Sort options in the View menu. Note that you do not need an open connection to a target to show and sort targets in the Navigation panel.

Showing Ports

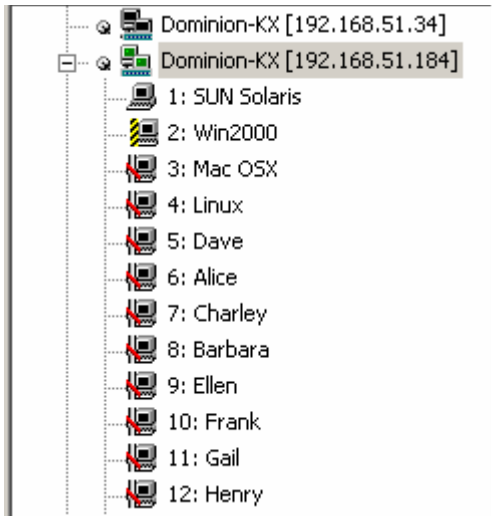
- Discovered Devices - Shows or hides discovered devices from the Navigator view. You will not see broadcast messages when this option is disabled (not selected).
- Unassigned Channels - Shows or hides channels with no assigned targets. Note that the default for Generation 1 (G1) devices is to show unassigned channels (option is enabled), whereas the default is to hide unassigned channels (option is disabled) for Generation 2 (G2) devices.
- Tools - Shows or hides the Admin and Diagnostic ports.
- Groups - Shows all port groups.

Note: These settings are saved from session to session.

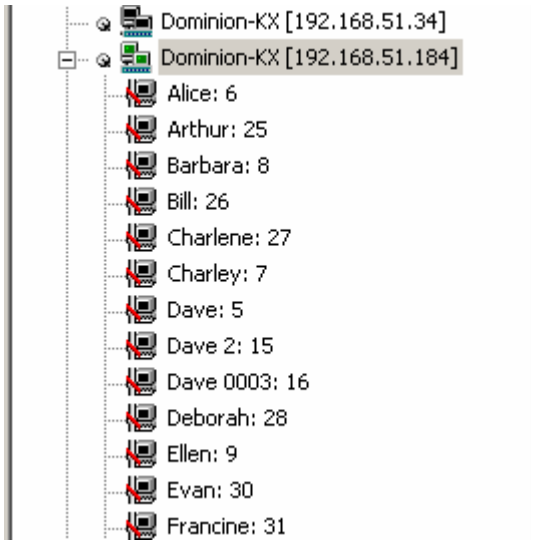
Sorting Ports

Use the Sort options on the View menu to organize port information. You are able to sort ports by channel number, channel name, or channel status.

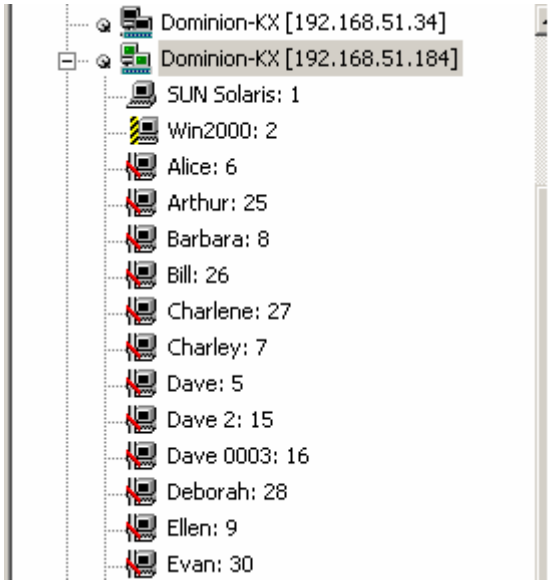
- Channel Number - When sorted by channel (View > Sort > Channel), ports are listed numerically.



- Name - When sorted by name (View > Sort > Name), port names are sorted alphanumerically within each group.



- Status - When sorted by status (View > Sort > Status), ports are sorted in the following order:
  - Active Channels
  - Busy Channels
  - Available Devices
  - Unavailable Devices



Note: Sorting ports does not apply to KX II-101.

Set Scan Group

a port scanning feature that searches for selected targets and displays them in a slide show view, allowing you to monitor up to 32 targets at one time. You can connect to targets or focus on a specific target as needed. Scans can include standard targets, blade servers, tiered Dominion devices, and KVM switch ports. Configure scan settings from either the Virtual KVM Client (VKC) or Active KVM Client (AKC). See Configure Scan Settings in VKC and AKC for more information.

Note: Scanning for tiered devices is not supported by the Multi-Platform Client (MPC).

When you start a scan, the Port Scan window opens. As each target is found, it is displayed as a thumbnail in a slide show. The slide show scrolls through the target thumbnails based on the default interval of 10 seconds or according to the interval you specify. As the scan scrolls through the targets, the target that is the focus of the slide show displays in the center of the page. See Configure Scan Settings in VKC and AKC.

Change the time between the slide show thumbnail rotation, the thumbnail focus interval, and the page display settings from the Scan Settings tab of the Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC) Tools > Options dialog. See Configure Scan Settings in VKC and AKC.

The name of the target is displayed below its thumbnail and in the task bar at the bottom of the window. If a target is busy, a blank screen is displayed instead of the target server access page.

The status of each target is indicated by green, yellow and red lights that are displayed below the target thumbnail and, as the target is the focus of the rotation, in the task bar. The status lights indicate the following:

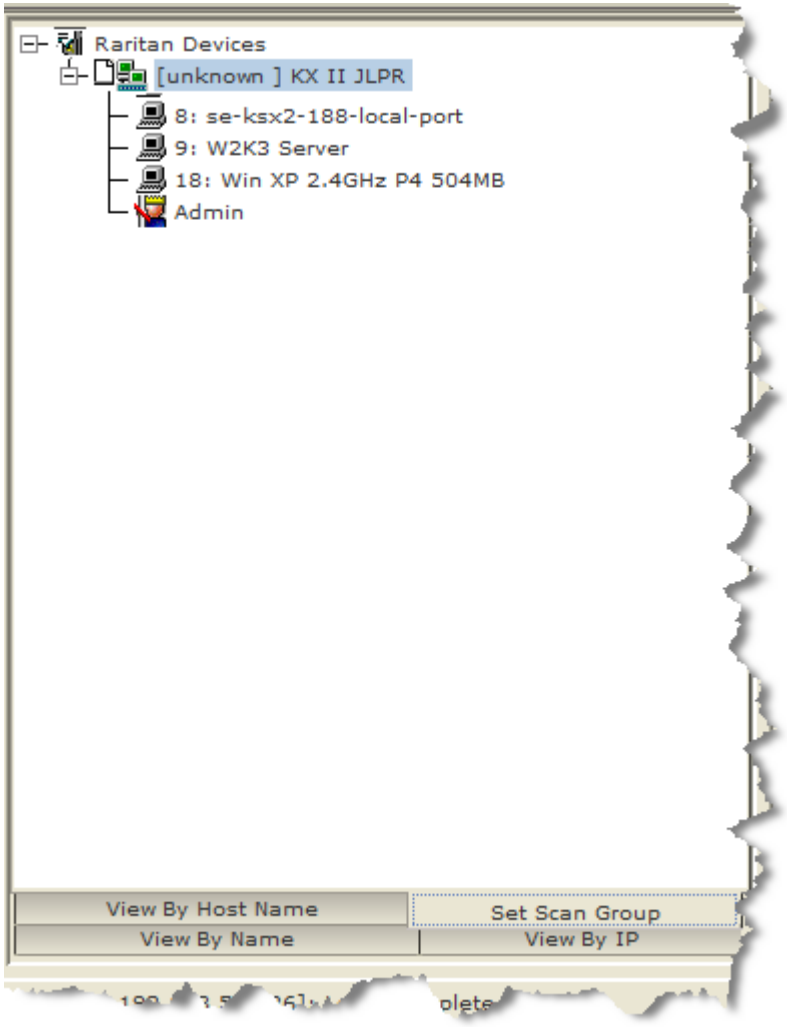
- Green - the target is up/idle or up/connected
- Yellow - the target is down but connected
- Red - the target is down/idle, busy, or otherwise not accessible

Note: This feature is only supported by the KX II.

To begin a scan in MPC:

1. Click on Set Scan at the bottom of the Navigator.
2. From the list of targets in the Navigator, use Ctrl + click select each target you want to include in the scan, or use Shift + click to select a range of targets.
3. Once you've selected all the targets to include in the scan, right click next to the selected targets and select Start Scan. The targets detected in the scan are displayed.

See ***Using Scan Options*** (on page 73) for information on the options available to you while scanning targets.



Using Scan Options

Following are options available to you while scanning targets. With the exception of the Expand/Collapse icon, all of these options are selected from the Options menu in the upper left of the Port Scan viewer. The options will return to their defaults when you close the window.

Note: Configure scan settings such as the display interval from either the Virtual KVM Client (VKC) or Active KVM Client (AKC). See Configure Scan Settings in VKC and AKC for more information.

Hide or View Thumbnails

- Use the Expand/Collapse icon  at the upper left of the window to hide or view thumbnails. Expanded is the default view.

Pause the Thumbnail Slide Show

- Pause thumbnails from rotating between one target and the next by selecting Options > Pause. Rotating thumbnails is the default setting.

Resume the Thumbnail Slide Show

- Resume the thumbnail rotation by selecting Options > Resume.

Size the Thumbnails in the Port Scan Viewer

- Enlarge the size of the thumbnails by selecting Options > Size > 360x240.
- Minimize the size of the thumbnails by selection Options > Size > 160x120. This is the default thumbnail size.

Change the Orientation of the Port Scan Viewer

- View thumbnails along the bottom of the Port Scan viewer by selecting Options > Split Orientation > Horizontal.
- View thumbnails along the right of the Port Scan viewer by selecting Options > Split Orientation > Vertical. This is the default view.

Toolbars

Standard Toolbar

The Standard toolbar provides one-click access to the most frequently-used commands.

To display the Standard toolbar:

- Choose View > Standard Toolbar.

Following is a list of the buttons in the standard toolbar as well as a description of the action performed once the buttons are selected. Additionally, if there are menu options or shortcut menu options that perform the same task, they are listed, too.

Button	Button name	Description
	New Profile	Creates a new Navigator entry for a Raritan device. Same result as choosing Connection > New Profile in the menu.
	Connection Properties	Opens the Modify Connection Properties dialog to manually adjust bandwidth options (such as connection speed, color depth, and so forth). Same as choosing Connection > Properties or choosing Connection Properties on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Video Settings	Opens the Video Settings dialog, allowing you to manually adjust video conversion parameters. Same as choosing Video > Video Settings or choosing Video Settings.
	Color Calibration	Adjusts color settings to reduce excess color noise. Same as choosing Video > Color Calibrate.
	Target Screenshot	Click to take a screenshot of the target server and save it to a file of your choosing.
	Audio	Click to connect to a digital audio device. *Note: This feature is only available in KX II*

Button	Button name	Description
		2.4.0 or higher.
	Synchronize Mouse	In dual-mouse mode, forces realignment of the target server mouse pointer with the mouse pointer. Same as choosing Mouse > Synchronize Mouse or choosing Synchronize Mouse on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Refresh Screen	Forces a refresh of the video screen. Same as choosing Video > Refresh Screen or choosing Refresh Screen on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Auto-sense Video Settings	Forces a refresh of the video settings (resolution, refresh rate). Same as choosing Video > Video Settings or choosing Video Settings on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Enter On-Screen Menu	Not applicable for the device. Used by the application with other Raritan products. Same as choosing Keyboard > Enter On-Screen Menu. *Note: This function is not available on the KSX II.*
	Exit On-Screen Menu	Not applicable for IP-Reach or Dominion. Used by the application with other Raritan products. Alternatively, select Esc on the keyboard. Same as choosing Keyboard > Exit On-Screen Menu. *Note: This function is not available on the KSX II.*
	Smart Card	Opens a dialog that allows you to select from a list of mounted smart card readers.
	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Del hot key combination to the target server. Same as choosing Keyboard > Send Ctrl+Alt+Del.

Button	Button name	Description
	Single Cursor Mode	Starts Single Cursor mode in which the local mouse pointer no longer appears onscreen. Same as choosing Mouse > Single Cursor Mode. Press Ctrl+Alt+X to exit this mode. Alternatively, choose Single/Double Cursor from the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Full Screen Mode	Maximizes the screen real estate to view the target server desktop. Same as choosing View > Target Screen Resolution (in MPC) or Full Screen (in RRC). Alternatively, press Ctrl+Left Alt+M to open the shortcut menu and then choose Full/Normal Screen or press the F key on your keyboard.
	Scaling	Increases or reduces the target video size so you can view the entire contents of the target server window without using the scroll bar.
	Show/Hide Navigator	Toggles the Navigator panel between visible and hidden. Same as choosing View > Navigator.
	Refresh Navigator	Forces a refresh of the data displayed in the Navigator.
	Show/Hide Browse All Devices	Toggles between displaying and not displaying Raritan devices in the Navigator that are automatically identified on the network and that do not have preconfigured profiles associated with them.
	About	Displays the application version information. Same as choosing Help in the menu bar.

MPC Connected Server(s) Toolbar

The Connected Server(s) toolbar is comprised of a button for each connected target server port, thus enabling quick access to connected targets. When you connect to a port, a button corresponding to that port is added to the toolbar and labeled with the name of the port. Conversely, when you disconnect from a port, the corresponding button is removed from the toolbar.

Note: In Single Mouse mode, the Connected Server(s) Toolbar appears on the target but cannot be accessed.

By default, the Connected Server(s) toolbar is enabled (visible). To disable it, deselect Connected Server(s) Toolbar in the View menu. Buttons corresponding to windows that do not support Full Screen mode are not shown in the toolbar. For example, serial ports, generation one (G1) admin ports, and G1 diagnostic ports are not displayed in the toolbar in Full Screen mode.

While in Full Screen mode, view the Connected Server(s) toolbar by hovering your mouse over the top of the screen. To use this feature, the Connected Servers Toolbar option must be selected in the View menu.

To display the Connected Server(s) toolbar (when not already visible):

- Choose View > Connected Server(s) Toolbar.

To view the window for a target server:

- Click the button that corresponds to the appropriate connected target server you want to view. The window for the corresponding target server is displayed and the button for the selected port is highlighted. In Full Screen mode, note that this action is window swapping, not video switching.

When you click a button that is already highlighted, the corresponding window is minimized. If you click that button again, the window is brought forward and maximized.

Status Bars

MPC Status Bar

The status bar displays session information about your connection to a Raritan device. This information includes:

Icon	Session information	Description
	Concurrent connections indicator	Indicates that multiple remote users are currently connected to the same target server on the device. One icon indicates a single user is connected, and two icons indicates two or more users are connected. Concurrent connection ability can be set globally under PC share mode on the Manager Security Settings page or set per individual user in the Concurrent Access Mode setting on the Manager User Account Settings page. For the device, concurrent connection ability can be set using the PC Share Mode option in the Security Settings page: PC-Share permits concurrent access and Private limits server access to one user at a time.
CAP, NUM, SCRL	Lock key indicators	Indicates the status of the current target KVM Server, in respect to the activation of the Caps-Lock, Num-Lock, and Scroll-Lock keys. If these keys are enabled on the target server being viewed, this affirmative status is reflected on the status bar.

Note: If a light is used on your keyboard to indicate the Scroll Lock, Num Lock, and Caps Lock key is active, it may or may not be in sync with the lock key indicator status displayed on the status bar. See the status bar as your guide if this occurs.

RRC Status Bar

The status bar displays session information about your connection to a Raritan device. This information includes:

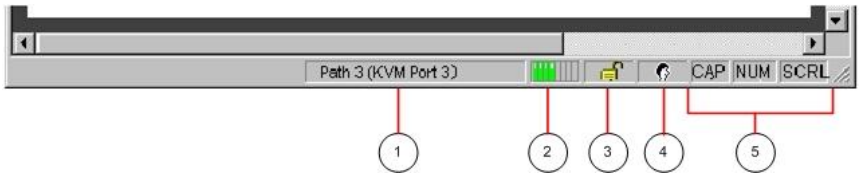


Diagram key	Session information	Description
1	Video sensing status/path indicator	Indicates when video sensing occurs during connections to target KVM server ports.
2	Bandwidth usage indicator	Indicates how much of your total available bandwidth is currently being used. The connection speed setting determines total available bandwidth. This setting is defined on the Compression tab of the Connection Properties dialog, which is accessed by choosing Connection > Properties, or pressing Ctrl+Left Alt+ M and then choosing Connection Properties.
3	Security indicator	Indicates whether the current remote connection is protected by encryption. Encryption requirements are set during configuration of your Raritan device. When a device is configured for no encryption or SSL authentication, the Security Indicator is represented on the status bar by an open lock icon. When SSL authentication, data encryption, or SSL encryption is applied, the security indicator is represented on the status bar by a closed lock.
4	Concurrent connections indicator	Indicates that multiple remote users are currently connected to the same target server on the device. One icon indicates a single user is connected, and two icons indicates two or more users are connected. Concurrent connection ability can be set globally under PC share mode on the Manager Security Settings page or set per individual user in the Concurrent Access Mode setting on the Manager User Account Settings page. For the device, concurrent connection ability can be set using the PC Share Mode option in the Security Settings page: PC-Share permits concurrent access and Private limits server access to one user at a time.

Diagram key	Session information	Description
5	Lock key indicators	Indicates the status of the current target KVM Server, in respect to the activation of the Caps-Lock, Num-Lock, and Scroll-Lock keys. If these keys are enabled on the target server being viewed, this affirmative status is reflected on the status bar.

Note: If a light is used on your keyboard to indicate the Scroll Lock, Num Lock, and Caps Lock key is active, it may or may not be in sync with the lock key indicator status displayed on the status bar. See the status bar as your guide if this occurs.

Screen Modes

Besides a standard view, full screen view and a scaling option are available. These options increase the remote desktop area and make viewing the target video easier.

MPC Full Screen Mode

Full Screen mode provides you with the ability to view the target server desktop in Full Screen mode, which removes all toolbars from view.

Activate Full Screen mode once you are connected to a target by doing one of the following:

- Click the Full Screen button  in the toolbar and then click OK in the confirmation message that appears.
- Choose View > Full Screen and then click OK in the confirmation message that appears.
- Press Ctrl+Left Alt+M to open the shortcut menu. Next, press the F key on your keyboard or use your mouse to choose Full/Normal Screen. Click OK in the confirmation message that appears.

Hover your mouse at the top of the screen while in full screen mode to display the MPC menus. To exit Full Screen mode, use the shortcut menu or click the Close icon  that appears at the top right of the page when you hover your mouse along the top of the screen.

While in Full Screen mode, you are able to view the Connect Server toolbar by hovering your mouse over the top of the screen. To use this feature, the Connected Servers Toolbar option must be selected in the View menu.

Additionally, while in Full Screen mode, your monitor's resolution may be adjusted to match the resolution of the target server (provided your graphics system supports it). If your graphics system does not support the resolution of the target system, you are not able to activate Full Screen mode and a message appears requesting that you change your video resolutions first.

Tip: To view the video resolutions your system supports in a Windows® operating system environment, access your computer's Control Panel from the Windows Start menu, double-click Display, and click the Settings tab.

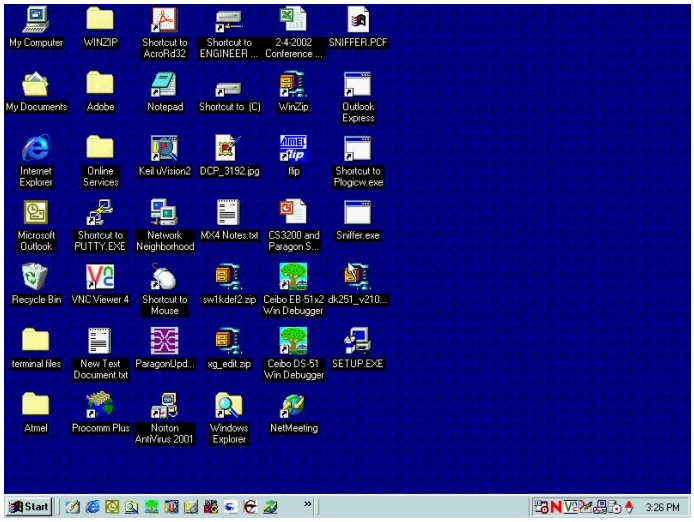
RRC Full Screen Mode

Full screen mode removes the surrounding RRC graphical interface and your local desktop area, filling your screen with the video from the target server. Your screen's resolution is adjusted to match the resolution of the target server (provided your graphics system supports it). If your graphics system does not support the resolution of the target system, you are unable to activate full screen mode and a message appears requesting that you change your video resolutions first.

Note: To view the video resolutions your system supports in a Windows® operating system environment, access your computer's Control Panel from the Windows Start menu, double-click on Display, and click on the Settings tab.

Activate full screen mode in one of the following ways once you are connected to a target:

- Click the Full Screen icon in the toolbar and then click OK in the confirmation message that appears.
- Choose View > Full Screen and then click OK in the confirmation message that appears.
- Press Ctrl+Left Alt+M to open the shortcut menu. Next, press the F key on your keyboard or use your mouse to choose Full/Normal Screen. Click OK in the confirmation message that appears.



Raritan.

MPC Scaling

Scaling your target window size allows you to view the entire contents of the target server window. This feature increases or reduces the size of the target video to fit the window size and maintains the aspect ratio. This allows you to see the entire target server desktop while in standard view.

To activate Scaling, do one of the following:

- Choose View > Scale Video.
- Click the Scaling button  on the toolbar.
- To exit this mode and return the target window to its previous size, deselect Scale Video on the View menu or click the Scaling button once again.

Note: Enabling Scale Video scales the complete target video image to fit the remote desktop area as it grows or shrinks. Combine this setting with target screen resolution for a 'full page' effect on targets with a higher resolution than your desktop.

RRC Scaling

Scaling your target window size allows you to view the entire contents of the target server window. This feature increases or reduces the size of the target video to fit the window size and maintains the aspect ratio. This allows you to see the entire target server desktop while in standard view.

To activate Scale Video mode, do one of the following:

- Choose View > Scale.
- Click the Scaling button  on the toolbar.

To exit this mode and return the target window to its previous size, choose Scale on the View menu or click the Scaling button once again.

Note: Enabling Scale Video scales the complete target video image to fit the remote desktop area as it grows or shrinks. Combine this setting with target screen resolution for a full page effect on targets with a higher resolution than your desktop.

Auto-Scroll

The auto-scroll feature automatically scrolls the video display in the direction of the cursor as the cursor approaches the edge of the display. A thin border appears around the perimeter of the remote desktop area to indicate the function is on. When enabled, if you see scroll bars and then move the cursor onto the border, the page automatically scrolls in the appropriate direction.

The scroll border is activated by selecting Show Scroll Borders in the Options dialog, which is accessed by choosing Tools > Options.

Connection Profiles

Connection profiles store important information about your Raritan device such as the IP address, custom TCP ports, preferred compression settings, and custom security keys. A profile is required to access devices outside your subnet and to access devices using a dial-up connection.

Through profiles, you can set up personalized connections. These profiles are not shared among other users.

The information collected when creating a new connection profile differs based on Generation 1 and Generation 2 devices.

Tip: If your Raritan device is configured to use a custom TCP port or a group security key, first create a connection profile to access the device.

Managing Profiles in KX, KSX and KX-101 G1 Devices

Creating, Modifying and Deleting Profiles in MPC

To create a profile:

1. There are two ways to create a profile:
   - For automatically discovered devices, right-click the device name in the Navigator and choose Add Profile from the shortcut menu.
   - For other devices, choose Connection > New Profile.

     The Add Connection dialog appears. Options are organized into three tabs.

   Note: The Compression and Security tabs are not available for Generation 2 devices.

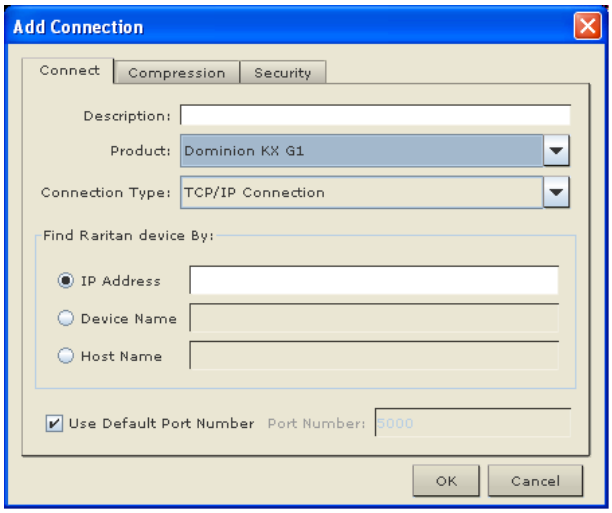
   Connect Tab

2. On the Connect tab, type a meaningful description of the device in the Description field. This description identifies the Raritan device in the Navigator.

3. From the Product drop-down, choose the Raritan product you are using.

TCP/IP Connections

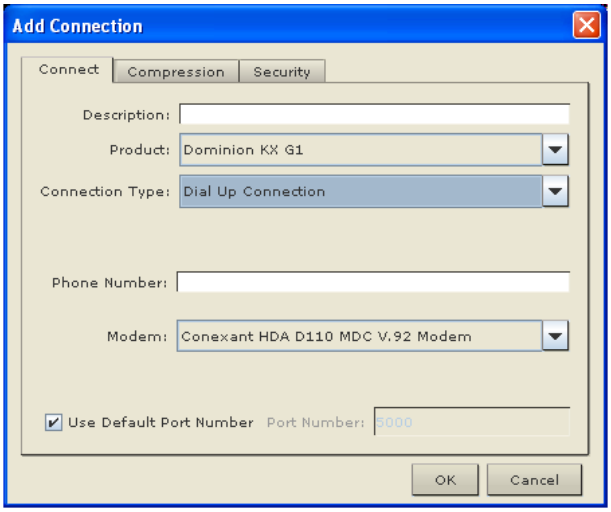
4. Select the type of connection from the Connection Type drop-down.
   a. If TCP/IP Connection is selected for a LAN/WAN connection, complete the information in the "Find Raritan device By" section:
   - Type the IP address assigned to your Raritan device.
   - Type the name assigned to your Raritan device during initial setup.
   - Type the Domain Name Server (DNS) name in the Host Name field. Use this option if you use a DNS server to resolve a DNS name to the IP address assigned to your Raritan device.



Dial-up Connections

   a. Select Dial Up Connection from the Connection Type drop-down for a direct analog modem connection to the Raritan device. Type the parameters that should be used to establish a connection.
   - Enter the phone number for the dial-up connection. Remember to include any additional codes that should be dialed to establish a connection, such as country codes, area codes, or outside line access codes.
   - Select the modem (as configured in Windows) from the drop-down list that will be used to dial and connect to your Raritan device.

Note: For security reasons, you must use the MPC standalone client if you require modem access. Further, one modem on a client PC can be used for only one device connection.



Note: Dial-up is not support in KX II-101.

5. Select the Use Default Port Number checkbox to use the default port number (5000). For TCP Ports, devices are automatically configured to use TCP Port 5000 when communicating with the client.

   If you do not want to use the default port number, deselect the checkbox and type the port number in the Port Number field.

   Compression Tab

6. Set the Connection Speed.

   Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. Devices can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available:

   - Auto Detect
   - 1G Ethernet
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)
   - 384 kb (Slow DSL/T1)

- 256 kb (Cable)
- 128 kb (Dual ISDN)
- 56 kb (ISP Modem)
- 33 kb (Fast Modem)
- 24 kb (Slow Modem)

Note: Raritan recommends that if you are connecting to the device via modem, you set the connection speed to 33kb.

7. Set the Color Depth.

   Devices can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list. Depending on the Raritan device in use, different options may be available:

   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White

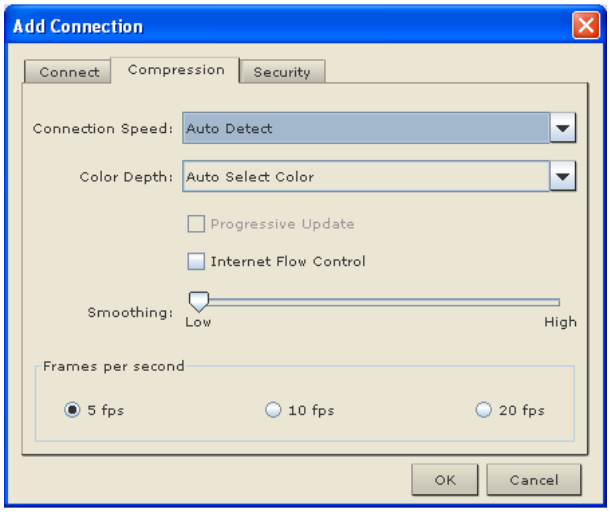
   Important: For most administrative tasks (server monitoring, reconfiguring, and so forth), administrators do not require the full 24-bit or 32-bit color spectrum made available by most video graphics cards. Attempting to transmit such high color depths wastes network bandwidth.

   Note: If you are connecting to the device via a modem, Raritan recommends setting the color depth to 4-bit gray.

8. Select Progressive Update to increase the usability in constrained bandwidth environments. When Progressive Update is enabled, the device initially sends an image of the remote desktop at lower color depths. Higher color depth images are provided as the bandwidth allows.

   Note: When Color Depth is set to Auto Select Color (default), Progressive Update is automatic. The device will enable/disable Progressive Update as required, disabling it for fast connections and enabling it for slow connections.

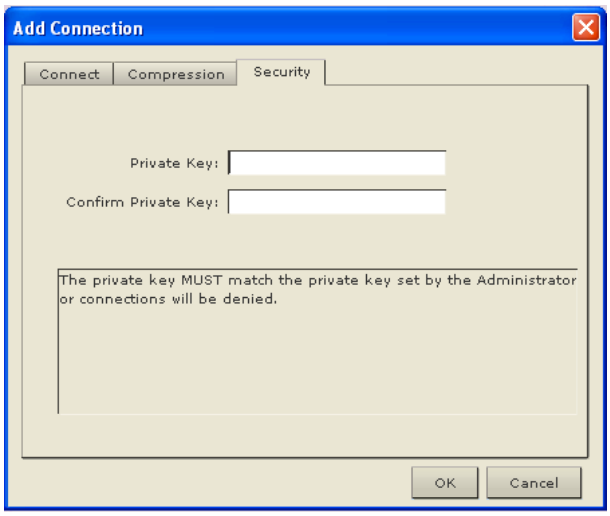
9. Selecting the Internet Flow Control checkbox ensures that packets transmitted by the device are received and reconstructed by the client application in the correct order. This is useful when using a device over an unpredictable public WAN (particularly in international scenarios).
10. Use the slider to select the desired level of video Smoothing (15-bit mode only). The level determines how aggressively to blend page regions with small color variation into a single, smooth color. Smoothing improves the appearance of the target video by reducing the video noise that is displayed.
11. Select "Frames per second". This setting instructs MPC on how often to redraw the video display of the target. This only affects the client display behavior and has no bearing on the data rate of the video being sent to the client. Setting this option higher makes the video appear smoother but also requires more processing power.



Security Tab

12. Enter the private security key in the Private Key field if your device is configured to use a private security key. Entering a security key allows you to gain the authorization required to initiate a connection to that device.
13. Retype the private security key in the Confirm Private Key field to ensure no typographical errors were made.

14. Click OK to create the connection profile.



To modify a profile:

1. Select the device in the Navigator panel and right-click it.
2. Choose Modify Profile. The Modify Connection dialog appears.
3. Update the fields as appropriate.
4. Click OK.

To delete a profile:

1. Select the device with a profile in the Navigator and right-click it.
2. Choose Delete Profile.
3. When prompted to confirm the deletion, click Yes to delete the profile for this device or click No to return to the application without deleting.

Note: The device only supports modem connections to the Administrative functions in MPC. Port functions are not supported via modem.

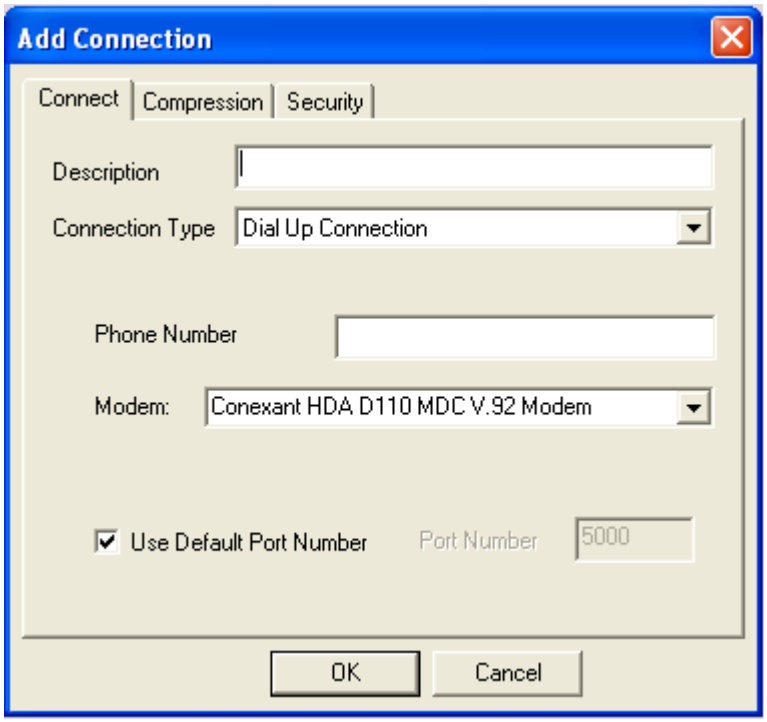
Creating, Modifying and Deleting Profiles in RRC

To create a profile:

1. There are two ways to create a profile:
   - For automatically discovered devices, right-click the device name in the Navigator and choose Add Profile from the shortcut menu.
   - For other devices, choose Connection > New Profile.

   The Add Connection dialog appears. Options are organized into three tabs.

Note: The Compression and Security tabs are not available for Generation 2 devices.



Connect Tab

2. On the Connect tab, type a meaningful description of the device in the Description field. This description identifies the Raritan device in the Navigator.
3. Select Dial Up Connection from the Connection Type drop-down for a direct analog modem connection to the Raritan device. Type the parameters that MPC or RRC should use to establish a connection. Dial up connection does not apply to Generation 2 (G2) or KX101.
   - Enter the phone number for the dial-up connection. Remember to include any additional codes that should be dialed to establish a connection, such as country codes, area codes, or outside line access codes.
   - Select the modem (as configured in Windows) from the drop-down list that will be used to dial and connect to your Raritan device.

Note: For security reasons, you must use the MPC standalone client if you require modem access. Further, one modem on a client PC can be used for only one device connection.

4. Select the Use Default Port Number checkbox to use the default port number (5000). For TCP Ports, devices are automatically configured to use TCP Port 5000 when communicating with the client.

   If you do not want to use the default port number, deselect the checkbox and type the port number in the Port Number field.

   Compression Tab

5. Set the Connection Speed.

   Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. Devices can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available:

   - Auto Detect
   - 1G Ethernet
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)
   - 384 kb (Slow DSL/T1)
   - 256 kb (Cable)
   - 128 kb (Dual ISDN)
   - 56 kb (ISP Modem)
   - 33 kb (Fast Modem)
   - 24 kb (Slow Modem)

6. Set the Color Depth.

   Devices can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list. Depending on the Raritan device in use, different options may be available:

   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White

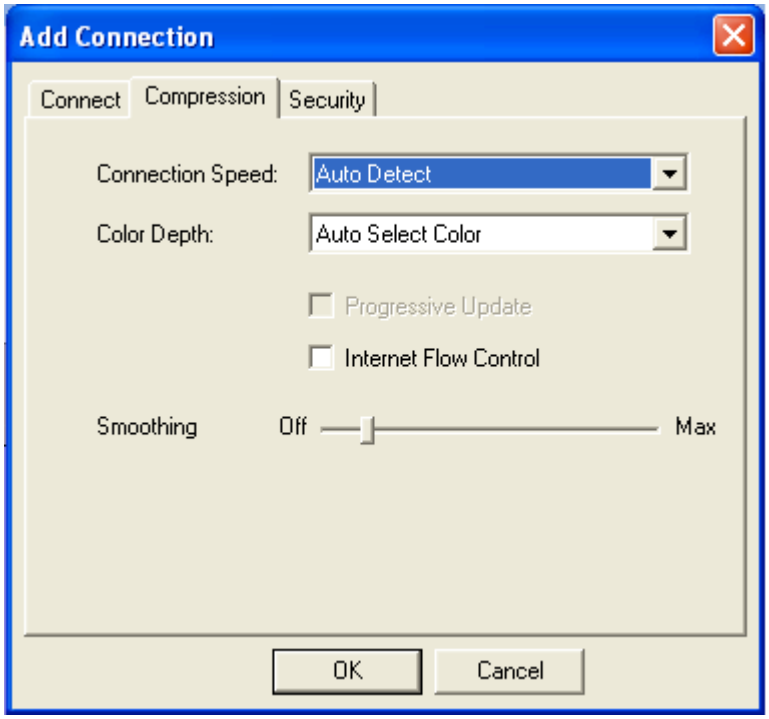
Important: For most administrative tasks (server monitoring, reconfiguring, and so forth), administrators do not require the full 24-bit or 32-bit color spectrum made available by most video graphics cards. Attempting to transmit such high color depths wastes network bandwidth.

7. Select Progressive Update to increase the usability in constrained bandwidth environments. When Progressive Update is enabled, the device initially sends an image of the remote desktop at lower color depths. Higher color depth images are provided as the bandwidth allows.

Note: When Color Depth is set to Auto Select Color (default), Progressive Update is automatic. The device will enable/disable Progressive Update as required, disabling it for fast connections and enabling it for slow connections.

8. Selecting the Internet Flow Control checkbox ensures that packets transmitted by the device are received and reconstructed by the client application in the correct order. This is useful when using a device over an unpredictable public WAN (particularly in international scenarios).

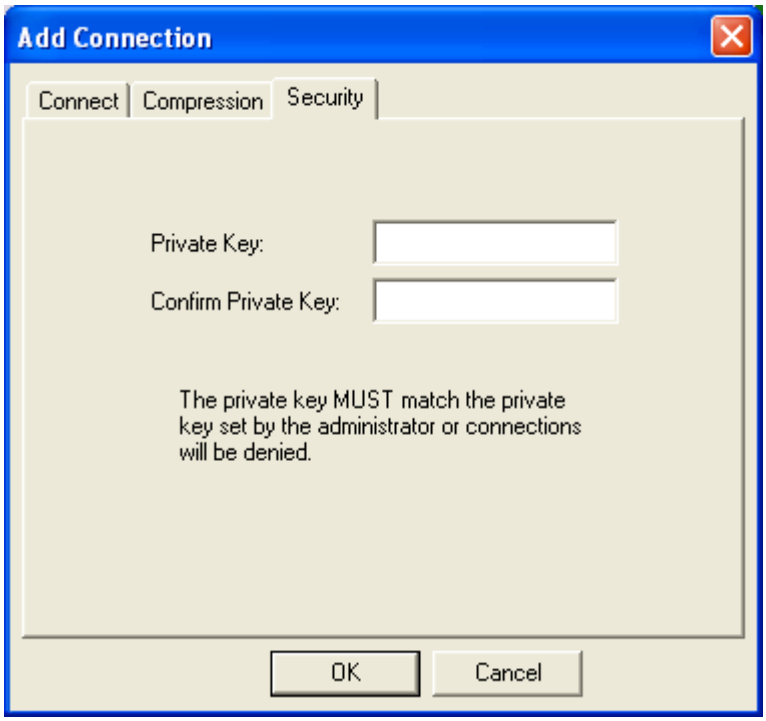
9. Use the slider to select the desired level of video Smoothing (15-bit mode only). The level determines how aggressively to blend page regions with small color variation into a single, smooth color. Smoothing improves the appearance of the target video by reducing the video noise that is displayed.



Security Tab

10. Enter the private security key in the Private Key field if your device is configured to use a private security key. Entering a security key allows you to gain the authorization required to initiate a connection to that device.
11. Retype the private security key in the Confirm Private Key field to ensure no typographical errors were made.

12. Click OK to create the connection profile.



Managing Profiles in KX, KSX and KX-101 G2 Devices

Creating, Modifying and Deleting Profiles in MPC - Generation 2 Devices

To create a profile:

1. There are two ways to create a profile:
   - For automatically discovered devices, right-click the device name in the Navigator and choose Add Profile from the shortcut menu.
   - For other devices, choose Connection > New Profile.

   The Add Connection dialog appears. Options are organized into three tabs.

   Note: The Compression and Security tabs are not available for Generation 2 devices.

2. On the Connect tab, type a meaningful description of the device in the Description field. This description identifies the Raritan device in the Navigator.
3. From the Product drop-down, choose the Raritan product you are using.
4. Select the type of connection from the Connection Type drop-down.

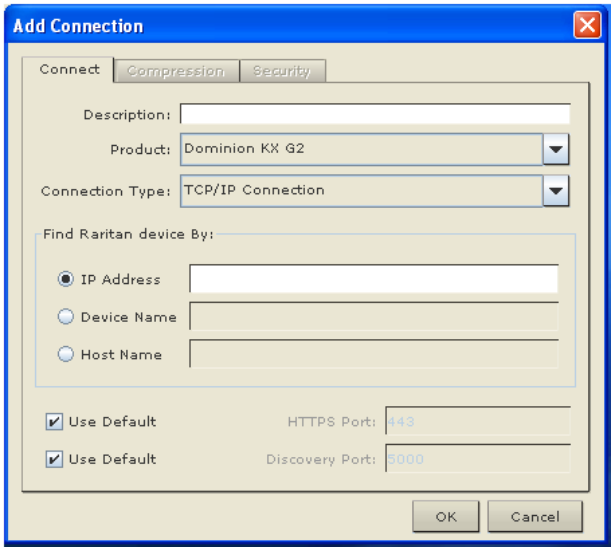
TCP/IP Connections

a. If TCP/IP Connection is selected for a LAN/WAN connection, complete the information in the "Find Raritan device By" section:

- Type the IP address assigned to your Raritan device.
- Type the name assigned to your Raritan device during initial setup.
- Type the Domain Name Server (DNS) name in the Host Name field. Use this option if you use a DNS server to resolve a DNS name to the IP address assigned to your Raritan device.

a. To use the default port settings for the HTTPS port (port 443) and the Discovery port (port 5000), leave their respective Use Default checkboxes selected. As long as the Use Default checkboxes are selected, the HTTPS Port and Discovery Port fields are not active.

If you would like to change the default ports to other ports, deselect the respective Use Default checkbox and enter the port in the appropriate field. For example, to change the HTTPS port, deselect its Use Default checkbox and enter the port number in the HTTPS field.



Dial-up Connection

b. Select Dial Up Connection from the Connection Type drop-down for a direct analog modem connection to the Raritan device. Type the parameters that should be used to establish a connection.

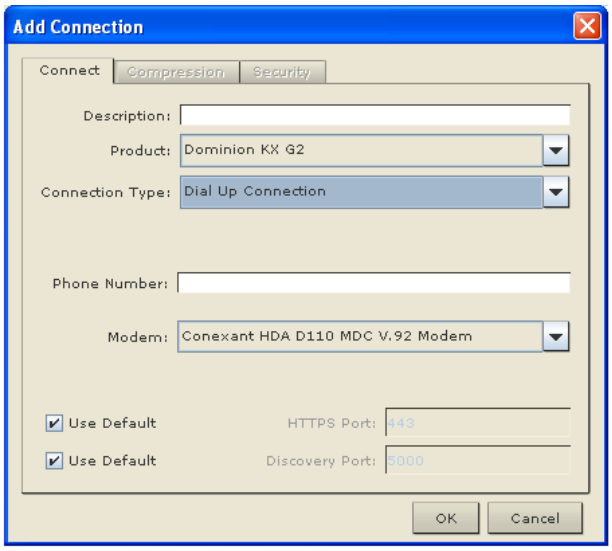
- Enter the phone number for the dial-up connection. Remember to include any additional codes that should be dialed to establish a connection, such as country codes, area codes, or outside line access codes.

- Select the modem (as configured in Windows) from the drop-down list that will be used to dial and connect to your Raritan device.

Note: For security reasons, you must use the MPC standalone client if you require modem access. Further, one modem on a client PC can be used for only one device connection.

a. To use the default port settings for the HTTPS port (port 443) and the Discovery port (port 5000), leave their respective Use Default checkboxes selected. As long as the Use Default checkboxes are selected, the HTTPS Port and Discovery Port fields are not active.

   If you would like to change the default ports to other ports, deselect the respective Use Default checkbox and enter the port in the appropriate field. For example, to change the HTTPS port, deselect its Use Default checkbox and enter the port number in the HTTPS field.



To modify a profile:

1. Select the device in the Navigator panel and right-click it.
2. Choose Modify Profile. The Modify Connection dialog appears.
3. Update the fields as appropriate.
4. Click OK.

To delete a profile:

1. Select the device with a profile in the Navigator and right-click it.
2. Choose Delete Profile.

3. When prompted to confirm the deletion, click Yes to delete the profile for this device or click No to return to the application without deleting.

Establishing a New Connection

Note: Depending on your version of the JRE™, you might receive a certificate message when using the standalone application to access a Dominion device. You have to accept the certificate in order to establish the connection.

To connect to a device, double-click the device's icon in the Navigator, then type your user name and password to connect. Right-click the device name in the Navigator and select New Connection.

Note: The default device login user name is admin and the default password is raritan. You have administrative privileges using these login credentials.

If you do not see an icon for your device in the Navigator, follow the instructions on creating new profiles, which is available in this section.

If you are having problems connecting to a device, be sure to check the following:

- User name - Raritan usernames *are not* case-sensitive.
- Password - Raritan passwords *are* case-sensitive.
- TCP Port - If you have configured your device to use a non-default TCP Port, this information must be entered into its connection profile.
- Firewall Settings - If you are accessing a device through a firewall, that firewall must be configured to allow two-way communication on TCP Port 5000 (or the custom TCP Port to which your device has been configured).
- Security Key - If you have configured your device to require a group security key, that key must be entered into the device's connection profile.

Note: If you are running MPC on Internet Explorer® with both a Microsoft® firewall and a non-Microsoft firewall utility installed, IE displays a message telling you that MPC is already running (even if it is not in fact running). To avoid this, deactivate one of your firewalls, or use a browser such as Firefox®.

Connection Information

To obtain information about your connection:

- Choose Connection > Connection Info. The Connection Info dialog appears.

Generation 1 Devices

The following information is displayed about a current connection to Generation 1 devices:

Connection information	Description
Device name	The name of your device.
IP address	The IP address of your device.
Port	The KVM Communication TCP/IP Port used to access the target device.
Data in/second	Data rate in.
Data out/second	Data rate out.
FPS	The frames per second transmitted for video.
Connect time	The duration of the connect time.
Horizontal resolution	The page resolution horizontally.
Vertical resolution	The page resolution vertically.
Refresh rate	How often the page is refreshed.
Protocol version	The RFB Protocol version.
Oldest supported version	The oldest supported version of the client software.
Hardware version	0 - Obsolete
Software version	3 (Software version)
Post code	Power on self-test error code. 0 = no error.
Network flags	A list of the various network options that have been enabled or disabled such as DHCP, dial-in, autodetection, and so on.
Security flags	A list of the various security options that have been enabled or disabled such as SSL encryption, SNMP, and so on.
Options	RFP and TR support enabled or disabled.
Frame grabber info	0 - not used
KME info	KME version number for systems that use the KME.
Serial Info	Serial devices
Video devices count	Number of video devices detected.

Connection information	Description
Serial devices count	Number of serial devices detected.
Reserved	0 - not used
FPS*	Frames per second

* Available only in MPC.

To copy this information:

- Click Copy to Clipboard in the Connection Info dialog. The information is now available to be pasted into the program of your choice.

Generation 2 Devices

The following information is displayed about a current connection to Generation 2 devices:

Connection information	Description
Device name	The name of your device.
IP address	The IP address of your device.
Port	The KVM Communication TCP/IP Port used to access the target device.
Data in/second	Data rate in.
Data out/second	Data rate out.
FPS	The frames per second transmitted for video.
Connect time	The duration of the connect time.
Horizontal resolution	The page resolution horizontally.
Vertical resolution	The page resolution vertically.
Refresh rate	How often the page is refreshed.
Protocol version	The RFB Protocol version.

To copy this information:

- Click Copy to Clipboard in the Connection Info dialog. The information is now available to be pasted into the program of your choice.

Connecting to a Remote KVM Console

Once you establish a connection with a Raritan device, that device's icon in the Navigator can be expanded to display all ports enabled for remote access.

Choose one of the following options to establish a remote KVM console connection:

- Double-click the KVM port. This method closes any previous connection before connecting to the new port.
- Right-click the port and choose Switch from the shortcut menu. This method closes any previous connection before connecting to the new port.
- Right-click the port and choose New Connection from the shortcut menu. This method allows you to connect to the selected port without closing any previous connections and creates a new connection if the device supports multiple concurrent connections.

Once connected, Raritan KVM over IP devices display real-time video output of the target server (this video is compressed and encrypted according to the configuration settings specified by the administrator). You now have complete, low-level control of the KVM console as if you were physically located next to the server.

- To close a connection, right-click the connected device and choose Disconnect.
- To exit completely, choose Connection > Exit.

Closing a Remote Connection

To close the connection:

1. Select the device in the Navigator and right-click it.
2. Choose Disconnect from the shortcut menu.

3. To exit completely, click Exit on the Connection menu

Shortcut Menu

To access the shortcut menu, use either the default keyboard combination of Ctrl+Left Alt+M or the keyboard combination you assign. See ***Changing the Shortcut Menu Keyboard Combination*** (on page 102) for more information.

TIP: If at some point you forget the keyboard combination used to open the shortcut menu, press Ctrl+Left Alt at the same time. The keyboard combination is displayed across the bottom of the page for five seconds.

Shortcut Menu Key Options

Execute any of the commands on the shortcut menu by either choosing the command in the menu or using a key combination. If you are using a key combination to execute a command, press Ctrl+Left Alt+M and then press the key on your keyboard that corresponds to the underlined letter in the shortcut menu. For example, press Ctrl+Left Alt+M+F to enter Full Screen mode. See the table below for information on invoking commands from the shortcut menu using keyboard combinations.

Note: You must use the Left Alt key on your keyboard when using the Ctrl+Left Alt combination.

To	Press Ctrl+Left Alt+M+
Toggle between Full/Normal screen mode*	F
Display connection information*	I
Display or set connection properties*	P
Display or set video settings*	V
Refresh the page	R
Synchronize mouse	Y
Change to/from single/double cursor mode	S
Send Ctrl+Alt+Del to the target system	D
Connect Drive	T
Connect CD-ROM/ISO Image	E
Send Ctrl+Alt+M to the target system	N
Exit a dialog or menu without altering the keyboard state	Esc

To	Press Ctrl+Left Alt+M+
Send Left Alt+Tab	T
Auto Sense	A
Calibrate Color	C

* If Full Screen mode is active, executing this command automatically ends Full Screen mode.

Changing the Shortcut Menu Keyboard Combination

To change the keyboard combination, do the following:

1. Choose Tools > Options to open the Options dialog.
2. From the Keyboard Shortcut Menu HotKey drop-down, select the keyboard combination you want to use to open the shortcut menu.
3. Click OK or Apply.

Once a new keyboard combination is assigned, the new combination is displayed in the shortcut menu and in the onscreen message that displays when the combination is used.

Keyboard Macros

A hot key combination is a set of keystrokes that performs an action when pressed. For example, the hot key combination Ctrl+Alt+0 might be created to minimize all windows.

A keyboard macro is a shortcut that sends a hot key combination to a target server. Using keyboard macros ensures that hot key combinations intended to be used on the target server are sent to and interpreted only by the target server, and not by the computer on which the client is running.

Raritan strongly suggests the use of keyboard macros instead of hot key combinations since certain hot key combinations have been found not to work properly, depending on the platform and behavioral difference between the application and web browser version. Specifically, using hot keys can result in your own client PC intercepting the command and performing the action instead of sending the command to the target server as intended.

Note: In MPC, foreign keyboard layouts are not supported when using keyboard macros, except for those keys listed in the Add Keyboard Macro dialog for Japanese and Korean.

Note: Keyboard macros created in AKC cannot be used in MPC and vice versa.

Building a Keyboard Macro

To build a macro:

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

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

Press Left Alt

Press F4

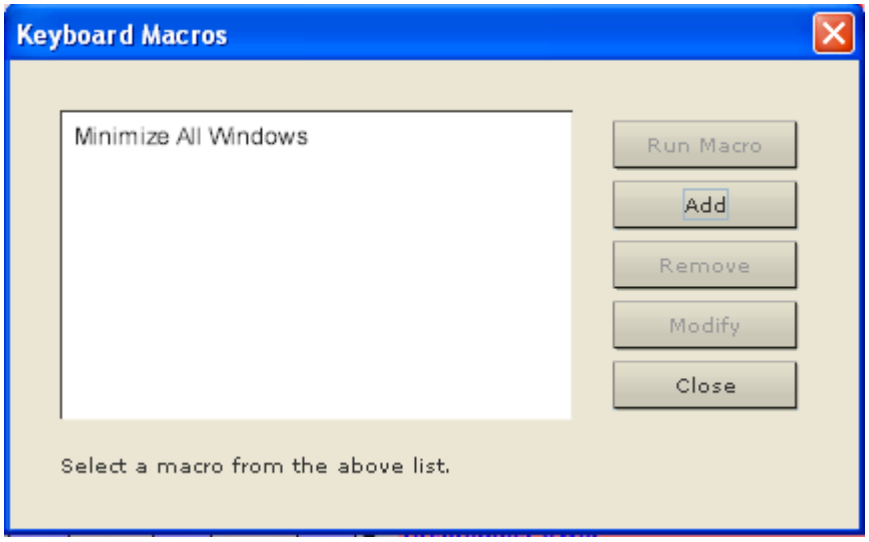
Esc

Release F4

Esc

Release Left Alt

6. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
   a. To remove a step in the sequence, select it and click Remove.
   b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.
7. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.
8. Click Close to close the Keyboard Macros dialog. The macro now appears on the Keyboard menu in the application. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.



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

1. Click the Keyboard > Sent Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target.

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

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

Running a Keyboard Macro

Once you have created a keyboard macro, execute it using the keyboard macro you assigned to it or by choosing it from the Keyboard menu.

Run a Macro from the Menu Bar

When you create a macro, it appears under the Keyboard menu. Execute the keyboard macro by clicking on it in the Keyboard menu.

Run a Macro Using a Keyboard Combination

If you assigned a keyboard combination to a macro when building it, you can execute the macro by pressing its assigned keystrokes. For example, press the keys Ctrl+Alt+0 simultaneously to minimize all windows on a Windows target server.

Modifying and Removing Keyboard Macros

To modify a macro:

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Choose the macro from among those listed.
3. Click Modify. The Add/Edit Macro dialog appears.
4. Make your changes.
5. Click OK.

To remove a macro:

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Choose the macro from among those listed.
3. Click Remove. The macro is deleted.

Ctrl+Alt+Del Macro

Due to its frequent use, a Ctrl+Alt+Delete macro is preprogrammed.

Clicking on the Ctrl+Alt+Delete button  in the toolbar sends this key sequence to the server or to the KVM switch to which you are currently connected.

In contrast, if you were to physically press the Ctrl+Alt+Del keys, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Send Text to Target

You are able to paste text from the client machine to the target using the Send Text to Target option on the Keyboard menu.

To send text to a target:

1. Select Keyboard > Send Text to Target.
2. In the Send Text dialog, paste the text from the client machine in the space provided.
3. If needed, select the "Target system is set to the US/International keyboard layout" checkbox to specify that a US/International English keyboard on the target.
4. Click OK.

Common Hot Key Exceptions for MPC

The following common hot key combinations are *not* sent to the target system:

Hot Key Combination	Description
Ctrl+Alt+Delete	The sequence is sent to the local system and the Windows® Security (Task Manager, Shutdown, and so on) dialog is displayed.
Ctrl+Left Alt+M	Brings up the shortcut menu.
Print Scrn	Treated locally and copies the page to the clipboard.
Alt+Tab	Switches between open Windows on the local machine.
Ctrl+Esc	Opens the Start menu on the local machine.
 + E	Windows button + E launches Windows Explorer® on the local machine.

Hot Key Combination	Description
 + F	Windows button + F is used to find files and folders on the local machine.
 + M	Windows button + M minimizes all windows on the local machine.

The following hot key combination exception affects both the remote KVM target and local machine:

Hot Key Combination	Description
Alt + F4	Depending on the focus, this combination closes the application window. Specifically, if the focus is on the application, the application closes. If the focus is on an application's title bar in the target's video, that application closes.

Following are limitations to specific keyboards and hot key combinations:

Hot Key Combination	Description
Alt Gr	Because of a limitation in the Java™ Runtime Environment (JRE™), Fedora®, Linux®, and Solaris™ clients receive an invalid response from Alt Gr on United Kingdom and US International language keyboards. For Fedora, Linux, and Solaris using Java 1.6, the keyPressed and keyReleased events for Alt Gr are identified as an "unknown key code".
Alt+SysRq+[key]	Since the SysRq keyboard stroke is used by some operating systems as a print shortcut, the Alt + SysRq + [key] combination is supported only as a macro when using the device with RRC and MPC to a Linux target.

Common Hot Key Combinations for RRC

The following common hot key combinations are *not* sent to the target system:

Hot Key Combination	Description
Ctrl+Alt+Delete	Reboots the computer. The sequence is sent to the local system and the Windows® Security (Task Manager, Shutdown, and so on) dialog is displayed.
Ctrl+Num Lock	This toggles the state of the Num Lock light if the Num Lock state on the local system is not the same as the target system.
Ctrl+Caps Lock	This toggles the state of the Caps Lock light if the Caps Lock state of the local system is not the same as the target system.
Ctrl+Scroll Lock	This toggles the state of the Scroll Lock light if the Scroll Lock state of the local system is not the same as the target system.
Ctrl+Left Alt+M	Brings up the shortcut menu.
Print Scrn	Treated locally and copies the page to the clipboard.

Following are limitations to specific keyboards and hot key combinations:

Hot Key Combination	Description
Alt+SysRq+[key]	Since the SysRq keyboard stroke is used by some operating systems as a print shortcut, the Alt + SysRq + [key] combination is supported only as a macro when using the device with RRC and MPC to a Linux® target.

Digital Audio

The KX II 2.4.0 (and later) supports end-to-end, bidirectional, digital audio connections for digital audio playback and capture devices from a remote client to a target server. The audio devices are accessed over a USB connection. A D2CIM-DVUSB and the current device firmware are required.

The digital audio feature supports:

- ***Saving Audio Settings*** (on page 37)
- ***Connecting to Multiple Targets from a Single Remote Client*** (on page 38)
- Connecting to a Single Target Server from Multiple Remote Clients
- Connecting and Disconnecting a Digital Audio Device
- ***Adjusting Capture and Playback Buffer Size (Audio Settings)*** (on page 41)

Windows®, Linux® and Mac® operating systems are supported. The Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC) support connections to audio devices.

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

Before you begin using the audio feature, Raritan recommends you review the audio related information documented in the following sections of Help:

- ***Supported Audio Device Formats*** (on page 109, on page 35)
- Recommendations for Dual Port Video
- Supported Mouse Modes
- CIMs Required for Dual Video Support
- ***Informational Notes*** **(on page 199),** ***Audio*** (see "***Audio Notes***" on page 205)

Supported Audio Device Formats

The KX II 2.4.0 (and later) supports one playback and capture device and one record device on a target at a time. The following audio device formats are supported:

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

Connecting and Disconnecting a Digital Audio Device

To connect to an audio device from the Multi-Platform Client (MPC):

1. Connect the audio device to the target prior to launching MPC. This must done prior to connecting to the device through the MPC.
2. Connect to the target through MPC.
3. Connect to the target from the Port Access page.
4. Once connected, click the Audio icon  in the toolbar. The Connect Audio Device dialog appears. A list of available audio device connected to the remote client PC is displayed.

   Note: If there are no available audio devices connected to the remote client PC, the Audio icon is grayed out. .

5. Check Connect Playback Device if you are connecting to a playback device.
6. Select the device that you wish to connect from the drop-down list.
7. Select the audio format for the playback device from the Format: drop-down.

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

8. Check Connect Recording Device if you are connecting a recording device.

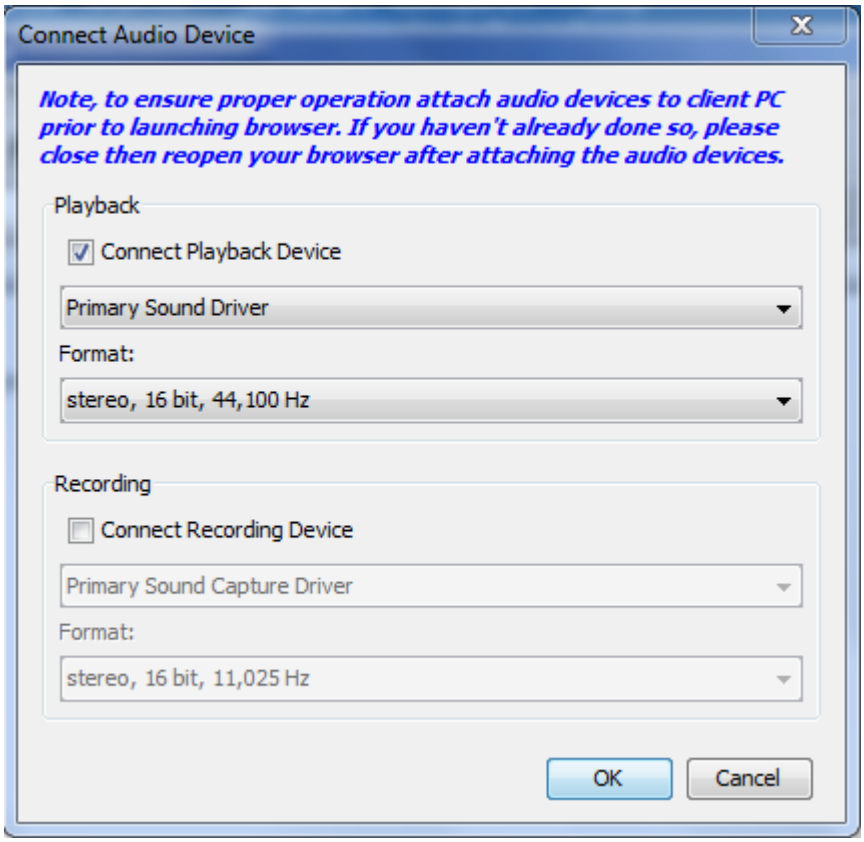
   Note: The device names listed in the Connect Recording Device drop-down are truncated to a maximum of 30 characters for Java clients.

9. Select the device that you wish to connect from the drop-down list.
10. Select the audio format for the recording device from the Format: drop-down.
11. Click OK. If the audio connection is established, a confirmation message appears. Click OK.

    If the connection was not established, an error message appears.

    Once an audio connection is established, the Audio menu is changed to Disconnect Audio. Additionally, the settings for the audio device are saved and applied to the audio device.

A Speaker icon is displayed in the status bar at the bottom of the client window. It is grayed out when no audio is being used. When the Speaker icon and Microphone icon are displayed in the status bar, the session is being captured as it is streamed.



To disconnect from the audio device:

Click the Audio icon in the toolbar and select OK when you are prompted to confirm the disconnect. A confirmation message appears. Click OK.

Video Properties

Refreshing the Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

- The Refresh Screen command forces a refresh of the video screen.
- The Auto-sense Video Settings command automatically detects the target server's video settings.
- The Calibrate Color command calibrates the video to enhance the colors being displayed.

In addition, you can manually adjust the settings using the Video Settings command.

To refresh the video settings, do one of the following:

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

If the video card you are using on the target uses custom software and you are accessing the target through MPC or VKC, you may need to change the maximum refresh rate of the monitor in order for the refresh rate to take effect on the target.

To adjust the monitor refresh rate:

1. In Windows®, select Display Properties > Settings > Advanced to open the Plug and Play dialog.
2. Click on the Monitor tab.
3. Set the 'Screen refresh rate' to any rate above 100Hz.
4. Click OK and then OK again to apply the setting.

Auto-Sense Video Settings

The Auto-sense Video Settings command forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.

To automatically detect the video settings, do the following:

- Choose Video > Auto-sense Video Settings or click the Auto-Sense Video Settings button  in the toolbar. A message stating that the auto adjustment is in progress appears.

Calibrating Color

Use the Calibrate Color command to optimize the color levels (hue, brightness, saturation) of the transmitted video images. The color settings are on a target server-basis.

Note: The Calibrate Color command applies to the current connection only.

To calibrate the color, do the following:

- Choose Video > Calibrate Color or click the Calibrate Color button  in the toolbar. The target device screen updates its color calibration.

Adjusting Video Settings

Use the Video Settings command to manually adjust the video settings.

To change the video settings:

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar to open the Video Settings dialog.
2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:
   a. Noise Filter

      The device can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.
      Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

   b. PLL Settings

      Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances this setting should not be changed because the autodetect is usually quite accurate.

      Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

   c. Brightness: Use this setting to adjust the brightness of the target server display.

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

e. Brightness Green - Controls the brightness of the green signal.

f. Brightness Blue - Controls the brightness of the blue signal.

g. Contrast Red - Controls the red signal contrast.

h. Contrast Green - Controls the green signal.

i. Contrast Blue - Controls the blue signal.

If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

---

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

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

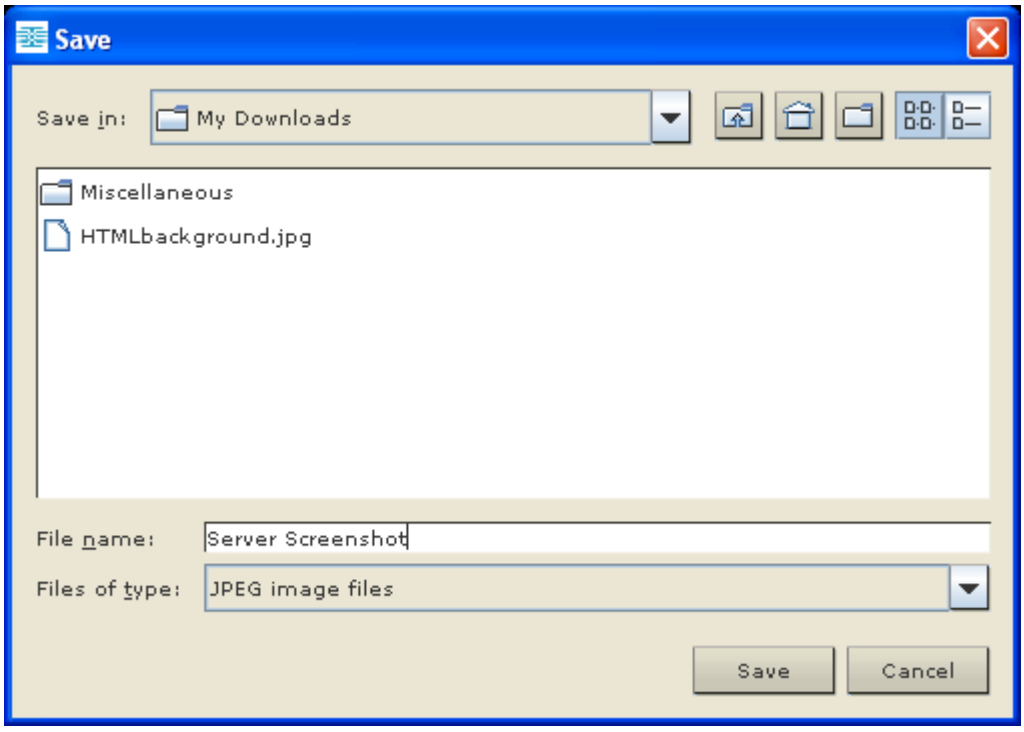
Using Screenshot from Target

You are able to take a screenshot of a target server using the Screenshot from Target server command. If needed, save this screenshot to a file location of your choosing as a bitmap, JPEG or PNG file.

To take a screenshot of the target server:

1. Select Video > Screenshot from Target or click the Screenshot from Target button  on the toolbar.
2. In the Save dialog, choose the location to save the file, name the file, and select a file format from the 'Files of type' drop-down.

3. Click Save to save the screenshot.



Changing the Maximum Refresh Rate

If the video card you are using on the target uses custom software and you are accessing the target through MPC or VKC, you may need to change the maximum refresh rate of the monitor in order for the refresh rate to take effect on the target.

To adjust the monitor refresh rate:

1. In Windows®, select Display Properties > Settings > Advanced to open the Plug and Play dialog.
2. Click on the Monitor tab.
3. Set the 'Screen refresh rate'.
4. Click OK and then OK again to apply the setting.

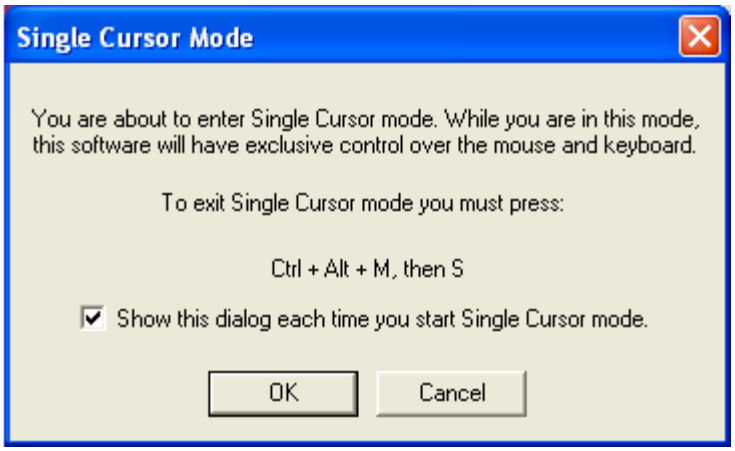
Mouse Options

Single Cursor Mode/Dual Cursor Mode

When remotely viewing a target server that uses a mouse, two mouse cursors are displayed on the remote desktop. When your mouse pointer lies within the remote desktop area, mouse movements and clicks are directly transmitted to the connected target server. The pointer, generated by the operating system, slightly leads the target server's mouse pointer during movement. This is a result of digital delay.

On fast LAN connections, you may want to disable the mouse pointer and view only the target server's pointer. To toggle between these two modes, choose Single/Double Cursor on the shortcut menu.

Alternatively, click the Single Mouse Pointer button  in the toolbar or choose Mouse > Single Cursor Mode.



When in Dual Cursor mode, press Ctrl+Left Alt+M and execute the Synchronize Mouse shortcut to force realignment of the mouse cursors. If the mouse cursors still remain out of sync, click the Auto-Sense Video Settings button  on the toolbar.

Note: When in Dual Cursor mode, if the dual mouse cursors are synchronized but left idle for five minutes or longer, the target mouse pointer automatically aligns itself with the upper left corner of the target window. Execute the Synchronize Mouse command to ensure local and target mouse pointer alignment.

Single Mouse Cursor mode for Apple® Mac® target servers is supported for MPC. Select Single Mouse Cursor on the Mouse menu in MPC to enter this mode. While in this mode, the cursor remains in the video window for the Mac Server. To exit, open the shortcut menu and press S on the keyboard.

Mouse Synchronization Options

In addition to synchronizing mouse cursors or toggling between single and dual cursor mode, the Mouse menu provides three options for synching cursors when in dual cursor mode:

Menu option	Description
Absolute	When connected to selected Dominion devices and targets with USB ports, the application uses absolute coordinates to keep the cursors in sync. See ***Absolute Mouse Mode*** (on page 28) for more information.
Intelligent	Under certain conditions, the application can detect the target mouse settings and synchronize the mouse cursors accordingly, accelerating the mouse on the target device. See ***Intelligent Mouse Mode*** (on page 27) for more details.
Standard	This is the standard mouse synchronization algorithm. See ***Standard Mouse Mode*** (on page 26) for more information.

Note: The Intelligent and Standard Mouse modes are available to all device targets. Absolute Mouse mode are only available to Mac® and Windows® operating system USB targets.

Automatic Mouse Synchronization

For Generation 1, devices When in Dual Cursor mode, the system will automatically align the mouse cursors when the cursor is inactive for 15 seconds. Enable this feature by clicking the Synchronize Mouse button  in the toolbar or selecting Tools > Options and selecting the "Auto-Sync mouse in two-cursor mode" checkbox.

Automatic Mouse Synchronization is available for Generation 2 devices when:

- A new connection is established
- Auto-sense is enabled
- Color calibration is enabled

Enable this feature in Generation 2 devices by clicking the Synchronize Mouse button  in the toolbar or selecting Mouse > Synchronize Mouse.

Absolute Mouse Mode

In this mode, absolute coordinates are used to keep the client and target cursors in sync, even when the target mouse is set to a different acceleration or speed. This mode is supported on servers with USB ports and is the default mode for VM and dual VM targets.

To enter absolute mouse mode:

- Choose Mouse > Absolute.

Note: The absolute mouse setting requires a USB target system and is the recommended mouse setting for KX II-101.

Note: For KX II, Absolute Mouse Synchronization is available for use with the virtual media-enabled USB CIM (D2CIM-VUSB and D2CIM-DVUSB) only.

Intelligent Mouse Mode

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

During synchronization, the mouse cursor does a “dance” in the top left corner of the screen and calculates the acceleration. For this mode to work properly, certain conditions must be met.

To enter intelligent mouse mode:

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

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

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as “Enhanced pointer precision" or “Snap mouse to default button in dialogs” should be disabled.
- Choose “Best Possible Video Mode” in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, Raritan recommends you do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

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

Standard Mouse Mode

Standard Mouse mode uses a standard mouse synchronization algorithm using relative mouse positions. Standard Mouse mode requires that mouse acceleration is disabled and other mouse parameters are set correctly in order for the client and server mouse to stay synchronized.

To enter Standard Mouse mode:

- Choose Mouse > Standard.

Connection and Video Properties

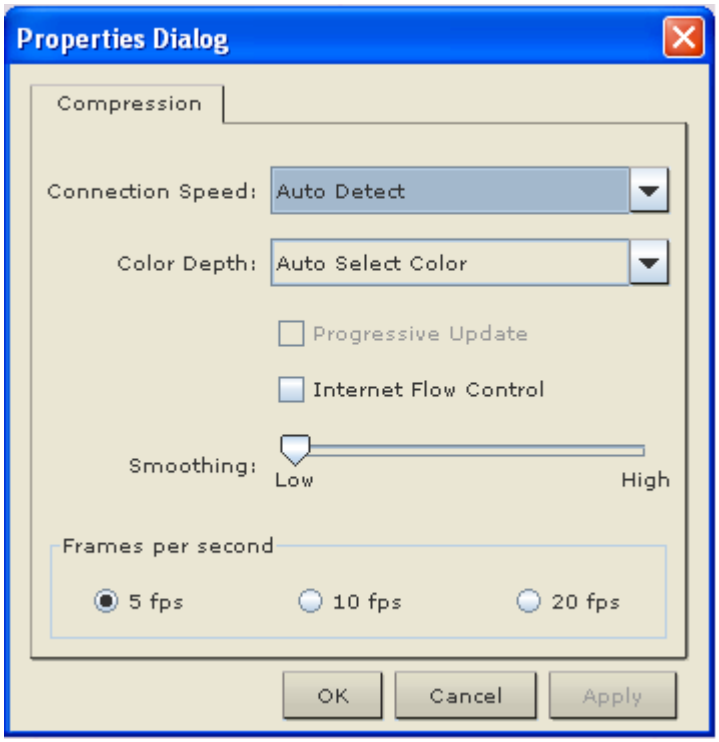
Dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. The device optimizes KVM output not only for LAN use but also for WAN and dial-up use. These devices can also control color depth and limit video output, offering an optimal balance between video quality and system responsiveness for any bandwidth constraint.

The parameters discussed in this section can be optimized in the Connection Properties dialog and Video Settings dialog. Connection properties are saved across subsequent connections to generation 2 devices once they are set and saved.

MPC Connection Properties - Generation 1 Devices

To adjust connection properties:

1. Choose Connection > Properties or click the Connection Properties button  in the toolbar. Update the settings in the Compression tab.



2. Set the Connection Speed.

   Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. Devices can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available:

   - Auto Detect
   - 1G Ethernet
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)

- 384 kb (Slow DSL/T1)
- 256 kb (Cable)
- 128 kb (Dual ISDN)
- 56 kb (ISP Modem)
- 33 kb (Fast Modem)
- 24 kb (Slow Modem)

3. Set the Color Depth.

   Devices can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list. Depending on the Raritan device in use, different options may be available:

   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White

   Important: For most administrative tasks (server monitoring, reconfiguring, and so forth), administrators do not require the full 24-bit or 32-bit color spectrum made available by most video graphics cards. Attempting to transmit such high color depths wastes network bandwidth.

   ---

4. Selecting the Internet Flow Control checkbox ensures that packets transmitted by the device are received and reconstructed by the client application in the correct order. This is useful when using a device over an unpredictable public WAN (particularly in international scenarios).
5. Use the slider to select the desired level of video Smoothing (15-bit mode only). The level determines how aggressively to blend page regions with small color variation into a single, smooth color. Smoothing improves the appearance of the target video by reducing the video noise that is displayed.
6. Select "Frames per second". This setting instructs MPC on how often to redraw the video display of the target. This only affects the client display behavior and has no bearing on the data rate of the video being sent to the client. Setting this option higher makes the video appear smoother but also requires more processing power.
7. Click OK to create the connection profile.

MPC Connection Properties - Generation 2 Devices

To adjust connection properties:

1. Choose Connection > Properties or click the Connection Properties button  in the toolbar. Update the settings in the Compression tab.
2. Set the Connection Speed.

   Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. Devices can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available:

   - Auto Detect
   - 1G Ethernet
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)
   - 384 kb (Slow DSL/T1)
   - 256 kb (Cable)
   - 128 kb (Dual ISDN)
   - 56 kb (ISP Modem)
   - 33 kb (Fast Modem)
   - 24 kb (Slow Modem)

   Note: KX II-101 does not support 1G Ethernet.

3. Set the Color Depth.

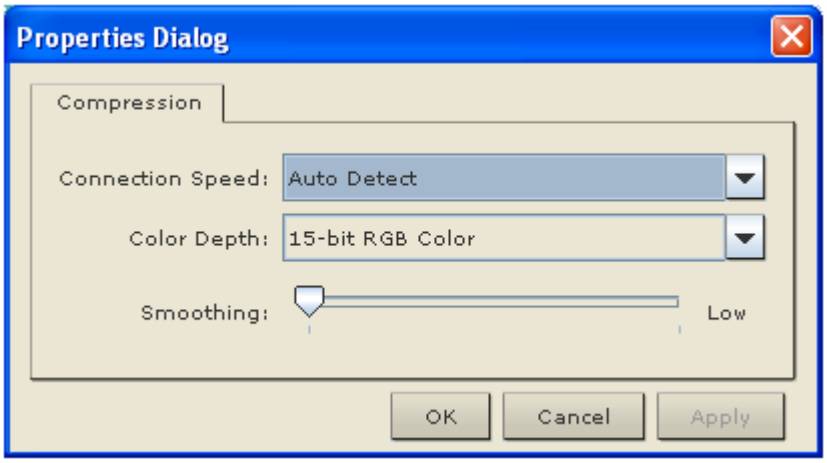
   Devices can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list. Depending on the Raritan device in use, different options may be available:

   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray

- 2-bit Gray
- Black and White

Important: For most administrative tasks (server monitoring, reconfiguring, and so forth), administrators do not require the full 24-bit or 32-bit color spectrum made available by most video graphics cards. Attempting to transmit such high color depths wastes network bandwidth.

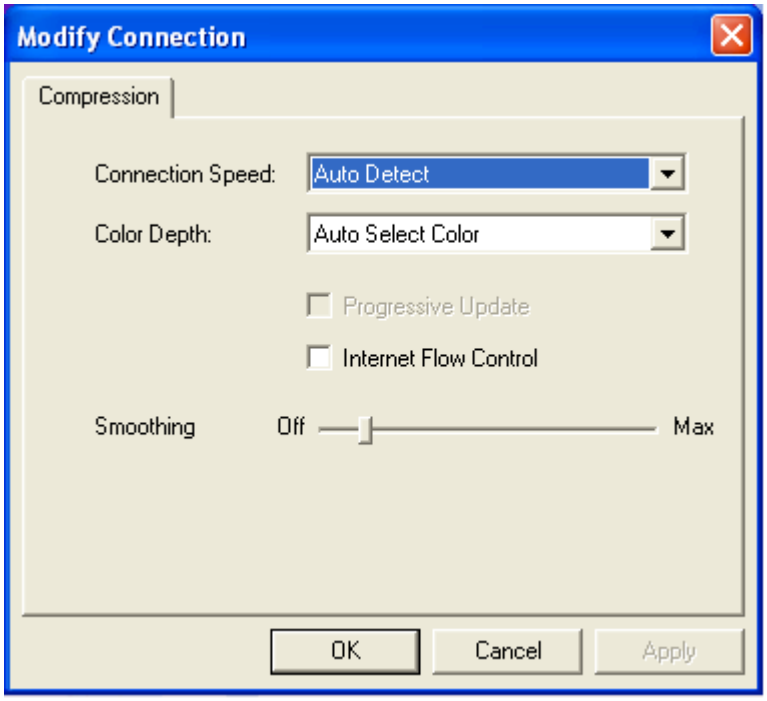
4. Use the slider to select the desired level of video Smoothing (15-bit mode only). The level determines how aggressively to blend page regions with small color variation into a single, smooth color. Smoothing improves the appearance of the target video by reducing the video noise that is displayed.
5. Click OK to create the connection profile.



RRC Connection Properties

To adjust connection properties:

1. Choose Connection > Properties or click the Connection Properties button  in the toolbar. Update the settings in the Compression tab.



2. Set the Connection Speed.

   Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. Devices can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available:

   - Auto Detect
   - 1G Ethernet
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)
   - 384 kb (Slow DSL/T1)

- 256 kb (Cable)
- 128 kb (Dual ISDN)
- 56 kb (ISP Modem)
- 33 kb (Fast Modem)
- 24 kb (Slow Modem)

3. Set the Color Depth.

   Devices can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list. Depending on the Raritan device in use, different options may be available:

   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White

   Important: For most administrative tasks (server monitoring, reconfiguring, and so forth), administrators do not require the full 24-bit or 32-bit color spectrum made available by most video graphics cards. Attempting to transmit such high color depths wastes network bandwidth.

4. Select Progressive Update to increase the usability in constrained bandwidth environments. When Progressive Update is enabled, the device initially sends an image of the remote desktop at lower color depths. Higher color depth images are provided as the bandwidth allows.

   Note: When Color Depth is set to Auto Select Color (default), Progressive Update is automatic. The device will enable/disable Progressive Update as required, disabling it for fast connections and enabling it for slow connections.

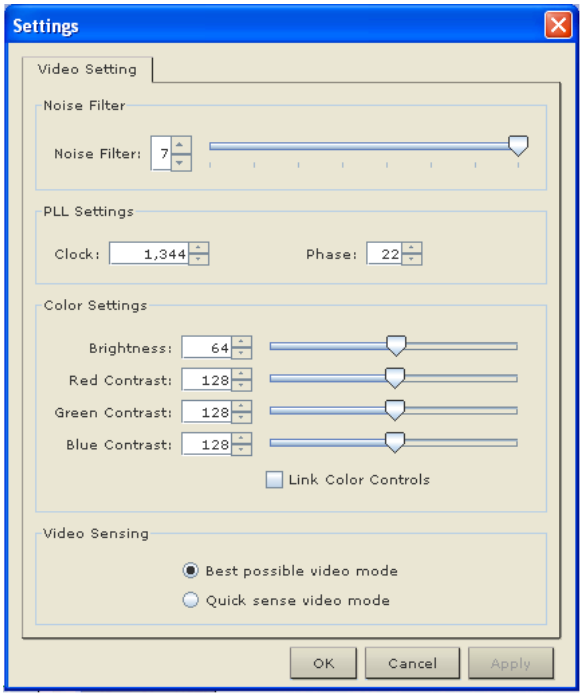
5. Selecting the Internet Flow Control checkbox ensures that packets transmitted by the device are received and reconstructed by the client application in the correct order. This is useful when using a device over an unpredictable public WAN (particularly in international scenarios).

6. Use the slider to select the desired level of video Smoothing (15-bit mode only). The level determines how aggressively to blend page regions with small color variation into a single, smooth color. Smoothing improves the appearance of the target video by reducing the video noise that is displayed.
7. Click OK to create the connection profile.

Video Settings

Video Settings - Generation 1 Devices

Following are instructions on configuring video settings for Generation 1 devices. These settings can be refreshed using the Color Calibration command by manually forcing a device to autodetect the video settings (on the Video menu, click Auto-sense Video Settings) or by changing the settings in this page. After you change a value, click Apply to test the setting. See ***Color Calibration*** (on page 132).



To configure Generation 1 devices:

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar to open the Settings dialog.
2. Adjust the following settings as required:
   a. Noise Filter

Devices can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired page changes. Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

Note: The default Noise Filter is 2. Raritan recommends that you lower this value to 0 (zero). Although higher settings will stop the needless transmission of false color variations, true and intentional small changes to a video image may not be transmitted.

---

b. PLL Settings

If the video image looks extremely blurry or unfocused, the PLL settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the clock and phase settings since doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

- Clock - Controls how quickly video pixels are displayed across the video page. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances this setting should not be changed because the autodetect is usually quite accurate.
- Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

a. Color Settings -Gain control can be thought of as contrast adjustment. Offset control can be thought of as brightness adjustment.

Select the Link Color Controls checkbox to make all slide adjusters move in unison when any one option is moved.

- Red Gain - Controls the amplification of the red signal.
- Red Offset - Controls the bias of the red signal.
- Green Gain - Controls the amplification of the green signal.
- Green Offset - Controls the bias of the green signal.
- Blue Gain - Controls the amplification of the blue signal.
- Blue Offset - Controls the bias of the blue signal.

a. Color Settings - Gain control can be thought of as contrast adjustment. Offset control can be thought of as brightness adjustment.

Select the Link Color Controls checkbox to make all slide adjusters move in unison when any one option is moved.

- Red Gain - Controls the amplification of the red signal.
- Red Offset - Controls the bias of the red signal.
- Green Gain - Controls the amplification of the green signal.
- Green Offset - Controls the bias of the green signal.
- Blue Gain - Controls the amplification of the blue signal.
- Blue Offset - Controls the bias of the blue signal.

3. Select the video sensing mode:
   - Best possible video mode - Devices will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
   - Quick sense video mode - Selecting this option will cause the device to use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
4. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.

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

Video Settings - Generation 2 Devices

To configure devices:

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar to open the Settings dialog.
2. Adjust the following settings as required:
   a. Noise Filter

   Devices can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired page changes. Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

Note: The default Noise Filter is 2. Raritan recommends that you lower this value to 0 (zero). Although higher settings will stop the needless transmission of false color variations, true and intentional small changes to a video image may not be transmitted.

b. PLL Settings

If the video image looks extremely blurry or unfocused, the PLL settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the clock and phase settings since doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

- Clock - Controls how quickly video pixels are displayed across the video page. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances this setting should not be changed because the autodetect is usually quite accurate.
- Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

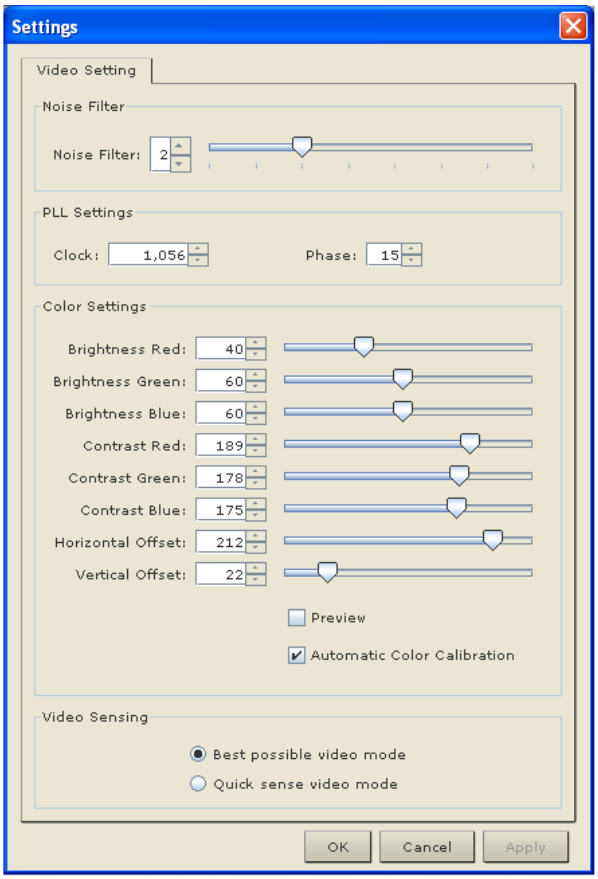
a. Color Settings

These settings control the brightness, contrast, and positioning of the target server display. Select the Link Color Controls checkbox to make all slide adjusters move in unison when any one option is moved.

- Brightness Red - Controls the brightness of the red signal; range is 0 - 127.
- Brightness Green - Controls the brightness of the green signal; range is 0 - 127.
- Brightness Blue - Controls the brightness of the blue signal; range is 0 - 127.
- Contrast Red - Controls the red signal contrast; range is 0 - 255.
- Contrast Green - Controls the green signal contrast; range is 0 - 255.
- Contrast Blue - Controls the blue signal contrast; range is 0 - 255.
- Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor; range is 0 - 512.
- Vertical Offset - Controls the vertical positioning of the target server display on your monitor; range is 0 - 128.

3. To preview the change prior to making the selection, check the Preview checkbox.
4. Check the Automatic Color Calibration checkbox to enable this feature.
5. Select the video sensing mode:
   - Best possible video mode - Devices will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
6. Quick sense video mode - Selecting this option will cause the device to use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
7. Select the video sensing mode:
   - Best possible video mode - Devices will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
   - Quick sense video mode - Selecting this option will cause the device to use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.

8. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.



Port Access Page Sort

To change the display sort order and/or view more ports on the same page:

1. Click the column heading by which you want to sort. The list of KVM target servers is sorted by that column.
2. In the Rows per Page, enter the number of ports to be displayed on the page and click Set.

Color Calibration

Use the Color Calibration command if the color levels (hue, brightness, and saturation) of the transmitted video images do not seem accurate. The device color settings remain the same when switching from one target KVM server to another, so you can perform color calibration once to affect all connected target servers.

1. Open a remote KVM connection to any server running a graphical user interface.

2. Ensure that a solid white color covers approximately 15% or more of the target server's desktop.

   TIP: Open Microsoft® Notepad and maximize the window.

3. On the Video menu, choose Calibrate Color or click the Color Calibration button  on the toolbar. The target device page updates its calibration.

   Tip: Specify automatic color calibration using Tools > Options. See **General Options** *(see "***General Options, Advanced Options, Client Launch Settings and Scan Settings***" on page 137) for more information.*

Help Options

This menu command provides version information about the Virtual KVM Client, in case you require assistance from Raritan Technical Support.

To obtain version information:

- Choose Help > About Raritan Multi-Platform Client.

Use the Copy to Clipboard button to copy the information contained in the dialog to a clipboard file so it can be accessed later (if needed).

Smart Cards (VKC, AKC and MPC)

Using the KX II 2.1.10 (and later) or KSX II 2.3.0 (and later), you are able to mount a smart card reader onto a target server to support smart card authentication and related applications. For a list of supported smart cards, smart card readers, and additional system requirements, see ***Supported and Unsupported Smart Card Readers*** (on page 44).

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

When accessing a server remotely, you can select an attached smart card reader and mount it onto the server. Smart card authentication is used with the target server, it is not used to log into the device. Therefore, changes to smart card PIN and credentials do not require updates to device accounts. When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached. Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS. When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

When PC-Share mode is enabled on the device, multiple users can share access to a target server. However, when a smart card reader is connected to a target, the device will enforce privacy regardless of the PC-Share mode setting. In addition, if you join a shared session on a target server, the smart card reader mounting will be disabled until exclusive access to the target server becomes available.

After a KVM session is established to the target server, a Smart Card menu and button are available in the Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC). Once the menu is opened or the Smart Card button is selected, the smart card readers that have been detected as attached to the remote client are displayed. From this dialog you can attach additional smart card readers, refresh the list of smart card readers attached to the target, and detach smart card readers. You are also able to remove or reinsert a smart card. This function can be used to provide notification to a target server OS that requires a removal/reinsertion in order to display the appropriate login dialog. Using this function allows the notification to be sent to a single target without affecting other active KVM sessions.

To mount a smart card reader:

1. Click the Smart Card menu and then select Smart Card Reader.

   Alternatively, click the Smart Card button  in the toolbar.
2. Select the smart card reader from the Select Smart Card Reader dialog.

3. Click Mount.
4. A progress dialog will open. Check the 'Mount selected card reader automatically on connection to targets' checkbox to mount the smart card reader automatically the next time you connect to a target. Click OK to begin the mounting process.

To update the smart card in the Select Smart Card Reader dialog:

- Click Refresh List if a new smart card reader has been attached to the client PC.

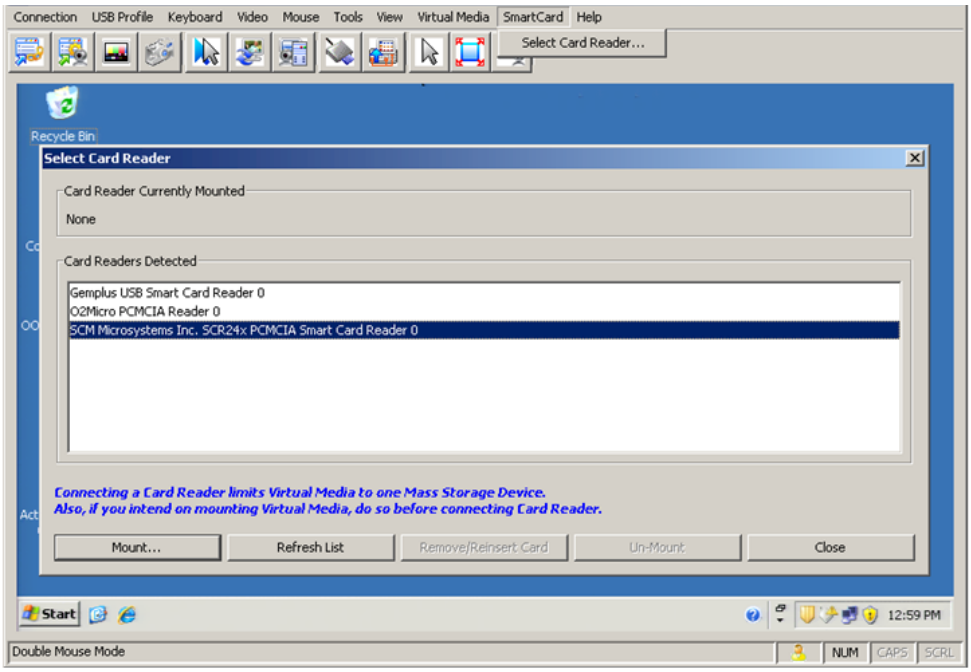
To send smart card remove and reinsert notifications to the target:

- Select the smart card reader that is currently mounted and click the Remove/Reinsert button.

To unmount a smart card reader:

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

Smart card reader mounting is also supported from the Local Console. See **Local Console Smart Card Access** in your Dominion device help.



Administrative Functions

Although your device provides a remote interface to administrative functions through the device manager, the client provides an interface to frequently-used administrative functions directly from its own interface. When logged into a device as an administrator, you can perform the administrative tasks discussed here.

Note: Most of the commands discussed here are available in both the Tools menu and in the shortcut menu that appears when you right-click the device in the Navigator panel.

Note to MPC Users

MPC assigns users one of two permissions: Administrator or User. You must belong to the Administrator group in order to receive administrative permissions. It is only when the user belongs to the Administrator group that they have access to backup, restore, and restart functions. This is true regardless of any device user group settings that may be applied to the user.

General Options, Advanced Options, Client Launch Settings and Scan Settings

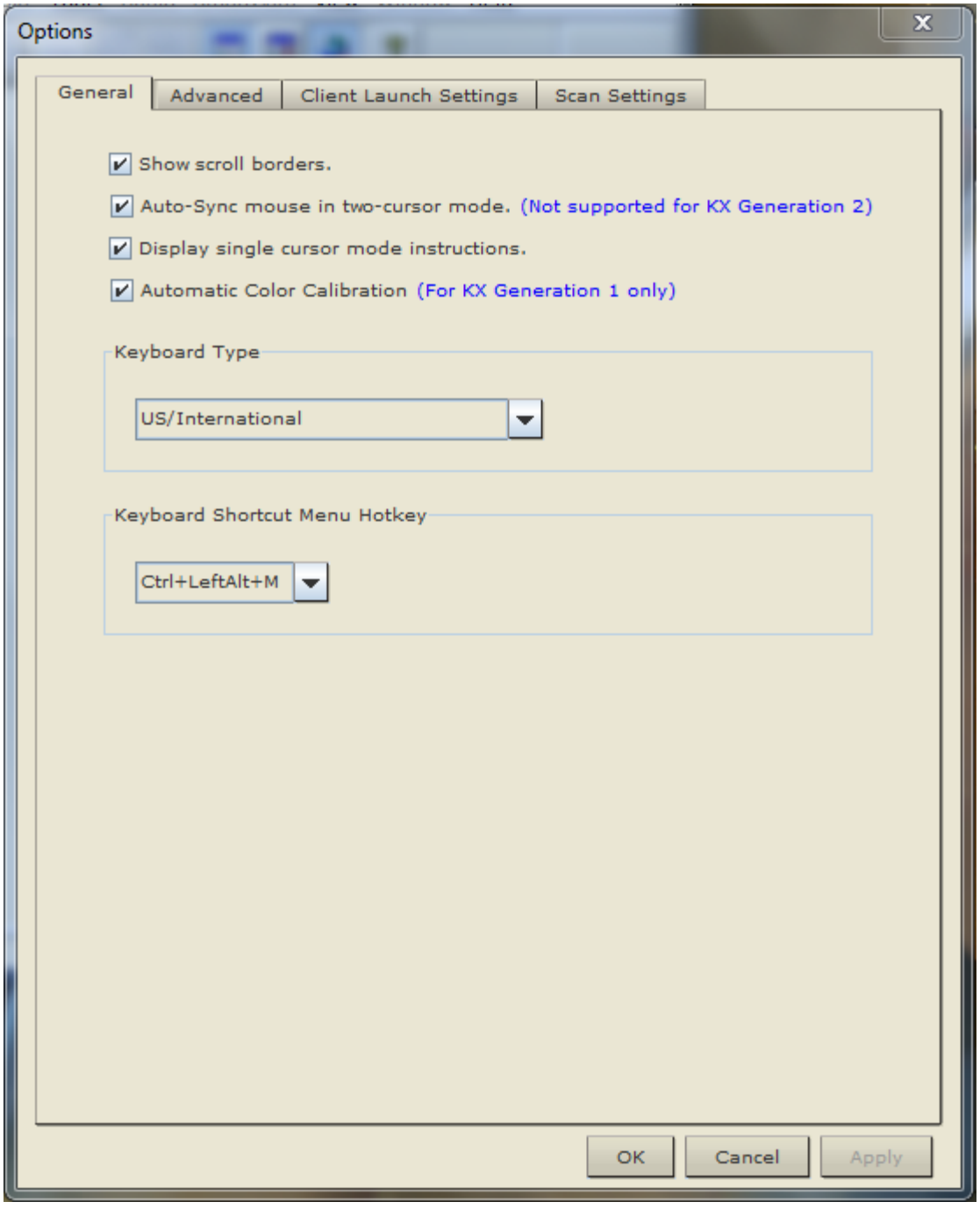
Options in MPC for KX II and KSX II

The Options available in the Tools menu allow you to customize scroll borders, mouse mode settings, Single Cursor mode, auto color calibration, hot key configuration, keyboard type, broadcast port, and logging.

For KX II users, you are able to change the default HTTP and/or HTTPS ports used by the device so that the device ports do not conflict with ports you may already be using. For example, if you are using the default HTTP port 80 for another purpose, changing the port will ensure the device does not attempt to use it.

Configuring client launch settings allows you to define the screen settings for a KVM session. KX II users can also configure scan settings.

Note: KSX II does not support scanning.


Options
General
Advanced
Client Launch Settings
Scan Settings
Show scroll borders.
Auto-Sync mouse in two-cursor mode. (Not supported for KX Generation 2)
Display single cursor mode instructions.
Automatic Color Calibration (For KX Generation 1 only)
Keyboard Type
US/International
Keyboard Shortcut Menu Hotkey
Ctrl+LeftAlt+M
OK
Cancel
Apply

General Options

To configure the general options in MPC:

1. Choose Tools > Options. The Options dialog appears and displays the General tab by default.

   General Options

2. Select the "Show scroll borders" checkbox to view the thin scroll borders designating the autoscroll area.

   Note: "Auto-Synch Mouse in two-cursor mode" is not available for use with the KX II and KSX II.

3. If you select the "Display single cursor mode instructions" checkbox, the Single Cursor Mode dialog will appear each time Single Cursor is enabled in the application. See ***Mouse Options*** (on page 116) for more information.
4. Select the Automatic Color Calibration checkbox to enable automatic color calibration. This option is available for KX generation 1 (G1) only.
5. Select the Keyboard Type from the drop-down list (depending on the Raritan device in use, different options may be available):
   - US/International
   - French (France)
   - German (Germany)
   - Japanese
   - United Kingdom
   - Korean (Korea)
   - French (Belgium)
   - Norwegian (Norway)
   - Portuguese (Portugal)
   - Danish (Denmark)
   - Swedish (Sweden)
   - German (Switzerland)
   - Hungarian (Hungary)
   - Spanish (Spain)
   - Italian (Italy)
   - Slovenian
   - Translation: French - US
   - Translation: French - US International

6. From the Keyboard Shortcut Menu HotKey drop-down, select the key combination you would like to use to invoke the ***Shortcut Menu*** (on page 101).
7. Click OK.

Keyboard Limitations

Japanese Kanji Keyboards

For Kanji keyboards, when using DCIM-USBs and MPC, the remote client cannot enter EISU mode by pressing the Caps Lock key (key#30). Local port access is not affected. You can access the DCIM-USBs using RRC or using the keyboard macro Shift + Caps Lock in MPC.

Slovenian Keyboards

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

Language Configuration on Linux

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

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

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

Advanced Settings

To configure advanced MPC settings:

1. Choose Tools > Options. The Options dialog appears.
2. Select the Advanced tab to configure advanced options.
3. From the KVM Switch OSUI Hot Key section, select the hot key to use when switching between target server displays.
4. Enter the HTTPS port and Discovery Port.
5. Select the Enable IPv6 Networking checkbox for IPv6 to enable IPv4 and IPv6 dual-stack operation.
6. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.
7. Click OK.

Client Launch Settings

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

Note: LX devices support this feature in MPC. LX does not support client launch setting in VKC and AKC.

To configure client launch settings:

1. Click Tools > Options. The Options dialog appears.
2. Click on the Client Launch Settings tab.
   - To configure the target window settings:

   a. Select 'Standard - sized to target Resolution' to open the window using the target's current resolution. If the target resolution is greater than the client resolution, the target window covers as much screen area as possible and scroll bars are added (if needed).

   b. Select Full Screen to open the target window in full screen mode.

   - To configure the monitor on which the target viewer is launched:

   a. Select 'Monitor Client Was Launched from' if you want the target viewer to be launched using the same display as the application that is being used on the client (for example, a web browser or applet).

b. Use Select From Detected Monitors to select from a list of monitors that are currently detected by the application. If a previously selected monitor is no longer detected, 'Currently Selected Monitor Not Detected' is displayed.

- To configure additional launch settings:

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

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

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

3. Click OK.

Configure Scan Settings in VKC and AKC

The KX II and LX provide a port scanning feature that searches for selected targets and displays them in a slide show view, allowing you to monitor up to 32 targets at one time. You can connect to targets or focus on a specific target as needed. Scans can include standard targets, blade servers, tiered Dominion devices, and KVM switch ports. Configure scan settings from either the Virtual KVM Client (VKC) or Active KVM Client (AKC). See Configure Scan Settings in VKC and AKC for more information. See Scanning Ports. Use the Scan Settings tab to customize the scan interval and default display options.

To set scan settings:

1. Click Tools > Options. The Options dialog appears.
2. Select the Scan Settings tab.
3. In the "Display Interval (10-255 sec):" field, specify the number of seconds you want the target that is in focus to display in the center of the Port Scan window.
4. In the "Interval Between Ports (10 - 255 sec):" field, specify the interval at which the device should pause between ports.
5. In the Display section, change the default display options for the thumbnail size and split orientation of the Port Scan window.
6. Click OK.

Options in MPC for KX II-101 and KX G1

The Options available in the Tools menu allow you to customize scroll borders, mouse mode settings, Single Cursor mode, auto color calibration, hot key configuration, keyboard type, broadcast port, and logging.

To configure the general options in MPC:

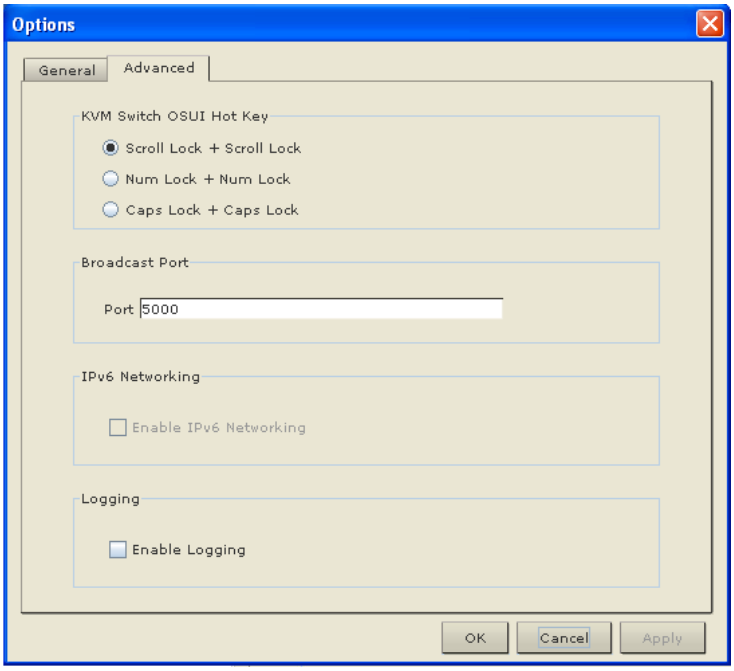
1. Choose Tools > Options. The Options dialog appears and displays the General tab by default.

   General Options

2. Select the "Show scroll borders" checkbox to view the thin scroll borders designating the autoscroll area.
3. Select the "Auto-Sync mouse in two-cursor mode" checkbox to enable automatic mouse synchronization.
4. If you select the "Display single cursor mode instructions" checkbox, the Single Cursor Mode dialog will appear each time Single Cursor is enabled in the application. See ***Mouse Options*** (on page 116) for more information.
5. Select the Automatic Color Calibration checkbox to enable automatic color calibration. This option is available for KX generation 1 (G1) only.
6. Select the Keyboard Type from the drop-down list (depending on the Raritan device in use, different options may be available):
   - US/International
   - French (France)
   - German (Germany)
   - Japanese
   - United Kingdom
   - Korean (Korea)
   - French (Belgium)
   - Norwegian (Norway)
   - Portuguese (Portugal)
   - Danish (Denmark)
   - Swedish (Sweden)
   - German (Switzerland)
   - Hungarian (Hungary)
   - Spanish (Spain)
   - Italian (Italy)

- Slovenian
- Translation: French - US
- Translation: French - US International

7. From the Keyboard Shortcut Menu HotKey drop-down, select the key combination you would like to use to invoke the ***Shortcut Menu*** (on page 101).
8. For advanced options, open the Advanced tab.



9. From the KVM Switch OSUI Hot Key section, select the hot key to use when switching between target server displays.
10. For the Broadcast Port, type the broadcast port number in the Port field if you want to use a port other then 5000.
11. Select the Enable IPv6 Networking checkbox for IPv6 to enable IPv4 and IPv6 dual-stack operation.

Note: KX II-101 devices are not IPv6 enabled, so this section does not apply to those devices.

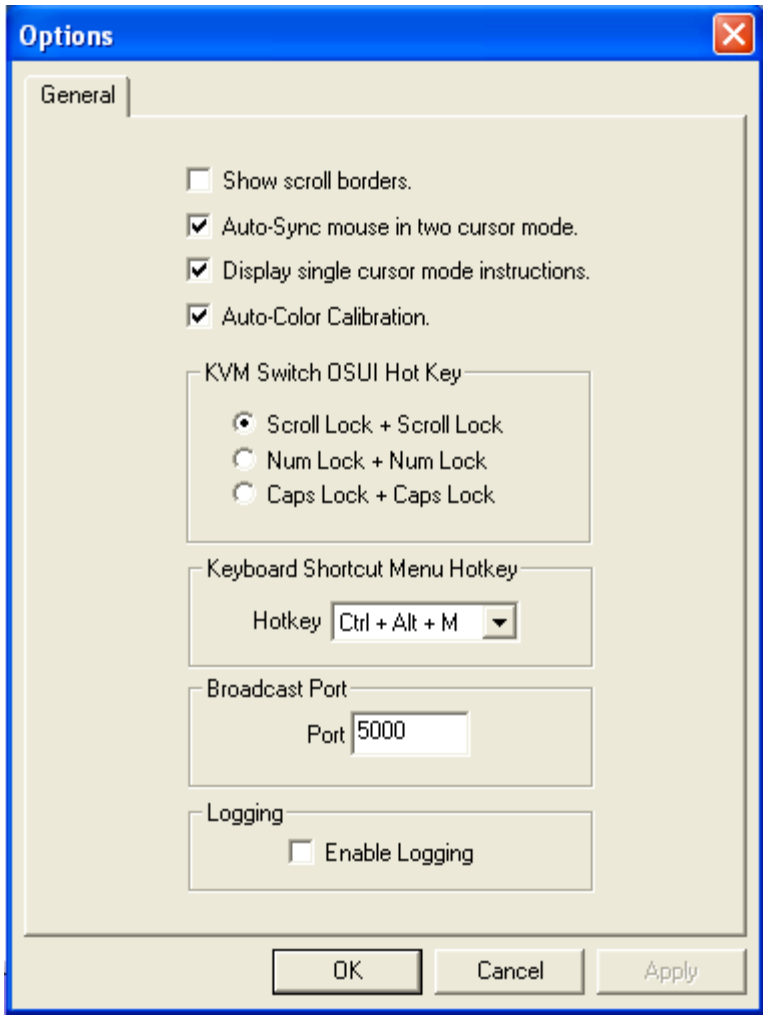
12. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.
13. Click OK when finished. Click Apply any time while making selections to apply it.

Options in RRC

The Options available in the Tools menu provide options that allow you to customize scroll borders, mouse mode settings, single cursor mode, auto color calibration, hot key configuration, keyboard type, broadcast port, and logging.

To configure the general options in RRC:

1. In RRC, choose Tools > Options to open the Options dialog.



2. Select the "Show scroll borders" checkbox to view the thin scroll borders that show the Auto-Scroll area.
3. Select the "Auto-Sync mouse in two cursor mode" checkbox to enable Automatic Mouse Synchronization.

4. If you select the "Display single cursor mode instructions" checkbox the Single Cursor Mode dialog appears each time Single Cursor is enabled in the application (see ***Mouse Options*** (on page 116) for more information).
5. Select Auto-Color Calibration to enable it.
6. In the KVM Switch OSUI Hot Key panel, select the radio button next to the hot key combination you would like to use.
7. In the Keyboard Type panel, click on the drop-down arrow and click on your keyboard choice.
8. In the Broadcast Port panel, type the broadcast port number in the Port field.
9. Click OK when finished. Click Apply any time during your selection to apply an option you have chosen.

Upgrading Device Firmware

To update a device's firmware:

1. Connect to the device by highlighting the device's icon in the Navigator.
2. Click Tools > Update > Update Device to perform firmware upgrades.
3. You are prompted to locate a Raritan firmware distribution file (*.RFP format), which can be found on the Raritan website (www.raritan.com) on the Firmware Upgrades page.

Ensure that you read all instructions included in Firmware Upgrade Guide carefully before upgrading a device.

Note: Copy the firmware update file on the Raritan website to a local machine before uploading. Do not load the file from a network drive.

Clearing ActiveX Controls

After upgrading the device to a newer firmware version, if you still see the previous RRC version, please use the steps below to clear the ActiveX® cache.

To remove TeleControl class files:

1. In Internet Explorer® 7, click Tools > Manage Addons > Enable or Disable Addons.
2. Select "Download ActiveX control 32 bit" from the Show drop down.
3. Select TeleControl class and then click Delete.

4. Close any open sessions of IE7.
5. Open a new IE7 session and go to Raritan's website to download the newest version of RRC.

Changing a Password

To update your password

1. Connect to a target by selecting it in the Navigator.
2. Highlight the target's icon in the Navigator and then choose Tools > Update > User Password. The Change Password dialog appears.

3. Type your current password in the Old Password field.
4. Type the new password in the New Password field.
5. Retype the password in the Confirm New Password field.
6. When finished, click OK.

Restarting a Device

To restart a device:

1. Select the device in the Navigator.
2. On the Tools menu, choose Restart Device.

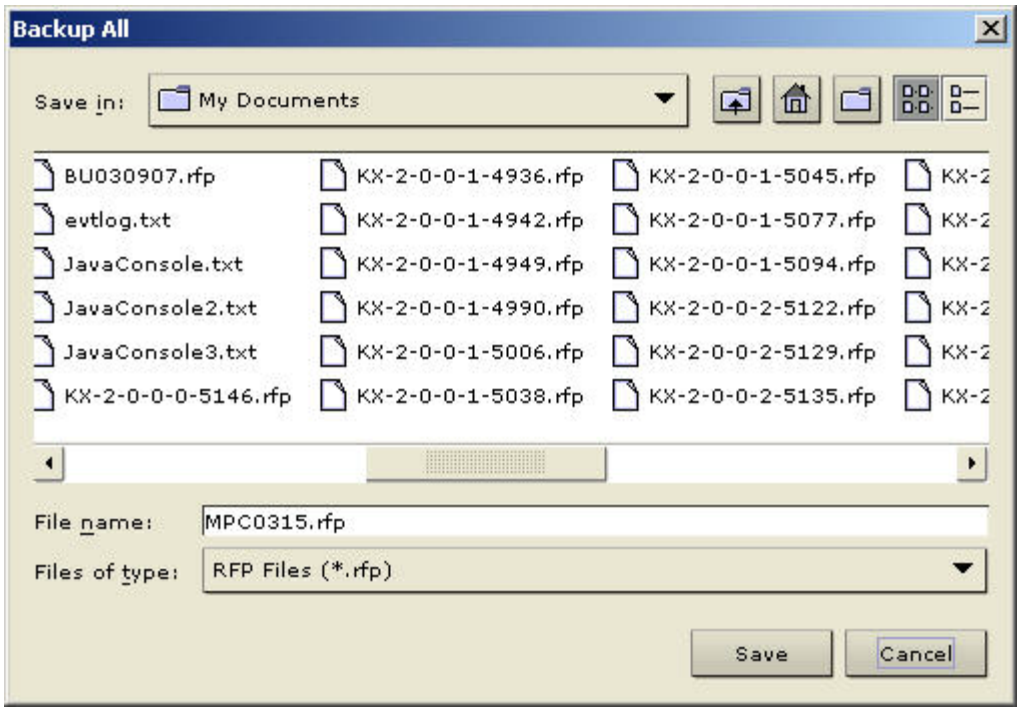
Backup and Restore Functions

In addition to using backup and restore for business continuity purposes, use this feature as a time-saving mechanism. For instance, you can quickly provide access from another Dominion device to your team by backing up the user configuration settings from the device in use and restoring those configurations to the new Dominion device.

Backing Up and Restoring an Entire System (Dominion KX II only)

To back up the entire system (both user and device configuration):

1. Choose Tools > Backup All. The Backup All dialog appears.

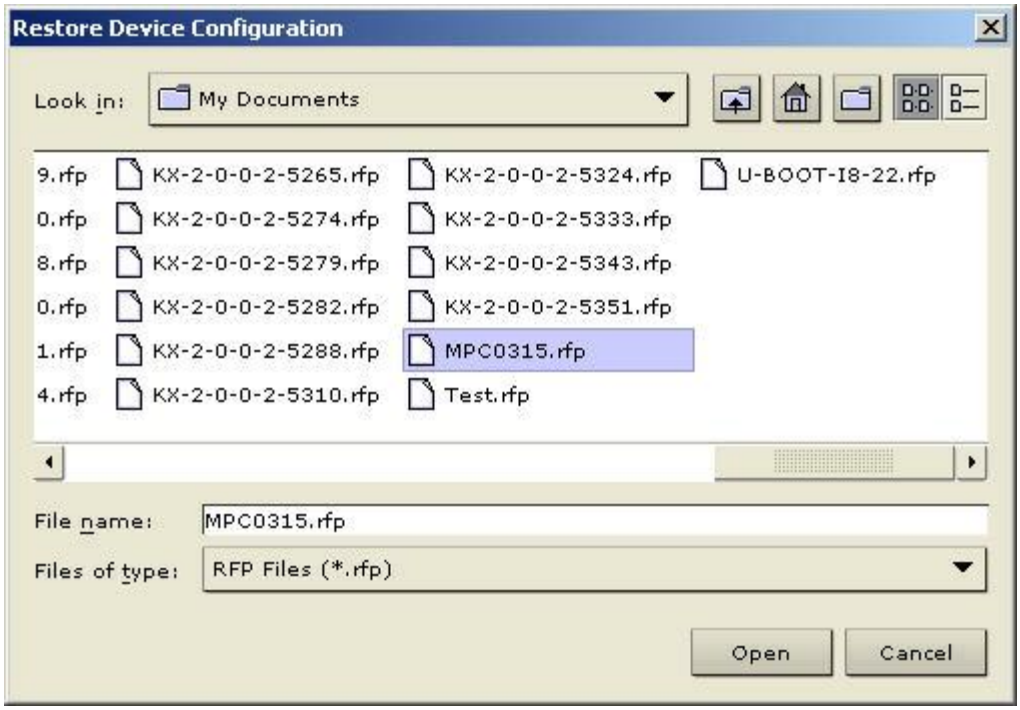


2. Navigate to the desired directory and give the backup file a name. (Backup files have an extension of .rfp).
3. Click Save. A message is displayed confirming the successful backup.
4. Click OK.

Note: Backups are always complete system backups. Restores can be complete or partial depending on your selection.

To restore:

1. Choose Tools > Restore Configuration. The Restore Device Configuration dialog appears.



2. Navigate to the appropriate directory and select the backup file.
3. Click Open. The Restore Packages dialog appears.
4. Select the type of restore you want to run:
   a. Full Restore - A complete restore of the entire system; generally used for traditional backup and restore purposes.
   b. Protected Restore - Everything is restored except device-specific information such as serial number, MAC Address, IP Address, name, port names, etc. With this option, you can setup one Dominion device and copy the configuration to multiple Dominion devices.
   c. Custom Restore - The following options are available:
   - User and Group Restore - This option includes only user and group information. Use this option to quickly setup users on a different Dominion device. This option restores the certificate and the private key file that were currently active when the backup occurred.

- Device Settings Restore - This option includes only device settings such as power associations, USB profiles, blade chassis related configuration parameters, and Port Group assignments. Use this option to quickly copy the device information.

5. Click OK.

Backing Up and Restoring a Device Configuration

To back up a device:

1. Download the device configuration to your local computer by selecting the device in the Navigator.
2. Click Tools > Save Device Configuration.

To restore a device configuration:

1. Upload the archived device configuration by selecting the device in the Navigator.
2. Click Tools > Restore Device Configuration.

   Note that device configuration is specific to a particular device and should not be restored to another device.

Backing Up and Restoring a User Configuration

To back up a device's user configuration:

1. Select the device in the Navigator.
2. Click Tools > Save User Configuration.

To restore a user configuration:

1. Upload a device's archived user configuration by selecting the device in the Navigator.
2. Click Tools > Restore User Configuration.

Note: Use these commands to easily transfer user and group information from one device to another.

Log Files

Activity Log for Generation 1 Devices

To download a detailed activity log for review or troubleshooting:

1. Select the device in the Navigator.

2. On the Tools menu, choose Save Activity Log.

Diagnostic Log (excluding KX II)

To download a detailed diagnostic log for reporting or analysis:

1. Select the device in the Navigator.
2. On the Tools menu, choose Save Diagnostic Log.

Broadcast Port

By default, all Raritan devices send data through Port 5000. This network traffic includes the autodiscovery broadcast. In the case of conflicts or to deal with firewall issues, you may want to use a different broadcast port.

MPC Broadcast Port

To change the autodiscovery port from the default broadcast port of 5000:

1. Select the device in the Navigator.
2. Choose Tools > Options. The Options dialog appears.
3. On the Advanced tab, type the new port number in the Discovery Port field.
4. Click OK.

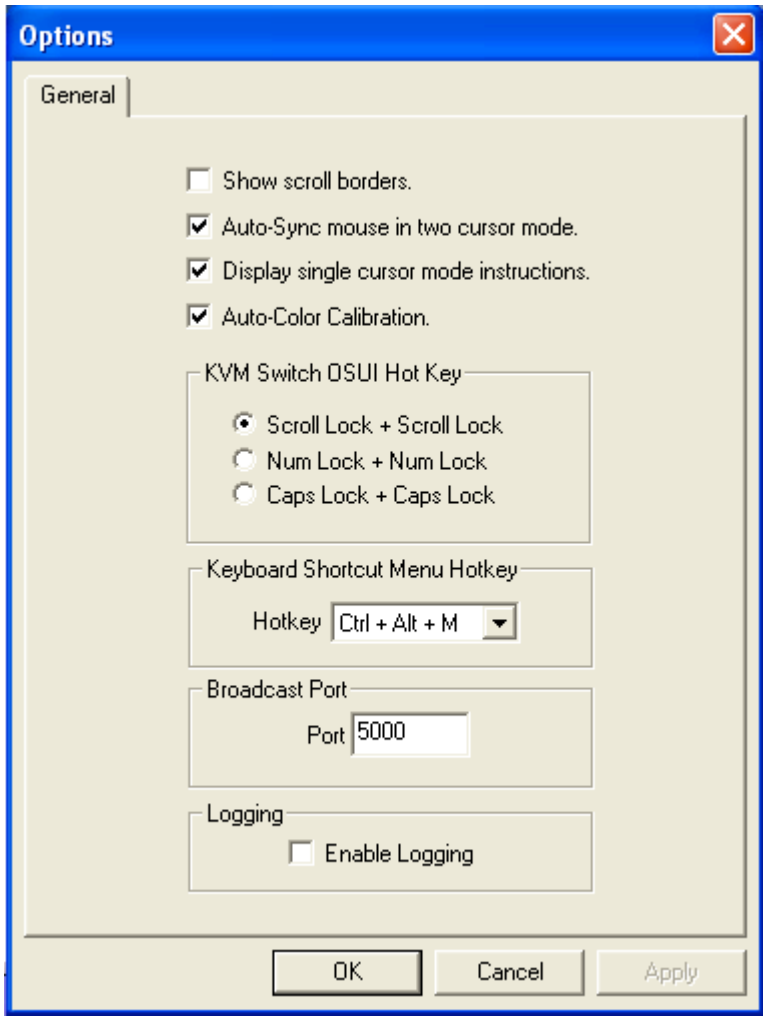
Note: If you want the application to autodiscover Raritan devices on the new broadcast port you entered in the Options dialog, you must configure all Raritan devices to use the new port number.

RRC Broadcast Port

To change the autodiscovery port from the default broadcast port of 5000:

1. Select the device in the Navigator.
2. On the Tools menu, choose Options. The Options dialog appears.
3. In the Broadcast Port field, type the new port number in the Port field and then click OK.

Note: If you want the application to autodiscover Raritan devices on the new broadcast port you entered in the Options window, you must configure all Raritan devices to use the new port number.

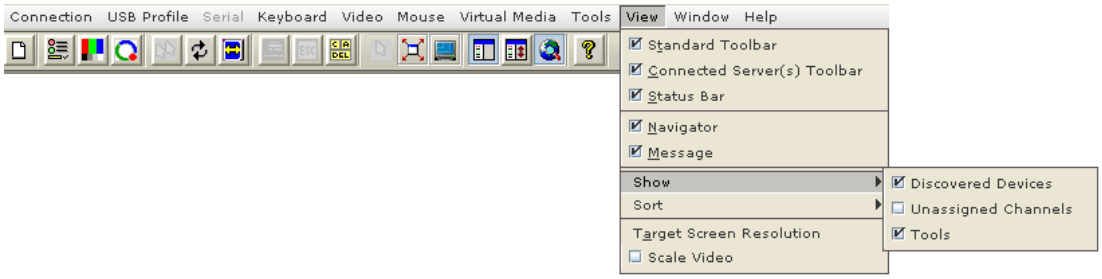


If you do not want to use the broadcasting function at all, it can be turned off.

To turn off broadcasting:

1. In RRC, select View > Show.
2. Deselect the Discovered Devices checkbox.

Broadcasting is turned off and the devices are not be displayed in the navigator.



Remote Power Management

AC power to associated targets can be managed when used with a properly configured Raritan Remote Power Control Strip (RPC strip). Three options are available when performing remote target power management:

- Power On
- Power Off
- Cycle Power

To change the power status of a target:

1. Select the target in the Navigator.
2. On the Tools menu, choose Power On, Power Off, or Cycle Power.

Import/Export Keyboard Macro Definitions

The functions contained in this section describe how to exchange keyboard macro definitions between users using import and export functions. The primary purpose of this function is to exchange data between copies of the client application.

Import/Export Keyboard Macros

Macros exported from Active KVM Client (AKC) cannot be imported into Multi-Platform Client (MPC) or Virtual KVM Client (VKC). Macros exported from MPC or VKC cannot be imported into AKC.

To import macros:

1. Choose Keyboard > Import Keyboard Macros to open the Import Macros dialog. Browse to the folder location of the macro file.
2. Click on the macro file and click Open to import the macro.
   a. If too many macros are found in the file, an error message is displayed and the import terminates once OK is selected.

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

3. Select the macros to be imported by checking their corresponding checkbox or using the Select All or Deselect All options.
4. Click OK to begin the import.
   a. If a duplicate macro is found, the Import Macros dialog appears. Do one of the following:
      - Click Yes to replace the existing macro with the imported version.
      - Click Yes to All to replace the currently selected and any other duplicate macros that are found.
      - Click No to keep the original macro and proceed to the next macro
      - Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are skipped as well.
      - Click Cancel to stop the import.
      - Alternatively, click Rename to rename the macro and import it. If Rename is selected, the Rename Macro dialog appears. Enter a new name for the macro in the field and click OK. The dialog closes and the process proceeds. If the name that is entered is a duplicate of a macro, an alert appears and you are required to enter another name for the macro.
   b. If during the import process the number of allowed, imported macros is exceeded, a dialog appears. Click OK to attempt to continue importing macros or click Cancel to stop the import process.

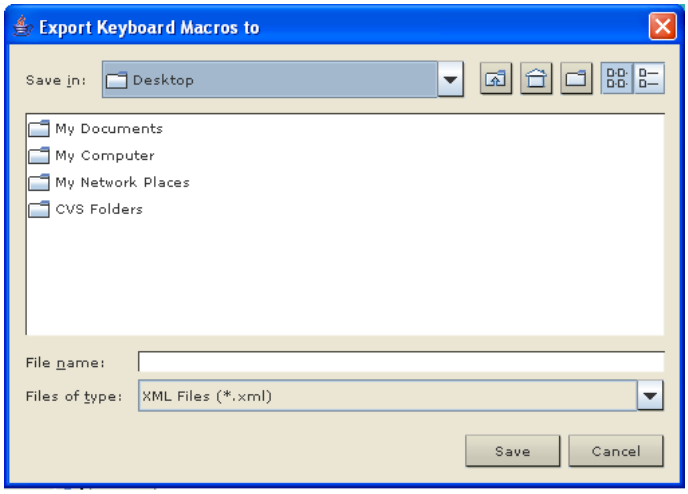
The macros are then imported. If a macro is imported that contains a hot key that already exists, the hot key for the imported macro is discarded.

To export macros:

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

2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.
3. Click Ok. An "Export Keyboard Macros to" dialog is displayed. Locate and select the macro file. By default, the macro exists on your desktop.

4. Select the folder to save the macro file to, enter a name for the file and click Save. If the macro already exists, you receive an alert message. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.



Import/Export RRC Keyboard Macros

To export RRC macros:

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

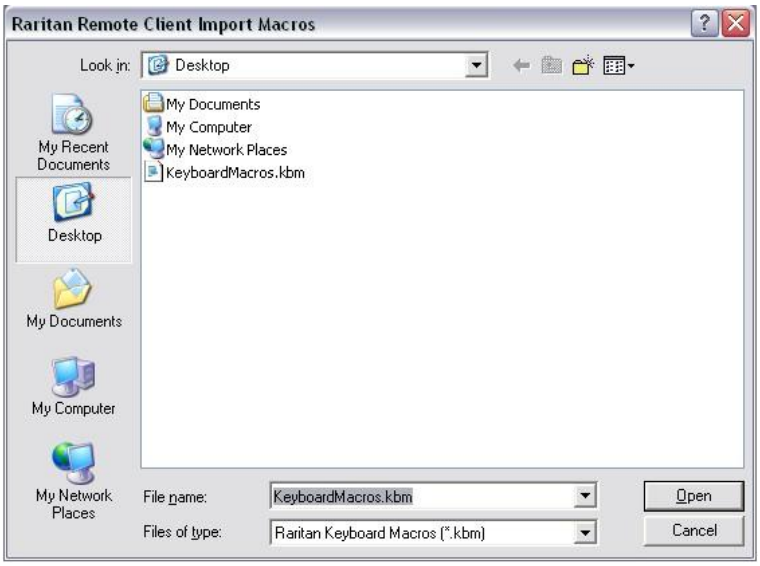
2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Unselect All options.
3. Click OK. The selected macro file(s) are moved to your desktop (by default).

   A select dialog from which you can locate and select the macro file appears. By default, the macro exists on your desktop.

4. Locate the macro file, click on it to select it and then click Save. If the macro already exists, you receive an alert message. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.

To import RRC macros:

1. Choose Tools > Import Macros to open the Import Macros dialog. By default, the macro exists on the desktop.

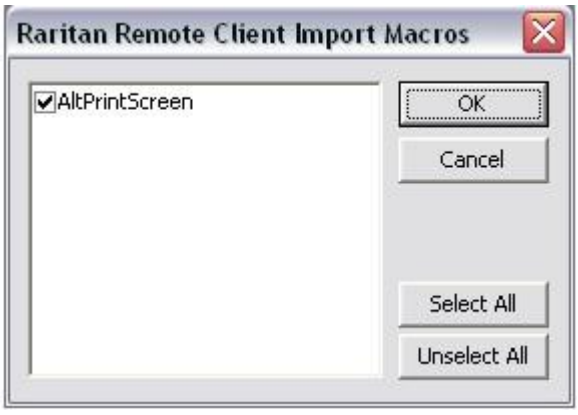


2. Click on the macro file and click Open to import the macro.

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

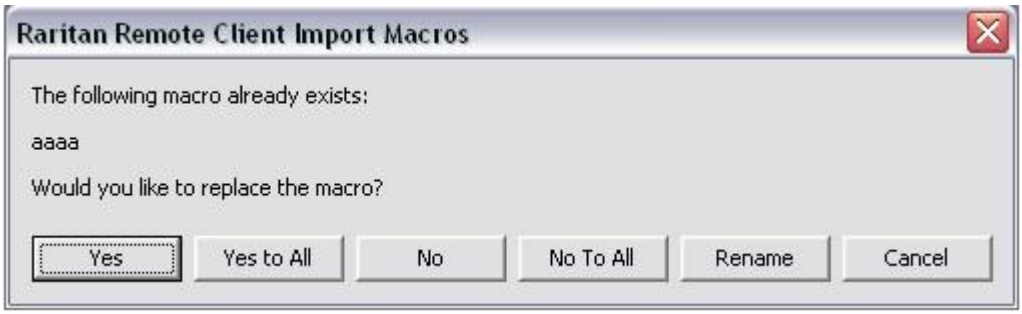
b. If the import fails, an error dialog appears and displays a message regarding why the import failed. Select OK to continue the import without importing the macros that cannot be imported.

3. Select the macros to be imported by checking their corresponding checkbox or using the Select All or Unselect All options.
4. Click OK to begin the import.

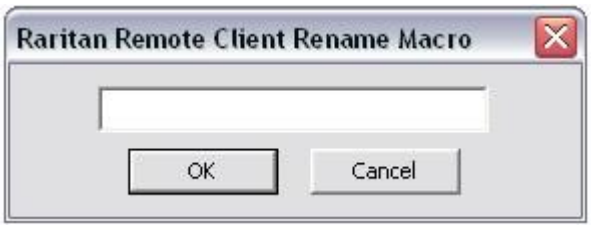


a. If a duplicate macro is found, a dialog appears. Do one of the following:

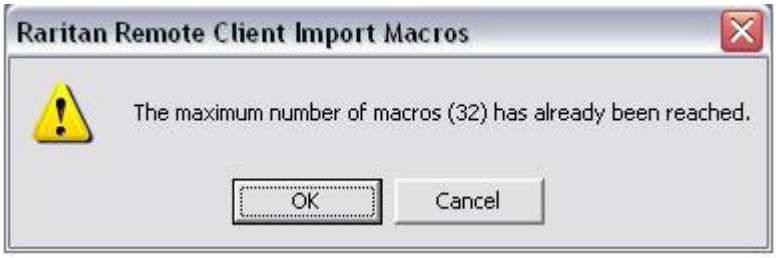
- Click Yes to replace the existing macro with the imported version.
- Click Yes to All to replace the currently selected and any other duplicate macros that are found.
- Click No to keep the original macro and proceed to the next macro
- Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are skipped as well.
- Click Cancel to stop the import.



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



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

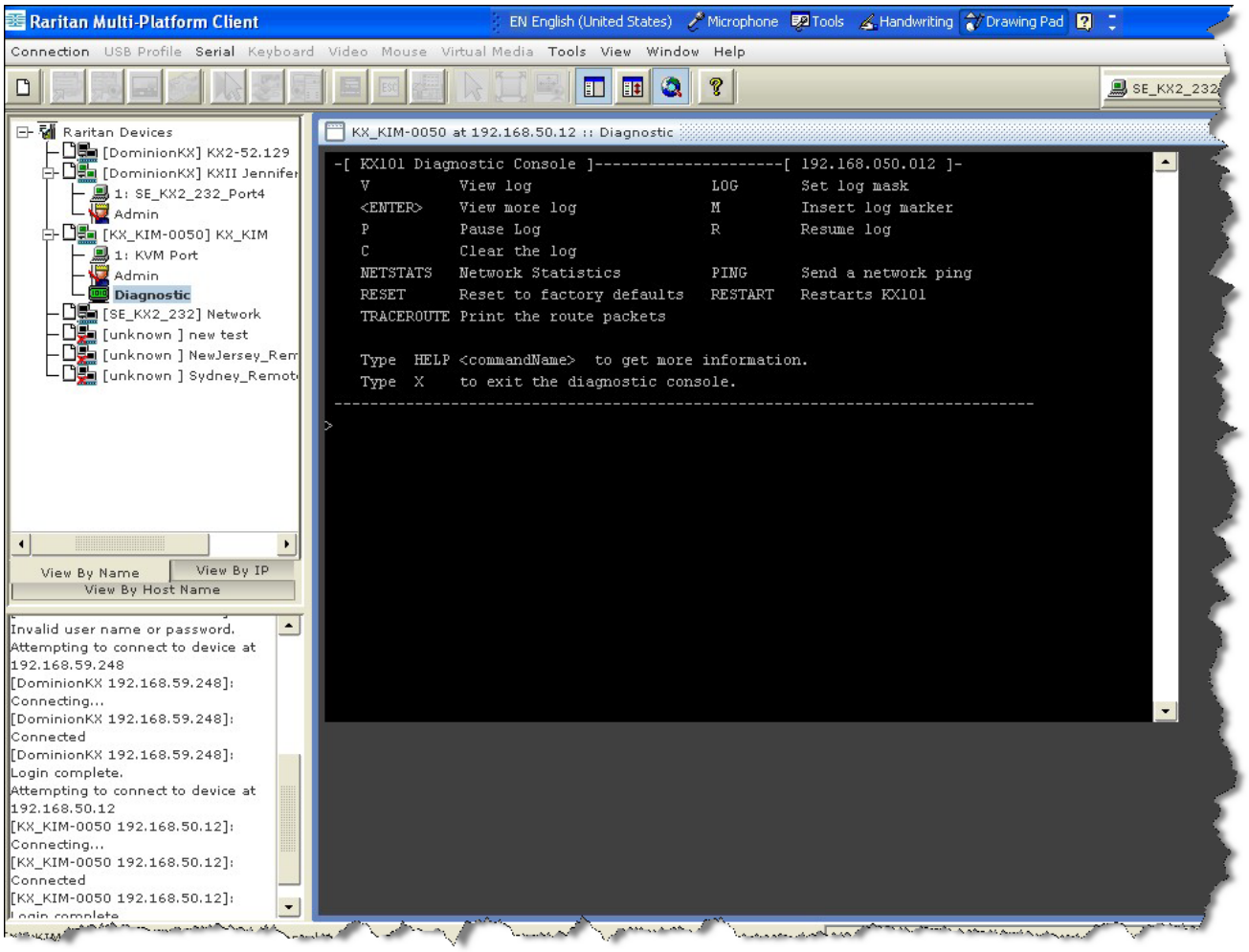


The macros are imported. If a macro is imported that contains a hot key that already exists, the hot key for the imported macro is discarded.

Accessing the MPC Diagnostic Interface (excluding KX II)

To access a device's diagnostic console:

- In the Navigator, scroll through the list of the targets associated with the device and then double-click the Diagnostic icon at the bottom of the target list.



Chapter 4 Virtual Media

In This Chapter

Overview

Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from a client PC and network file servers. The supports virtual media access of hard drives and remotely mounted images. Virtual media sessions are secured using 256-bit AES or RC4 encryption.

With this feature, media mounted on a client PC and network file servers is essentially "mounted virtually" by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself. In addition to data file support via virtual media files are supported by virtual media via a USB connection.

Digital CIMs, D2CIM-VUSB CIM and D2CIM-DVUSB (computer interface module) support virtual media sessions to KVM target servers supporting the USB 2.0 interface. These CIMs also support Absolute Mouse Synchronization as well as remote firmware update.

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
- Record and playback of digital audio*

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

- Internal and USB-mounted CD and DVD drives
- USB mass storage devices
- PC hard drives
- ISO images (disk images)
- Digital audio devices*

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

Note: Items marked with an asterisk (*) are not support by the LX.

KX II 2.4.0 and Higher Users

The following client operating systems are supported:

- Windows
- Mac OS X 10.5, 10.6 and 10.7
- Red Hat Desktop 4.0 and 5.0
- Open SUSE 10, 11

- Fedora 13 and 14

The Virtual KVM Client (VKC) and Multi-Platform Client (MPC) can be used to mount virtual media types with the exception of Mac OS X 10.5, which is supported exclusively by MPC.

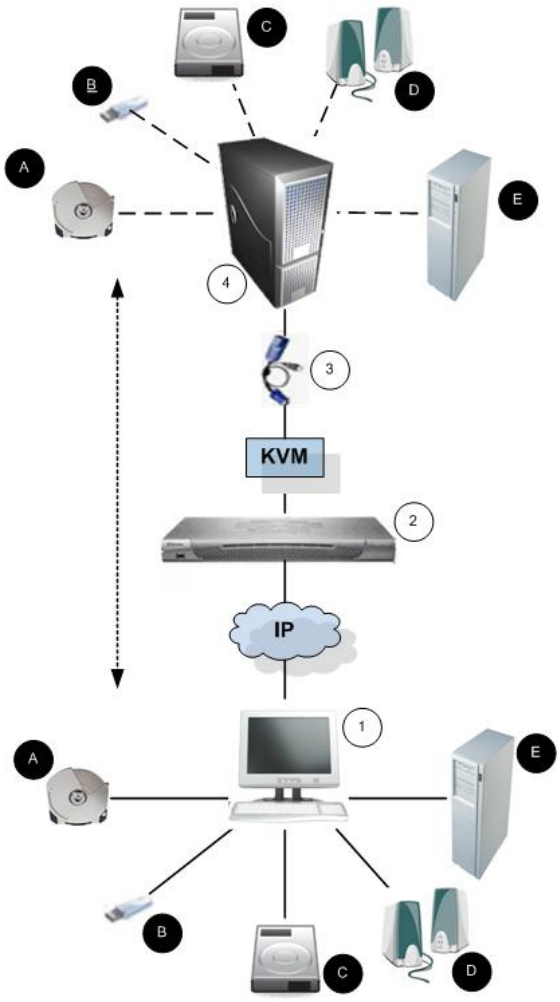


Diagram key			
1	Desktop PC	B	USB mass storage device
2		C	PC hard drive
3	CIM	D	Audio speakers
4	Target server	E	Remote file server (ISO images)
A	CD/DVD drive		

Note: Audio is not supported by the LX.

Prerequisites for Using Virtual Media

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. These drives are accessible for the duration of the KVM session.

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

To use virtual media, connect/attach the media to the client or network file server that you want to access from the target server. This need not be the first step, but it must be done prior to attempting to access this media.

The following conditions must be met in order to use virtual media:

Dominion Device

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

Client PC

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

Note: If you are using Microsoft Vista or Windows 7, disable User Account Control or select Run as Administrator when starting Internet Explorer. To do this, click the Start Menu, locate IE, right-click and select Run as Administrator.

Target Server

- KVM target servers must support USB connected drives.
- KVM target servers running Windows 2000 must have all of the recent patches installed.
- USB 2.0 ports are both faster and preferred.

Virtual Media in a Windows XP Environment

If you are running the Virtual KVM Client or Active KVM Client in a Windows® XP environment, users must have Administrator privileges to access any virtual media type other than CD-ROM connections, ISOs and ISO images.

Virtual Media in a Linux Environment

KX II 2.4.0 (and later), KSX II 2.5.0 (and later) and LX 2.4.5 (and later) support virtual media in a Linux® environment. Following is important information for Linux users regarding using virtual media.

Active System Partitions

You cannot mount active system partitions from a Linux client.

Linux Ext3/4 drive partitions need to be unmounted via umount /dev/<device label> prior to a making a virtual media connection.

Drive Partitions

The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows and Linux cannot read Mac formatted partitions
- Only Windows Fat partitions are supported by Linux

Root User Permission Requirement

Your virtual media connection can be closed if you mount a CD ROM from a Linux client to a target and then unmount the CD ROM. The connection also closes when a floppy drive has been mounted and then a floppy disk is removed. To avoid these issues, you must be a root user.

Mapped Drives

Mapped drives from Linux clients are not locked when mounted onto connected targets. This applies only to KX II 2.4.0 (and later) and LX 2.4.5 (and later).

Permissions

Users must have the appropriate access permissions in order to connect the Drive/CD-ROM to the target. This can be checked using:

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0

brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

In the above example, the permission must be changed to allow read access.

On a system that supports ACLs in its file utilities, the ls command changes its behavior in the following way:

- For files that have a default ACL or an access ACL that contains more than the three required ACL entries, the ls(1) utility in the long form produced by ls -l displays a plus sign (+) after the permission string.

This is indicated in the example provided here for /dev/sr0, use getfacl –a /dev/sr0 to see if the user has been provided access as part of an ACL. In this case they have and are therefore able to connect the cd-rom onto the target even though the output of the ls –l command may indicate otherwise.

```
guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl: Removing leading '/' from absolute path names
# file: dev/sr0
# owner: root
# group: cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---
```

A similar check of the permissions for a removable device shows:

```
guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1


guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
&gt;  getfacl -a /dev/sdb1
getfacl: Removing leading '/' from absolute path names
# file: dev/sdb1
# owner: root
# group: disk
user::rw-
group::rw-
other::---
```

This requires that the user is provided read only permissions for the removable device:

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

The drive is then available to connect to the target.

Virtual Media in a Mac Environment

KX II 2.4.0 (and later), KSX II 2.5.0 (and later) and LX 2.4.5 (and later) support virtual media in Mac® environment. Following is important information for Mac users regarding using virtual media.

Active System Partitions

You cannot use virtual media to mount active system partitions for a Mac client.

Drive Partitions

The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows cannot read Mac formatted partitions
- Windows FAT and NTFS are supported by Mac
- Mac users must unmount any devices that are already mounted in order to connect to a target server. Use >diskutil umount /dev/disk1s1 to unmount the device and diskutil mount /dev/disk1s1 to remount it.

Mapped Drives

- Mapped drives from Mac clients are not locked when mounted onto connected targets. This applies only to KX II 2.4.0 (and later) and LX 2.4.5 (and later).

Conditions when Read/Write is Not Available

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

- For Linux® and Mac® clients
- For all hard drives
- When the drive is write-protected
- When the user does not have Read/Write permission:
  - Port Permission Access is set to None or View
  - Port Permission VM Access is set to Read-Only or Deny

Using Virtual Media

See ***Prerequisites for Using Virtual Media*** (on page 166) before proceeding with using virtual media.

To use virtual media:

1. If you plan to access file server ISO images, identify those file servers and images through the Remote Console File Server Setup page.

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

2. Open a KVM session with the appropriate target server.
   a. Open the Port Access page from the Remote Console.
   b. Connect to the target server from the Port Access page:
   - Click the Port Name for the appropriate server.
   - Choose the Connect command from the Port Action menu. The target server opens in a Virtual KVM Client window.

3. Connect to the virtual media.

For:	Select this VM option:
Local drives	Connect Drive
Local CD/DVD drives	Connect CD-ROM/ISO
ISO Images	Connect CD-ROM/ISO
File Server ISO Images	Connect CD-ROM/ISO

Upon completion, disconnect the virtual media. See ***Disconnecting Virtual Media*** (on page 175).

Virtual Media File Server Setup (File Server ISO Images Only)

Note: This feature is only required when using virtual media to access file server ISO images. ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

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

Use the Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using virtual media. File server ISO images specified here are available for selection in the Remote Server ISO Image Hostname and Image drop-down lists in the Map Virtual Media CD/ISO Image dialog. See ***Mounting CD-ROM/DVD-ROM/ISO Images*** (on page 174).

To designate file server ISO images for virtual media access:

1. Choose Virtual Media from the Remote Console. The File Server Setup page opens.
2. Check the Selected checkbox for all media that you want accessible as virtual media.
3. Enter information about the file server ISO images that you want to access:
   - IP Address/Host Name - Host name or IP address of the file server.
   - Image Path - Full path name of the location of the ISO image. For example, /sharename0/path0/image0.iso, \sharename1\path1\image1.iso, and so on.

   Note: The host name cannot exceed 232 characters in length.
4. Click Save. All media specified here are now available for selection in the Map Virtual Media CD/ISO Image dialog.

Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to technical limitations of third-party software used by the LX, KX, KSX or KX101 G2 device.

Note: If you are connecting to a Windows 2003® server and attempt to load an ISO image from the server, you may receive an error stating "Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password". If this occurs, disable "Microsoft Network Server: Digitally Sign Communications" option on the server under the Domain Controllers policies.

Connecting to Virtual Media

Mounting Local Drives

This option mounts an entire drive, which means the entire disk drive is mounted virtually onto the target server. Use this option for hard drives and external drives only. It does not include network drives, CD-ROM, or DVD-ROM drives. This is the only option for which Read/Write is available.

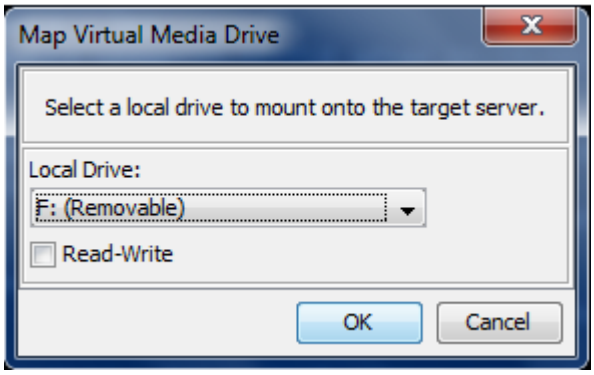
Note: KVM target servers running the Windows XP® operating system may not accept new mass storage connections after an NTFS-formatted partition (for example, the local C drive) has been redirected to them.

If this occurs, close the Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.

Note: In the KX II 2.1.0 (and later), when you mount an external drive such as a floppy drive, the LED light on the drive will remain on because the device is checking the drive every 500 milliseconds to verify the drive is still mounted.

To access a drive on the client computer:

1. From the Virtual KVM Client, choose Virtual Media > Connect Drive. The Map Virtual Media Drive dialog appears. ()



2. Choose the drive from the Local Drive drop-down list.
3. If you want Read and Write capabilities, select the Read-Write checkbox. This option is disabled for nonremovable drives. See the ***Conditions when Read/Write is Not Available*** (on page 170) for more information. When checked, you will be able to read or write to the connected USB disk.

WARNING: Enabling Read/Write access can be dangerous! Simultaneous access to the same drive from more than one entity can result in data corruption. If you do not require Write access, leave this option unselected.

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

Mounting CD-ROM/DVD-ROM/ISO Images

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

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

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

1. From the Virtual KVM Client, choose Virtual Media > Connect CD-ROM/ISO Image. The Map Virtual Media CD/ISO Image dialog appears.
2. For internal and external CD-ROM or DVD-ROM drives:
   a. Choose the Local CD/DVD Drive option.
   b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.
   c. Click Connect.
3. For ISO images:
   a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
   b. Click Browse.
   c. Navigate to the path containing the disk image you want to use and click Open. The path is populated in the Image Path field.
   d. Click Connect.
4. For remote ISO images on a file server:
   a. Choose the Remote Server ISO Image option.
   b. Choose Hostname and Image from the drop-down list. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the File Server Setup page will be in the drop-down list.
   c. File Server Username - User name required for access to the file server. The name can include the domain name such as mydomain/username.

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

e. Click Connect.

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

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

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

Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to third-party software technical limitations.

Disconnecting Virtual Media

To disconnect the virtual media drives:

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

Note: In addition to disconnecting the virtual media using the Disconnect command, simply closing the KVM connection closes the virtual media as well.

Chapter 5 Raritan Serial Console

In This Chapter

Overview

The standalone Raritan Serial Console (RSC) is used to make direct connections to a serial target without going through the device. The user specifies the device address and the port number (target), and is then connected.

RSC System Requirements

The following requirements must be met to support the Raritan Serial Console:

- The RSC works with JRE™ version 1.6.
- Your system may require configuration adjustments depending on the operating system and browser. The JRE provides configuration instructions with the JRE download. Browse to the page at ***http://www.java.com/en/download/help/testvm.xml*** (***http://www.java.com/en/download/help/testvm.xml \o http://www.java.com/en/download/help/testvm.xml***) to determine the JRE version currently installed on your system. If you do not have a compatible version of the JRE, go to ***http://www.java.com*** (***http://www.java.com***) and click the Download Now button.
- Minimum 1 GHz PC with 512 MB RAM.

Ensure that Java™ can be started from the command line. To do this, environment variables must be configured. Make a note of the exact path where Java was installed. (The path information is used later.)

IMPORTANT: When launching RSC from a browser, Raritan highly recommends that Java Applet Caching be disabled and that you perform the following steps to make sure that Java does not create problems for the system's memory.

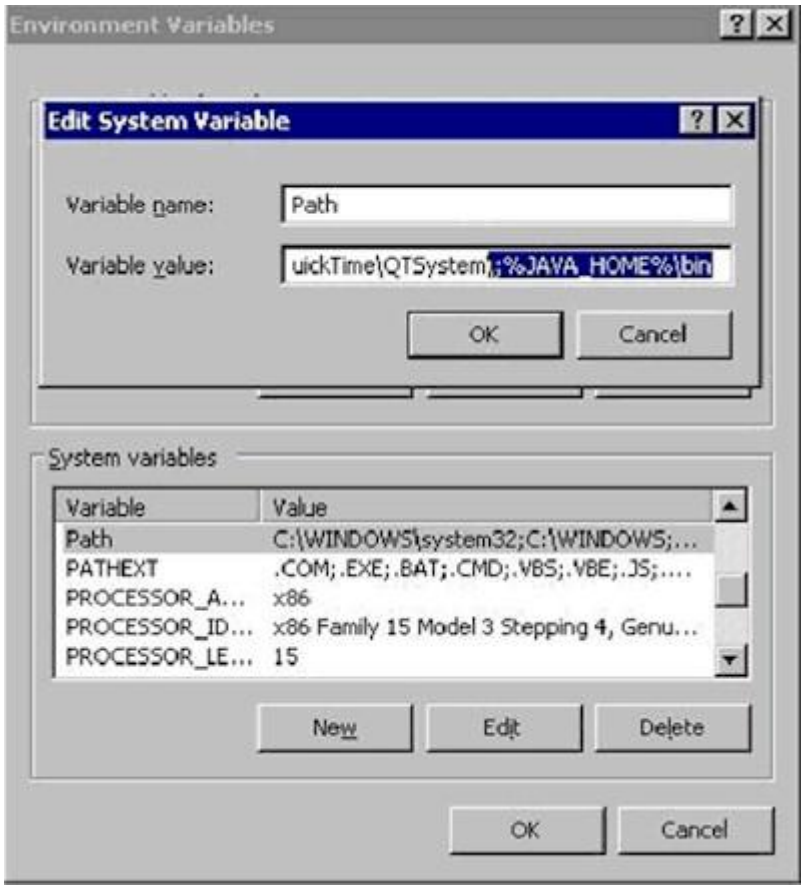
Setting Windows OS Variables

1. Choose Start > Control Panel > System.

2. Click the Advanced tab and then click Environment Variables.

3. In the System variables section, click New.
4. In the New System Variable dialog, add JAVA_HOME to the Variable name block and the path you wrote down earlier in the Variable value block.
5. Click OK.
6. Select the PATH variable and click Edit.
7. Add %JAVA_HOME%\bin to the end of the current Variable value. Ensure a semicolon (;) separates the new value from the last value in the string.

8. Click OK.



9. Select the CLASSPATH variable and click Edit.
10. Ensure the CLASSPATH Variable value is configured properly; that is, its value must have a period (.) in it. If, for any reason, there is no CLASSPATH variable defined, create one.

Setting Linux OS Variables

To set Java™ for a specific user, open and edit the .profile file located in the /home/Username folder.

To set Java for all users, open the .profile file in your /etc folder:

1. Find the line where you set your path:

```
export
PATH=$PATH:/home/username/somefolder
```

2. Before that line you must set your JAVA_HOME and then modify your PATH to include it by adding the following lines:

```
export
JAVA_HOME=/home/username/j2sdk1.6/
export PATH=$PATH:$JAVA_HOME/bin
```

3. Save the file.

Setting UNIX OS Variables

To check the latest JRE™ version on Sun Solaris™:

1. Launch a terminal window on the Sun Solaris desktop.
2. Type `java-version` in the command line and press Enter. The currently-installed version of Java™ Runtime Environment (JRE) appears.
   - If your path variable is not set to where the Java binaries have been installed, you may not be able to see the JRE version.
   - Assuming JRE 1.6 is installed in /usr/local/java: you must set your PATH variable.
   - To set a path for the bash shell:

```
export
PATH=$PATH:/usr/local/java/j2re1.6/bin
```

   - To set path for tcsh or csh:

```
set
PATH = ($PATH /usr/local/java/j2re1.6/bin)
```

   - These commands can either be typed at the terminal each time you log in, or add them to your .bashrc for bash shell or .cshrc for csh and tcsh so that each time you log in, the path is already set. See your shell documentation if you encounter problems.
3. If the JRE is version 1.6 or later, proceed with the RSC installation. If the JRE is an older version than 1.6, go to the Sun website at (http://java.sun.com/products/) to download the latest Runtime Environment.

Installing RSC on Windows

You must have administrative privileges to install RSC.

To install RSC on a Windows® operating system:

1. Log on to a Windows machine.
2. Download, or copy from a known location, the RSC-installer.jar installation file.
3. Double-click the executable file to start the installer program. The splash page appears.
4. Click Next. The installation path page appears.
5. Change the path, if desired.
6. Click Next. The installation progress page appears.

   Note: The standalone version of Raritan Serial Console (RSC) is available from the Raritan website (www.raritan.com) on the Support page.

7. Click Next. The Windows shortcut page appears.
8. Specify the desired Program Group for the shortcut.
9. Click Next. The installation finished page appears.
10. Click Done.

Installing RSC for Sun Solaris and Linux

You must have administrative privileges to install RSC.

1. Log in to your Sun Solaris™ machine.
2. Download, or copy from a known location, the RSC-installer.jar installation file.
3. Open a terminal window and change to the directory where the installer is saved.
4. Type *java -jar RSC-installer.jar* and press Enter to run the installer.
5. Click Next after the initial page loads. The Set Installation Path page opens.
   a. Select the directory where you want to install RSC and click Next.
   b. Click Browse to navigate to a non-default directory.
   c. Click Next when the installation is complete.

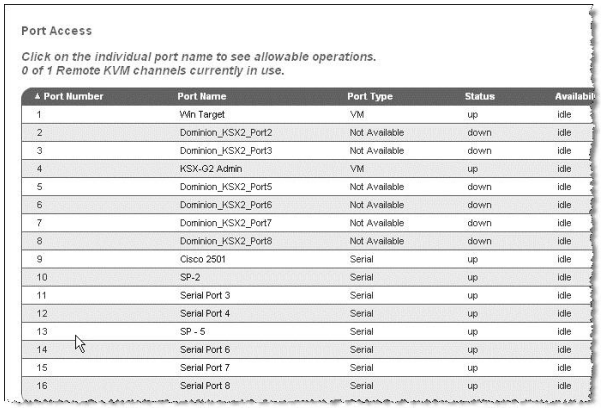
d. Click Next again. The installation is complete. The final page indicates where you can find an uninstaller program and provides the option to generate an automatic installation script.

6. Click Done to close the Installation dialog.

Opening RSC from the Remote Console

To open the Raritan Serial Console (RSC) from the Remote Console:

1. Select the Port Access tab.



2. Click the name of the serial port you want to access for the RSC.

Note: A security pop-up screen appears only if you used https to connect to the RSC.

3. If you're using Dominion DSX:
   - Click Yes. A Warning - Security pop-up screen appears.
   - Click Yes to access the Raritan Serial Console from the Port page.

Note: If you click Always, you will not receive the security page for future access.

   - The Raritan Serial Console window appears.

   If you're using Dominion KSX or KX:
   - Click Connect to start connecting to the target port for RSC, and the Raritan Serial Console window appears.
   - The Raritan Serial Console window appears.

Note: Download the standalone Raritan Serial Console from the Raritan website (www.raritan.com) on the Support page.

To open RSC from the Windows® desktop:

1. Double-click the shortcut or use the Start menu to open the standalone RSC. The Raritan Serial Console Login connection properties window appears.
2. Enter the device's IP address, account information, and the desired target (port).
3. Click Start. RSC opens with a connection to the port.

Note: If you experience unrecognized characters or blurry pages in the RSC window due to localization support, try changing the font to Courier New. Click Emulator > Settings > Display and select Courier New for Terminal Font Properties or GUI Font Properties.

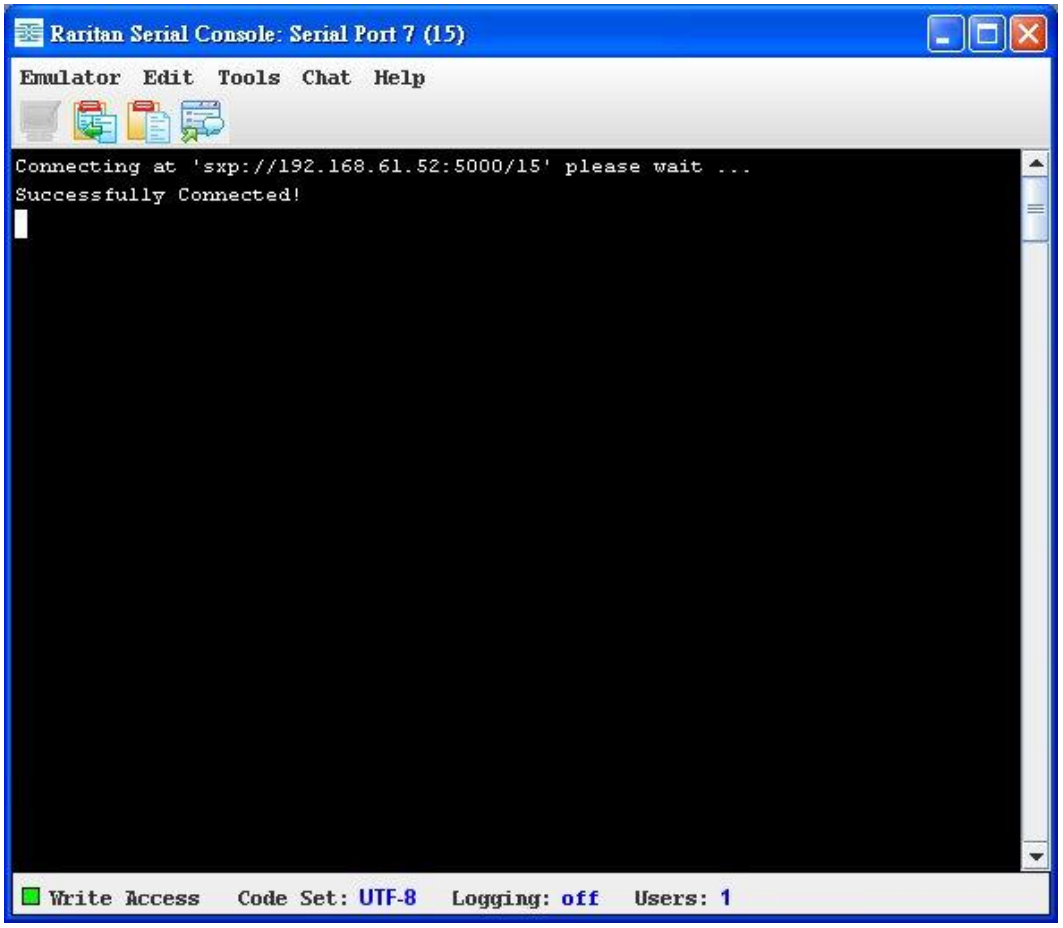
Note: When RSC connects to a serial target, hitting Ctrl + _ or Ctrl + ^ + _ does not cause information to be sent. However, hitting the Ctrl + Shift + _ or the Ctrl + Shift + ^ will cause information to be sent.

To open RSC on Sun™ Solaris™:

1. Open a terminal window and change to the directory where you installed the RSC.
2. Type `./start.sh` and press Enter to open RSC.
3. Double-click the desired device to establish a connection.
4. Type your user name and password.
5. Click OK to log on.

Raritan Serial Console Interface

Important: The Raritan Serial Console page usually opens in a separate window behind the Port page. With some versions of Java™ on the Windows® operating system, the page opens in front of the Port page.



Default RSC Option Values

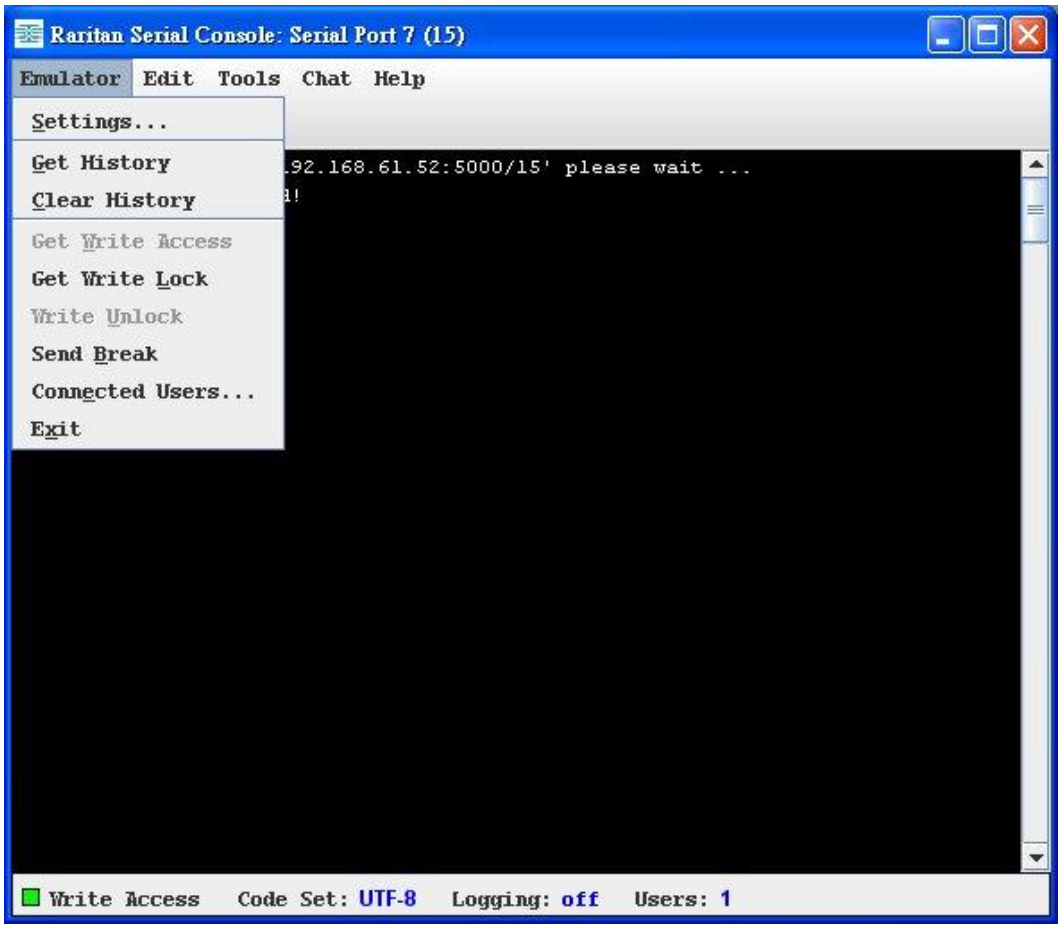
The following default values apply to the GUI font properties, colors and fonts defined in RSC:

Item	Value
Font properties	Lucida Console
GUI font properties	Lucida Console
Colors	White foreground and black

Item	Value
	background

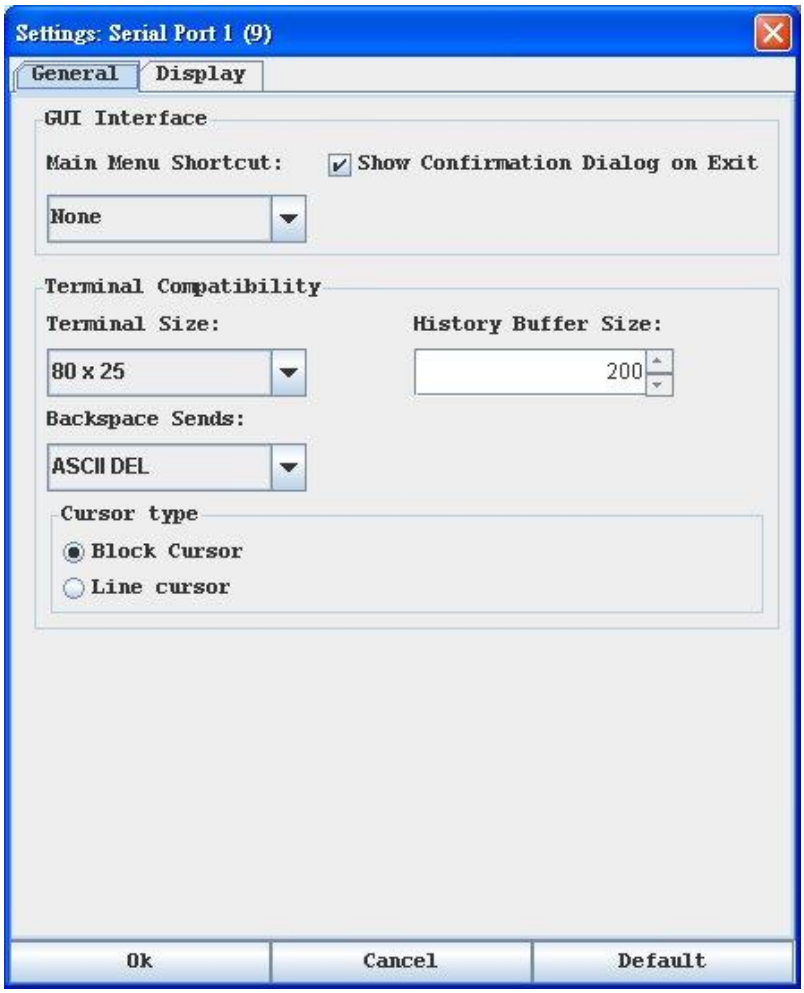
Emulator

1. Change the default user Idle Timeout setting before launching the RSC for the first time or it times out in 10 minutes and display a host termination message.
2. Click the Emulator drop-down menu to display a list of topics.



Settings

1. Choose Emulator > Settings. The Settings page displays the General tab with the default settings.

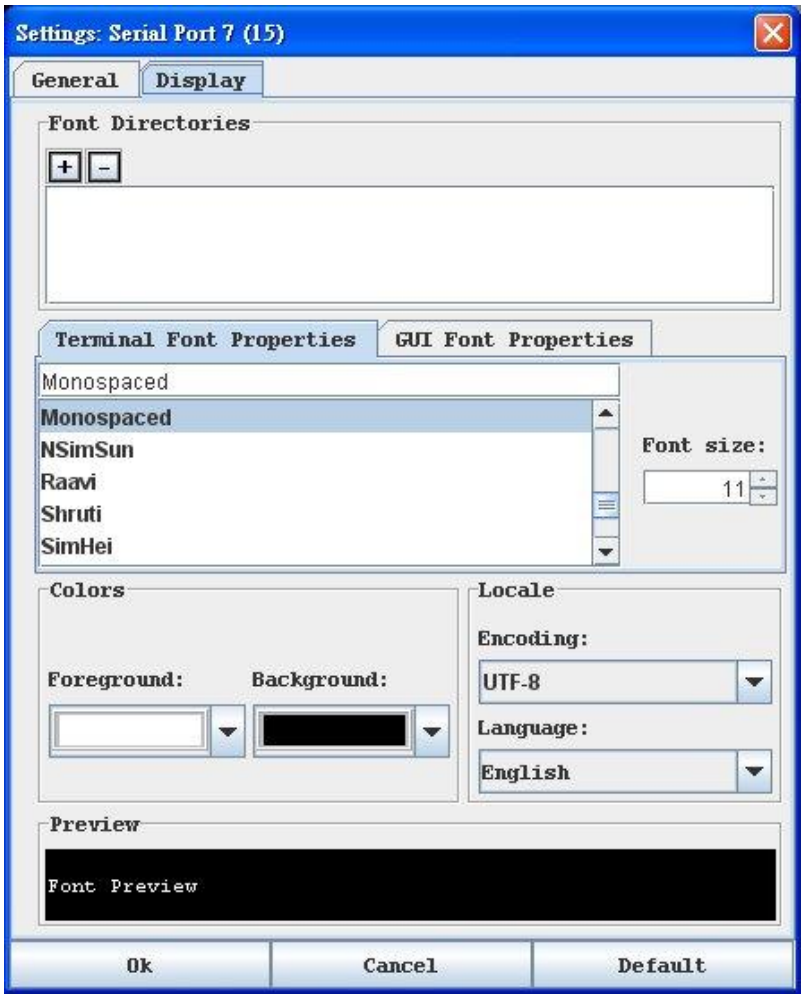


2. Accept the Main Menu Shortcut default of None or choose one of the following from the Main Menu Shortcut drop-down menu:
   - F10
   - Alt
3. Accept the Show Confirmation Dialog on Exit default or uncheck it.
4. Accept the Terminal Size default or choose a size from the Terminal Size drop-down menu.
5. Accept the Backspace Sends default of ASCII DEL or choose Control-H from the Backspace Sends drop-down menu.
6. Accept the History Buffer Size default of 75 or use the arrows to change the buffer size.

7. Accept the Cursor type default of Block Cursor or select Line Cursor.
8. Click OK.

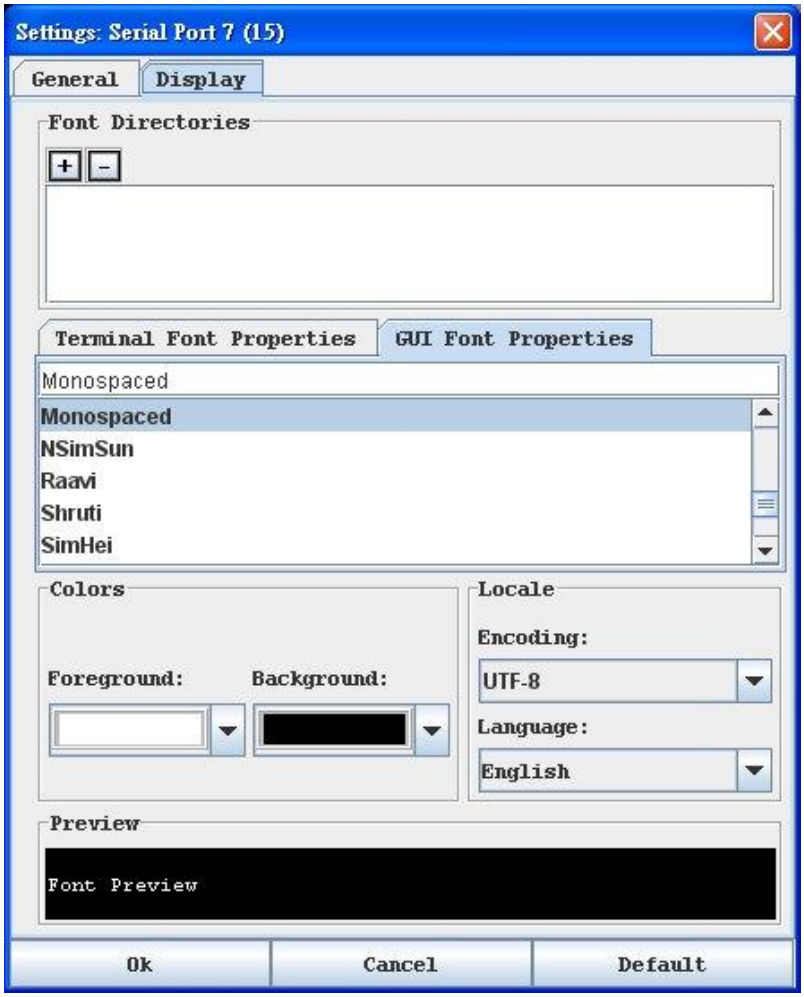
Display Settings

1. Choose Emulator > Settings, and then click the Display tab.



2. Click Default to accept the Default settings. Then click Ok to close the Display Settings dialog. However, if you want to change the settings, perform the following steps:
3. Accept the Terminal Font Properties default of Lucida Console or choose a font from the scrolling list of Terminal Font Properties.
4. If you want to change the size of the font, choose a font size by clicking the up or down arrows. The result of selected font and font size is displayed in the Preview box.

5. Click the GUI Font Properties tab and accept the default of Lucida Console or choose a font from the scrolling list of GUI Font Properties.



Note: For Simplified Chinese characters, Raritan Serial Console supports EUC-CN encoding system.

6. Choose the following from their drop-down menus:
   - Foreground Color
   - Background Color
7. Choose one of the following from the Encoding drop-down menu:
   - US-ASCII
   - ISO-8859-1
   - ISO-8859-15
   - UTF-8

- Shift-JIS
- EUC-JP
- EUC-CN
- EUC-KR

8. Choose one of the following from the Language drop-down menu:
   - English
   - Bulgarian
   - Japanese
   - Korean
   - Chinese
9. Click Ok to close the Display Settings dialog. If you changed the Language setting, the RSC changes to that language when the Display Settings dialog is closed.

Note: If you experience unrecognized characters or blurry pages in the RSC window due to localization support, try changing the font to Courier New.

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.

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

Note: The 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 administrators and operators can 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 Raritan Serial Console via the Get Write Access command.

To enable Write access, choose Emulator > Write Access.

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

Get Write Lock

- Choose Emulator > Get Write Lock. If the Get Write Lock is not available, a request rejected message appears.

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 Administrator privileges can send a break.
- Users who are Operator or Observers cannot send a break.

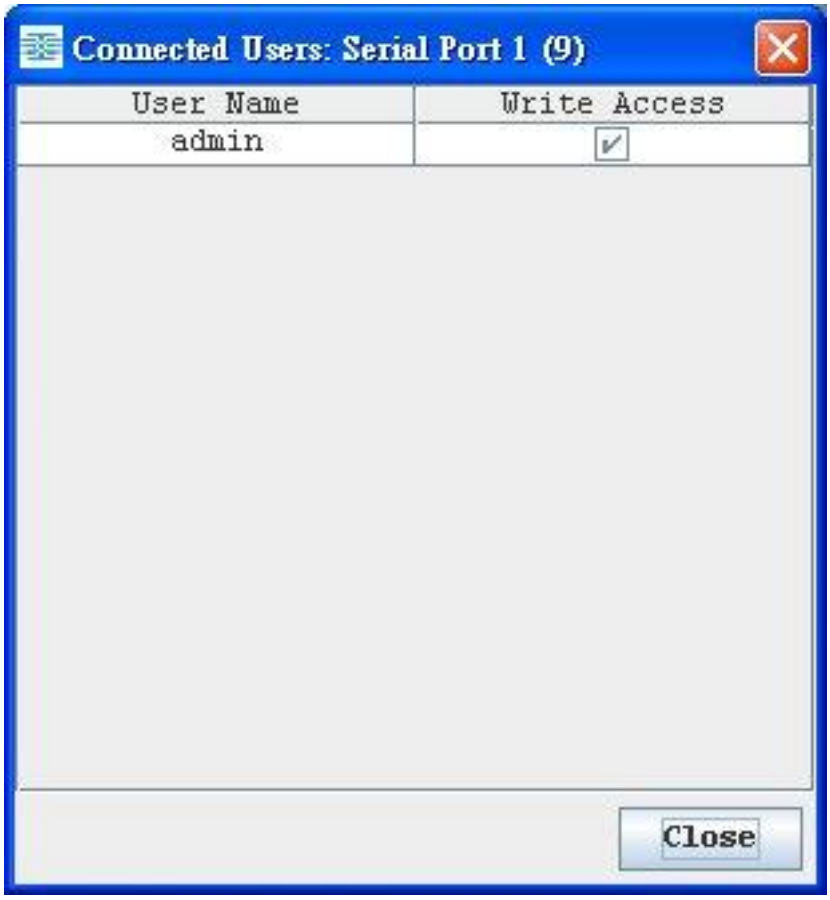
To send an intentional break to a Sun Solaris server:

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

Connected Users

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

1. Choose Emulator > Connected Users, a Connected Users page is displayed.



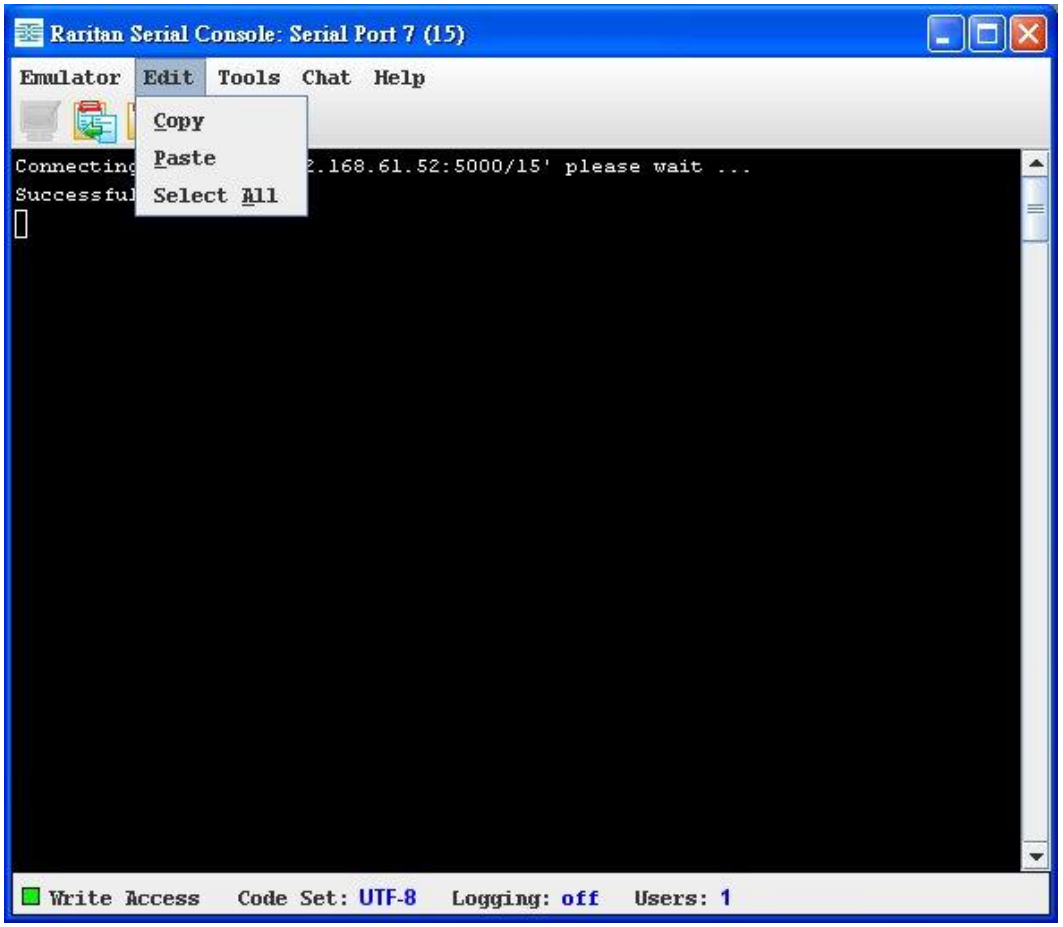
2. A check mark appears in the Write access column after the name of the user who has Write access to the console.
3. Click Close to close the Connected Users window.

Exit

1. Choose Emulator > Exit to close the Raritan Serial Console. The Exit Confirmation page appears.
2. Click Yes.

Edit

Use the Copy, Paste, and Select All text commands to relocate and/or re-use important text.



To copy and paste all text:

1. Choose Edit > Select All.
2. Choose Edit > Copy.
3. Position the cursor at the location where you want to paste the text.
4. Click once to make that location active.
5. Choose Edit > Paste.

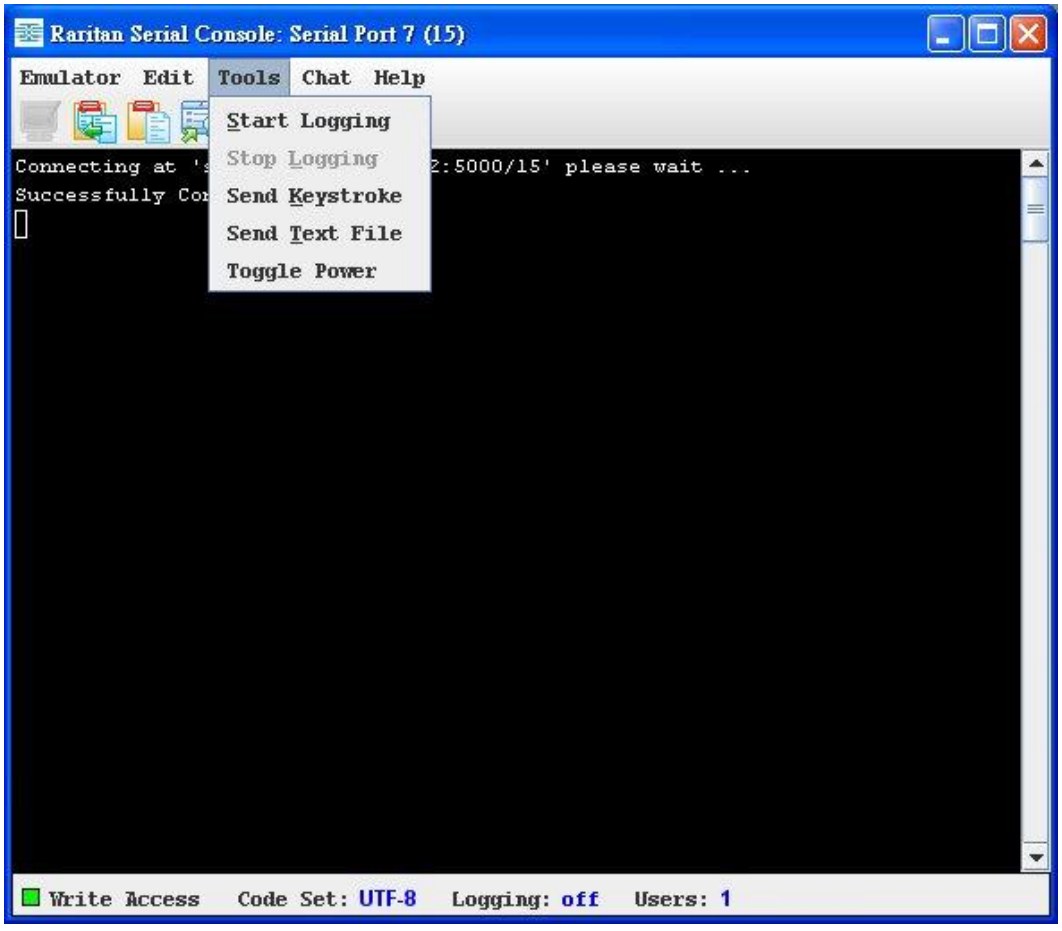
Note: The copy-paste limit of text in Raritan Serial Console is 9999 lines.

Keyboard shortcuts to highlight, copy, and paste all or partial lines of text:

- Click and drag your mouse over the text you wish to copy.
- Use Ctrl+C to copy text.
- Position the cursor where you want to paste the text and click in that location to make it active.
- Use Ctrl+V to paste text.

Tools

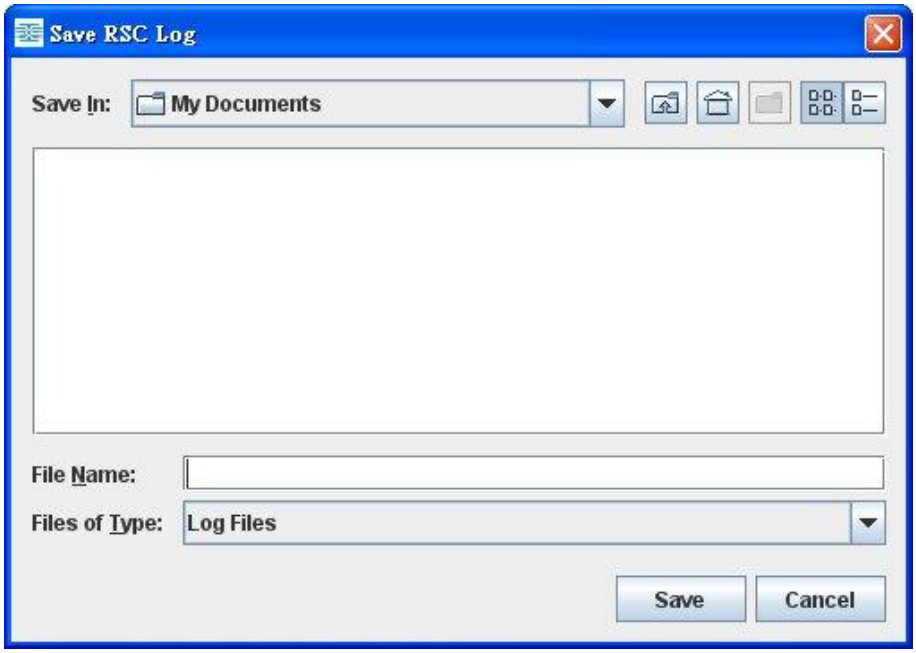
- Click the Tools menu to display a list of topics.



Start Logging

The Start Logging function allows you to collect raw console data from the target device and save it to a file on your computer. When you start RSC, the Logging indicator on the status bar indicates whether logging is on or off.

1. Choose Tools > Start Logging.
2. Choose an existing file or provide a new file name in the Save RSC Log dialog.
   - When an existing file is selected for logging, data gets appended to the contents.
   - If you provide a new file name, a new file is created.



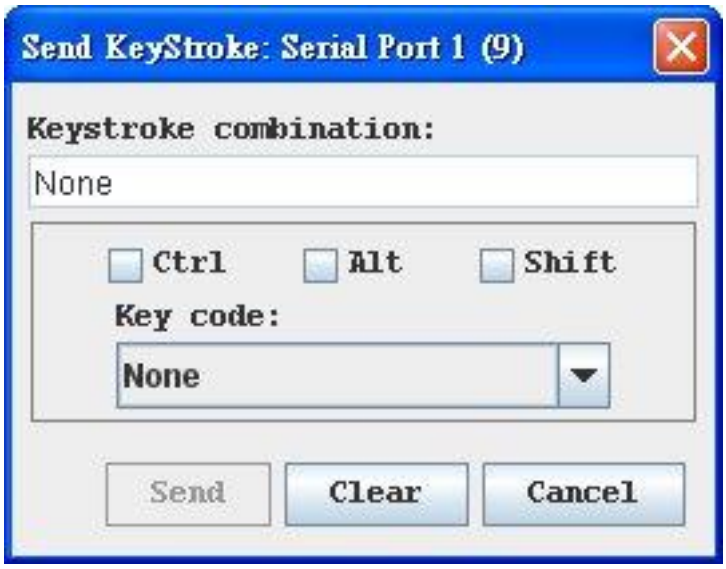
3. Click Save after selecting or creating a file.

Stop Logging

Choose Tools > Stop Logging. The logging stops.

Send Keystroke

1. Choose Tools > Send Keystroke. A Send Keystroke dialog appears:



2. Enter the keystroke combinations that you want and select a Key Code name from the drop-down menu.
3. Send the keystroke combinations.

Send Text File

1. Choose Tools > Send Text File. A Send Text File screen appears.
2. Open the directory of the Text file.
3. Click on or enter the File Name of the Text file.
4. Click Open.
   - When you click Open, it sends whatever file you selected directly to the port.
   - If there is a loopback plug inserted, you will see the file displayed.
   - If there is currently no target connected, then nothing will be visible on the screen.

Toggle Power

The Toggle Power function lets you power on or off the device that is connected to the associated outlet on a Power Distribution Unit (PDU). For example, if a router is connected to one of the outlets on the PDU, you can toggle the router's power on or off.

You must configure the association of outlets to the target port of the device before you can use the Toggle Power feature. Assign a power port to the serial target from the Device Settings > Port Configuration tab of the device. If you have not done this, the system displays a message stating that the target is not associated with a power outlet.

Note: If RSC is launched through CC-SG (version 4.x onwards) by users without the permission to toggle power, the option Toggle Power will appear as disabled.

---

1. Select Toggle Power to turn the device (router) on or off. A prompt appears displaying the current status of the outlet(s). You can turn the device on or off depending on its current status.
2. If you select No, the system returns you to the RSC screen.
3. If you select Yes, the system sends the power command to either turn on or off the outlets associated to the target port of the device.

If you receive a:

- Hardware error message: this means that the PDU command failed.

Software error message: this means that another user is controlling the power outlet and the power control command cannot be sent.

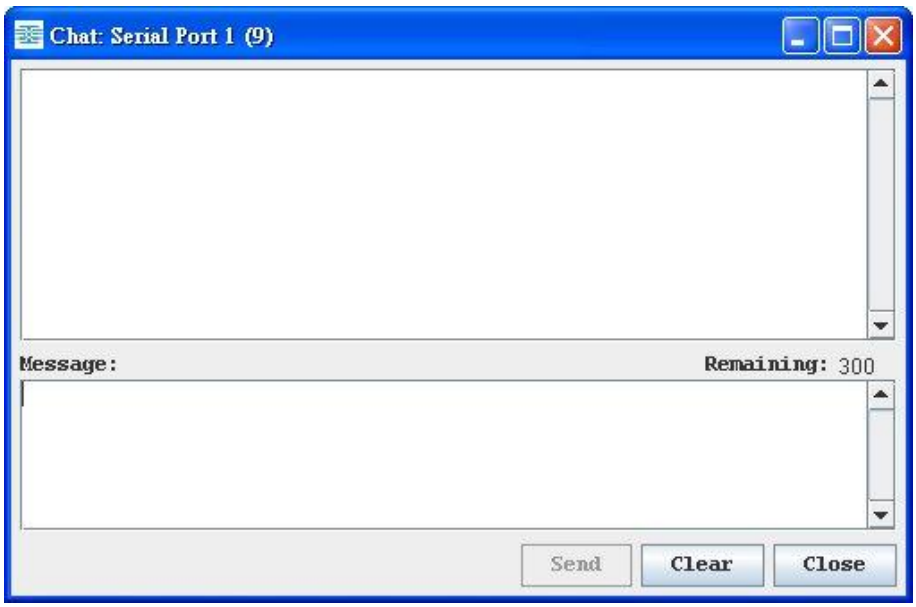
Chat

When using browser access over SSL, an interactive chat feature called Chat allows you and other users on the same port to communicate. The maximum length of a chat message is 300 characters.

Note: When a chat is initiated, a chat window appears on the monitors of all SSL users logged on to the port. If a user is logged into a port multiple times, multiple chat messages do not appear to that user.

To open chat:

- Choose Chat > Chat.



To clear text in a chat text box:

- Click Clear to delete the typed text.

Help

Help Topics include online assistance for operating the Raritan Serial Console and release information about Raritan Serial Console.

Help Topics

To access help topics:

- Choose Help > Help Topics. A list of help topics are displayed.

About Raritan Serial Console

The About Raritan Serial Console dialog displays the copyright and version information (name and revision number) of the console terminal emulation software. When contacting Raritan for technical support or when performing a software upgrade, you may be asked for this information.

To access 'About' information:

- Choose Help > About Raritan Serial Console. An About Raritan Serial Console message appears.

Appendix A Informational Notes

In This Chapter

Overview

Following are important information notes on using Raritan devices with Raritan KVM and serial clients.

Java Runtime Environment (JRE)

Important: It is recommended that you disable Java™ caching and clear the Java cache. Please refer to your Java documentation or the KVM and Serial Access Clients Guide for more information.

The LX, KX II, KX II-101 and KX II-101-V2 Remote Console and MPC require the Java Runtime Environment™ (JRE™) to function since the Remote Console checks the Java version. If the version is incorrect or outdated, you will be prompted to download a compatible version.

Raritan recommends using JRE version 1.7 for optimum performance, but the Remote Console and MPC function with JRE version 1.6.x and later with the exception of 1.6.2.

Note: In order for multi-language keyboards to work in the LX, KX II, KX II-101 and KX II-101-V2 Remote Console (Virtual KVM Client), install the multi-language version of JRE.

IPv6 Support Notes

Operating System IPv6 Support Notes

Java

Java™ 1.6 supports IPv6 for the following:

- Solaris™ 10 (and later)
- Linux® kernel 2.1.2 (and later)/RedHat 6.1 (and later)
- Solaris 10 (and later)
- Windows XP® SP1 and Windows 2003®, Windows Vista® and Windows 7 operating systems

The following IPv6 configurations *are not* supported by Java:

- J2SE does not support IPv6 on Microsoft® Windows®.

Linux

- It is recommended that Linux kernel 2.4.0 or higher is used when using IPv6.
- An IPv6-enabled kernel will need to be installed or the kernel will need to be rebuilt with IPv6 options enabled.
- Several network utilities will also need to be installed for Linux when using IPv6. For detailed information, refer to http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html

Windows

- Windows XP and Windows 2003 users will need to install the Microsoft IPv6 service pack to enable IPv6.
- For AKC with IPv6 on Windows XP, add the executable kxgui.exe to your firewall exception list. View your log file on the client to identify the full path for the location of the file kxgui.exe.

Samba

- IPv6 is not supported for use with virtual media when using Samba.

AKC Download Server Certification Validation IPv6 Support Notes

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

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` when there is a leading 0

  or

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

Keyboard Notes

Non-US Keyboards

French Keyboard

Caret Symbol (Linux® Clients Only)

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

To obtain the caret symbol:

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

Alternatively, create a macro consisting of the following commands:

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

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

Accent Symbol (Windows XP® Operating System Clients Only)

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 7 results in the accented character displaying twice when using French keyboards with Windows XP clients.

Note: This does not occur with Linux clients.

Numeric Keypad

From the Virtual KVM Client and the Multi-Platform Client, the numeric keypad symbols display as follows when using a French keyboard:

Numeric keypad symbol	Displays as
/	;
.	;

Tilde Symbol

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

To obtain the tilde symbol:

Create a macro consisting of the following commands:

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

Keyboard Language Preference (Fedora Linux Clients)

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

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

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

When using a Hungarian keyboard from a Linux client, the Latin letter U with Double Acute and the Latin letter O with Double Acute work only with JRE 1.6.

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

To set the keyboard language using System Settings:

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

To set the keyboard language using the Keyboard Indicator:

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

Mac Keyboard Keys Not Supported for Remote Access

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

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

As a result, the Virtual KVM Client and the Multi-Platform Client (MPC) are unable to process these keys from a Mac client's keyboard.

Fedora Notes

Resolving Fedora Core Focus

Using the Multi-Platform Client (MPC), occasionally there is an inability to log in to an LX, KX II or KSX II device, or to access KVM target servers (Windows®, SUSE, and so forth). In addition, the Ctrl+Alt+M key combination may not bring up the Keyboard Shortcut menu. This situation occurs with the following client configuration: Fedora® Core 6 and Firefox® 1.5 or 2.0.

Through testing, it has been determined that installation of libXp resolves window focusing issues with Fedora Core 6. Raritan has tested with libXp-1.0.0.8.i386.rpm; this resolved all of the keyboard focus and popup-menu problems.

Note: libXp is also required for the SeaMonkey (formerly Mozilla®) browser to work with the Java™ plug-in.

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target server running Fedora® 7, if the target and local mouse pointers lose synchronization, changing the mouse mode from or to Intelligent or Standard may improve synchronization. Single mouse mode may also provide for better control.

To resynchronize the mouse cursors:

- Use the Synchronize Mouse option from the Virtual KVM Client.

VKC and MPC Smart Card Connections to Fedora Servers

If you are using a smart card to connect to a Fedora® server via MPC or VKC upgrade the pcsc-lite library to 1.4.102-3 or above.

Note: This feature is available on the KSX II 2.3.0 (and later) and KX II 2.1.10 (and later).

Resolving Issues with Firefox Freezing when Using Fedora

If you are accessing Firefox® and are using a Fedora® server, Firefox may freeze when it is opening. To resolve this issue, install the libnpjp2.so Java™ plug-in on the server.

Video Mode and Resolution Notes

SUSE/VESA Video Modes

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

To configure the SUSE video display:

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

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

Supported Video Resolutions Not Displaying

When using a CIM, there are some video resolutions, as listed in Supported Video Resolutions, that may not be available to you for selection by default.

To view all available video resolutions if they do not appear:

1. Plug the monitor in.
2. Next, unplug the monitor and plug in the CIM. All video resolutions will not be available and can be used.

Audio Notes

Note: This feature is available with the KX II 2.4.0 (and later).

Number of Supported Audio/Virtual Media and Smartcard Connections

Following are the number of simultaneous Audio/Virtual Media and Smartcard connections that can be made from a client to a target:

- 1 smartcard
- 1 virtual media
- 1 Smartcard and 1 virtual media
- 2 virtual media

Audio Playback and Capture Issues

Features that May Interrupt an Audio Connection

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

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

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

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

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

Note: This feature is available with the KX II 2.4.0 (and later).

Audio in a Linux Environment

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

- Linux® users, use the default audio device for playback. Sound may not come through if a non-default sound card is selected.
- SuSE 11 clients require Javas_1_6_0-sun-alsa (ALSA support for java-1_6_0-sun) to be installed via YAST.
- For Logitech headsets with a built in a mic, only the Mono Capture option is available.
- If you are running SUSE 11 and using an ALSA driver, log out of KX II and then log back in in order to display the device. Additionally, if you connect and disconnect the audio device a number of times, the device may be listed several times vs. just once as it should.
- Using the audio feature with a Fedora Core 13 target set to mono 16 bit, 44k may cause considerable interference during playback.

Note: This feature is available with the KX II 2.4.0 (and later).

Audio in a Mac Environment

Following are known issues in a Mac® environment.

- On Mac clients, only one playback device is listed on the Connect Audio panel when accessing the device through the Virtual KVM Client (VKC) and Multi-Platform Client (MPC). The device listed is the default and is displayed on the Connect Audio panel as Java Sound Audio Engine.
- Using audio on a Mac target through Skype® may cause the audio to be corrupted.

Note: This feature is available with the KX II 2.4.0 (and later).

Audio in a Windows Environment

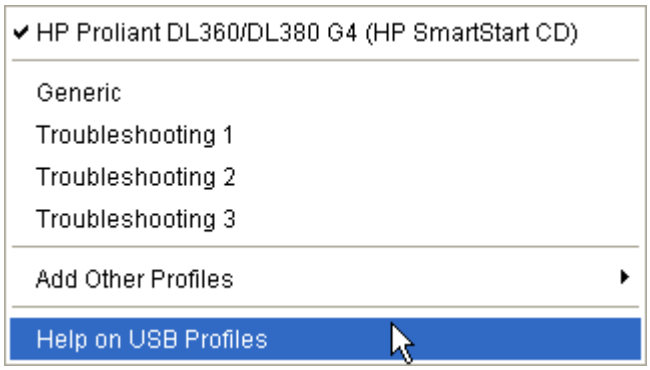
On Windows® 64-bit clients, only one playback device is listed on the Connect Audio panel when accessing the device through the Virtual KVM Client (VKC) and Multi-Platform Client (MPC). The audio device is the default device and is listed on the Connect Audio panel as Java Sound Audio Engine.

Note: This feature is available with the KX II 2.4.0 (and later).

USB Port and Profile Notes-kxii,ksxii,kvm,lx

Help Choosing USB Profiles

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



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

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®, Mac OS X®).

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

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

The USB Profile Menu selections are configurable via the Console Device Settings > Port Configuration page.

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

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

Changing a USB Profile when Using a Smart Card Reader

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

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

Virtual Media Notes

Virtual Media via VKC and AKC in a Windows Environment

Windows XP® operating system administrator and standard user privileges vary from those of the Windows Vista® operating system and the Windows 7® operating system.

When enabled in Vista or Windows 7, User Access Control (UAC) provides the lowest level of rights and privileges a user needs for an application. For example, a Run as Administrator option is provided for Internet Explorer® for Administrator level tasks; otherwise these are not be accessible even though the user has an Administrator login.

Both of these features affect the types of virtual media that can be accessed by users via Virtual KVM Client (VKC) and Active KVM Client (AKC). See your Microsoft® help for additional information on these features and how to use them.

Following is a list virtual media types users can access via VKC and AKC when running in a Windows environment. The features are broken down by client and the virtual media features that are accessible to each Windows user role.

Windows XP

If you are running VKC and AKC in a Windows XP environment, users must have Administrator privileges to access any virtual media type other than CD-ROM connections, ISOs and ISO images.

Windows Vista and Windows 7

If you are running VKC and AKC in a Windows Vista or Windows 7 environment and UAC is enabled, the following virtual media types can be accessed depending on the user's Windows role:

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

Virtual Media Not Refreshed After Files Added

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

Virtual Media Linux Drive Listed Twice

For KX II 2.4.0 (and later) and LX 2.4.5 (and later), users who are logged in to Linux™ clients as root users, the drives are listed twice in the Local Drive drop-down. For example, you will see eg /dev/sdc and eg /dev/sdc1 where the first drive is the boot sector and the second drive is the first partition on the disk.

Accessing Virtual Media on a Windows 2000

A virtual media local drive cannot be accessed on a Windows 2000® server using a D2CIM-VUSB.

Disconnecting Mac and Linux Virtual Media USB Drives

In a Linux® or Mac® environment:

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

Target BIOS Boot Time with Virtual Media

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

To shorten the boot time:

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

Virtual Media Connection Failures Using High Speed for Virtual Media Connections

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

CIM Notes

Windows 3-Button Mouse on Linux Targets

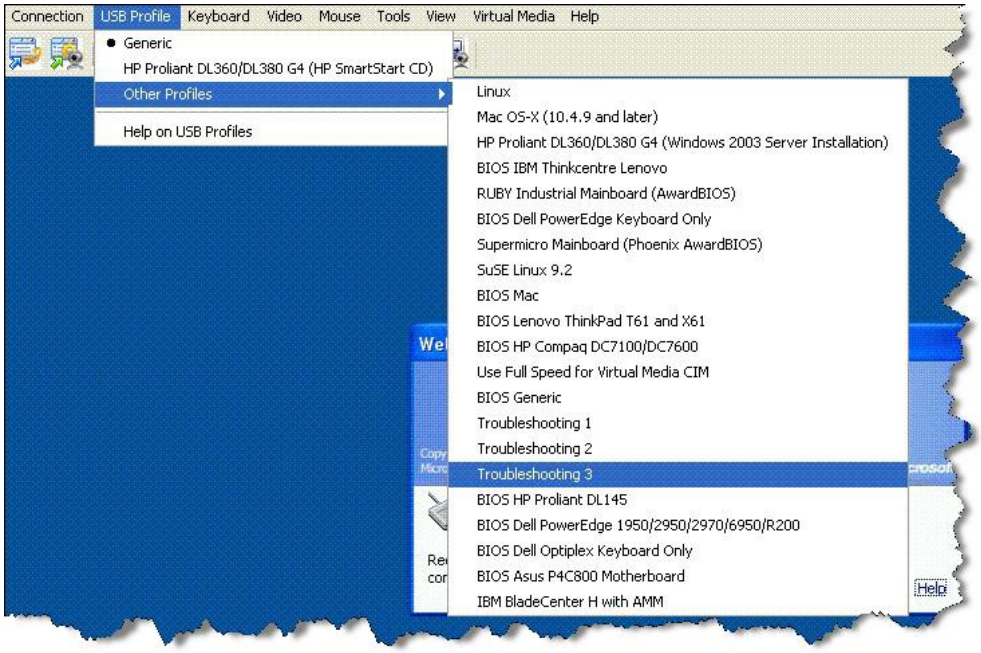
When using a 3-button mouse on a Windows® client connecting to a Linux® target, the left mouse button may get mapped to the center button of the Windows client 3-button mouse.

Windows 2000 Composite USB Device Behavior for Virtual Media

The Windows 2000® operating system does not support USB composite devices, like Raritan's D2CIM-VUSB, in the same manner as non-composite USB devices.

As a result, the "Safely Remove Hardware" system tray icon does not appear for drives mapped by the D2CIM-VUSB and a warning message may appear when disconnecting the device. Raritan has not observed any problems or issues from this message, however.

Raritan's US engineering department has developed a configuration which supports the "Safely Remove Hardware" icon and avoids this Windows message. This configuration requires the use of the D2CIM-DVUSB virtual media adapter and the Troubleshooting 3 USB Profile, which configures the D2CIM-DVUSB as a non-composite USB device supporting a single virtual media connection. Raritan has successfully tested this configuration in the US and Japan.



CC-SG Notes

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

When the Virtual KVM Client is launched from CommandCenter Secure Gateway (CC-SG) in proxy mode, the Virtual KVM Client version is unknown. In the About Raritan Virtual KVM Client dialog, the version is displayed as "Version Unknown".

Single Mouse Mode - Connecting to a Target Under

When using Firefox® to connect to a KX II or KSX II target under CC-SG control using DCIM-PS2 or DCIM-USBG2, if you change to Single Mouse Mode in the Virtual KVM Client, the VKC window will no longer be the focus window and the mouse will not respond. If this occurs, left click on the mouse or press Alt+Tab to return the focus to the VKC window.

Proxy Mode and MPC

If you are using KX II in a CC-SG configuration, do not use the CC-SG proxy mode if you are planning to use the Multi-Platform Client (MPC).

Moving Between Ports on a Device

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

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5991
Email: support.japan@raritan.com

Europe

Europe
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom
Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany
Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com