



Dominion LX

User Guide
Release 2.4.5

Copyright © 2011 Raritan, Inc.

LX-v2.4.5-0A-E

October 2011

255-80-8009-00

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2011 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

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.



Rack Mount Safety Guidelines

In Raritan products which require Rack Mounting, please follow these precautions:

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

Contents

Chapter 1 Introduction	1
LX Overview.....	2
LX Photos	4
Package Contents.....	7
LX Client Applications.....	7
Hardware	8
Software.....	9
LX Help	9
Related Documentation	10
Terminology	10
Chapter 2 Installation and Configuration	12
Overview	12
Default Login Information.....	12
Getting Started.....	13
Step 1: Configure the KVM Target Servers.....	13
Step 2: Configure Network Firewall Settings.....	26
Step 3: Connect the Equipment.....	27
Step 4: Configure the LX	29
Valid Special Characters for Target Names	33
Step 5: Launch the LX Remote Console	34
Step 6: Configure the Keyboard Language (Optional)	35
Step 7: Configure Tiering (Optional).....	36
Chapter 3 Working with Target Servers	37
LX Interfaces.....	37
LX Local Console Interface: LX Devices	38
LX Remote Console Interface.....	38
Launching the LX Remote Console.....	38
Interface and Navigation.....	40
Scanning Ports	45
Managing Favorites	48
Logging Out	51
Proxy Server Configuration for Use with MPC, VKC and AKC.....	51
Virtual KVM Client (VKC) and Active KVM Client (AKC)	53
About the Virtual KVM Client	53
About the Active KVM Client	53
Toolbar.....	55
Connection Properties	57
Connection Information	59

Keyboard Options.....	59
Video Properties.....	65
Mouse Options.....	70
Tool Options.....	75
View Options.....	78
Help Options.....	80
Multi-Platform Client (MPC).....	80
Launching MPC from a Web Browser.....	80

Chapter 4 Virtual Media 82

Overview.....	83
Prerequisites for Using Virtual Media.....	85
Virtual Media in a Linux Environment.....	86
Conditions when Read/Write is Not Available.....	88
Using Virtual Media.....	88
Virtual Media File Server Setup (File Server ISO Images Only).....	89
Connecting to Virtual Media.....	90
Disconnecting Virtual Media.....	93

Chapter 5 User Management 94

User Groups.....	94
User Group List.....	95
Relationship Between Users and Groups.....	95
Adding a New User Group.....	95
Modifying and Existing User Group.....	99
Users.....	99
User List.....	100
Adding a New User.....	100
Modifying an Existing User.....	101
Logging a User Off (Force Logoff).....	101
Authentication Settings.....	102
Implementing LDAP/LDAPS Remote Authentication.....	103
Returning User Group Information from Active Directory Server.....	107
Implementing RADIUS Remote Authentication.....	108
Returning User Group Information via RADIUS.....	111
RADIUS Communication Exchange Specifications.....	111
User Authentication Process.....	113
Changing a Password.....	114

Chapter 6 Device Management 115

Network Settings.....	115
Network Basic Settings.....	116
LAN Interface Settings.....	118
Device Services.....	119
Enabling SSH.....	119
HTTP and HTTPS Port Settings.....	120
Entering the Discovery Port.....	120

Configuring and Enabling Tiering	121
Enabling Direct Port Access via URL	124
Enabling the AKC Download Server Certificate Validation	125
Configuring Modem Settings	126
Configuring Date/Time Settings	127
Event Management.....	128
Configuring Event Management - Settings.....	129
Configuring Ports	131
Configuring Standard Target Servers.....	132
Configuring KVM Switches	132
Configuring LX Local Port Settings.....	134
Changing the Default GUI Language Setting	136

Chapter 7 Security Management **138**

Security Settings	138
Login Limitations.....	139
Strong Passwords	140
User Blocking.....	142
Encryption & Share.....	144
SSL Certificates	147

Chapter 8 Maintenance **149**

Audit Log.....	149
Device Information	150
Backup and Restore	151
Upgrading CIMs	153
Upgrading Firmware	153
Upgrade History	155
Rebooting the LX	155

Chapter 9 Diagnostics **157**

Network Interface Page	157
Network Statistics Page.....	158
Ping Host Page	160
Trace Route to Host Page	160
Device Diagnostics	161

Chapter 10 Command Line Interface (CLI) **163**

Overview	163
Accessing the LX Using CLI	164
SSH Connection to the LX.....	164
SSH Access from a Windows PC.....	164
SSH Access from a UNIX/Linux Workstation	164

Contents

Logging In	165
Navigation of the CLI	165
Completion of Commands	165
CLI Syntax -Tips and Shortcuts.....	166
Common Commands for All Command Line Interface Levels	166
Initial Configuration Using CLI	167
Setting Parameters	167
Setting Network Parameters.....	167
CLI Prompts	168
CLI Commands	168
Security Issues	169
Administering the LX Console Server Configuration Commands.....	169
Configuring Network	169
Interface Command	170
Name Command	171
IPv6 Command.....	171

Chapter 11 LX Local Console **172**

Overview	172
Simultaneous Users.....	172
LX Local Console Interface: LX Devices	173
Security and Authentication	173
Supported Video Resolutions - Local Console	174
Port Access Page (Local Console Server Display)	174
Accessing a Target Server	175
Scanning Ports - Local Console	176
Using Scan Options	177
Hot Keys and Connect Keys.....	177
Connect Key Examples	178
Special Sun Key Combinations	178
Returning to the LX Local Console Interface	179
Local Port Administration.....	179
Configuring LX Local Console Local Port Settings.....	180
LX Local Console Factory Reset.....	182
Resetting the LX Using the Reset Button	183

Appendix A Specifications **184**

LX Specifications	184
LED Indicators	186
Supported Operating Systems (Clients)	186
Supported Browsers	187
Supported CIMS and Operating Systems.....	188
Supported Video Resolutions	189
Target Server Connection Distance and Video Resolution.....	190

Certified Modems.....	190
Remote Connection	190
Supported Keyboard Languages	191
TCP and UDP Ports Used	193
Events Captured in the Audit Log and Syslog	194
Network Speed Settings	195

Appendix B Updating the LDAP Schema 197

Returning User Group Information.....	197
From LDAP/LDAPS	197
From Microsoft Active Directory	197
Setting the Registry to Permit Write Operations to the Schema	198
Creating a New Attribute.....	198
Adding Attributes to the Class	199
Updating the Schema Cache.....	201
Editing rcigroup Attributes for User Members.....	201

Appendix C Informational Notes 205

Overview	205
Java Runtime Environment (JRE)	205
IPv6 Support Notes.....	206
Keyboards.....	207
Non-US Keyboards.....	207
Macintosh Keyboard.....	209
Fedora.....	210
Resolving Fedora Core Focus.....	210
Mouse Pointer Synchronization (Fedora).....	210
Resolving Issues with Firefox Freezing when Using Fedora	210
Video Modes and Resolutions	211
SUSE/VESA Video Modes	211
Supported Video Resolutions Not Displaying.....	211
VM-CIMs and DL360 USB Ports	211
MCUTP	212
Virtual Media.....	213
Virtual Media via VKC and AKC in a Windows Environment	213
Virtual Media Not Refreshed After Files Added.....	214
Active System Partitions.....	214
Drive Partitions	214
Virtual Media Linux Drive Listed Twice	215
Mac and Linux Locked, Mapped Drives	215
Accessing Virtual Media on a Windows 2000 Server Using a D2CIM-VUSB	215
Target BIOS Boot Time with Virtual Media.....	215
Virtual Media Connection Failures Using High Speed for Virtual Media Connections....	215
CIMs.....	215
Windows 3-Button Mouse on Linux Targets.....	215
Windows 2000 Composite USB Device Behavior for Virtual Media.....	216
MCUTP CIM Behavior	216

Appendix D Frequently Asked Questions	217
Chapter 12 LX FAQs.....	218
Index	223

Chapter 1 Introduction

In This Chapter

LX Overview	2
LX Photos	4
Package Contents	7
LX Client Applications.....	7
Hardware	8
Software.....	9
LX Help.....	9

LX Overview

The LX® KVM-over-IP switches give one to two remote users, with an independent local port, BIOS-level access and control of up to 16 servers. When implementing tiering functionality, users can easily control up to 256 computers from a single console. These appliances, specifically designed for small to midsize businesses (SMBs), offer economical, remote access from anywhere, efficient reliable server management, and a minimum initial investment that provides affordable scalability.

The LX comes standard with Raritan's Universal Virtual Media™, providing the widest variety of CD, DVD, USB, internal and remote drives that can be mounted locally, enabling remote management tasks and eliminating the need to travel. For a clear, crisp view, the modern architecture platform supports high definition (HD) 1920x1080 remote video resolution and a common, modern, browser-based GUI for both local and remote access, requires little training, provides at-the-rack productivity, and ensures efficient use of all IT resources. Servers can be accessed from Windows®, Linux®, Sun® or Macintosh® through the leading browsers or stand-alone, with no client license fees.

With cabling bundles options, SMB IT staff can minimize their initial investment today while preserving the option for added functionality tomorrow.

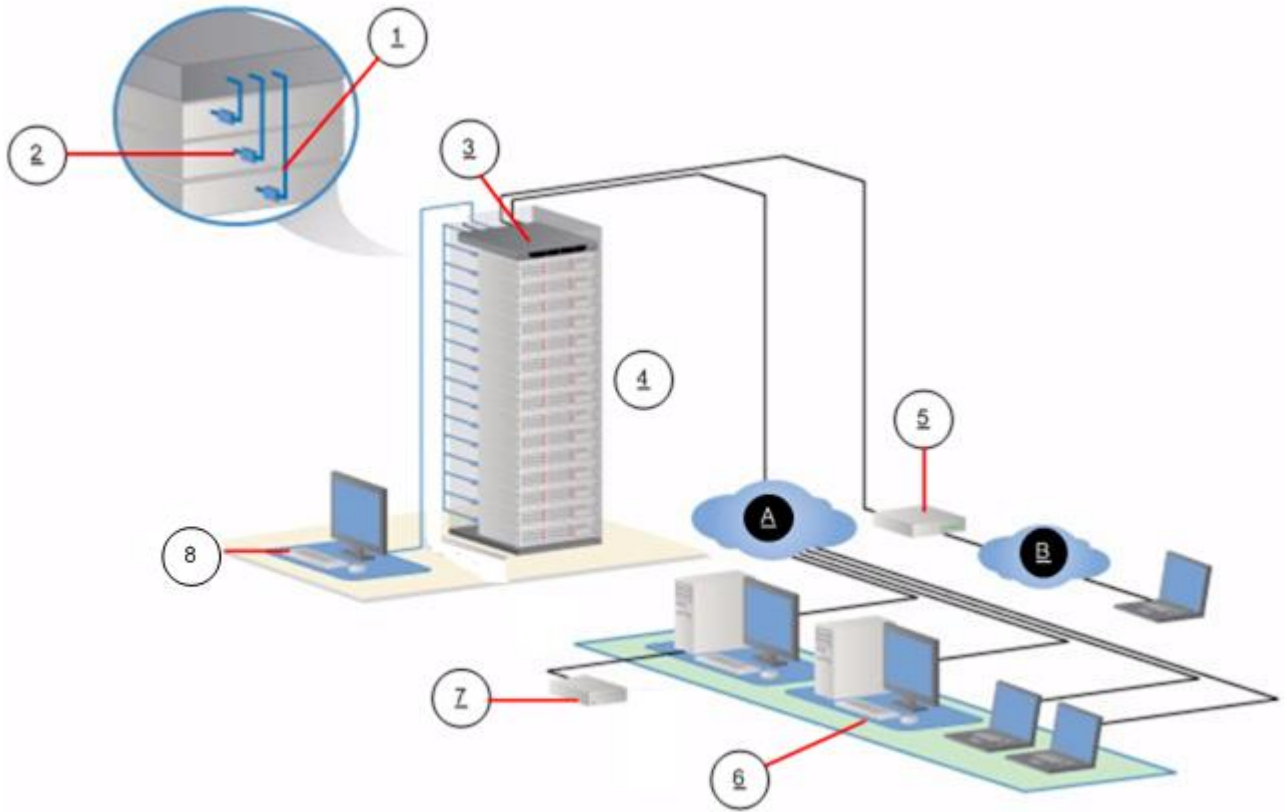


Diagram key			
1	Cat5 cable	6	Remote (network) access
2	Computer Interface Module (CIM)	7	Local access
3	LX	A	IP LAN/WAN
4	Remote KVM and serial devices	B	PSTN
5	Modem		

LX Photos



LX 108



LX 116



LX 216



Package Contents

Each LX ships as a fully-configured stand-alone product in a standard 1U 19" rackmount chassis. Each LX device ships with the following contents:

Amount included	Item
1	LX device
1	Rackmount kit
1	AC power cord
1	LX Quick Setup Guide
1	Application note
1	Warranty card

LX Client Applications

The following client applications can be used in the LX:

Product	Works with...				
	MPC	RRC	VKC	RSC	AKC
LX 2.4.5 (or later)	✓	■	✓	■	✓

See the **KVM and Serial Client Guide** for additional information on the client applications. Also see the **Working with Target Servers** (on page 37) section of this guide, which contains information on using the clients with the LX.

Note: MPC and VKC require the Java™ Runtime Environment (JRE™). AKC is .NET based.

Hardware

- Integrated KVM-over-IP remote access
- 8 and 16 server port models
- Up to 2 video channels that allows up to 2 users to connect to the LX at once
- Multiple user capacity (1/2 remote users; 1 local user)
- UTP (Cat5/5e/6) server cabling
- Ethernet port (10/100/1000 LAN)
- Field upgradable
- Local user port for in-rack access
 - Three back panel USB 2.0 ports for supported USB devices
 - Fully concurrent with remote user access
 - Local graphical user interface (GUI) for administration
- Modem support
- Front and rear LED indicators for the device status, boot-up and firmware upgrades
- Hardware Reset button
- Serial port to connect to an external modem
- 19" rack-mountable (brackets included)

Software

- Virtual media support in Windows®, Mac® and Linux® environments with D2CIM-VUSB and D2CIM-DVUSB CIMs
- Port scanning and thumbnail view of targets within a configurable scan set
- Absolute Mouse Synchronization with D2CIM-VUSB CIM and D2CIM-DVUSB CIMs
- Plug-and-Play
- Web-based access and management
- Intuitive graphical user interface (GUI)
- 256-bit encryption of complete KVM signal, including video and virtual media
- LDAP, Active Directory®, RADIUS, or internal authentication and authorization
- DHCP or fixed IP addressing
- SNMP and Syslog management
- IPv4 and IPv6 support
- LX and generic tiering

LX Help

The LX help provides information on how to install, set up, and configure the LX. It also includes information on accessing target servers, using virtual media, managing users and security, and maintaining and diagnosing the LX.

See the LX release notes for important information on the current release before you begin using the LX.

A PDF version of the help can be downloaded from the Raritan **Firmware and Documentation** page on the Raritan website. Raritan recommends that you refer to the Raritan website for the most up-to-date user guides available.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriptlets. Consult your browser help for information on enabling these features.

Related Documentation

The LX help is accompanied by the LX Quick Setup Guide, which can be found on the Raritan **Firmware and Documentation** page of **Raritan's website** (<http://www.raritan.com/support/firmware-and-documentation>).

Installation requirements and instructions for client applications used with the LX can be found in the **KVM and Serial Access Clients Guide**, also found on the Raritan website. Where applicable, specific client functions used with the LX are included in the help.

Terminology

Help uses the following terminology for typical LX components:

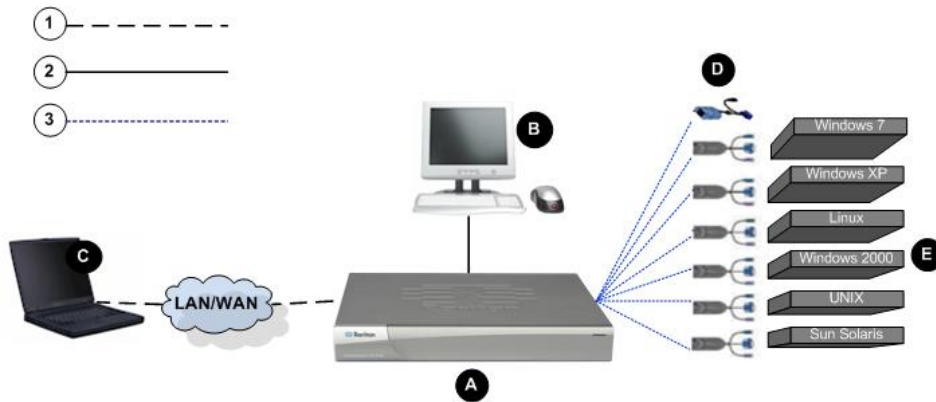


Diagram Key	
1	TCP/IP IPv4 and/or IPv6 added
2	KVM (Keyboard, Video, Mouse)
3	UTP Cable (Cat5/5e/6)
A	LX
B	Local Access Console Local User - an optional user console (consisting of a keyboard, mouse, and multi-sync VGA monitor) attached directly to the LX to control KVM target servers (directly at the rack, not through the network).
C	Remote PC Networked computers used to access and control KVM target servers connected to the LX.
D	CIMS Dongles that connect to each target server. Available for all of the supported operating systems.
E	Target Servers KVM Target Servers - servers with video cards and user interfaces (for example, Windows® operating system®, Linux®, Solaris™, etc.) accessed remotely via the LX.

See Supported CIMS and Operating Systems - LX for a list of the supported operating systems and CIMS.

Chapter 2 Installation and Configuration

In This Chapter

Overview12
Default Login Information12
Getting Started13

Overview

This section provides a brief overview of the installation process. Each step is further detailed in the remaining sections of this chapter.

- ▶ **To install and configure the LX:**
 - **Step 1: Configure the KVM Target Servers** (on page 13)
 - **Step 2: Configure Network Firewall Settings** (on page 26)
 - **Step 3: Connect the Equipment** (on page 27)
 - **Step 4: Configure the LX** (on page 29)
 - **Step 5: Launch the LX Remote Console** (on page 34)
 - **Step 6: Configure the Keyboard Language (Optional)** (on page 35)
 - **Step 7: Configure Tiering (Optional)** (on page 36)

Also included in this section is the default login information you will need. Specifically, the default IP address, user name and password. See **Default Login Information** (on page 12).

Default Login Information

Default	Value
User name	The default user name is admin. This user has administrative privileges.
Password	The default password is raritan. Passwords are case sensitive and must be entered in the exact case combination in which they were created. For example, the default password raritan must be entered entirely in lowercase letters. The first time you start the LX, you are required to change the default password.
IP address	The LX ships with the default IP address of 192.168.0.192.

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

Getting Started

Step 1: Configure the KVM Target Servers

KVM target servers are the computers that are accessed and controlled via the LX. Before installing the LX, configure all KVM target servers to ensure optimum performance. This configuration applies only to KVM target servers, not to the client workstations (remote PCs) used to access the LX remotely.

Desktop Background

For optimal bandwidth efficiency and video performance, use solid color backgrounds whenever possible. Backgrounds featuring photos or complex gradients might degrade performance.

Supported Video Resolutions

Ensure that each target server's video resolution and refresh rate are supported by the LX and that the signal is noninterlaced.

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. See **Target Server Connection Distance and Video Resolution** (on page 190).

The LX supports these resolutions:

Resolutions	
640x350 @70Hz	1024x768@85
640x350 @85Hz	1024x768 @75Hz
640x400 @56Hz	1024x768 @90Hz
640x400 @84Hz	1024x768 @100Hz
640x400 @85Hz	1152x864 @60Hz
640x480 @60Hz	1152x864 @70Hz
640x480 @66.6Hz	1152x864 @75Hz

Resolutions	
640x480 @72Hz	1152x864 @85Hz
640x480 @75Hz	1152x870 @75.1Hz
640x480 @85Hz	1152x900 @66Hz
720x400 @70Hz	1152x900 @76Hz
720x400 @84Hz	1280x720@60Hz
720x400 @85Hz	1280x960 @60Hz
800x600 @56Hz	1280x960 @85Hz
800x600 @60Hz	1280x1024 @60Hz
800x600 @70Hz	1280x1024 @75Hz
800x600 @72Hz	1280x1024 @85Hz
800x600 @75Hz	1360x768@60Hz
800x600 @85Hz	1366x768@60Hz
800x600 @90Hz	1368x768@60Hz
800x600 @100Hz	1400x1050@60Hz
832x624 @75.1Hz	1440x900@60Hz
1024x768 @60Hz	1600x1200 @60Hz
1024x768@70	1680x1050@60Hz
1024x768@72	1920x1080@60Hz

Mouse Modes

The LX operates in Absolute Mouse Mode™, Intelligent Mouse Mode and Standard Mouse Mode.

Mouse parameters do not have to be altered for Absolute Mouse Synchronization but a D2CIM-VUSB or D2CIM-DVUSB is required. For both the Standard and Intelligent Mouse Modes, mouse parameters must be set to specific values. Mouse configurations vary on different target operating systems. Consult your operating system documentation for additional details.

Intelligent Mouse Mode works well on most Windows platforms but may produce unpredictable results when Active Desktop is set on the target. Do not use an animated mouse for Intelligent Mouse Mode.

Windows XP, Windows 2003 and Windows 2008 Settings

► **To configure KVM target servers running Microsoft® Windows XP® operating system, Windows 2003® operating system or Windows 2008® operating systems:**

1. Configure the mouse settings:
 - a. Choose Start > Control Panel > Mouse.
 - b. Click the Pointer Options tab.
 - c. In the Motion group:
 - Set the mouse motion speed setting to exactly the middle speed.
 - Disable the "Enhance pointer precision" option.
 - Disable the Snap To option.
 - Click OK.

Note: When you are running Windows 2003 on your target server, if you access the server via KVM and perform any one off the actions listed below, mouse synchronization may be lost if it has been previously enabled. You will need to select the Synchronize Mouse command from the Mouse menu in the client to enable it again. Following are the actions that may cause this to occur:

- Opening a text editor.

- Accessing the Mouse Properties, Keyboard Properties, and Phone and Modem Properties from the Windows Control Panel.

2. Disable transition effects:
 - a. Select the Display option from the Control Panel.
 - b. Click the Appearance tab.
 - c. Click Effects.
 - d. Deselect the "Use the following transition effect for menus and tooltips" option.
 - e. Click OK.
3. Close the Control Panel.

Note: For KVM target servers running Windows XP, Windows 2000 or Windows 2008, you may wish to create a user name that will be used only for remote connections through the LX. This will enable you to keep the target server's slow mouse pointer motion/acceleration settings exclusive to the LX connection.

Windows XP, 2000, and 2008 login pages revert to preset mouse parameters that differ from those suggested for optimal LX performance. As a result, mouse synchronization may not be optimal for these screens.

Note: Proceed only if you are comfortable adjusting the registry on Windows KVM target servers. You can obtain better LX mouse synchronization at the login pages by using the Windows registry editor to change the following settings: HKey_USERS\DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Windows 7 and Windows Vista Settings

► **To configure KVM target servers running Windows Vista® operating system:**

1. Configure the mouse settings:
 - a. Choose Start > Settings > Control Panel > Mouse.
 - b. Select "Advanced system settings" from the left navigation panel. The System Properties dialog opens.
 - c. Click the Pointer Options tab.
 - d. In the Motion group:
 - Set the mouse motion speed setting to exactly the middle speed.
 - Disable the "Enhanced pointer precision" option.
 - Click OK.
2. Disable animation and fade effects:
 - a. Select the System option from the Control Panel.
 - b. Select Performance Information then Tools > Advanced Tools > Adjust to adjust the appearance and performance of Windows.
 - c. Click the Advanced tab.
 - d. Click Settings in the Performance group to open the Performance Options dialog.
 - e. Under Custom options, deselect the following checkboxes:
 - Animation options:

- Animate controls and elements inside windows
 - Animate windows when minimizing and maximizing
 - Fade options:
 - Fade or slide menus into view
 - Fade or slide ToolTips into view
 - Fade out menu items after clicking
3. Click OK and Close the Control Panel.

► **To configure KVM target servers running Windows 7® operating system:**

1. Configure the mouse settings:
 - a. Choose Start > Control Panel > Hardware and Sound > Mouse.
 - b. Click the Pointer Options tab.
 - c. In the Motion group:
 - Set the mouse motion speed setting to exactly the middle speed.
 - Disable the "Enhanced pointer precision" option.
 - Click OK.
2. Disable animation and fade effects:
 - a. Select Control Panel > System and Security.
 - b. Select System and then select "Advanced system settings" from the left navigation panel. The System Properties dialog appears.
 - c. Click the Advanced tab.
 - d. Click the Settings button in the Performance group to open the Performance Options dialog.
 - e. Under Custom options, deselect the following checkboxes:
 - Animation options:
 - Animate controls and elements inside windows
 - Animate windows when minimizing and maximizing
 - Fade options:
 - Fade or slide menus into view
 - Fade or slide ToolTips into view
 - Fade out menu items after clicking
3. Click OK and Close the Control Panel.

Windows 2000 Settings

► **To configure KVM target servers running Microsoft® Windows 2000® operating system:**

1. Configure the mouse settings:
 - a. Choose Start > Control Panel > Mouse.
 - b. Click the Motion tab.
 - Set the acceleration to None.
 - Set the mouse motion speed setting to exactly the middle speed.
 - Click OK.
2. Disable transition effects:
 - a. Select the Display option from the Control Panel.
 - b. Click the Effects tab.
 - Deselect the "Use the following transition effect for menus and tooltips" option.
3. Click OK and close the Control Panel.

Note: For KVM target servers running Windows XP, Windows 2000 or Windows 2008, you may wish to create a user name that will be used only for remote connections through the LX. This will enable you to keep the target server's slow mouse pointer motion/acceleration settings exclusive to the LX connection.

Windows XP, 2000, and 2008 login pages revert to preset mouse parameters that differ from those suggested for optimal LX performance. As a result, mouse synchronization may not be optimal for these screens.

Note: Proceed only if you are comfortable adjusting the registry on Windows KVM target servers. You can obtain better LX mouse synchronization at the login pages by using the Windows registry editor to change the following settings: HKey_USERS\DEFAULT\Control Panel\Mouse: > MouseSpeed = 0; MouseThreshold 1=0; MouseThreshold 2=0.

Linux Settings (Red Hat 9)

Note: The following settings are optimized for Standard Mouse mode only.

► **To configure KVM target servers running Linux® (graphical user interface):**

1. Configure the mouse settings:

- a. Choose Main Menu > Preferences > Mouse. The Mouse Preferences dialog appears.
- b. Click the Motion tab.
- c. Within the Speed group, set the Acceleration slider to the exact center.
- d. Within the Speed group, set the Sensitivity towards low.
- e. Within the Drag & Drop group, set the Threshold towards small.
- f. Close the Mouse Preferences dialog.

Note: If these steps do not work, issue the `xset mouse 1 1` command as described in the Linux command line instructions.

2. Configure the screen resolution:
 - a. Choose Main Menu > System Settings > Display. The Display Settings dialog appears.
 - b. From the Display tab, select a Resolution supported by the LX.
 - c. From the Advanced tab, verify that the Refresh Rate is supported by the LX.

Note: Once connected to the target server, in many Linux graphical environments, the `<Ctrl> <Alt> <+>` command will change the video resolution, scrolling through all available resolutions that remain enabled in the `XF86Config` or `/etc/X11/xorg.conf`, depending on your X server distribution.

► **To configure KVM target servers running Linux (command line):**

1. Set the mouse acceleration to exactly 1 and set the threshold to exactly 1. Enter this command: `xset mouse 1 1`. This should be set for execution upon login.
2. Ensure that each target server running Linux is using a resolution supported by the LX at a standard VESA resolution and refresh rate.
3. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values:
 - a. Go to the Xfree86 Configuration file `XF86Config`.
 - b. Using a text editor, disable all non-LX supported resolutions.
 - c. Disable the virtual desktop feature (not supported by the LX).
 - d. Check blanking times (+/- 40% of VESA standard).
 - e. Restart computer.

Note: If you change the video resolution, you must log off of the target server and log back in for the video settings to take effect.

Note for Red Hat 9 KVM Target Servers

If you are running Red Hat® 9 on the target server using a USB CIM, and are experiencing problems with the keyboard and/or mouse, there is an additional configuration setting you can try.

Tip: You might have to perform these steps even after a fresh OS installation.

► **To configure Red Hat 9 servers using USB CIMs:**

1. Locate the configuration file (usually /etc/modules.conf) in your system.
2. Using the editor of your choice, make sure that the alias usb-controller line in the modules.conf file is as follows:

```
alias usb-controller usb-uhci
```

Note: If there is another line using usb-uhci in the /etc/modules.conf file, it needs to be removed or commented out.

3. Save the file.
4. Reboot the system in order for the changes to take effect.

Linux Settings (Red Hat 4)

Note: The following settings are optimized for Standard Mouse mode only.

► **To configure KVM target servers running Linux® (graphical user interface):**

1. Configure the mouse settings:
 - a. Red Hat 5 users, choose Main Menu > Preferences > Mouse. Red Hat 4 users, choose System > Preferences > Mouse. The Mouse Preferences dialog appears.
 - b. Click on the Motion tab.
 - c. Within the Speed group, set the Acceleration slider to the exact center.
 - d. Within the Speed group, set the Sensitivity towards low.
 - e. Within the Drag & Drop group, set the Threshold towards small.
 - f. Close the Mouse Preferences dialog.

Note: If these steps do not work, issue the `xset mouse 1 1` command as described in the Linux command line instructions.

2. Configure the screen resolution:
 - a. Choose Main Menu > System Settings > Display. The Display Settings dialog appears.
 - b. On the Settings tab, select a Resolution supported by the LX.
 - c. Click OK.

Note: Once connected to the target server, in many Linux graphical environments, the <Ctrl> <Alt> <+> command will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config or /etc/X11/xorg.conf, depending on your X server distribution

Note: If you change the video resolution, you must log out of the target server and log back in for the video settings to take effect.

SUSE Linux 10.1 Settings

Note: Do not attempt to synchronize the mouse at the SUSE Linux® login prompt. You must be connected to the target server to synchronize the mouse cursors.

► **To configure the mouse settings:**

1. Choose Desktop > Control Center. The Desktop Preferences dialog appears.
2. Click Mouse. The Mouse Preferences dialog appears.
3. Open the Motion tab.
4. Within the Speed group, set the Acceleration slider to the exact center position.
5. Within the Speed group, set the Sensitivity slider to low.
6. Within the Drag & Drop group, set the Threshold slider to small.
7. Click Close.

► **To configure the video:**

1. Choose Desktop Preferences > Graphics Card and Monitor. The Card and Monitor Properties dialog appears.
2. Verify that a Resolution and Refresh Rate is in use that is supported by the LX. See **Supported Video Resolutions** for more information.

Note: If you change the video resolution, you must log out of the target server and log back in for the video settings to take effect.

Make Linux Settings Permanent

Note: These steps may vary slightly depending on the specific version of Linux® in use.

► **To make your settings permanent in Linux (prompt):**

1. Choose System Menu > Preferences > Personal > Sessions.
2. Click the Session Options tab.
3. Select the "Prompt on log off" checkbox and click OK. This option prompts you to save your current session when you log out.
4. Upon logging out, select the "Save current setup" option from the dialog.
5. Click OK.

Tip: If you do not want to be prompted upon log out, follow these procedures instead.

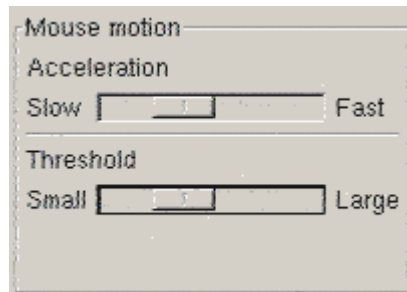
► **To make your settings permanent in Linux (no prompt):**

1. Choose Desktop > Control Center > System > Sessions.
2. Click the Session Options tab.
3. Deselect the "Prompt on the log off" checkbox.
4. Select the "Automatically save changes to the session" checkbox and click OK. This option automatically saves your current session when you log out.

Sun Solaris Settings

► **To configure KVM target servers running Sun™ Solaris™:**

1. Set the mouse acceleration value to exactly 1 and the threshold to exactly 1. This can be performed from:
 - The graphical user interface.



- The command line `xset mouse a t` where *a* is the acceleration and *t* is the threshold.

- All KVM target servers must be configured to one of the display resolutions supported by the LX. The most popular supported resolutions for Sun machines are:

Display resolution	Vertical refresh rate	Aspect ratio
1600 x 1200	60 Hz	4:3
1280 x 1024	60,75,85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60,70,75,85 Hz	4:3
800 x 600	56,60,72,75,85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60,72,75,85 Hz	4:3

- KVM target servers running the Solaris operating system must output VGA video (H-and-V sync, not composite sync).

► **To change your Sun video card output from composite sync to the nondefault VGA output:**

- Issue the `Stop+A` command to drop to bootprom mode.
- Issue the following command to change the output resolution: `setenv output-device screen:r1024x768x70`
- Issue the `boot` command to reboot the server.

You can also contact your Raritan representative to purchase a video output adapter:

If you have:	Use this video output adapter:
Sun 13W3 with composite sync output	APSSUN II Guardian converter
Sun HD15 with composite sync output	1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync
Sun HD15 with separate sync output	APKMSUN Guardian converter

Note: Some of the standard Sun background screens may not center precisely on certain Sun servers with dark borders. Use another background or place a light colored icon in the upper left hand corner.

Mouse Settings

► **To configure the mouse settings (Sun Solaris 10.1):**

- Choose Launcher. Application Manager - Desktop Controls opens.

2. Choose Mouse Style Manager. The Style Manager - Mouse dialog appears.
3. Set the Acceleration slider to 1.0.
4. Set the Threshold slider to 1.0.
5. Click OK.

Accessing the Command Line

1. Right click.
2. Choose Tools > Terminal. A terminal window opens. (It is best to be at the root to issue commands.)

Video Settings (POST)

Sun systems have two different resolution settings: a POST resolution and a GUI resolution. Run these commands from the command line.

Note: 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using.

► To check current POST resolution:

- Run the following command as the root: `# eeprom output-device`

► To change POST resolution:

1. Run `# eeprom output-device=screen:r1024x768x75.`
2. Log out or restart computer.

Video Settings (GUI)

The GUI resolution can be checked and set using different commands depending on the video card in use. Run these commands from the command line.

Note: 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using.

Card	To check resolution:	To change resolution:
32-bit	# /usr/sbin/pgxconfig -prconf	<ol style="list-style-type: none"> # /usr/sbin/pgxconfig -res 1024x768x75 Log out or restart computer.
64-bit	# /usr/sbin/m64config -prconf	<ol style="list-style-type: none"> # /usr/sbin/m64config -res 1024x768x75 Log out or restart computer.
32-bit and 64-bit	# /usr/sbin/fbconfig -prconf	<ol style="list-style-type: none"> # /usr/sbin/fbconfig -res 1024x768x75 Log out or restart computer.

IBM AIX 5.3 Settings

Follow these steps to configure KVM target servers running IBM® AIX™ 5.3.

► **To configure the mouse:**

1. Go to Launcher.
2. Choose Style Manager.
3. Click Mouse. The Style Manager - Mouse dialog appears.
4. Use the sliders to set the Mouse acceleration to 1.0 and Threshold to 1.0.
5. Click OK.

► **To configure the video:**

1. From the Launcher, select Application Manager.
2. Select System_Admin.
3. Choose Smit > Devices > Graphic Displays > Select the Display Resolution and Refresh Rate.
4. Select the video card in use.
5. Click List. A list of display modes is presented.
6. Select a resolution and refresh rate supported by the LX. See Supported Video Resolutions for more information.

Note: If you change the video resolution, you must log out of the target server and log back in for the video settings to take effect.

Make UNIX Settings Permanent

Note: These steps may vary slightly depending on the type of UNIX® (for example, Solaris™, IBM® AIX™) and the specific version in use.

1. Choose Style Manager > Startup. The Style Manager - Startup dialog appears.
2. On the Logout Confirmation dialog, select the On option. This option prompts you to save your current session when you log out.

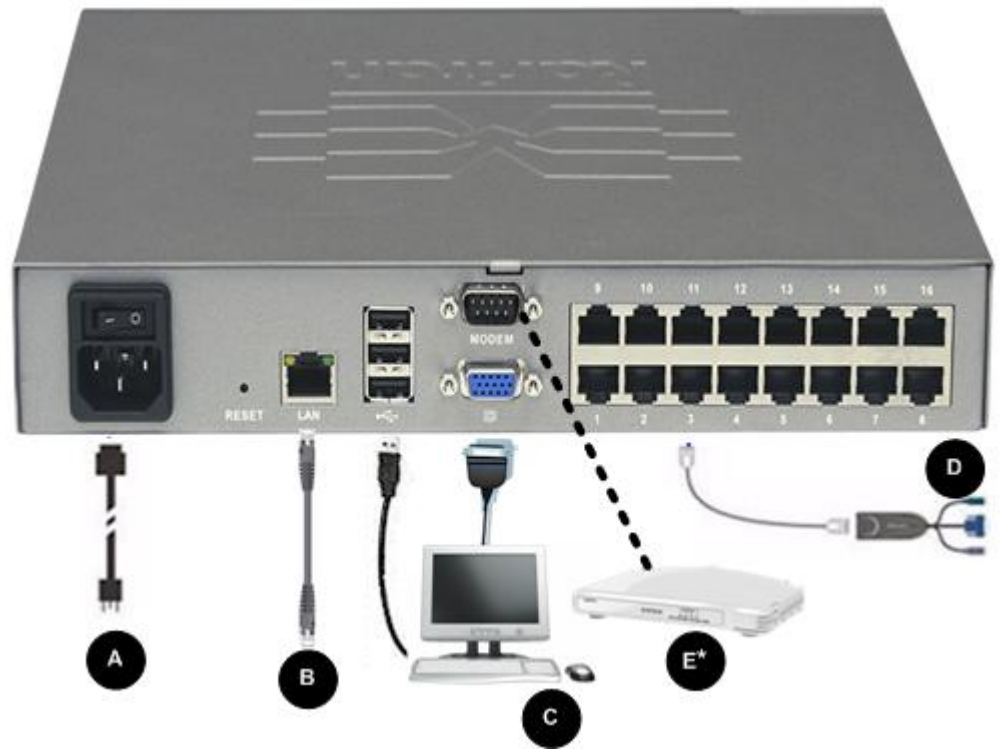
Apple Macintosh Settings

For KVM target servers running an Apple Macintosh® operating system, the preferred method is to use the D2CIM-VUSB and Absolute Mouse Synchronization.

Step 2: Configure Network Firewall Settings

To enable remote access to the LX, your network and firewall must allow communication on TCP Port 5000. Alternatively, configure the LX to use a different TCP port, then allow communication on that port. To access the LX via a web browser, your firewall must allow access to TCP Port 443 (Standard HTTPS). Access to TCP Port 80 (Standard HTTP) enables automatic redirection of HTTP requests to HTTPS.

Step 3: Connect the Equipment



A. AC Power

► **To connect the power supply:**

- Attach the included AC power cord to the LX and plug it into an AC power outlet.

B. Network Port

► **To connect the network:**

- Connect a standard Ethernet cable (included) from the network port to an Ethernet switch, hub, or router.

C. Local Access Port (Local PC)

For convenient access to target servers while at the rack, use the LX Local Access port. While the Local Access port is required for installation and setup, it is optional for subsequent use. The Local Access port also provides a graphical user interface from the LX Local Console for administration and target server access. See Configuring LX Local Port Settings for additional information.

► **To connect the local port:**

- Attach a multi-sync VGA monitor, mouse and keyboard to the respective Local User ports using a USB keyboard and mouse. The port connections are located on the back panel of the LX.

Connection	Description
Monitor	Attach a standard multi-sync VGA monitor to the HD15 (female) video port.
Keyboard	Attach a standard USB keyboard to one of the USB Type A (female) ports.
Mouse	Attach a standard USB mouse to one of the USB Type A (female) ports.

D. Target Server Ports

For convenient access to target servers while at the rack, use the LX Local Access port. While the Local Access port is required for installation and setup, it is optional for subsequent use. The Local Access port also provides a graphical user interface from the LX Local Console for administration and target server access. See Configuring LX Local Port Settings for additional information.

► **To connect a target server to the LX:**

1. Use the appropriate Computer Interface Module (CIM). See **Supported Operating Systems (Clients)** (on page 186) for information on compatible CIMS.
2. Attach the UTP (Cat5/5e/6) cable of your CIM to the video port of your target server. Ensure that your target server's video has already been configured to a supported resolution and refresh rate. For Sun servers, ensure that your target server's video card is set to output standard VGA (H-and-V sync) and not composite sync.

3. Attach the keyboard/mouse connector of your CIM to the corresponding ports on your target server. Using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an available server port on the back of your LX device.

Note: The DCIM-USB G2 provides a small slide switch on the back of the CIM. Move the switch to P for PC-based USB target servers. Move the switch to S for Sun USB target servers.

A new switch position takes effect only after the CIM is power-cycled. To power-cycle the CIM, remove the USB connector from the target server and plug it back in a few seconds later.

E. Modem Port (Optional)

The LX features a dedicated modem port for remote access even when the LAN/WAN is unavailable. Using a straight-through serial (RS-232) cable, connect an external serial modem to the port labeled MODEM on the back of the LX. See **Specifications** (on page 184) for a list of certified modems and **Configuring Modem Settings** (on page 126) for information on configuring the modem.

Note: Raritan recommends configuring the modem by enabling the CD (carrier detect) setting.

Step 4: Configure the LX

The first time you power up the LX device, there is some initial configuration that you need to perform through the LX Local Console:

- Change the default password
- Assign the IP address
- Name the KVM target servers

The LX can be configured remotely via web browser. This requires the workstation have an appropriate Java Runtime Environment (JRE) version installed.

Changing the Default Password

The LX ships with a default password. The first time you start the LX you are required to change that password.

► To change the default password:

1. Once the unit has booted, enter the default username (admin) and password (raritan). Click Login.
2. Enter the old password (raritan), enter a new password and then enter the new password again. Passwords can be up to 64 characters in length and can consist of English, alphanumeric and special characters. Click Apply. Click OK on the Confirmation page.

Note: The default password can also be changed from the Raritan Multi-Platform Client (MPC).

Assigning an IP Address

These procedures describe how to assign an IP address on the Network Settings page. For complete information about all of the fields and the operation of this page, see **Network Settings** (on page 115).

► To assign an IP address:

1. Choose Device Settings > Network. The Network Settings page opens.
2. Specify a meaningful Device Name for your LX device. Up to 32 alphanumeric characters using valid special characters and no spaces.
3. In the IPv4 section, enter or select the appropriate IPv4-specific network settings:
 - a. Enter the IP Address if needed. The default IP address is 192.168.0.192.
 - b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
 - c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.
 - d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.
 - e. Select the IP Auto Configuration. The following options are available:
 - None (Static IP) - This option requires that you manually specify the network parameters.

This is the recommended option because the LX is an infrastructure device and its IP address should not change.
 - DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

With this option, network parameters are assigned by the DHCP server. If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.
4. If IPv6 is to be used, enter or select the appropriate IPv6-specific network settings in the IPv6 section:
 - a. Select the IPv6 checkbox to activate the fields in the section.
 - b. Enter a Global/Unique IP Address. This is the IP address assigned to the LX.

- c. Enter the Prefix Length. This is the number of bits used in the IPv6 address.
- d. Enter the Gateway IP Address.
- e. Link-Local IP Address. This address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present. **Read-Only**
- f. Zone ID. This identifies the device with which the address is associated. **Read-Only**
- g. Select the IP Auto Configuration. The following options are available:
 - None - Use this option if you do not want an auto IP configuration and prefer to set the IP address yourself (static IP). This is the default and recommended option.

If None is selected for the IP auto configuration, the following Network Basic Settings fields are enabled: Global/Unique IP Address, Prefix Length, and Gateway IP Address allowing you to manually set the IP configuration.
 - Router Discovery - Use this option to automatically assign IPv6 addresses that have Global or Unique Local significance beyond that of the Link Local, which only applies to a directly connected subnet.
5. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.
6. If Use the Following DNS Server Addresses is selected, regardless of whether DHCP is selected or not, the addresses entered in this section will be used to connect to the DNS server.

Enter the following information if the Following DNS Server Addresses option is selected. These addresses are the primary and secondary DNS addresses that will be used if the primary DNS server connection is lost due to an outage.

 - a. Primary DNS Server IP Address
 - b. Secondary DNS Server IP Address
7. When finished, click OK.

See LAN Interface Settings for information in configuring this section of the Network Settings page.

*Note: In some environments, the default LAN Interface Speed & Duplex setting Autodetect (autonegotiator) does not properly set the network parameters, which results in network issues. In these instances, setting the LX LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. See the **Network Settings** (on page 115) page for more information.*

Configuring Date/Time Settings (Optional)

► **To set the date and time:**

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens.
2. Choose your time zone from the Time Zone drop-down list.
3. To adjust for daylight savings time, check the "Adjust for daylight savings time" checkbox.
4. Choose the method you would like to use to set the date and time:
 - User Specified Time - Choose this option to input the date and time manually. For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).
 - Synchronize with NTP Server - Choose this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
5. For the Synchronize with NTP Server option:
 - a. Enter the IP address of the Primary Time server.
 - b. Enter the IP address of the Secondary Time server. **Optional**
6. Click OK.

Naming Target Servers

► **To name the target servers:**

1. Connect all of the target servers if you have not already done so. See **Step 3: Connect the Equipment** for a description of connecting the equipment.
2. Using the LX Local Console, choose Device Settings > Port Configuration and then click the Port Name of the target server you want to name.
3. Enter a name for the server, which can be up to 32 alphanumeric and special characters. Click OK.

Valid Special Characters for Target Names

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

Remote Authentication***Supported Protocols***

To simplify management of usernames and passwords, the LX provides the ability to forward authentication requests to an external authentication server. Two external authentication protocols are supported: LDAP/LDAPS and RADIUS.

Note on Microsoft Active Directory

Microsoft® Active Directory® uses the LDAP/LDAPS protocol natively, and can function as an LDAP/LDAPS server and authentication source for the LX. If it has the IAS (Internet Authorization Server) component, a Microsoft Active Directory server can also serve as a RADIUS authentication source.

Create User Groups and Users

As part of the initial configuration, you must define user groups and users in order for users to access the LX.

The LX uses system-supplied default user groups and allows you to create groups and specify the appropriate permissions to suit your needs.

User names and passwords are required to gain access to the LX. This information is used to authenticate users attempting to access your LX. See **User Management (on page 94)** for details on adding and editing user groups and users.

Step 5: Launch the LX Remote Console

► To launch the LX Remote Console:

1. Log in to any workstation with network connectivity to your LX, and that has Microsoft .NET[®] and/or Java Runtime Environment[®] installed (JRE[®] is available on the **Java website <http://java.sun.com/>**).
2. Launch a supported web browser such as Internet Explorer[®] or Firefox[®].
3. Enter the URL: *http://IP-ADDRESS* or *http://IP-ADDRESS/akc* for .NET, where IP-ADDRESS is the IP address assigned to your LX. You can also use https, the DNS name of the LX assigned by the administrator (provided that a DNS server has been configured), or type the IP address in the browser (LX always redirects the IP address from HTTP to HTTPS.)
4. Enter your username and password. Click Login.

Access and Control Target Servers Remotely

The LX Port Access page provides a list of all LX ports, as well as the connected target servers, their status, and availability.

Accessing a Target Server

► To access a target server:

1. Click the Port Name of the target you want to access. The Port Action Menu is displayed.
2. Choose Connect from the Port Action menu. A KVM window opens with a connection to the target.

Switching between Target Servers**▶ To switch between KVM target servers:**

1. While already using a target server, access the LX Port Access page.
2. Click the port name of the target you want to access. The Port Action menu appears.
3. Choose Switch From in the Port Action menu. The new target server you selected is displayed.

Disconnecting a Target Server**▶ To disconnect a target server:**

- Click the port name of the target you want to disconnect. When Port Action menu appears, click Disconnect.

Step 6: Configure the Keyboard Language (Optional)

Note: This step is not required if you are using the US/International language keyboard.

If you are using a non-US language, the keyboard has to be configured for the appropriate language. In addition, the keyboard language for the client machine and the KVM target servers has to match.

Consult the documentation for your operating system for additional information about changing the keyboard layout.

Changing the Keyboard Layout Code (Sun Targets)

Use this procedure if you are using a DCIM-SUSB and would like the keyboard layout changed to another language.

▶ To change the keyboard layout code (DCIM-SUSB only):

1. Open a Text Editor window on the Sun™ workstation.
2. Check that the Num Lock key is active and press the left Ctrl key and the Del key on your keyboard. The Caps Lock light starts to blink, indicating that the CIM is in Layout Code Change mode. The text window displays: Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX).
3. Type the layout code desired (for example, 31 for the Japanese keyboard).
4. Press Enter.
5. Shut down the device and power on once again. The DCIM-SUSB performs a reset (power cycle).
6. Verify that the characters are correct.

Step 7: Configure Tiering (Optional)

LX and generic tiering are supported by the LX. See the **Device Management (on page 115)** section for more information on this feature.

Connect from a target server port on the base device to the tier LX Local Access port video/keyboard/mouse ports using a D2CIM-DVUSB.

► **To enable tiering:**

1. From the tier base, choose Device Settings > Device Services. The Device Service Settings page appears.
2. Select Enable Tiering as Base.
3. In the Base Secret field, enter the secret shared between the base and the tiered devices. This secret is required for the tiered devices to authenticate the base device. You will enter the same secret word for the tiered device.
4. Click OK.
5. Enable the tiered devices. From the tiered device, choose Device Settings > Local Port Settings.
6. In the Enable Local Ports section of the page, select Enable Local Port Device Tiering.
7. In the Tier Secret field, enter the same secret word you entered for the base device on the Device Settings page.
8. Click OK.

Chapter 3 Working with Target Servers

In This Chapter

- LX Interfaces37
- LX Local Console Interface: LX Devices38
- LX Remote Console Interface38
- Proxy Server Configuration for Use with MPC, VKC and AKC51
- Virtual KVM Client (VKC) and Active KVM Client (AKC).....53
- Multi-Platform Client (MPC).....80

LX Interfaces

There are several user interfaces in the LX, providing you with easy access anytime, anywhere to targets. These include the LX Local Console, the LX Remote Console, the Virtual KVM Client (VKC), the Active KVM Client (AKC), and the Multi-Platform Client (MPC). The following table identifies these interfaces and their use for target server access and administration locally and remotely:

User Interface	Local		Remote	
	Access	Admin	Access	Admin
LX Local Console	✓	✓		
LX Remote Console			✓	✓
Virtual KVM Client (VKC)			✓	
Multi-Platform Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

The following sections of the help contain information about using specific interfaces to access the LX and manage targets:

- Local Console
- Remote Console
- Virtual KVM Client
- Multi-Platform Client

LX Local Console Interface: LX Devices

When you are located at the server rack, the LX provides standard KVM management and administration via the LX Local Console. The LX Local Console provides a direct KVM (analog) connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports.

There are many similarities among the LX Local Console and the LX Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

The LX Local Console Factory Reset option is available in the LX Local Console but not the LX Remote Console.

LX Remote Console Interface

The LX Remote Console is a browser-based graphical user interface that allows you to log in to KVM target servers and serial targets connected to the LX and to remotely administer the LX.

The LX Remote Console provides a digital connection to your connected KVM target servers. When you log into a KVM target server using the LX Remote Console, a Virtual KVM Client window opens.

There are many similarities among the LX Local Console and the LX Remote Console graphical user interfaces, and where there are differences, they are noted in the user manual. The following options are available in the LX Remote Console but not the LX Local Console:

- Virtual Media
- Favorites
- Backup/Restore
- Firmware Upgrade
- SSL Certificates

Launching the LX Remote Console

Important: Regardless of the browser used, you must allow pop-ups from the device's IP address to launch the LX Remote Console.

Depending on your browser and security settings, you may see various security and certificate warnings. It is necessary to accept these warnings to launch the LX Remote Console.

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

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

► **To launch the LX Remote Console:**

1. Log in to any workstation with network connectivity to your LX, and that has Microsoft .NET® and/or Java Runtime Environment® installed (JRE® is available on the **Java website <http://java.sun.com/>**).
2. Launch a supported web browser such as Internet Explorer® or Firefox®.
3. Enter the URL: *http://IP-ADDRESS* or *http://IP-ADDRESS/akc* for .NET, where IP-ADDRESS is the IP address assigned to your LX. You can also use https, the DNS name of the LX assigned by the administrator (provided that a DNS server has been configured), or type the IP address in the browser (LX always redirects the IP address from HTTP to HTTPS.)
4. Type your user name and password. If this is the first time logging in, log in with the factory default user name (admin) and password (raritan, all lower case). You will be prompted to change the default password. Click Login.

See **Virtual KVM Client (VKC) and Active KVM Client (AKC)** (on page 53) for information on the LX functions available via the Remote Console.

Interface and Navigation

LX Interface

Both the LX Remote Console and the LX Local Console interfaces provide a web-based interface for device configuration and administration, as well as target server list and selection. The options are organized into various tabs.

After a successful login, the Port Access page opens listing all ports along with their status and availability. Two tabs are provided on the page - View by Port and Set Scan. On the View by Port tab, sort by Port Number, Port Name, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading. Change the number of ports displayed on the page by entering a number in the Rows per Page field at the bottom right of the page and clicking Set. See **Port Access Page** (on page 43) for more information.

Use the Set Scan tab to scan for up to 32 targets that are connected to the LX. See **Scanning Ports** (on page 45).

Left Panel

The left panel of the LX interface contains the following information. Note that some information is conditional and will only be displayed if you are a certain of user, are using certain features, and so on. Conditional information is noted here.

Information	Description	When displayed?
Time & Session	The date and time the current session started.	Always
User	Username	Always
State	The current state of the application, either idle or active. If idle, the application tracks and displays the time the session has been idle.	Always
Your IP	The IP address used to access the LX.	Always
Last Login	The last login date and time.	Always
Device Information	Information specific to the LX you are using.	Always
Device Name	Name assigned to the device.	Always
IP Address	The IP address of the LX.	Always
Firmware	Current version of firmware.	Always
Device Model	Model of the LX	Always
Configured As Base or Configured As Tiered*	If you are using a tiering configuration, this indicates if the LX you are accessing is the base device or a tiered device.	When the LX is part of a tiered configuration
Port States	The statuses of the ports being used by the LX.	Always
Connected Users	The users, identified by their username and IP address, who are currently connected to the LX.	Always

Information	Description	When displayed?
Online Help	Links to online help.	Always
Favorite Devices	See Managing Favorites (on page 48).	Always

LX Console Navigation

The LX Console interfaces provide many methods for navigation and making your selections.

▶ **To select an option (use any of the following):**

- Click on a tab. A page of available options appears.
- Hover over a tab and select the appropriate option from the menu.
- Click the option directly from the menu hierarchy displayed (breadcrumbs).

▶ **To scroll through pages longer than the screen:**

- Use Page Up and Page Down keys on your keyboard.
- Use the scroll bar on the right.

Port Access Page

After successfully logging on to the LX Remote Console, the Port Access page appears. By default, the View by Port tab will be displayed on the Port Access page. This page lists all of the LX ports, the connected KVM target servers, and their status and availability. The Port Access page provides access to the KVM target servers connected to the LX. KVM target servers are servers that you want to control through the LX device. They are connected to the LX ports at the back of the device.

Note: For each connection to a KVM target server, a new Virtual KVM Client window opens.

If you are using a tiered configuration in which a base LX device is used to access multiple other tiered devices, the tiered devices are viewed on the Port Access page by clicking on the Expand Arrow icon ► to the left of the tier device name. See **Configuring and Enabling Tiering** (on page 121) for more information on tiering.

The port scanning feature is accessed from the Set Scan tab on the Port Access page. The feature allows you to define a set of targets to be scanned. Thumbnail views of the scanned targets are also available. Select a thumbnail to open that target in its Virtual KVM Client window.

► To use the Port Access page:

1. From the LX Remote Console, click the Port Access tab. The Port Access page opens.

The KVM target servers are initially sorted by Port Number. You can change the display to sort on any of the columns.

- Port Number - Numbered from 1 to the total number of ports available for the LX device.
- Port Name - The name of the LX port. Initially, this is set to Dominion-LX-Port# but you can change the name to something more descriptive. When you click a Port Name link, the Port Action Menu appears.

Note: Do not use apostrophes for the Port (CIM) Name.

- Type - The type of server or CIM.
 - Status - The status for standard servers is either up or down.
 - Availability - The availability of the server.
2. Click the Port Name of the target server you want to access. The Port Action Menu appears. See Port Action Menu for details on available menu options.
 3. Choose the desired menu command from the Port Action Menu.
 4. Define a set of ports to be scanned on the LX using the Set Scan function. See **Scanning Ports** (on page 45).

► **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.

Port Action Menu

When you click a Port Name in the Port Access list, the Port Action menu appears. Choose the desired menu option for that port to execute it. Note that only currently available options, depending on the port's status and availability, are listed in the Port Action menu:

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

Note: This option is not available from the LX Remote Console for an available port if all connections are busy.

- **Switch From** - Switches from an existing connection to the selected port (KVM target server). This menu item is available only for KVM targets. This option is visible only when a Virtual KVM Client is opened.

Note: This menu item is not available on the LX Local Console.

- **Disconnect** - Disconnects this port and closes the Virtual KVM Client page for this target server. This menu item is available only when the port status is up and connected, or up and busy.

Note: This menu item is not available on the LX Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.

Scanning Ports

The LX provides 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, tiered Dominion devices, and KVM switch ports.

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 **Scan Settings** (on page 78)

You can 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 **Scan Settings** (on page 78).

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

This feature is available from the Local Port, Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC).

*Note: MPC uses a different method for initiating a scan than the other Raritan clients. See **Set Scan Group** in the **KVM and Serial Client Guide** for details. The scan results and scan options differ between the Remote Console and the Local Console. See **Scanning Ports - Local Console** (on page 176).*

► To scan for targets:

1. Click the Set Scan tab on the Port Access page.
2. Select the targets you want to include in the scan by selecting the checkbox to the left of each target, or select the checkbox at the top of the target column to select all targets.

3. Leave the Up Only checkbox selected if you only want targets that are up to be included in the scan. Deselect this checkbox if you want to include all targets, whether up or down.
4. Click Scan to begin the scan. As each target is scanned, it is displayed in slide show view on the page.
5. Click Options > Pause to pause the slide show and stop it from moving between targets, click Options > Resume to resume the slide show.
6. Click on a target thumbnail to scan it next.
7. Connect to a target by double clicking on its thumbnail.

View By Port		Set Scan		
▲ No.	Name	Type	Status	Availability
1	Dominion_LX_Port1	Not Available	down	idle
2	Dominion_LX_Port2	Not Available	down	idle
3	Dominion_LX_Port3	Not Available	down	idle
4	Dominion_LX_Port4	Not Available	down	idle
5	Dominion_LX_Port5	Not Available	down	idle
6	Dominion_LX_Port6	Not Available	down	idle
7	Dominion_LX_Port7	Not Available	down	idle
8	Dominion_LX_Port8	Not Available	down	idle
9	Dominion_LX_Port9	Not Available	down	idle
10	ion	Not Avai		idle

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.

▶ 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.

Managing Favorites

A Favorites feature is provided so you can organize and quickly access the devices you use frequently. The Favorite Devices section is located in the lower left side (sidebar) of the Port Access page and provides the ability to:

- Create and manage a list of favorite devices
- Quickly access frequently-used devices
- List your favorites either by Device Name, IP Address, or DNS hostname
- Discover LX devices on its subnet (before and after login)
- Retrieve discovered LX devices from the connected Dominion device (after login)

▶ **To access a favorite LX device:**

- Click the device name (listed beneath Favorite Devices). A new browser opens to that device.

▶ **To display favorites by name:**

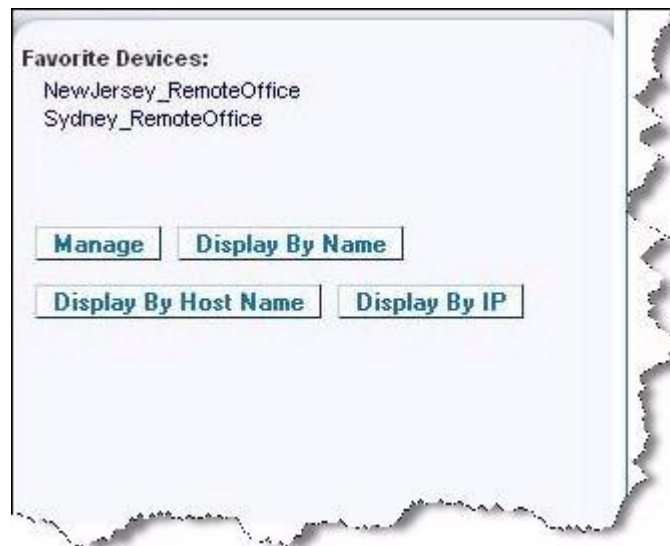
- Click Display by Name.

▶ **To display favorites by IP Address:**

- Click Display by IP.

▶ **To display favorites by the host name:**

- Click Display by Host Name.



Manage Favorites Page

► **To open the Manage Favorites page:**

- Click Manage in the left panel. The Manage Favorites page appears and contains the following:

Use:	To:
Favorites List	Manage your list of favorite devices.
Discover Devices - Local Subnet	Discover Raritan devices on the client PC's local subnet.
Discover Devices - LX Subnet	Discover the Raritan devices on the LX device subnet.
Add New Device to Favorites	Add, edit, and delete devices from your list of Favorites.

Favorites List Page

From the Favorites List page, you can add, edit, and delete devices from your list of favorites.

► **To open the Favorites List page:**

- Choose Manage > Favorites List. The Favorites List page opens.

Discovering Devices on the Local Subnet

This option discovers the devices on your local subnet, which is the subnet where the LX Remote Console is running. These devices can be accessed directly from this page or you can add them to your list of favorites. See ***Favorites List Page*** (on page 49).

► **To discover devices on the local subnet:**

1. Choose Manage > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page appears.
2. Choose the appropriate discovery port:
 - To use the default discovery port, select the Use Default Port 5000 checkbox.
 - To use a different discovery port:
 - a. Deselect the Use Default Port 5000 checkbox.
 - b. Type the port number in the Discover on Port field.

- c. Click Save.
3. Click Refresh. The list of devices on the local subnet is refreshed.

▶ **To add devices to your Favorites List:**

1. Select the checkbox next to the device name/IP address.
2. Click Add.

▶ **To access a discovered device:**

- Click the device name or IP address for that device. A new browser opens to that device.

Discovering Devices on the LX Subnet

This option discovers devices on the device subnet, which is the subnet of the LX device IP address itself. You can access these devices directly from this the Subnet page or add them to your list of favorites. See ***Favorites List Page*** (on page 49).

This feature allows multiple LX devices to interoperate and scale automatically. The LX Remote Console automatically discovers the LX devices, and any other Raritan device, in the subnet of the LX.

▶ **To discover devices on the device subnet:**

1. Choose Manage > Discover Devices - LX Subnet. The Discover Devices - LX Subnet page appears.
2. Click Refresh. The list of devices on the local subnet is refreshed.

▶ **To add devices to your Favorites List:**

1. Select the checkbox next to the device name/IP address.
2. Click Add.

▶ **To access a discovered device:**

- Click the device name or IP address for that device. A new browser opens to that device.

Adding, Deleting and Editing Favorites

▶ **To add a device to your favorites list:**

1. Choose Manage > Add New Device to Favorites. The Add New Favorite page appears.
2. Type a meaningful description.
3. Type the IP Address/Host Name for the device.

4. Change the discovery Port (if necessary).
5. Select the Product Type.
6. Click OK. The device is added to your list of favorites.

► **To edit a favorite:**

1. From the Favorites List page, select the checkbox next to the appropriate LX device.
2. Click Edit. The Edit page appears.
3. Update the fields as necessary:
 - Description
 - IP Address/Host Name - Type the IP address of the LX device
 - Port (if necessary)
 - Product Type
4. Click OK.

► **To delete a favorite:**

Important: Exercise caution in the removal of favorites. You are not prompted to confirm their deletion.

1. Select the checkbox next to the appropriate LX device.
2. Click Delete. The favorite is removed from your list of favorites.

Logging Out

► **To quit the LX:**

- Click Logout in the upper right-hand corner of the page.

Note: Logging out also closes any open Virtual KVM Client and serial client sessions.

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
```

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

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** (on page 124))
- 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.

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.

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.

About the Active KVM Client

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).

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.

AKC Supported .NET Framework, Operating Systems and Browsers

.NET Framework

AKC requires Windows .NET® version 3.5, and will work with both 3.5 and 4.0 installed but will not work with 4.0 alone.

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)

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.

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 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.

Toolbar

Button	Button Name	Description
	Connection Properties	Opens the Modify Connection Properties dialog from which you can manually adjust bandwidth options (such as connection speed, color depth, and so forth).
	Video Settings	Opens the Video Settings dialog, allowing you to manually adjust video conversion parameters.
	Color Calibration	Adjusts color settings to reduce excess color noise. Same as choosing Video > Color Calibrate. <hr/> <i>Note: Not available in KX II-101-V2.</i>
	Target Screenshot	Click to take a screenshot of the target server and save it to a file of your choosing.
	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. <hr/> <i>Note: This feature is available with the KX II 2.4.0 (and later).</i> <hr/> <i>Note: This feature is not supported by the LX.</i>
	Synchronize Mouse	Dual-mouse mode forces the realignment of the target server mouse pointer with the mouse pointer. <hr/> <i>Note: Not available in KX II-101-V2.</i>
	Refresh Screen	Forces a refresh of the video screen.
	Auto-sense Video Settings	Forces a refresh of the video settings (resolution, refresh rate).
	Smart Card	Opens a dialog that allows you to select from a list of smart card readers connected to a client PC. <hr/> <i>Note: This feature is available on the KSX II 2.3.0 (and later) and the KX II 2.1.10 (and later).</i> <hr/> <i>Note: This feature is not supported by the LX.</i>


Button	Button Name	Description
	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Del hot key combination to the target server.
	Single Cursor Mode	<p>Starts Single Cursor mode in which the local mouse pointer no longer appears onscreen.</p> <p>Press Ctrl+Alt+O to exit this mode.</p> <hr/> <p><i>Note: Not available in KX II-101-V2.</i></p>
	Full Screen Mode	Maximizes the screen real estate to view the target server desktop.
	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.

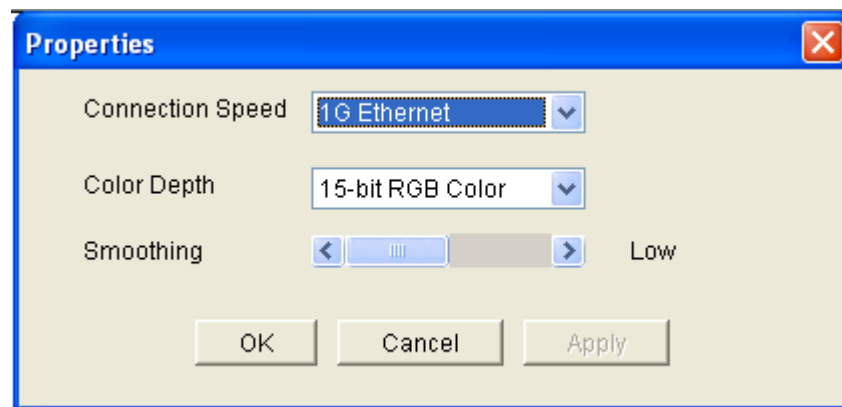
Connection Properties

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.



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

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.

Note: KX II-101 does not support AKC.

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.

Note: KX II-101 does not support AKC.

► **To import macros:**

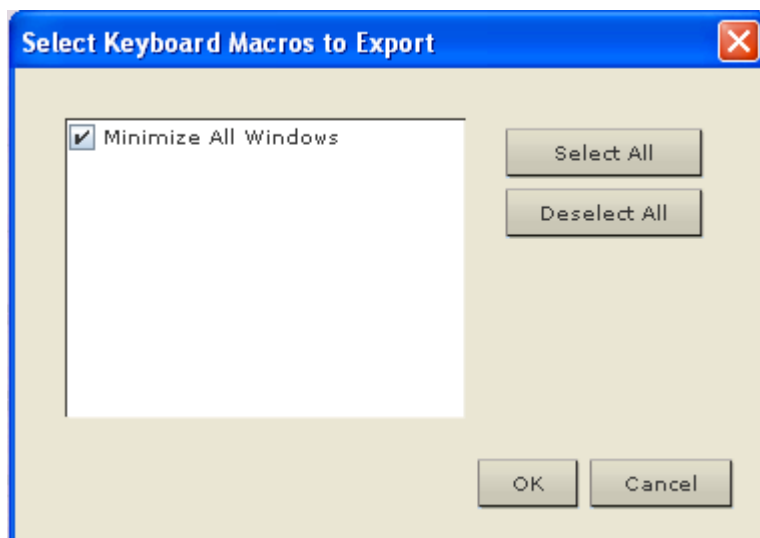
1. Choose Keyboard > Import Keyboard Macros to open the Import Macros dialog. Browse to the folder location of the macro file.
2. Click on the macro file and click Open to import the macro.
 - a. If too many macros are found in the file, an error message is displayed and the import terminates once OK 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.

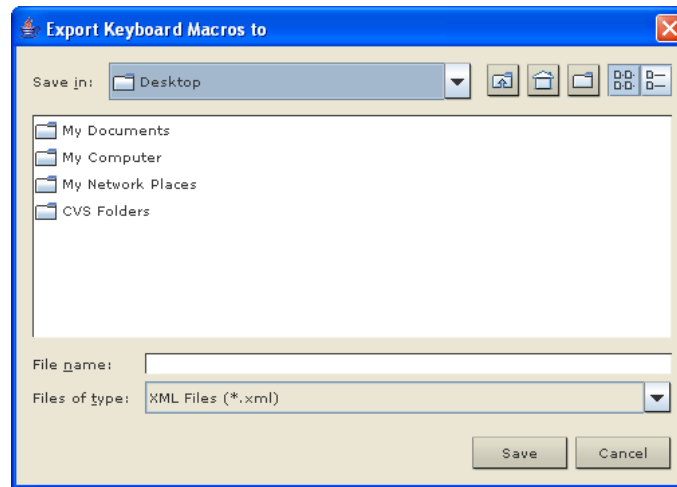
► **To export macros:**

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. A dialog from which to locate and select the macro file appears. 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.
6. To use the Send Text to Target function for the macro, click the Construct Macro from Text button.
7. For example, create a macro to close a window by selecting Left Ctrl + Esc. This appears in the Macro Sequence box as follows:

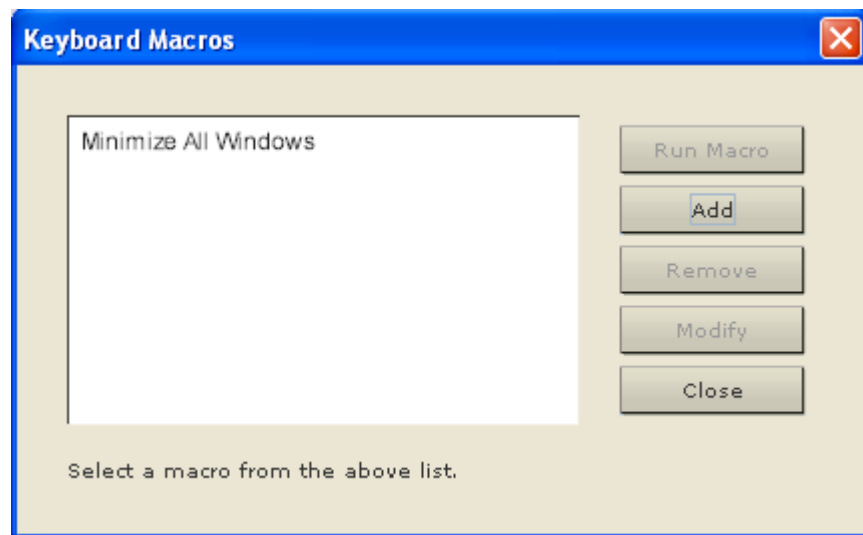
Press Left Ctrl

Release Left Ctrl

Press Esc

Release Esc

8. 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.
9. 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.
10. 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.



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.

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.

Note: The KX II-101 does support color calibration.


► 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.

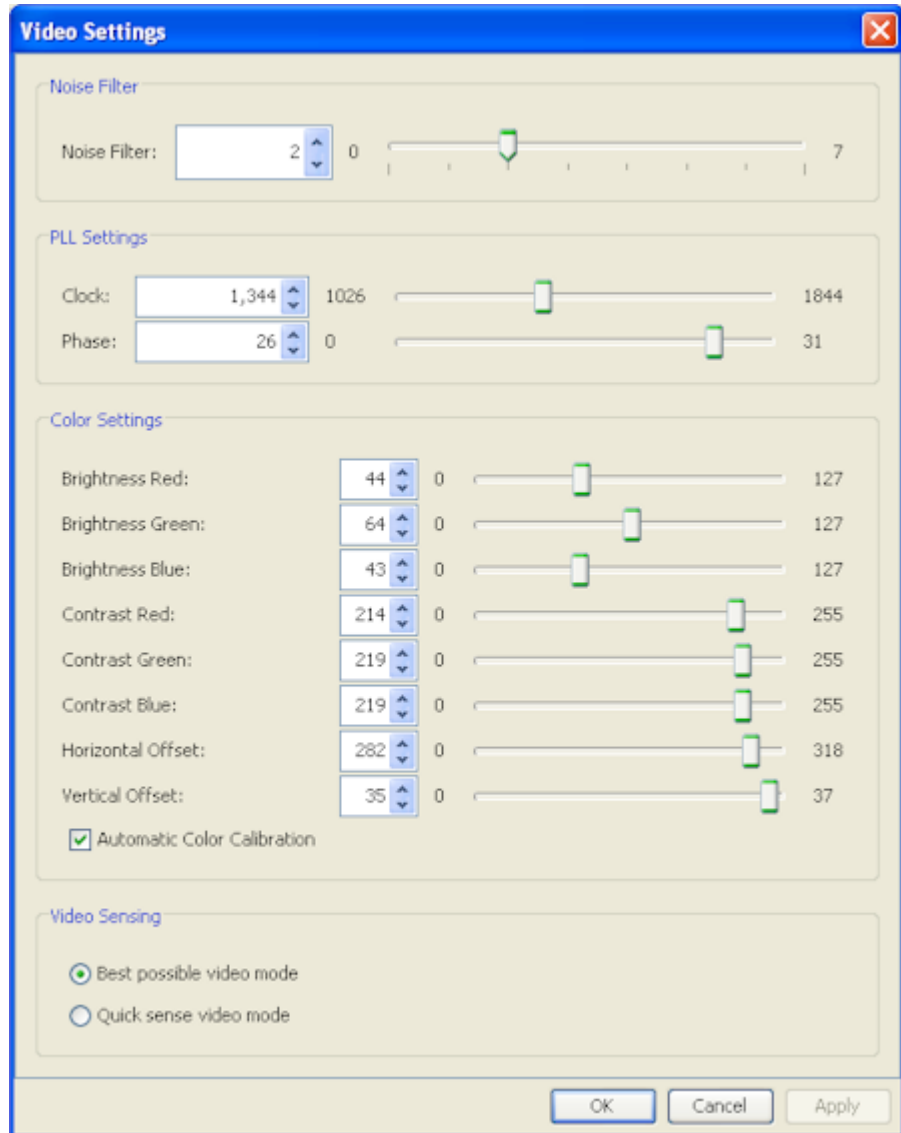
- c. Brightness: Use this setting to adjust the brightness of the target server display.
- d. Brightness Red - Controls the brightness of the target server display for the red signal.
- e. Brightness Green - Controls the brightness of the green signal.
- f. Brightness Blue - Controls the brightness of 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.

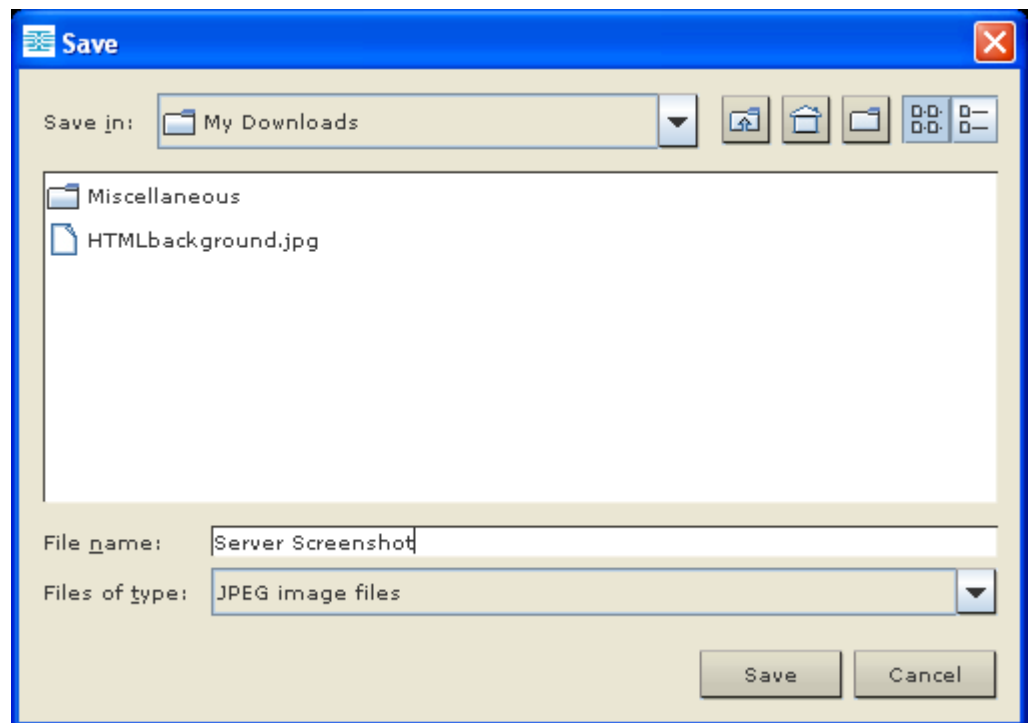


Using Screenshot from Target

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 `xset mouse 1 1` command.
 - 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: For LX, Absolute Mouse Synchronization is available for use with the virtual media-enabled USB CIM (D2CIM-VUSB and D2CIM-DVUSB) only.

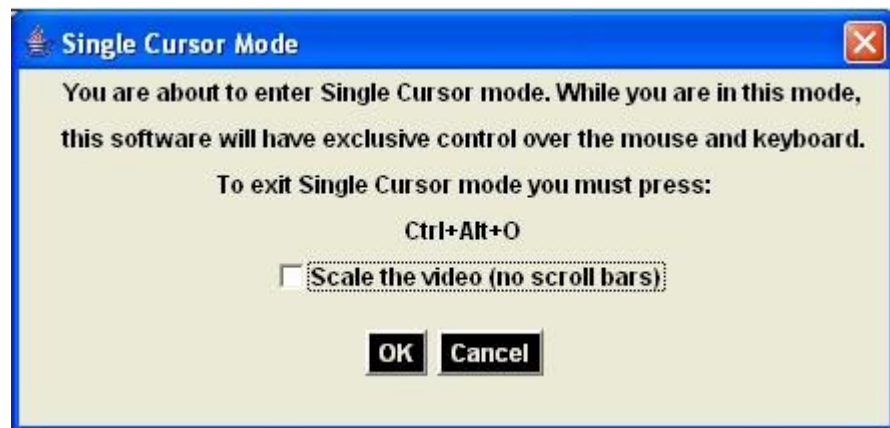
Single Mouse Mode

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 using VM as a client.

► **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:**

- 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

Language	Configuration method
Norwegian	Keyboard Indicator
Danish	Keyboard Indicator
Swedish	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Italian	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

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

Client Launch Settings

LX users can configure client launch settings that allow you to define the screen settings for a KVM session.

Note: This feature is available in MPC, not AKC or VKC.

► 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.

Scan Settings

The LX provides 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, tiered Dominion devices, and KVM switch ports. See **Scanning Ports** (on page 45). 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 75).

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 75).

▶ 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.

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).

Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) is a graphical user interface for the Raritan product lines, providing remote access to target servers connected to Raritan KVM over IP devices. For details on using MPC, see the **KVM and Serial Access Clients Guide** available on Raritan's website on the same page as the user guide. Instructions on launching MPC are provided there.

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help.

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 Mac 10.5 and 10.6 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.

Chapter 4 Virtual Media

In This Chapter

Overview.....	83
Using Virtual Media	88
Disconnecting Virtual Media.....	93

Overview

Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from a client PC and network file servers. The LX supports virtual media access of hard drives and remotely mounted images.

The 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

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)

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

The following client operating systems are supported:

- Windows
- Mac OS X 10.5
- Mac OS X 10.6
- 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.

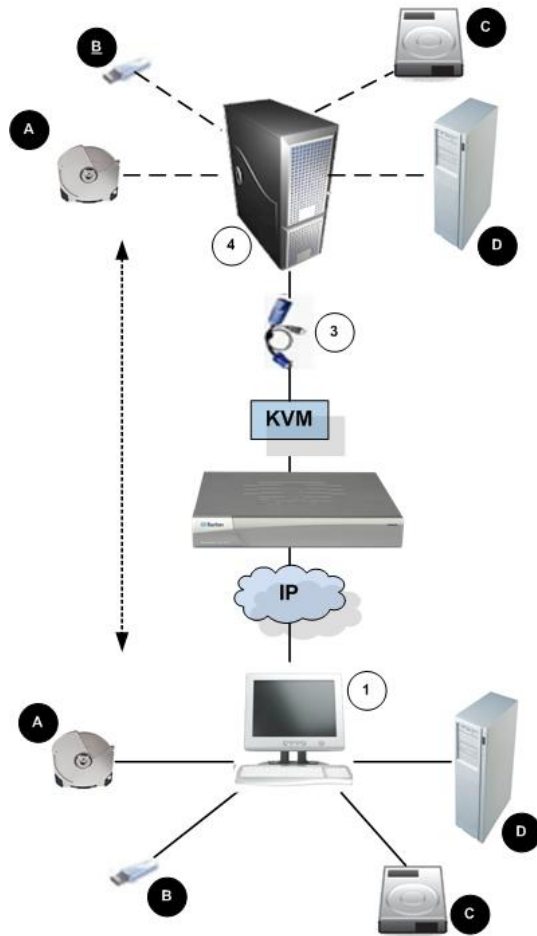


Diagram key			
1	Desktop PC	A	CD/DVD drive
2	LX	B	USB mass storage device
3	CIM	C	PC hard drive
4	Target server	D	Remote file server (ISO images)

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 Linux Environment

Following is important information for Linux® users regarding using virtual media.

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.

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
> 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.

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 85) before you begin 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. See **Virtual Media File Server Setup (File Server ISO Images Only)** (on page 89).

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 of your tasks, disconnect the virtual media. See **Disconnecting Virtual Media** (on page 93).

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 91).

► **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".

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 the "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.

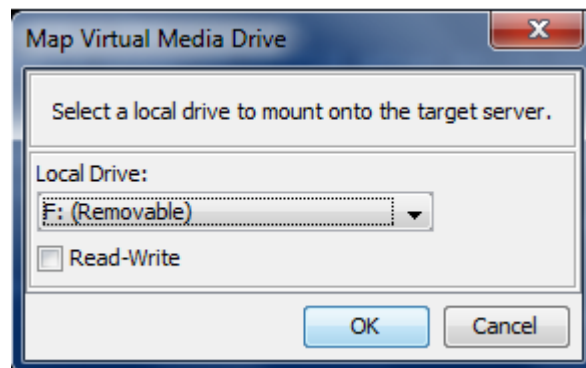
Note: KVM target servers running certain versions of the Windows operating system may not accept new mass storage connections after an NTFS-formatted partition (for example, the local C drive) has been redirected to them.

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 88) 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 Connect. 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 User Management

In This Chapter

User Groups	94
Users	99
Authentication Settings.....	102
Changing a Password	114

User Groups

The LX stores an internal list of all user and group names to determine access authorization and permissions. This information is stored internally in an encrypted format. There are several forms of authentication and this one is known as local authentication. All users have to be authenticated. If the LX is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

Every LX is delivered with three default user groups. These groups cannot be deleted:

User	Description
Admin	Users that are members of this group have full administrative privileges. The original, factory-default user is a member of this group and has the complete set of system privileges. In addition, the Admin user must be a member of the Admin group.
Unknown	This is the default group for users who are authenticated externally using LDAP/LDAPS or RADIUS or who are unknown to the system. If the external LDAP/LDAPS or RADIUS server does not identify a valid user group, the Unknown group is used. In addition, any newly created user is automatically put in this group until assigned to another group.
Individual Group	An individual group is essentially a “group” of one. That is, the specific user is in its own group, not affiliated with other real groups. Individual groups can be identified by the “@” in the Group Name. The individual group allows a user account to have the same rights as a group.

Up to 254 user groups can be created in the LX. Up to 254 user groups can be created in the LX.

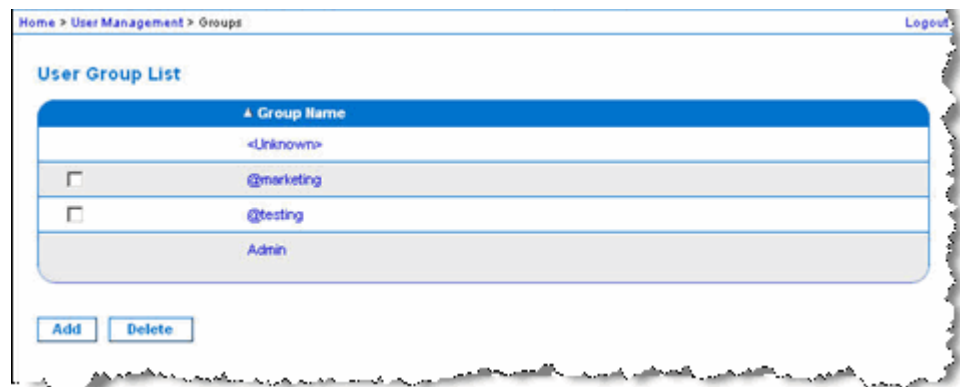
User Group List

User groups are used with local and remote authentication (via RADIUS or LDAP/LDAPS). It is a good idea to define user groups before creating individual users since, when you add a user, you must assign that user to an existing user group.

The User Group List page displays a list of all user groups, which can be sorted in ascending or descending order by clicking on the Group Name column heading. From the User Group List page, you can also add, modify, or delete user groups.

► To list the user groups:

- Choose User Management > User Group List. The User Group List page opens.



Relationship Between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your LX into groups saves time by allowing you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

You may also choose not to associate specific users with groups. In this case, you can classify the user as “Individual.”

Upon successful authentication, the device uses group information to determine the user's permissions, such as which server ports are accessible, whether rebooting the device is allowed, and other features.

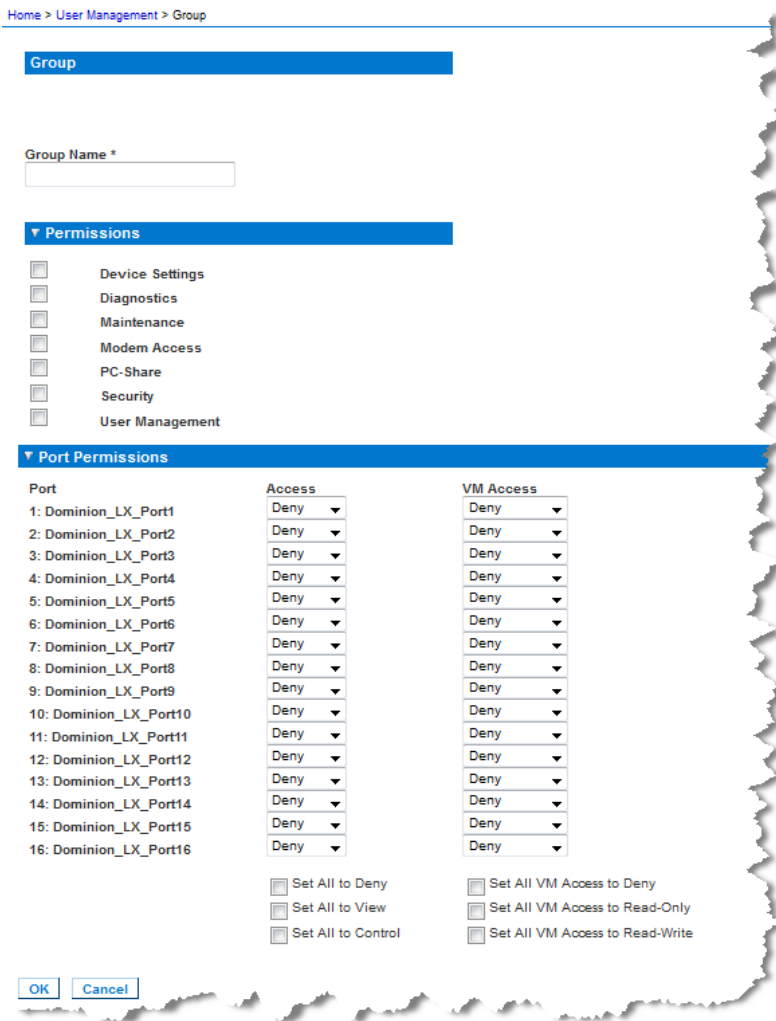
Adding a New User Group

► To add a new user group:

1. Select User Management > Add New User Group or click Add on the User Group List page.

2. Type a descriptive name for the new user group into the Group Name field (up to 64 characters).
3. Select the checkboxes next to the permissions you want to assign to all of the users belonging to this group. See **Setting Permissions** (on page 96).
4. Click OK.

Note: Several administrative functions are available within MPC and from the LX Local Console. These functions are available only to members of the default Admin group.



Setting Permissions

Important: Selecting the User Management checkbox allows the members of the group to change the permissions of all users,

including their own. Carefully consider granting these permissions.

Permission	Description
Device Settings	Network settings, date/time settings, port configuration (channel names and so on), event management (SNMP, Syslog), virtual media file server setups.
Diagnostics	Network interface status, network statistics, ping host, trace route to host, LX diagnostics.
Maintenance	Backup and restore database, firmware upgrade, factory reset, reboot.
Modem Access	Permission to use the modem to connect to the LX device.
PC-Share	<p>Simultaneous access to the same target by multiple users.</p> <p>If you are using a tiered configuration in which a base LX device is used to access multiple other tiered devices, all devices must share the same PC-Share setting. See Configuring and Enabling Tiering (on page 121) for more information on tiering.</p>
Security	SSL certificate, security settings (VM Share, PC-Share).
User Management	<p>User and group management, remote, authentication (LDAP/LDAPS/RADIUS), login settings.</p> <p>If you are using a tiered configuration in which a base LX device is used to access multiple other tiered devices, user, user group and remote authentication settings must be consistent across all devices. See Configuring and Enabling Tiering (on page 121) for more information on tiering.</p>

Setting Port Permissions

For each server port, you can specify the access type the group has, as well as the type of port access to the virtual media. Please note that the default setting for all permissions is Deny.

Port access	
option	Description
Deny	Denied access completely
View	View the video but not interact with the connected target server.
Control	Control the connected target server. Control must be assigned to the group if VM. In order for all users in a user group to see KVM switches that are added, each user must be granted Control access. If they don't have this permission and a KVM switch is added at a later time, they will not be able to see the switches.

VM access	
option	Description
Deny	Virtual media permission is denied altogether for the port.
Read-Only	Virtual media access is limited to read access only.
Read-Write	Complete access (read, write) to virtual media.

If you are using a tiered configuration in which a base LX device is used to access multiple other tiered devices, the tiered device enforces individual port control levels. See **Configuring and Enabling Tiering** (on page 121) for more information on tiering.

Setting Permissions for an Individual Group

► **To set permissions for an individual user group:**

1. Locate the group from among the groups listed. Individual groups can be identified by the @ in the Group Name.
2. Click the Group Name. The Group page opens.
3. Select the appropriate permissions.
4. Click OK.

Modifying and Existing User Group

Note: All permissions are enabled for the Admin group and cannot be changed.

▶ **To modify an existing user group:**

1. From the Group page, change the appropriate fields and set the appropriate permissions.
2. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. See **Setting Permissions** (on page 96).
3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See **Setting Port Permissions** (on page 98).
4. Click OK.

▶ **To delete a user group:**

Important: If you delete a group with users in it, the users are automatically assigned to the <unknown> user group.

Tip: To determine the users belonging to a particular group, sort the User List by User Group.

1. Choose a group from among those listed by checking the checkbox to the left of the Group Name.
2. Click Delete.
3. When prompted to confirm the deletion, click OK.

Users

Users must be granted user names and passwords to gain access to the LX. This information is used to authenticate users attempting to access your LX. Up to 254 users can be created for each user group.

If you are using a tiered configuration in which a base LX device is used to access multiple other tiered devices, users will need permission to access the base device and permissions to access each individual tiered device (as needed). When users log on to the base device, each tiered device is queried and the user can access each target server they have permissions to. See **Configuring and Enabling Tiering** (on page 121) for more information on tiering.

User List

The User List page displays a list of all users including their user name, full name, and user group. The list can be sorted on any of the columns by clicking on the column name. From the User List page, you can also add, modify, or delete users.

► **To view the list of users:**

- Choose User Management > User List. The User List page opens.



Home > User Management > Users Logout

User List

Username	Full Name	User Group
admin	Admin	Admin
<input type="checkbox"/> marketing	Addie Consumer	@marketing
<input type="checkbox"/> tester	Joe Tester	@tester

Adding a New User

It is a good idea to define user groups before creating LX users because, when you add a user, you must assign that user to an existing user group. See **Adding a New User Group** (on page 95).

From the User page, you can add new users, modify user information, and reactivate users that have been deactivated.

Note: A user name can be deactivated when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings page. See Security Settings.

► **To add a new user:**

1. Select User Management > Add New User or click Add on the User List page.
2. Type a unique name in the Username field (up to 16 characters).
3. Type the person's full name in the Full Name field (up to 64 characters).
4. Type a password in the Password field and retype the password in the Confirm Password field (up to 64 characters).
5. Choose the group from the User Group drop-down list.

If you do not want to associate this user with an existing User Group, select Individual Group from the drop-down list. For more information about permissions for an Individual Group, see **Setting Permissions for an Individual Group** (on page 98).

- To activate the new user, leave the Active checkbox selected. Click OK.

Modifying an Existing User

► **To modify an existing user:**

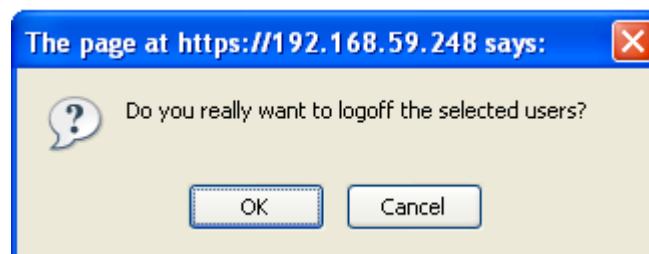
- Open the User List page by choosing User Management > User List.
- Locate the user from among those listed on the User List page.
- Click the user name. The User page opens.
- On the User page, change the appropriate fields. See **Adding a New User** (on page 100) for information about how to get access the User page.
- To delete a user, click Delete. You are prompted to confirm the deletion.
- Click OK.

Logging a User Off (Force Logoff)

If you are an administrator, you are able to log off another locally authenticated user who is logged on to the LX.

► **To log off a user:**

- Open the User List page by choosing User Management > User List or click the Connected User link in the left panel of the page.
- Locate the user from among those listed on the User List page and select the checkbox next to their name.
- Click Force User Logoff.
- Click OK on the Logoff User dialog to forcefully log the user off.



- A confirmation message is displayed to indicate that the user was logged off. This message contains the date and time the log off occurred. Click OK to close the message.

Authentication Settings

Authentication is the process of verifying that a user is who he says he is. Once a user is authenticated, the user's group is used to determine his system and port permissions. The user's assigned privileges determine what type of access is allowed. This is called authorization.

When the LX is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

If you are using a tiered configuration in which a base LX device is used to access multiple other tiered devices, the base device and the tiered devices must use the same authentication settings.

From the Authentication Settings page you can configure the type of authentication used for access to your LX.

Note: When remote authentication (LDAP/LDAPS or RADIUS) is selected, if the user is not found, the local authentication database will also be checked.

► **To configure authentication:**

1. Choose User Management > Authentication Settings. The Authentication Settings page opens.
2. Choose the option for the authentication protocol you want to use (Local Authentication, LDAP/LDAPS, or RADIUS). Choosing the LDAP option enables the remaining LDAP fields; selecting the RADIUS option enables the remaining RADIUS fields.
3. If you choose Local Authentication, proceed to step 6.
4. If you choose LDAP/LDAPS, read the section entitled Implementing LDAP Remote Authentication for information about completing the fields in the LDAP section of the Authentication Settings page.
5. If you choose RADIUS, read the section entitled Implementing RADIUS Remote Authentication for information about completing the fields in the RADIUS section of the Authentication Settings page.
6. Click OK to save.

► **To return to factory defaults:**


- Click Reset to Defaults.

Implementing LDAP/LDAPS Remote Authentication

Lightweight Directory Access Protocol (LDAP/LDAPS) is a networking protocol for querying and modifying directory services running over TCP/IP. A client starts an LDAP session by connecting to an LDAP/LDAPS server (the default TCP port is 389). The client then sends operation requests to the server, and the server sends responses in turn.

Reminder: Microsoft Active Directory functions natively as an LDAP/LDAPS authentication server.

► To use the LDAP authentication protocol:

1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Select the LDAP radio button to enable the LDAP section of the page.
3. Click the  icon to expand the LDAP section of the page.

Server Configuration

4. In the Primary LDAP Server field, type the IP address or DNS name of your LDAP/LDAPS remote authentication server (up to 256 characters). When the Enable Secure LDAP option is selected and the Enable LDAPS Server Certificate Validation option is selected, the DNS name must be used to match the CN of LDAP server certificate.
5. In the Secondary LDAP Server field, type the IP address or DNS name of your backup LDAP/LDAPS server (up to 256 characters). When the Enable Secure LDAP option is selected, the DNS name must be used. Note that the remaining fields share the same settings with the Primary LDAP Server field. **Optional**
6. Type of External LDAP Server.
7. Select the external LDAP/LDAPS server. Choose from among the options available:
 - Generic LDAP Server.
 - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
8. Type the name of the Active Directory Domain if you selected Microsoft Active Directory. For example, *acme.com*. Consult your Active Directory Administrator for a specific domain name.

9. In the User Search DN field, enter the Distinguished Name of where in the LDAP database you want to begin searching for user information. Up to 64 characters can be used. An example base search value might be: `cn=Users,dc=raritan,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.
10. Enter the Distinguished Name of the Administrative User in the DN of Administrative User field (up to 64 characters). Complete this field if your LDAP server only allows administrators to search user information using the Administrative User role. Consult your authentication server administrator for the appropriate values to type into this field. An example DN of Administrative User value might be: `cn=Administrator,cn=Users,dc=testradius,dc=com`.

Optional

11. If you entered a Distinguished Name for the Administrative User, you must enter the password that will be used to authenticate the Administrative User's DN against the remote authentication server. Enter the password in the Secret Phrase field and again in the Confirm Secret Phrase field (up to 128 characters).

Authentication Settings

Local Authentication
 LDAP
 RADIUS

▼ LDAP

Server Configuration

Primary LDAP Server

Secondary LDAP Server (optional)

Type of External LDAP Server
 ▼

Active Directory Domain

User Search DN

DN of Administrative User (optional)

Secret Phrase of Administrative User

Confirm Secret Phrase

LDAP/LDAP Secure

12. Select the Enable Secure LDAP checkbox if you would like to use SSL. This will enable the Enable LDAPS Server Certificate Validation checkbox. Secure Sockets Layer (SSL) is a cryptographic protocol that allows LX to communicate securely with the LDAP/LDAPS server.
13. The default Port is 389. Either use the standard LDAP TCP port or specify another port.
14. The default Secure LDAP Port is 636. Either use the default port or specify another port. This field is only used when the Enable Secure LDAP checkbox is selected.

15. Select the Enable LDAPS Server Certificate Validation checkbox to use the previously uploaded root CA certificate file to validate the certificate provided by the server. If you do not want to use the previously uploaded root CA certificate file, leave this checkbox deselected. Disabling this function is the equivalent of accepting a certificate that has been signed by an unknown certifying authority. This checkbox is only available when the Enable Secure LDAP checkbox has been enabled.

Note: When the Enable LDAPS Server Certificate Validation option is selected, in addition to using the Root CA certificate for validation, the server hostname must match the common name provided in the server certificate.

16. If needed, upload the Root CA Certificate File. This field is enabled when the Enable Secure LDAP option is selected. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use Browse to navigate to the certificate file. If you are replacing a certificate for the LDAP/LDAPS server with a new certificate, you must reboot the LX in order for the new certificate to take effect.

LDAP / Secure LDAP

Enable Secure LDAP

Port
389

Secure LDAP Port
636

Enable LDAPS Server Certificate Validation

Root CA Certificate File
Browse...

Upload

Note: Reboot device after certificate file is uploaded.

Test LDAP Server Access

17. The LX provides you with the ability to test the LDAP configuration from the Authentication Settings page due to the complexity sometimes encountered with successfully configuring the LDAP server and LX for remote authentication. To test the LDAP configuration, enter the login name and password in the "Login for testing" field and the "Password for testing" field respectively. This is the username and password you entered to access the LX and that the LDAP server will use to authenticate you. Click Test.

Once the test is completed, a message will be displayed that lets you know the test was successful or, if the test failed, a detailed error message will be displayed. It will display successful result or detail error message in failure case. It also can display group information retrieved from remote LDAP server for the test user in case of success.

The image shows a dialog box titled "Test LDAP Server Access". Inside the dialog, there are two text input fields. The first is labeled "Login for testing" and the second is labeled "Password for testing". Below these fields is a button labeled "Test".

Returning User Group Information from Active Directory Server

The LX supports user authentication to Active Directory® (AD) without requiring that users be defined locally on the LX. This allows Active Directory user accounts and passwords to be maintained exclusively on the AD server. Authorization and AD user privileges are controlled and administered through the standard LX policies and user group privileges that are applied locally to AD user groups.

IMPORTANT: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, the LX still supports this configuration and you do not need to perform the following operations. See *Updating the LDAP Schema* (on page 197) for information about updating the AD LDAP/LDAPS schema.

► **To enable your AD server on the LX:**

1. Using the LX, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as KVM_Admin and KVM_Operator.
2. On your Active Directory server, create new groups with the same group names as in the previous step.
3. On your AD server, assign the LX users to the groups created in step 2.
4. From the LX, enable and configure your AD server properly. See *Implementing LDAP/LDAPS Remote Authentication* (on page 103).


Important Notes

- Group Name is case sensitive.
- The LX provides the following default groups that cannot be changed or deleted: Admin and <Unknown>. Verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match the LX group configuration, the LX automatically assigns the group of <Unknown> to users who authenticate successfully.
- If you use a dialback number, you must enter the following case-sensitive string: *msRADIUSCallbackNumber*.
- Based on recommendations from Microsoft, Global Groups with user accounts should be used, not Domain Local Groups.

Implementing RADIUS Remote Authentication

Remote Authentication Dial-in User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for network access applications.

► To use the RADIUS authentication protocol:

1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Click the RADIUS radio button to enable the RADIUS section of the page.
3. Click the  icon to expand the RADIUS section of the page.
4. In the Primary Radius Server and Secondary Radius Server fields, type the IP address of your primary and optional secondary remote authentication servers, respectively (up to 256 characters).
5. In the Shared Secret fields, type the server secret used for authentication (up to 128 characters).

The shared secret is a character string that must be known by both the LX and the RADIUS server to allow them to communicate securely. It is essentially a password.

6. The Authentication Port default is port is 1812 but can be changed as required.
7. The Accounting Port default port is 1813 but can be changed as required.
8. The Timeout is recorded in seconds and default timeout is 1 second, but can be changed as required.

The timeout is the length of time the LX waits for a response from the RADIUS server before sending another authentication request.

9. The default number of retries is 3 Retries.

This is the number of times the LX will send an authentication request to the RADIUS server.

10. Choose the Global Authentication Type from among the options in the drop-down list:
- PAP - With PAP, passwords are sent as plain text. PAP is not interactive. The user name and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.
 - CHAP - With CHAP, authentication can be requested by the server at any time. CHAP provides more security than PAP.

Home > User Management > Authentication Settings

Authentication Settings

Local Authentication
 LDAP
 RADIUS

▶ LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Secondary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Global Authentication Type
 ▼

Cisco ACS 5.x for RADIUS Authentication

If you are using a Cisco ACS 5.x server, after you have configured the LX for RADIUS authentication, complete the following steps on the Cisco ACS 5.x server.

Note: The following steps include the Cisco menus and menu items used to access each page. Please refer to your Cisco documentation for the most up to date information on each step and more details on performing them.

- Add the LX as a AAA Client (**Required**) - Network Resources > Network Device Group > Network Device and AAA Clients
- Add/edit users (**Required**) - Network Resources > Users and Identity Stores > Internal Identity Stores > Users
- Configure Default Network access to enable CHAP Protocol (**Optional**) - Policies > Access Services > Default Network Access
- Create authorization policy rules to control access (**Required**) - Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
 - Dictionary Type: RADIUS-IETF
 - RADIUS Attribute: Filter-ID
 - Attribute Type: String
 - Attribute Value: Raritan:G{KVM_Admin} (where KVM_Admin is group name created locally on Dominion KVM Switch). Case sensitive.
- Configure Session Conditions (Date and Time) (**Required**) - Policy Elements > Session Conditions > Date and Time
- Configure/create the Network Access Authorization Policy (**Required**) - Access Policies > Access Services > Default Network Access>Authorization

Returning User Group Information via RADIUS

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

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

```
Raritan:G{GROUP_NAME}:D{Dial Back Number}
```

where *GROUP_NAME* is a string denoting the name of the group to which the user belongs and Dial Back Number is the number associated with the user account that the LX modem will use to dial back to the user account.

RADIUS Communication Exchange Specifications

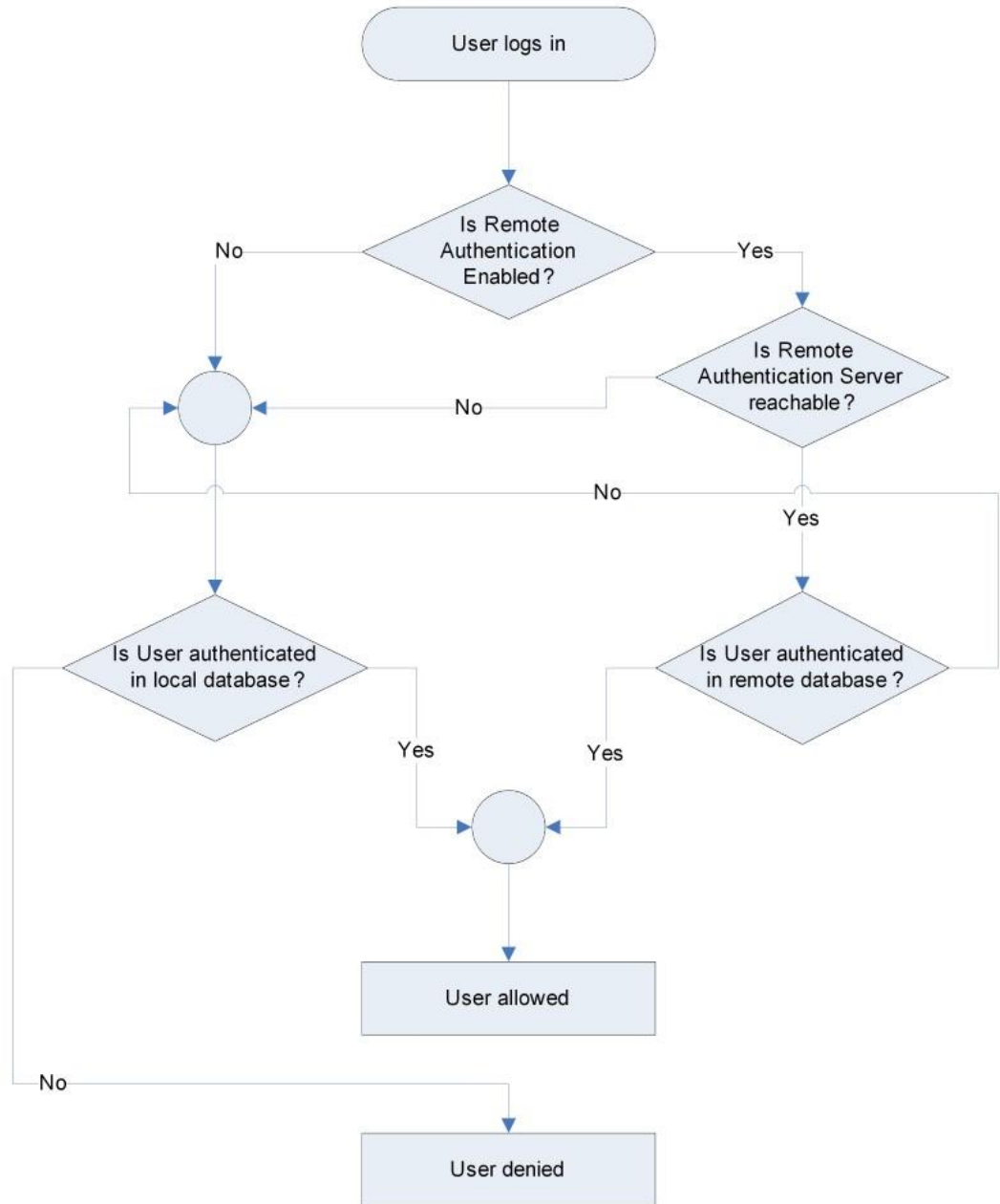
The LX sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
Log in	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP address for the LX.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
User-Password(2)	The encrypted password.
Accounting-Request(4)	
Acct-Status (40)	Start(1) - Starts the accounting.
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the LX.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
Log out	
Accounting-Request(4)	

Attribute	Data
Acct-Status (40)	Stop(2) - Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the LX.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

User Authentication Process

Remote authentication follows the process specified in the flowchart below:



Changing a Password

► **To change your password:**

1. Choose User Management > Change Password. The Change Password page opens.
2. Type your current password in the Old Password field.
3. Type a new password in the New Password field. Retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and special characters.
4. Click OK.
5. You will receive confirmation that the password was successfully changed. Click OK.

*Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, see **Strong Passwords** (on page 140).*

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

Chapter 6 Device Management

In This Chapter

Network Settings	115
Device Services	119
Configuring Modem Settings	126
Configuring Date/Time Settings	127
Event Management	128
Configuring Ports	131
Changing the Default GUI Language Setting	136

Network Settings

Use the Network Settings page to customize the network configuration (for example, the IP address, discovery port, and LAN interface parameters) for your LX.

There are two options available to set up your IP configuration:

- None (default) - This is the recommended option (static IP). Since the LX is part of your network infrastructure, you most likely do not want its IP address to change frequently. This option allows you to set the network parameters.
- DHCP - With this option, the IP address is automatically assigned by a DHCP server.

▶ **To change the network configuration:**

1. Choose Device Settings > Network. The Network Settings page opens.
2. Update the Network Basic Settings. See **Network Basic Settings** (on page 116).
3. Update the LAN Interface Settings. See LAN Interface Settings.
4. Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.

▶ **To reset to factory defaults:**

- Click Reset to Defaults.

Network Basic Settings

These procedures describe how to assign an IP address on the Network Settings page. For complete information about all of the fields and the operation of this page, see **Network Settings** (on page 115).

► **To assign an IP address:**

1. Choose Device Settings > Network. The Network Settings page opens.
2. Specify a meaningful Device Name for your LX device. Up to 32 alphanumeric characters using valid special characters and no spaces.
3. In the IPv4 section, enter or select the appropriate IPv4-specific network settings:
 - a. Enter the IP Address if needed. The default IP address is 192.168.0.192.
 - b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
 - c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.
 - d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.
 - e. Select the IP Auto Configuration. The following options are available:
 - None (Static IP) - This option requires that you manually specify the network parameters.

This is the recommended option because the LX is an infrastructure device and its IP address should not change.
 - DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

With this option, network parameters are assigned by the DHCP server. If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.
4. If IPv6 is to be used, enter or select the appropriate IPv6-specific network settings in the IPv6 section:
 - a. Select the IPv6 checkbox to activate the fields in the section.
 - b. Enter a Global/Unique IP Address. This is the IP address assigned to the LX.
 - c. Enter the Prefix Length. This is the number of bits used in the IPv6 address.

- d. Enter the Gateway IP Address.
- e. Link-Local IP Address. This address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present. **Read-Only**
- f. Zone ID. This identifies the device with which the address is associated. **Read-Only**
- g. Select the IP Auto Configuration. The following options are available:
 - None - Use this option if you do not want an auto IP configuration and prefer to set the IP address yourself (static IP). This is the default and recommended option.

If None is selected for the IP auto configuration, the following Network Basic Settings fields are enabled: Global/Unique IP Address, Prefix Length, and Gateway IP Address allowing you to manually set the IP configuration.
 - Router Discovery - Use this option to automatically assign IPv6 addresses that have Global or Unique Local significance beyond that of the Link Local, which only applies to a directly connected subnet.
5. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.
6. If Use the Following DNS Server Addresses is selected, regardless of whether DHCP is selected or not, the addresses entered in this section will be used to connect to the DNS server.

Enter the following information if the Following DNS Server Addresses option is selected. These addresses are the primary and secondary DNS addresses that will be used if the primary DNS server connection is lost due to an outage.

 - a. Primary DNS Server IP Address
 - b. Secondary DNS Server IP Address
7. When finished, click OK.

See LAN Interface Settings for information in configuring this section of the Network Settings page.

*Note: In some environments, the default LAN Interface Speed & Duplex setting Autodetect (autonegotiator) does not properly set the network parameters, which results in network issues. In these instances, setting the LX LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. See the **Network Settings** (on page 115) page for more information.*

Basic Network Settings

Device Name *
se-xx2-232

IPv4 Address

IP Address: 192.168.51.55
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.51.126
Preferred DHCP Host Name:
IP Auto Configuration: DHCP

IPv6 Address

Global Unique IP Address: / Prefix Length:
Gateway IP Address:
Link-Local IP Address: Zone ID: %1
IP Auto Configuration: None

Obtain DNS Server Address Automatically
 Use the Following DNS Server Addresses

Primary DNS Server IP Address: 192.168.59.2
Secondary DNS Server IP Address: 192.168.51.10

OK Reset To Defaults Cancel

LAN Interface Settings

The current parameter settings are identified in the Current LAN interface parameters field.

1. Choose Device Settings > Network. The Network Settings page opens.

2. Choose the LAN Interface Speed & Duplex from the following options:
 - Autodetect (default option)
 - 10 Mbps/Half - Both LEDs blink
 - 10 Mbps/Full - Both LEDs blink
 - 100 Mbps/Half - Yellow LED blinks
 - 100 Mbps/Full - Yellow LED blinks
 - 1000 Mbps/Full (gigabit) - Green LED blinks
 - Half-duplex provides for communication in both directions, but only one direction at a time (not simultaneously).
 - Full-duplex allows communication in both directions simultaneously.

Note: Occasionally there are problems running at 10 Mbps in either half or full duplex. If you are experiencing problems, try another speed and duplex setting.

See **Network Speed Settings** (on page 195) for more information.
3. Select the Bandwidth.
4. Click OK to apply the LAN settings.

Device Services

The Device Services page allows you to configure the following functions:

- Enable SSH access
- Enable tiering for the base LX
- Enter the discovery port
- Enable direct port access
- Enable the AKC Download Server Certificate Validation feature if you are using AKC

Enabling SSH

Enable SSH access to allow administrators to access the LX via the SSH v2 application.

► **To enable SSH access:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select Enable SSH Access.

3. Enter the SSH Port information. The standard SSH TCP port number is 22 but the port number can be changed to provide a higher level of security operations.
4. Click OK.

HTTP and HTTPS Port Settings

You are able to configure HTTP and/or HTTPS ports used by the LX. 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.

► **To change the HTTP and/or HTTPS port settings:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Enter the new ports in the HTTP Port and/or HTTPS Port fields.
3. Click OK.

Entering the Discovery Port

The LX discovery occurs over a single, configurable TCP Port. The default is Port 5000, but you can configure it to use any TCP port except 80 and 443. To access the LX from beyond a firewall, your firewall settings must enable two-way communication through the default Port 5000 or a non-default port configured here.

► **To enable the discovery port:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Enter the Discovery Port.
3. Click OK.

Configuring and Enabling Tiering

LX and generic tiering are supported by the LX. The tiering feature allows you to access LX targets through one base LX device.

Note: Base and tiered devices must all be operating with the same firmware revision.

Devices can be added and removed from a configuration as needed up to a maximum of two tiered levels.

When setting up the devices, you will use specific CIMS for specific configurations. See **Tiering - Target Types, Supported CIMS and Tiering Configurations** (on page 122) for a description of the targets that can be included in a tiered configuration, CIM compatibility and device configuration information.

Before adding tiered devices, you must enable tiering for the base device and the tiered devices. Enable base devices on the Device Settings page. Enable tiered devices on the Local Port Settings page. Once devices are enabled and configured, they appear on the Port Access page (**Port Access Page** (on page 43)).

When the LX is configured to function as a base device or tiered device, they will be displayed as:

- Configured As Base Device in the Device Information section of the left panel of the LX interface for base devices.
- Configured As Tier Device in the Device Information section of the left panel of the LX interface for tiered devices.
- The base device will be identified as Base in the left panel of the tiered device's interface under Connect User.
- Target connections to a tier port from the base will be displayed as 2 ports connected.

The base device provides remote and local access over a consolidated port list from the Port Access page. Tiered devices provide remote access from their own port lists. Local access is not available on the tiered devices when Tiering is enabled.

Port configuration, including changing the CIM name, must be done directly from each device. It cannot be done from the base device for tiered target ports.

Tiering also supports the use of KVM switches to switch between servers. See **Configuring KVM Switches** (on page 132).

Enabling Tiering

Connect from a target server port on the base device to the tier LX Local Access port video/keyboard/mouse ports using a D2CIM-DVUSB.

► To enable tiering:

1. From the tier base, choose Device Settings > Device Services. The Device Service Settings page appears.
2. Select Enable Tiering as Base.
3. In the Base Secret field, enter the secret shared between the base and the tiered devices. This secret is required for the tiered devices to authenticate the base device. You will enter the same secret word for the tiered device.
4. Click OK.
5. Enable the tiered devices. From the tiered device, choose Device Settings > Local Port Settings.
6. In the Enable Local Ports section of the page, select Enable Local Port Device Tiering.
7. In the Tier Secret field, enter the same secret word you entered for the base device on the Device Settings page.
8. Click OK.

Tiering - Target Types, Supported CIMS and Tiering Configurations

Port configuration, including changing the CIM name, must be done directly from each device. It cannot be done from the base device for tiered target ports.

Unsupported and Limited Features on Tiered Targets

The following features are not supported on tiered targets:

- Virtual media tiered devices
- MCCAT as a tiered device

Cabling Example in Tiered Configurations

The following diagram illustrates the cabling configurations between an LX tiered device and an LX base device.

Connect from a target server port on the base device to the tier LX Local Access port video/keyboard/mouse ports using a D2CIM-DVUSB.

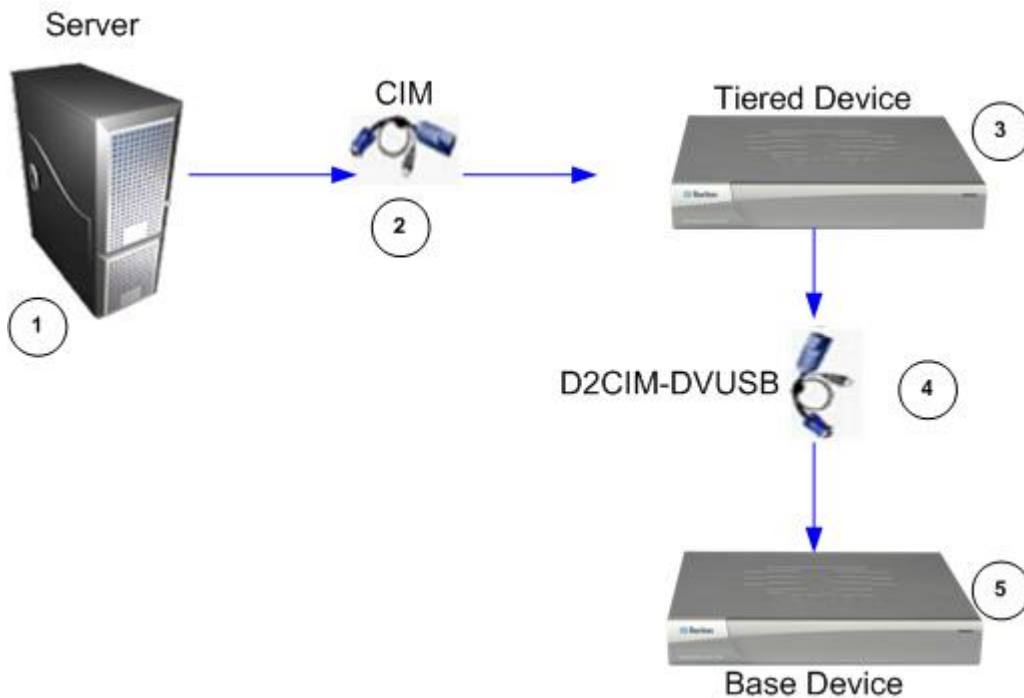


Diagram key	
1	Target server
2	CIM from target server to the LX tiered device
3	LX tiered device
4	D2CIM-DVUSB CIM from the LX tiered device to the LX base device
5	LX base device

Enabling Direct Port Access via URL

Direct port access allows users to bypass having to use the device's Login dialog and Port Access page. This feature also provides the ability to enter a username and password directly and proceed to the target if the username and password is not contained in the URL.

The following is important URL information regarding direct port access:

If you are using VKC and direct port access:

- `https://IPAddress/dpa.asp?username=username&password=password&port=port number`

If you are using AKC and direct port access:

- `https://IPAddress/dpa.asp?username=username&password=password&port=port number&client=akc`

Where:

- Username and password are optional. If they are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.
- The port may be a port number or port name. If you are using a port name, the name must be unique or an error is reported. If the port is omitted altogether, an error is reported.
- Client=akc is optional unless you are using the AKC client. If client=akc is not included, VKC is used as the client.

► **To enable direct port access:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select Enable Direct Port Access via URL if you would like users to have direct access to a target via the Dominion device by passing in the necessary parameters in the URL.
3. Click OK.

Enabling the AKC Download Server Certificate Validation

If you are using the AKC client, you can choose to use the Enable AKC Download Server Certificate Validation feature or opt not to use this feature.

Option 1: Do Not Enable AKC Download Server Certificate Validation (default setting)

If you do not enable AKC Download Server Certificate Validation, all Dominion device users must:

- 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.

Option 2: Enable AKC Download Server Certificate Validation

If you do enable AKC Download Server Certificate Validation:

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

► To install the self-signed certificate when using Windows Vista® operating system and Windows 7® operating system:

1. Include the LX IP address in the Trusted Site zone and ensure 'Protected Mode' is off.
2. Launch Internet Explorer® using the LX IP address as the URL. A Certificate Error message will be displayed.
3. Select View Certificates.
4. On the General tab, click Install Certificate. The certificate is then installed in the Trusted Root Certification Authorities store.
5. After the certificate is installed, the LX IP address should be removed from the Trusted Site zone.

► To enable AKC download server certificate validation:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select the Enable AKC Download Server Certificate Validation checkbox or you can leave the feature disabled (default).
3. Click OK.

Configuring Modem Settings

► **To configure modem settings:**

1. Click Device Settings > Modem Settings to open the Modem Settings page.
2. Select the Enable Modem checkbox. This will enable the Serial Line Speed and Modem Init String field.
3. The Serial Line Speed of the modem is set to 115200.
4. Enter the initial modem string in the Modem Init String field. If the modem string is left blank, the following string is sent to the modem by default: ATZ OK AT OK.

This information is used to configure modem settings. Because different modems have different ways of settings these values, this document does not specify how to set these values, rather the user should refer to the modem to create the appropriate modem-specific string.

- a. Modem Settings:
 - Enable RTS/CTS flow control
 - Send data to the computer on receipt of RTS
 - CTS should be configured to only drop if required by flow control.
 - DTR should be configured for Modem resets with DTR toggle.
 - DSR should be configured as always on.
 - DCD should be configured as enabled after a carrier signal is detected. (that is, DCD should only be enabled when modem connection is established with the remote side)
5. Enter the IPv4 modem server address in the Modem Server IPv4 Address field and the client modem address in the Modem Client IPv4 Address field.

Note: The modem client and server IP addresses must be on the same subnet and cannot overlap the device's LAN subnet.

- Click OK to commit your changes or click Reset to Defaults to return the settings to their defaults.

Modem Settings

Enable Modem

Serial Line Speed
115200 bits/s

Modem Init String
ATQ0&D3&C1

Modem Server IPv4 Address
10.0.0.1

Modem Client IPv4 Address
10.0.0.2

OK Reset To Defaults Cancel

See **Certified Modems** (on page 190) for information on certified modems that work with the LX. For information on settings that will give you the best performance when connecting to the LX via modem, see **Creating, Modifying and Deleting Profiles in MPC - Generation 2 Devices** in the **KVM and Serial Access Clients Guide**.

Note: Modem access directly to the LX HTML interface is not supported. You must use standalone MPC to access the LX via modem.

Configuring Date/Time Settings

Use the Date/Time Settings page to specify the date and time for the LX. There are two ways to do this:

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

► To set the date and time:

- Choose Device Settings > Date/Time. The Date/Time Settings page opens.
- Choose your time zone from the Time Zone drop-down list.
- To adjust for daylight savings time, check the "Adjust for daylight savings time" checkbox.

4. Choose the method you would like to use to set the date and time:
 - User Specified Time - Choose this option to input the date and time manually. For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).
 - Synchronize with NTP Server - Choose this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
5. For the Synchronize with NTP Server option:
 - a. Enter the IP address of the Primary Time server.
 - b. Enter the IP address of the Secondary Time server. **Optional**
6. Click OK.

Home > Device Settings > Date/Time Settings

Date/Time Settings

Time Zone
(GMT -05:00) US Eastern

Adjust for daylight savings time

User Specified Time

Date (Month, Day, Year)
May 09, 2008

Time (Hour, Minute)
10 : 18

Synchronize with NTP Server

Primary Time server
[Text Field]

Secondary Time server
[Text Field]

Event Management

The LX Event Management feature allows you enable and disable the distribution of system events to SNMP Managers, the Syslog and the audit log.

Configuring Event Management - Settings

SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. The LX offers SNMP Agent support through Event Management.

► To configure SNMP (enable SNMP logging):

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Select SNMP Logging Enabled. This enables the remaining SNMP fields.
3. In the Name, Contact, and Location fields, type the SNMP agent's name (that is, the device's name) as it appears in the LX Console interface, a contact name related to this device, and where the Dominion device is physically located.
4. Type the Agent Community String (the device's string). An SNMP community is the group to which devices and management stations running SNMP belong. It helps define where information is sent. The community name is used to identify the group. The SNMP device or agent may belong to more than one SNMP community.
5. Specify whether the community is Read-Only or Read/Write using the Type drop-down list.
6. Configure up to five SNMP managers by specifying their Destination IP/Hostname, Port # and Community.
7. Click the Click here to view the Dominion SNMP MIB link to access the SNMP Management Information Base.
8. Click OK.

► To configure the Syslog (enable Syslog forwarding):

1. Select Enable Syslog Forwarding to log the device's messages to a remote Syslog server.
2. Type the IP Address/Hostname of your Syslog server in the IP Address field.
3. Click OK.

► **To reset to factory defaults:**

- Click Reset To Defaults.

Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

Home > Device Settings > Event Management - Settings

SNMP Configuration

SNMP Logging Enabled

Name

LX

Contact

Location

Agent Community String

Type

Read-Only ▾

Destination IP/Hostname	Port #	Community
	162	public
	162	public
	162	public
	162	public
	162	public

[Click here to view the Dominion LX SNMP MIB](#)

SysLog Configuration

Enable Syslog Forwarding

IP Address/Host Name

OK

Reset To Defaults

Cancel

Configuring Ports

The Port Configuration page displays a list of the LX ports. Ports connected to KVM target servers are displayed in blue. For ports with no CIM connected or with a blank CIM name, a default port name of Dominion-LX_Port# is assigned, where Port# is the number of the LX physical port.

When a port's status is down, Not Available is displayed as its status. A port may be down when the port's CIM has removed or powered down.

After you have renamed the port, use Reset to Default at any time to return it to its default port name.

► **To access a port configuration:**

1. Choose Device Settings > Port Configuration. The Port Configuration Page opens.

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

- Port Number - Numbered from 1 to the total number of ports available for the LX device.
- Port Name - The name assigned to the port. Alternatively, rename ports that are currently not connected to the LX via a CIM and, as such, have a status of Not Available. To rename a port with a status of Not Available, do one of the following:
 - Rename the port. When a CIM is attached the CIM name will be used.
 - Rename the port, and select 'Persist name on Next CIM Insertion'. When a CIM is attached the name that has been assigned will be copied into the CIM.
 - Reset the port, including the name, to factory defaults by selecting 'Reset to Defaults'. When a CIM is attached the CIM name will be used.

Note: Do not use apostrophes for the Port (CIM) Name.

- Port Type:

- DCIM - Dominion CIM
 - Not Available - No CIM connected
 - MCUTP - Master Console MCUTP, CIM in a cable
 - PCIM - Paragon CIM
 - Dual - VM - Virtual media CIM (D2CIM-VUSB and D2CIM-DVUSB)
 - KVM Switch - Generic KVM Switch connection
2. Click the Port Name for the port you want to edit. The Port page for KVM opens.

Configuring Standard Target Servers

► **To name the target servers:**

1. Connect all of the target servers if you have not already done so. See **Step 3: Connect the Equipment** (on page 27) for a description of connecting the equipment.
2. Choose Device Settings > Port Configuration. The Port Configuration page opens.
3. Click the Port Name of the target server you want to rename. The Port Page opens.
4. Select Standard KVM Port as the subtype for the port.
5. Assign a name to identify the server connected to that port. The name can be up to 32 characters, and alphanumeric and special characters are allowed.
6. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.
7. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.
8. Click OK.

Configuring KVM Switches

The LX allows tier attachments to generic analog KVM switches supporting hot key switching. A variety of KVM hot key sequences are provided to choose from. Select one to match the hot key sequence supported on the analog KVM switch connected to via this port. That will allow targets on the tiered analog KVM switch to be accessible from a consolidated port list on the Port Access page.

Important: In order for user groups to see the KVM switch that you create, you must first create the switch and then create the group. If

an existing user group needs to see the KVM switch you are creating, you must recreate the user group.

► **To configure KVM switches:**

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name of the target server you want to rename. The Port Page opens.
3. Select KVM Switch.
4. Select the KVM Switch Model.

Note: Only one switch will appear in the drop-down.

5. Select KVM Switch Hot Key Sequence.
6. Enter the Maximum Number of Target Ports (2-32).
7. In the KVM Switch Name field, enter the name you want to use to refer to this port connection.
8. Activate the targets that the KVM switch hot key sequence will be applied to. Indicate the KVM switch ports have targets attached by selecting 'Active' for each of the ports.
9. In the KVM Managed Links section of the page, you are able to configure the connection to a web browser interface if one is available.
 - a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.
 - b. URL Name - Enter the URL to the interface.
 - c. Username - Enter the username used to access the interface.
 - d. Password - Enter the password used to access the interface.
 - e. Username Field - Enter the username parameter that will be used in the URL. For example `username=admin`, where `username` is the username field.
 - f. Password Field - Enter the password parameter that will be used in the URL. For example `password=raritan`, where `password` is the password field.
10. Click OK.

► **To change the active status of a KVM switch port or URL:**

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name of the target server you want to rename. The Port Page opens.
3. Deselect the Active checkbox next to the KVM switch target port or URL to change its active status.
4. Click OK.

Configuring LX Local Port Settings

From the Local Port Settings page, you can customize many settings for the LX Local Console including keyboard, hot keys, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

► **To configure the local port settings:**

Note: Some changes you make to the settings on the Local Port Settings page will restart the browser you are working in. If a browser restart will occur when a setting is changed, it is noted in the steps provided here.

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.
2. Select the checkbox next to the Enable Standard Local Port to enable it. Deselect the checkbox to disable it. By default, the standard local port is enabled but can be disabled as needed. The browser will be restarted when this change is made. If you are using the tiering feature, this feature will be turned off since both features cannot be used at the same time.
3. If you are using the tiering feature, select the Enable Local Port Device Tiering checkbox and enter the tiered secret word in the Tier Secret field. In order to configure tiering, you must also configure the base device on the Device Services page. See **Configuring and Enabling Tiering** (on page 121) for more information on tiering.
4. If needed, configure the Local Port Scan Mode settings. These settings apply to Scan Settings feature, which is accessed from the Port page. See **Scanning Ports** (on page 45).
 - 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.
 - In the "Interval Between Ports (10 - 255 sec):" field, specify the interval at which the device should pause between ports.

5. Choose the appropriate keyboard type from among the options in the drop-down list. The browser will be restarted when this change is made.
 - US
 - US/International
 - United Kingdom
 - French (France)
 - German (Germany)
 - JIS (Japanese Industry Standard)
 - Simplified Chinese
 - Traditional Chinese
 - Dubeolsik Hanguk (Korean)
 - German (Switzerland)
 - Portuguese (Portugal)
 - Norwegian (Norway)
 - Swedish (Sweden)
 - Danish (Denmark)
 - Belgian (Belgium)

Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for LX Local Console functions.

Note: 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.

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

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

7. Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target. You can then use the hot key to disconnect from the target and return to the local port GUI. Once the local port connect key is created, it will appear in the Navigation panel of the GUI so you can use it as a reference. See Connect Key Examples for examples of connect key sequences.
8. Set the Video Switching Delay from between 0 - 5 seconds, if necessary. Generally 0 is used unless more time is needed (certain monitors require more time to switch the video).
9. If you would like to use the power save feature:
 - a. Select the Power Save Mode checkbox.
 - b. Set the amount of time (in minutes) in which Power Save Mode will be initiated.
10. Choose the resolution for the LX Local Console from the drop-down list. The browser will be restarted when this change is made.
 - 800x600
 - 1024x768
 - 1280x1024
11. Choose the refresh rate from the drop-down list. The browser will be restarted when this change is made.
 - 60 Hz
 - 75 Hz
12. Choose the type of local user authentication.
 - Local/LDAP/RADIUS. This is the recommended option. For more information about authentication, see **Remote Authentication** (on page 33).
 - None. There is no authentication for Local Console access. This option is recommended for secure environments only.
13. Click OK.

Changing the Default GUI Language Setting

The LX GUI supports the following localized languages:

- Japanese
- Simplified Chinese
- Traditional Chinese

► **To change the GUI language:**

1. Select Device Settings > Language. The Language Settings page opens.

2. From the Language drop-down, select the language you want to apply to the GUI.
3. Click Apply. Click Reset Defaults to change back to English.

Note: Once you apply a new language, the online help is also localized to match your language selection.

Chapter 7 Security Management

In This Chapter

Security Settings.....	138
SSL Certificates.....	147

Security Settings

From the Security Settings page, you can specify login limitations, user blocking, password rules, and encryption and share settings.

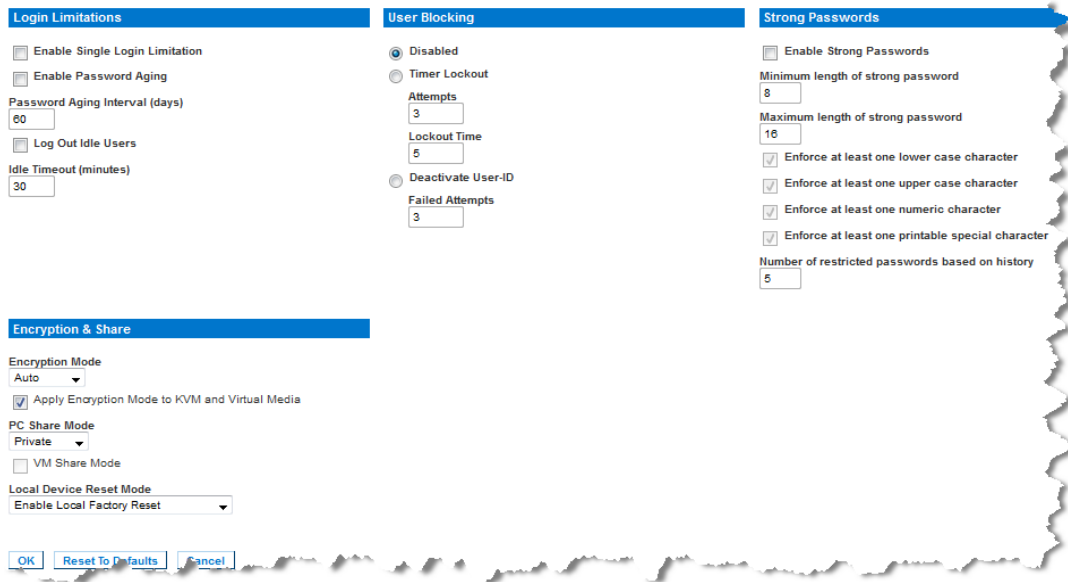
Raritan SSL certificates are used for public and private key exchanges, and provide an additional level of security. Raritan web server certificates are self-signed. Java applet certificates are signed by a VeriSign certificate. Encryption guarantees that your information is safe from eavesdropping and these certificates ensure that you can trust that the entity is Raritan, Inc.

► **To configure the security settings:**

1. Choose Security > Security Settings. The Security Settings page opens.
2. Update the **Login Limitations** (on page 139) settings as appropriate.
3. Update the **Strong Passwords** (on page 140) settings as appropriate.
4. Update the **User Blocking** (on page 142) settings as appropriate.
5. Update the **Encryption & Share** (on page 144) settings as appropriate.
6. Click OK.

► **To reset back to defaults:**

- Click Reset to Defaults.

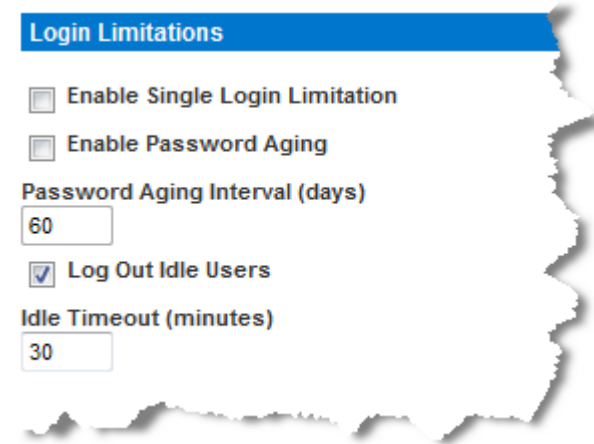


Login Limitations

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

Limitation	Description
Enable single login limitation	When selected, only one login per user name is allowed at anytime. When deselected, a given user name/password combination can be connected into the device from several client workstations simultaneously.
Enable password aging	When selected, all users are required to change their passwords periodically based on the number of days specified in Password Aging Interval field. This field is enabled and required when the Enable Password Aging checkbox is selected. Enter the number of days after which a password change is required. The default is 60 days.
Log out idle users, After (1-365 minutes)	Select the "Log off idle users" checkbox to automatically disconnect users after the amount of time you specify in the "After (1-365 minutes)" field. If there is no activity from the keyboard or mouse, all sessions and all resources are logged out. If a virtual media session is in progress,

Limitation	Description
	<p>however, the session does not timeout.</p> <p>The After field is used to set the amount of time (in minutes) after which an idle user will be logged out. This field is enabled when the Log Out Idle Users option is selected. Up to 365 minutes can be entered as the field value</p>



Strong Passwords

Strong passwords provide more secure local authentication for the system. Using strong passwords, you can specify the format of valid LX local passwords such as minimum and maximum length, required characters, and password history retention.

Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one nonalphabetical character (punctuation character or number). In addition, the first four characters of the password and the user name cannot match.

When selected, strong password rules are enforced. Users with passwords not meeting strong password criteria will automatically be required to change their password on their next login. When deselected, only the standard format validation is enforced. When selected, the following fields are enabled and required:

Field	Description
Minimum length of strong password	Passwords must be at least 8 characters long. The default is 8, but it can be up to 63.
Maximum length of strong	The default is 8 minimum and 16 the is

Field	Description
password	the default maximum.
Enforce at least one lower case character	When checked, at least one lower case character is required in the password.
Enforce at least one upper case character	When checked, at least one upper case character is required in the password.
Enforce at least one numeric character	When checked, at least one numeric character is required in the password.
Enforce at least one printable special character	When checked, at least one special character (printable) is required in the password.
Number of restricted passwords based on history	This field represents the password history depth. That is, the number of prior passwords that cannot be repeated. The range is 1-12 and the default is 5.

Strong Passwords

Enable Strong Passwords

Minimum length of strong password

8

Maximum length of strong password

16

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one printable special character

Number of restricted passwords based on history

5

User Blocking

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts.

The three options are mutually exclusive:

Option	Description
Disabled	The default option. Users are not blocked regardless of the number of times they fail authentication.

Option	Description
Timer Lockout	<p>Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled:</p> <ul style="list-style-type: none"> ▪ Attempts - The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10 and the default is 3 attempts. ▪ Lockout Time - The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes and the default is 5 minutes. <hr/> <p><i>Note: Users in the role of Administrator are exempt from the timer lockout settings.</i></p>
Deactivate User-ID	<p>When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field:</p> <ul style="list-style-type: none"> ▪ Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10. <p>When a user-ID is deactivated after the specified number of failed attempts, the administrator must change the user password and activate the user account by selecting the Active checkbox on the User page.</p>

User Blocking

- Disabled
- Timer Lockout
- Attempts
-
- Lockout Time
-
- Deactivate User-ID
- Failed Attempts
-

Encryption & Share

Using the Encryption & Share settings you can specify the type of encryption used, PC and VM share modes, and the type of reset performed when the LX Reset button is pressed.

WARNING: If you select an encryption mode that is not supported by your browser, you will not be able to access the LX from your browser.

► **To configure encryption and share:**

1. Choose one of the options from the Encryption Mode drop-down list. When an encryption mode is selected, a warning appears, stating that if your browser does not support the selected mode, you will not be able to connect to the LX. The warning states "When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the LX."

Encryption mode	Description
Auto	This is the recommended option. The LX autonegotiates to the highest level of encryption possible.
RC4	Secures user names, passwords and KVM data, including video transmissions using the RSA RC4 encryption method. This is a 128-bit Secure Sockets Layer (SSL) protocol that provides a private communications channel between the LX device and the Remote PC during initial connection authentication.
AES-128	The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. 128 is the key length. When AES-128 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See Checking Your Browser for AES Encryption (on page 146) for more information.
AES-256	The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology

Encryption mode	Description
	specification for the encryption of electronic data. 256 is the key length. When AES-256 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See Checking Your Browser for AES Encryption (on page 146) for more information.

Note: MPC will always negotiate to the highest encryption and will match the Encryption Mode setting if not set to Auto.

Note: If you are running Windows XP® operating system with Service Pack 2, Internet Explorer® 7 cannot connect remotely to the LX using AES-128 encryption.

2. Apply Encryption Mode to KVM and Virtual Media. When selected, this option applies the selected encryption mode to both KVM and virtual media. After authentication, KVM and virtual media data is also transferred with 128-bit encryption.
3. PC Share Mode. Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one LX and concurrently view and control the same target server through the device. Click the drop-down list to select one of the following options:
 - Private - No PC share. This is the default mode. Each target server can be accessed exclusively by only one user at a time.
 - PC-Share - KVM target servers can be accessed by up to eight users (administrator or non-administrator) at one time. Each remote user has equal keyboard and mouse control, however, note that uneven control will occur if one user does not stop typing or moving the mouse.
4. If needed, select VM Share Mode. This option is enabled only when PC-Share mode is enabled. When selected, this option permits the sharing of virtual media among multiple users, that is, several users can access the same virtual media session. The default is disabled.
5. If needed, select Local Device Reset Mode. This option specifies which actions are taken when the hardware Reset button (at the back of the device) is depressed. For more information, see **Resetting the LX Using the Reset Button** (on page 183). Choose one of the following options:

Local device reset mode	Description
Enable Local Factory Reset (default)	Returns the LX device to the factory defaults.

Local device reset mode	Description
Enable Local Admin Password Reset	Resets the local administrator password only. The password is reset to raritan.
Disable All Local Resets	No reset action is taken.

Checking Your Browser for AES Encryption

The LX supports AES-256. If you do not know if your browser uses AES, check with the browser manufacturer or navigate to the <https://www.fortify.net/sslcheck.html> website using the browser with the encryption method you want to check. This website detects your browser's encryption method and displays a report.

Note: Internet Explorer® 6 does not support AES 128 or 256-bit encryption.

AES 256 Prerequisites and Supported Configurations

AES 256-bit encryption is supported on the following web browsers only:

- Firefox® 2.0.0.x and 3.0.x (and later)
- Internet Explorer 7 and 8

In addition to browser support, AES 256-bit encryption requires the installation of Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files.

Jurisdiction files for various JREs™ are available at the “other downloads” section of the following link:

- JRE1.6 - http://java.sun.com/javase/downloads/index_jdk5.jsp

SSL Certificates

The LX uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. When establishing a connection, the LX has to identify itself to a client using a cryptographic certificate.

It is possible to generate a Certificate Signing Request (CSR) and install a certificate signed by the Certificate Authority (CA) on the LX. The CA verifies the identity of the originator of the CSR. The CA then returns a certificate containing its signature to the originator. The certificate, bearing the signature of the well-known CA, is used to vouch for the identity of the presenter of the certificate.

Note: The CSR must be generated on the LX.

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

1. Select Security > SSL Certificate.
2. Complete the following fields:
 - a. Common name - The network name of the LX once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the LX with a web browser but without the prefix "http://". In case the name given here and the actual network name differ, the browser will pop up a security warning when the LX is accessed using HTTPS.
 - b. Organizational unit - This field is used for specifying to which department within an organization the LX belongs.
 - c. Organization - The name of the organization to which the LX belongs.
 - d. Locality/City - The city where the organization is located.
 - e. State/Province - The state or province where the organization is located.
 - f. Country (ISO code) - The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.
 - g. Challenge Password - Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimum length of this password is four characters.
 - h. Confirm Challenge Password - Confirmation of the Challenge Password.
 - i. Email - The email address of a contact person that is responsible for the LX and its security.

- j. Key length - The length of the generated key in bits. 1024 is the default.
 - k. Select the Create a Self-Signed Certificate checkbox (if applicable).
3. Click Create to generate the Certificate Signing Request (CSR).

► **To download a CSR certificate:**

1. The CSR and the file containing the private key used when generating it can be downloaded by clicking Download.

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

2. Send the saved CSR to a CA for certification. You will get the new certificate from the CA.

► **To upload a CSR:**

1. Upload the certificate to the LX by clicking Upload.

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

Certificate Signing Request (CSR)	Certificate Upload
<p>The following CSR is pending:</p> <pre>countryName = US stateOrProvinceName = DC localityName = Washington organizationName = ACME Corp. organizationalUnitName = Marketing Dept. commonName = John Doe emailAddress = johndoe@acme.com</pre>	<p>SSL Certificate File</p> <input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Download"/> <input type="button" value="Delete"/>	<input type="button" value="Upload"/>

After completing these three steps the LX has its own certificate that is used for identifying the card to its clients.

Important: If you destroy the CSR on the LX there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above. To avoid this, use the download function so you will have a copy of the CSR and its private key.

Chapter 8 Maintenance

In This Chapter

Audit Log.....	149
Device Information.....	150
Backup and Restore	151
Upgrading CIMs.....	153
Upgrading Firmware	153
Upgrade History.....	155
Rebooting the LX.....	155

Audit Log

A log is created of the LX system events. The audit log can contain up to approximately 2K worth of data before it starts overwriting the oldest entries. To avoid losing audit log data, export the data to a syslog server or SNMP manager. Configure the syslog server or SNMP manager from the Device Settings > Event Management page. See **Events Captured in the Audit Log and Syslog** (on page 194) for information on what is captured in the audit log and syslog.

► **To view the audit log for your LX:**

1. Choose Maintenance > Audit Log. The Audit Log page opens.

The Audit Log page displays events by date and time (most recent events listed first). The Audit Log provides the following information:

- Date - The date and time that the event occurred based on a 24-hour clock.
- Event - The event name as listed in the Event Management page.
- Description - Detailed description of the event.

► **To save the audit log:**

Note: Saving the audit log is available only on the LX Remote Console, not on the Local Console.

1. Click Save to File. A Save File dialog appears.
2. Choose the desired file name and location and click Save. The audit log is saved locally on your client machine with the name and location specified.

► **To page through the audit log:**

- Use the [Older] and [Newer] links.

Device Information

The Device Information page provides detailed information about your LX device and the CIMs in use. This information is helpful should you need to contact Raritan Technical Support.

► **To view information about your LX and CIMs:**

- Choose Maintenance > Device Information. The Device Information page opens.

The following information is provided about the LX:

- Model
- Hardware Revision
- Firmware Version
- Serial Number
- MAC Address

The following information is provided about the CIMs in use:

- Port (number)
- Name
- Type of CIM - DCIM or VM
- Firmware Version
- Serial Number of the CIM - this number is pulled directly from the supported CIMs.

Note: Only the numeric portion of the serial numbers are displayed for the DCIM-USB, DCIM-PS2 and DCIM-USB G2 CIMs. For example, XXX1234567 is displayed. The serial number prefix GN is displayed for CIMs that have field configured serial numbers.

Device Information

Model: DLX-116
Hardware Revision: 0x10
Firmware Version: 2.4.5.1.79
Serial Number: HKK1600002
MAC Address: 00:0d:5d:00:01:96

CIM Information

▲ Port	Name	Type	Firmware Version	Serial Number
4	FC15	Dual-VM	3A88	GN000D5D01339E3C3D3F6D70666936
8	FC11	Dual-VM	3A88	PQ21010199
13	Dominion_LX_Port13	MCUTP	N/A	N/A
16	DominionLX	Dual-VM	3A88	PQ28450291

Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your LX.

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

► **To access the Backup/Restore page:**

- Choose Maintenance > Backup/Restore. The Backup/Restore page opens.

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

► **If you are using Firefox® or Internet Explorer® 5 or earlier, to backup your LX:**

1. Click Backup. A File Download dialog appears.
2. Click Save. A Save As dialog appears.
3. Choose the location, specify a file name, and click Save. A Download Complete dialog appears.
4. Click Close. The backup file is saved locally on your client machine with the name and location specified.

► **If you are using Internet Explorer 6 or later, to backup your LX:**

1. Click Backup. A File Download dialog appears that contains an Open button. Do not click Open.

In IE 6 (and later), IE is used as the default application to open files, so you are prompted to open the file versus save the file. To avoid this, you must change the default application that is used to open files to WordPad®.

2. To do this:
 - a. Save the backup file. The backup file is saved locally on your client machine with the name and location specified.
 - b. Once saved, locate the file and right-click on it. Select properties.
 - c. In general tab, click Change and select WordPad.

► **To restore your LX:**

WARNING: Exercise caution when restoring your LX to an earlier version. Usernames and password in place at the time of the backup will be restored. If you do not remember the old administrative usernames and passwords, you will be locked out of the LX.

In addition, if you used a different IP address at the time of the backup, that IP address will be restored as well. If the configuration uses DHCP, you may want to perform this operation only when you have access to the local port to check the IP address after the update.

1. Choose the type of restore you want to run:
 - Full Restore - A complete restore of the entire system. Generally used for traditional backup and restore purposes.
 - Protected Restore - Everything is restored except device-specific information such as IP address, name, and so forth. With this option, you can setup one LX and copy the configuration to multiple LX devices.
 - Custom Restore - With this option, you can select User and Group Restore, Device Settings Restore, or both:
 - User and Group Restore - This option includes only user and group information. This option *does not* restore the certificate and the private key files. Use this option to quickly set up users on a different LX.
 - Device Settings Restore - Use this option to quickly copy the device information.
2. Click Browse. A Choose File dialog appears.
3. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.

4. Click Restore. The configuration (based on the type of restore selected) is restored.

Upgrading CIMs

Use this procedure to upgrade CIMs using the firmware versions stored in the memory of your LX device. In general, all CIMs are upgraded when you upgrade the device firmware using the Firmware Upgrade page.

Note: Only D2CIM-VUSB and D2CIM-DVUSB can be upgraded from this page.

► **To upgrade CIMs using the LX memory:**

1. Choose Maintenance > CIM Firmware Upgrade. The CIM Upgrade from page opens.
The Port (number), Name, Type, Current CIM Version, and Upgrade CIM Version are displayed for easy identification of the CIMs.
2. Check the Selected checkbox for each CIM you want to upgrade.
3. Click Upgrade. You are prompted to confirm the upgrade.
4. Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes or less per CIM.

Upgrading Firmware

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

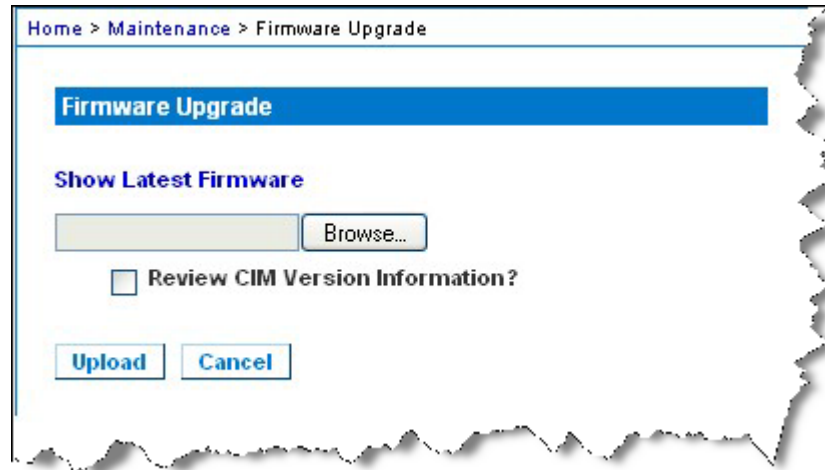
Important: Do not turn off your LX unit or disconnect CIMs while the upgrade is in progress - doing so will likely result in damage to the unit or CIMs.

► **To upgrade your LX unit:**

1. Locate the appropriate Raritan firmware distribution file (*.RFP) on the **Raritan website <http://www.raritan.com>** on the Firmware Upgrades web page.
2. Unzip the file. Please read all instructions included in the firmware ZIP files carefully before upgrading.

Note: Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.

3. Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens.



4. Click Browse to navigate to the directory where you unzipped the upgrade file.
5. Select the Review CIM Version Information? checkbox if you would like information displayed about the versions of the CIMs in use.
6. Click Upload from the Firmware Upgrade page. Information about the upgrade and version numbers is displayed for your confirmation (if you opted to review CIM information, that information is displayed as well):

Note: At this point, connected users are logged out, and new login attempts are blocked.

7. Click Upgrade. Please wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the unit reboots (1 beep sounds to signal that the reboot has completed).

As prompted, close the browser and wait approximately 5 minutes before logging in to the LX again.

For information about upgrading the device firmware using the Multi-Platform Client, see **Upgrading Device Firmware** in the **KVM and Serial Access Clients Guide**.

Note: Firmware upgrades are not supported via modem.

Upgrade History

The LX provides information about upgrades performed on the LX and attached CIMS.

► **To view the upgrade history:**

- Choose Maintenance > Upgrade History. The Upgrade History page opens.

Information is provided about the LX upgrade(s) that have been run, the final status of the upgrade, the start and end times, and the previous and current firmware versions. Information is also provided about the CIMS, which can be obtained by clicking the show link for an upgrade. The CIM information provided is:

- Type - The type of CIM
- Port - The port where the CIM is connected
- User - The user who performed the upgrade
- IP - IP address firmware location
- Start Time - Start time of the upgrade
- End Time - end time of the upgrade
- Previous Version - Previous CIM firmware version
- Upgrade Version - Current CIM firmware version
- CIMS - Upgraded CIMS
- Result - The result of the upgrade (success or fail)

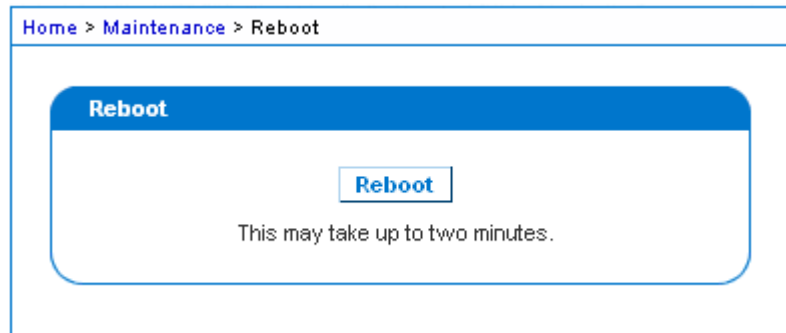
Rebooting the LX

The Reboot page provides a safe and controlled way to reboot your LX. This is the recommended method for rebooting.

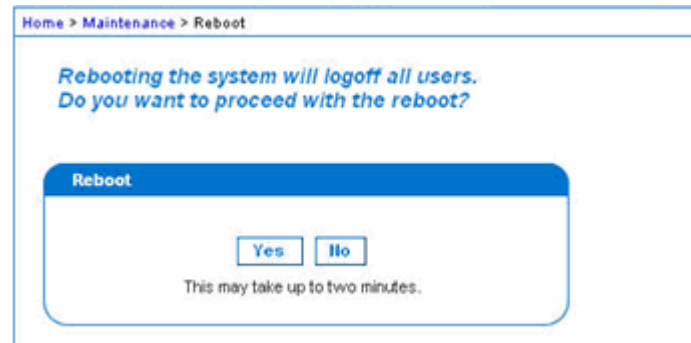
Important: All KVM and serial connections will be closed and all users will be logged off.

► **To reboot your LX:**

1. Choose Maintenance > Reboot. The Reboot page opens.



2. Click Reboot. You are prompted to confirm the action. Click Yes to proceed with the reboot.



Chapter 9 Diagnostics

In This Chapter

Network Interface Page	157
Network Statistics Page.....	158
Ping Host Page.....	160
Trace Route to Host Page.....	160
Device Diagnostics	161

Network Interface Page

The LX provides information about the status of your network interface.

► **To view information about your network interface:**

- Choose Diagnostics > Network Interface. The Network Interface page opens.

The following information is displayed:

- Whether the Ethernet interface is up or down.
- Whether the gateway is pingable or not.
- The LAN port that is currently active.

► **To refresh this information:**

- Click Refresh.

Network Interface

Refresh

Result:

```
Link state: autonegotiation on, 100 Mbps, full duplex, link ok
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0d:5d:ca:b1:f8 brd ff:ff:ff:ff:ff:ff
inet 192.168.51.101/24 brd 192.168.51.255 scope global eth0
LAN 1 is active.
```

Network Statistics Page

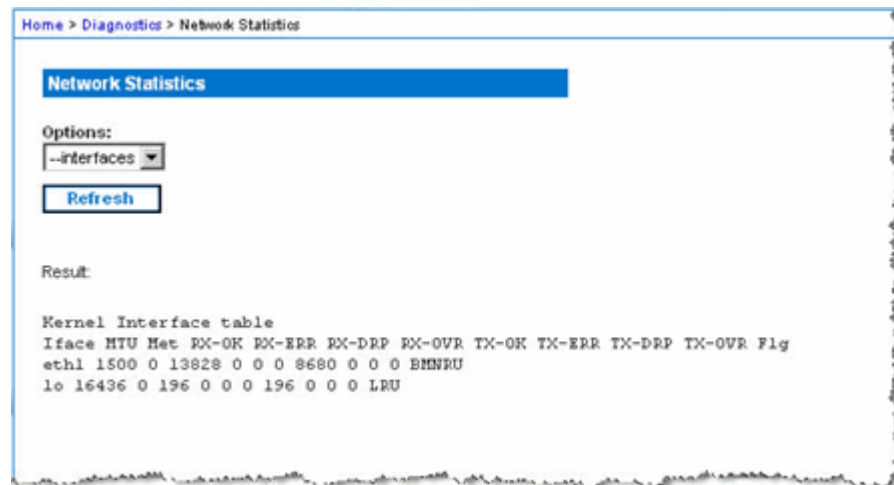
The LX provides statistics about your network interface.

► **To view statistics about your network interface:**

1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
2. Choose the appropriate option from the Options drop-down list:
 - Statistics - Produces a page similar to the one displayed here.



- Interfaces - Produces a page similar to the one displayed here.



Home > Diagnostics > Network Statistics

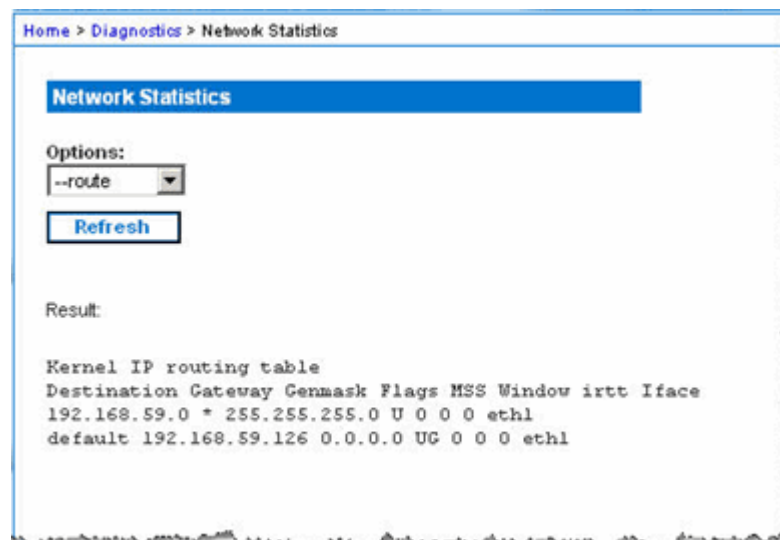
Network Statistics

Options:

Result:

```
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1 1500 0 13828 0 0 0 8680 0 0 0 BMNRU
lo 16436 0 196 0 0 0 196 0 0 0 LRU
```

- Route - Produces a page similar to the one displayed here.



Home > Diagnostics > Network Statistics

Network Statistics

Options:

Result:

```
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.59.0 * 255.255.255.0 U 0 0 0 eth1
default 192.168.59.126 0.0.0.0 UG 0 0 0 eth1
```

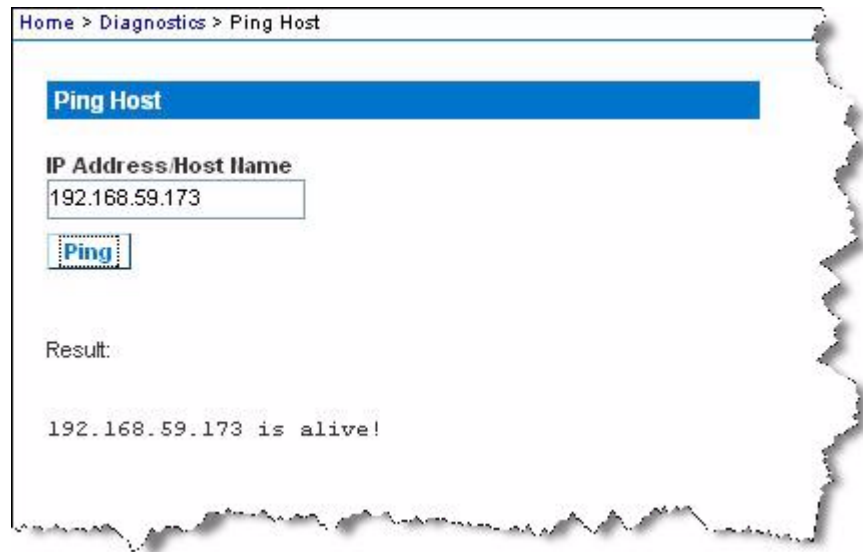
3. Click Refresh. The relevant information is displayed in the Result field.

Ping Host Page

Ping is a network tool used to test whether a particular host or IP address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another LX is accessible.

► **To ping the host:**

1. Choose Diagnostics > Ping Host. The Ping Host page appears.



2. Type either the hostname or IP address into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Click Ping. The results of the ping are displayed in the Result field.

Trace Route to Host Page

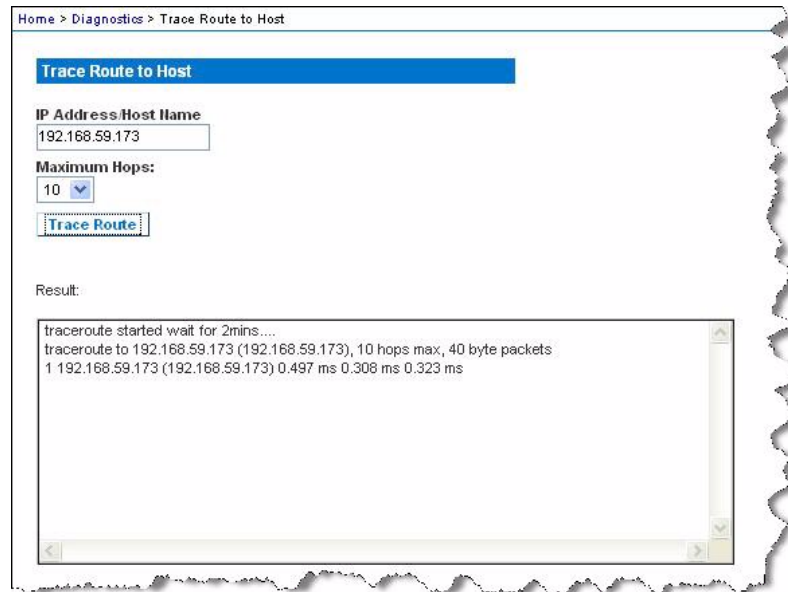
Trace route is a network tool used to determine the route taken to the provided hostname or IP address.

► **To trace the route to the host:**

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens.
2. Type either the IP address or host name into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Choose the maximum hops from the drop-down list (5 to 50 in increments of 5).
4. Click Trace Route. The trace route command is executed for the given hostname or IP address and the maximum hops. The output of trace route is displayed in the Result field.



Device Diagnostics

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

Device diagnostics downloads the diagnostics information from the LX to the client machine. Two operations can be performed on this page:

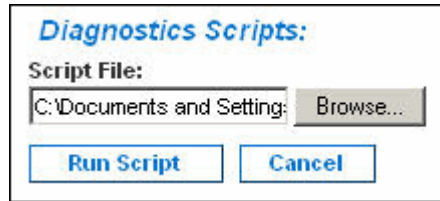
- Execute a special diagnostics script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the device and executed. Once this script has been executed, you can download the diagnostics messages using the Save to File function.
 - Download the device diagnostic log for a snapshot of diagnostics messages from the LX device to the client. This encrypted file is then sent to Raritan Technical Support. Only Raritan can interpret this file.
-

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

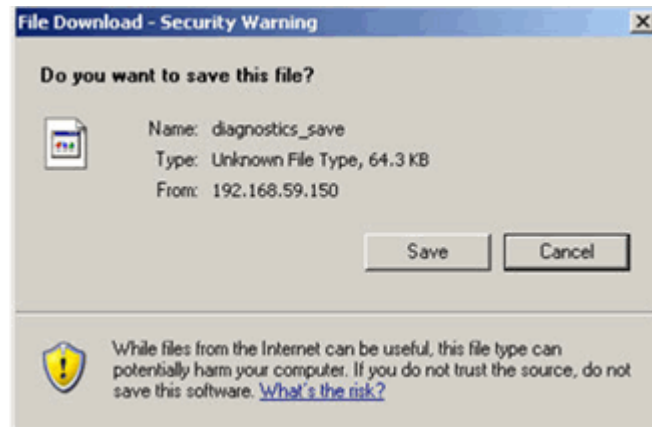
► **To run the LX System diagnostics:**

1. Choose Diagnostics > LX Diagnostics. The LX Diagnostics page opens.

2. To execute a diagnostics script file emailed to you from Raritan Technical Support:
 - a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.
 - b. Click Browse. A Choose File dialog box opens.
 - c. Navigate to and select the diagnostic file.
 - d. Click Open. The file is displayed in the Script File field.



- e. Click Run Script. Send this file to Raritan Technical Support.
3. To create a diagnostics file to send to Raritan Technical Support:
 - a. Click Save to File. The File Download dialog opens.



- b. Click Save. The Save As dialog box opens.
 - c. Navigate to the desired directory and click Save.
 - d. Email this file as directed by Raritan Technical Support.

Chapter 10 Command Line Interface (CLI)

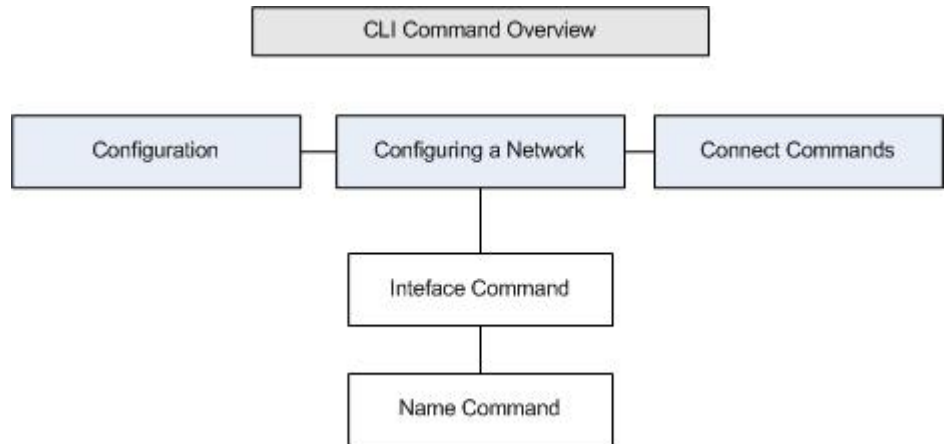
In This Chapter

Overview.....	163
Accessing the LX Using CLI.....	164
SSH Connection to the LX.....	164
Logging In.....	165
Navigation of the CLI.....	165
Initial Configuration Using CLI.....	167
CLI Prompts.....	168
CLI Commands.....	168
Administering the LX Console Server Configuration Commands.....	169
Configuring Network.....	169

Overview

The Command Line Interface (CLI) can be used to configure the LX network interface and perform diagnostic functions provided you have the appropriate permissions to do so.

The following figures describe an overview of the CLI commands. See **CLI Commands** (on page 168) for a list of all the commands, which include definitions and links to the sections in this chapter that give examples of these commands.



The following common commands can be used from all levels of the CLI to the preceding figure: top, history, log off, quit, show, and help.

Accessing the LX Using CLI

Access the LX by using one of the following methods:

- SSH (Secure Shell) via IP connection

A number of SSH clients are available and can be obtained from the following locations:

- Putty - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- SSH Client from ssh.com - www.ssh.com <http://www.ssh.com>
- Applet SSH Client - www.netbeans.org/ssh
<http://www.netbeans.org/ssh>
- OpenSSH Client - www.openssh.org <http://www.openssh.org>

SSH Connection to the LX

Use any SSH client that supports SSHv2 to connect to the LX. You must enable SSH access from the Devices Services page.

Note: For security reasons, SSH V1 connections are not supported by the LX.

SSH Access from a Windows PC

► **To open an SSH session from a Windows® PC:**

1. Launch the SSH client software.
2. Enter the IP address of the LX server. For example, 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click Open.

The `login as:` prompt appears.

See **Logging In** (on page 165).

SSH Access from a UNIX/Linux Workstation

► **To open an SSH session from a UNIX®/Linux® workstation and log in as the user admin, enter the following command:**

```
ssh -l admin 192.168.30.222
```

The Password prompt appears.

See **Logging In** (on page 165).

Logging In

► **To log in, enter the user name admin as shown:**

1. Log in as `admin`
2. The Password prompt appears. Enter the default password: `raritan`
The welcome message displays. You are now logged on as an administrator.

After reviewing the following **Navigation of the CLI** (on page 165) section, perform the Initial Configuration tasks.

Navigation of the CLI

Before using the CLI, it is important to understand CLI navigation and syntax. There are also some keystroke combinations that simplify CLI use.

Completion of Commands

The CLI supports the completion of partially-entered commands. After entering the first few characters of an entry, press the Tab key. If the characters form a unique match, the CLI will complete the entry.

- If no match is found, the CLI displays the valid entries for that level.
- If multiple matches are found, the CLI displays all valid entries.

Enter additional text to make the entry unique and press the Tab key to complete the entry.

CLI Syntax -Tips and Shortcuts

Tips

- Commands are listed in alphabetical order.
- Commands are not case sensitive.
- Parameter names are single word without underscore.
- Commands without arguments default to show current settings for the command.
- Typing a question mark (?) after a command produces help for that command.
- A pipe symbol (|) indicates a choice within an optional or required set of keywords or arguments.

Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter to execute the command.
- Press Tab to complete a command. For example, `Admin Port > Conf.` The system then displays the `Admin Port > Config >` prompt.

Common Commands for All Command Line Interface Levels

Following are the commands that are available at all CLI levels. These commands also help navigate through the CLI.

Commands	Description
top	Return to the top level of the CLI hierarchy, or the “username” prompt.
history	Display the last 200 commands the user entered into the LX CLI.
help	Display an overview of the CLI syntax.
quit	Places the user back one level.
logout	Logs out the user session.

Initial Configuration Using CLI

*Note: These steps, which use the CLI, are optional since the same configuration can be done via KVM. See **Getting Started** (on page 13) for more information.*

LX devices come from the factory with default factory settings. When you first power up and connect to the device, you must set the following basic parameters so the device can be accessed securely from the network:

1. Reset the administrator password. All LX devices are shipped with the same default password. Therefore, to avoid security breaches it is imperative that you change the admin password from raritan to one customized for the administrators who will manage the LX device.
2. Assign the IP address, subnet mask, and gateway IP address to allow remote access.

Setting Parameters

To set parameters, you must be logged on with administrative privileges. At the top level, you will see the "Username" > prompt, which for the initial configuration is "admin". Enter the top command to return to the top menu level.

Note: If you have logged on with a different user name, that user name will appear instead of admin.

Setting Network Parameters

Network parameters are configured using the interface command.

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1
mode auto
```

When the command is accepted, the device automatically drops the connection. You must reconnect to the device using the new IP address and the user name and password you created in the resetting factory default password section.

Important: If the password is forgotten, the LX will need to be reset to the factory default from the Reset button on the back of the LX. The initial configuration tasks will need to be performed again if this is done.

The LX now has the basic configuration and can be accessed remotely via SSH, GUI, or locally using the local serial port. The administrator needs to configure the users and groups, services, security, and serial ports to which the serial targets are attached to the LX.

CLI Prompts

The Command Line Interface prompt indicates the current command level. The root portion of the prompt is the login name. For a direct admin serial port connection with a terminal emulation application, Admin Port is the root portion of a command.

```
admin >
```

For SSH, admin is the root portion of the command:

```
admin > config > network >
```

0

CLI Commands

- Enter `admin > help`.

Command	Description
config	Change to config sub menu.
diagnostics	Change to diag sub menu.
help	Display overview of commands.
history	Display the current session's command line history.
listports	List accessible ports.
logout	Logout of the current CLI session.
top	Return to the root menu.
userlist	List active user sessions.

- Enter `admin > config > network`.

Command	Description
help	Display overview of commands.
history	Display the current session's command line history.
interface	Set/get network parameters.
ipv6_interface	Set/get IPv6 network parameters.
logout	Logout of the current CLI session.
name	Device name configuration.
quit	Return to previous menu.
stop	Return to the root menu.

Security Issues

Elements to consider when addressing security for console servers:

- Encrypting the data traffic sent between the operator console and the LX device.
- Providing authentication and authorization for users.
- Security profile.

The LX supports each of these elements; however, they must be configured prior to general use.

Administering the LX Console Server Configuration Commands

Note: CLI commands are the same for SSH and Local Port access sessions.

The Network command can be accessed in the Configuration menu for the LX.

Configuring Network

The network menu commands are used to configure the LX network adapter.

Commands	Description
interface	Configure the LX device network interface.
name	Network name configuration

Commands	Description
ipv6	Set/get IPv6 network parameters.

Interface Command

The Interface command is used to configure the LX network interface. The syntax of the interface command is:

```
interface [ipauto <none|dhcp>] [ip <ipaddress>]
[mask <subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)
ip <ipaddress> IP Address
mask <subnetmask> Subnet Mask
gw <ipaddress> Gateway IP Address
mode <mode> Set Ethernet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Interface Command Example

The following command enables the interface number 1, sets the IP address, mask, and gateway addresses, and sets the mode to auto detect.

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12
mode auto
```

Name Command

The name command is used to configure the network name. The syntax of the name is:

```
name [devicename <devicename>] [hostname <hostname>]
```

Device name configuration

```
devicename <devicename>    Device Name
hostname    <hostname>     Preferred host name (DHCP
only)
```

Name Command Example

The following command sets the network name:

```
Admin > Config > Network > name devicename My-KSX2
```

IPv6 Command

Use the IPv6_command to set IPv6 network parameters and retrieve existing IPv6 parameters.

Chapter 11 LX Local Console

In This Chapter

Overview.....	172
Simultaneous Users	172
LX Local Console Interface: LX Devices	173
Security and Authentication.....	173
Supported Video Resolutions - Local Console.....	174
Port Access Page (Local Console Server Display)	174
Accessing a Target Server	175
Scanning Ports - Local Console	176
Hot Keys and Connect Keys.....	177
Special Sun Key Combinations	178
Returning to the LX Local Console Interface.....	179
Local Port Administration.....	179
Resetting the LX Using the Reset Button.....	183

Overview

The LX provides at-the-rack access and administration via its local port, which features a browser-based graphical user interface for quick, convenient switching between servers. The LX Local Console provides a direct analog connection to your connected servers, which provides the same performance as if you were directly connected to the server's keyboard, mouse, and video ports. The LX Local Console provides the same administrative functionality as the LX Remote Console.

Simultaneous Users

The LX Local Console provides an independent access path to the connected KVM target servers. Using the Local Console does not prevent other users from simultaneously connecting over the network. And even when remote users are connected to the LX, you can still simultaneously access your servers from the rack via the Local Console.

LX Local Console Interface: LX Devices

When you are located at the server rack, the LX provides standard KVM management and administration via the LX Local Console. The LX Local Console provides a direct KVM (analog) connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports.

There are many similarities among the LX Local Console and the LX Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

The LX Local Console Factory Reset option is available in the LX Local Console but not the LX Remote Console.

Security and Authentication

In order to use the LX Local Console, you must first authenticate with a valid username and password. The LX provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port. In either case, the LX allows access only to those servers to which a user has access permissions. See **User Management** (on page 94) for additional information on specifying server access and security settings.

If your LX has been configured for external authentication services (LDAP/LDAPS, RADIUS, or Active Directory), authentication attempts at the Local Console also are authenticated against the external authentication service.

Note: You can also specify no authentication for Local Console access; this option is recommended only for secure environments.

► **To use the LX Local Console:**

1. Connect a keyboard, mouse, and video display to the local ports at the back of the LX.
2. Start the LX. The LX Local Console interface displays.

Supported Video Resolutions - Local Console

Ensure that each target server's video resolution and refresh rate are supported by the LX and that the signal is noninterlaced.

The LX Local Console provides the following resolutions to support various monitors:

- 800x600
- 1024x768
- 1280x1024

Each of these resolutions supports a refresh rate of 60Hz and 75Hz.

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. See **Target Server Connection Distance and Video Resolution** (on page 190).

Port Access Page (Local Console Server Display)

After you login to the LX Local Console, the Port Access page opens. This page lists all of the LX ports, the connected KVM target servers, and their status and availability.

If you are using a tiered configuration in which a base LX device is used to access multiple other tiered devices, the tiered devices are viewed on the Port Access page by clicking on the Expand Arrow icon ► to the left of the tier device name. See **Configuring and Enabling Tiering** (on page 121) for more information on tiering.

► To use the Port Access page:

1. Log in to the Local Console.
2. Click the Port Access tab. The Port Access page opens.

The KVM target servers are initially sorted by Port Number. You can change the display to sort on any of the columns.

- Port Number - Numbered from 1 to the total number of ports available for the LX device.
- Port Name - The name of the LX port. Initially, this is set to Dominion-LX-Port# but you can change the name to something more descriptive. When you click a Port Name link, the Port Action Menu appears.

Note: Do not use apostrophes for the Port (CIM) Name.

- Type - The type of server or CIM.
- Status - The status for standard servers is either up or down.

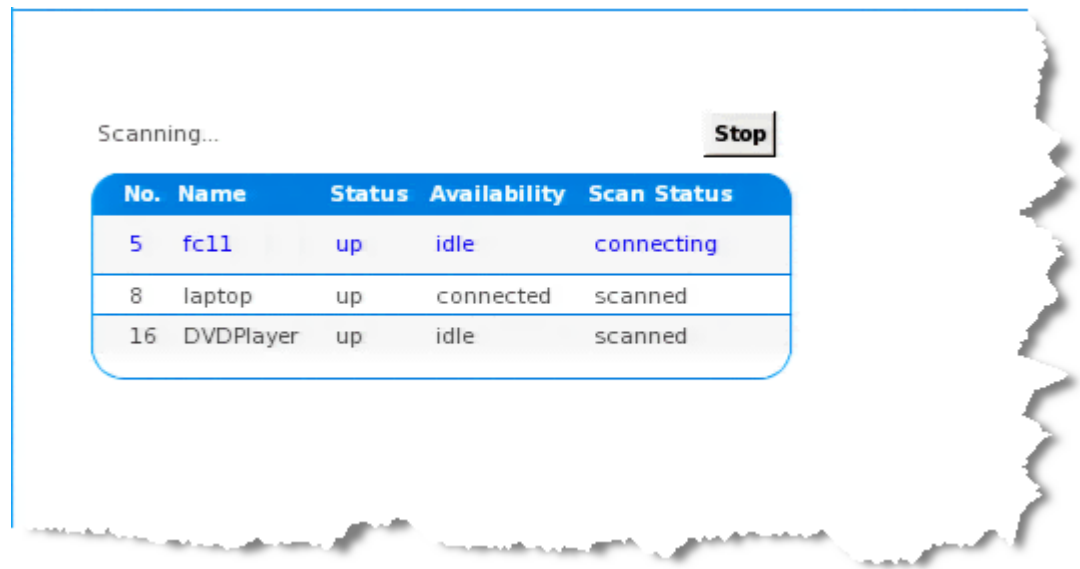
- Availability - The availability of the server.
3. Click the Port Name of the target server you want to access. The Port Action Menu appears. See Port Action Menu for details on available menu options.
 4. Choose the desired menu command from the Port Action Menu.
- ▶ **To change the display sort order 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.

Accessing a Target Server

- ▶ **To access a target server:**
1. Click the Port Name of the target you want to access. The Port Action Menu is displayed.
 2. Choose Connect from the Port Action menu. The video display switches to the target server interface.

Scanning Ports - Local Console

The LX scanning feature is supported by the Local Console. The targets that are found during the scan are displayed on the Scan page one at a time, which is different from the Remote Console port slide show. Each target is displayed on the page for 10 seconds by default, allowing you to view the target and connect to it. Use the Local Port ConnectKey sequence to connect to a target when it is displayed and the DisconnectKey sequence to disconnect from the target.



► To scan for targets:

1. From the Local Console, click the Set Scan tab on the Port Access page.
2. Select the targets you want to include in the scan by selecting the checkbox to the left of each target, or select the checkbox at the top of the target column to select all targets.
3. Leave the Up Only checkbox selected if you only want targets that are up to be included in the scan. Deselect this checkbox if you want to include all targets, whether up or down.
4. Click Scan to begin the scan. A Port Scan window opens. As each target is found, it is displayed in the window.
5. Connect to a target when it is displayed by using the ConnectKey sequence.
6. Click Stop Scan to stop the scan.

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.

▶ 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.

Hot Keys and Connect Keys

Because the LX Local Console interface is completely replaced by the interface for the target server you are accessing, a hot key is used to disconnect from a target and return to the local port GUI. A connect key is used to connect to a target or switch between targets.

The Local Port hot key allows you to rapidly access the LX Local Console user interface when a target server is currently being viewed. The default is to press the Scroll Lock key twice in rapid succession, but you can designate another key combination (available in the Local Port Settings page) as the hot key. See [Configuring LX Local Console Local Port Settings](#) for more information.

Connect Key Examples
Standard servers

Connect key action	Key sequence example
Access a port from the local port GUI	Access port 5 from the local port GUI: <ul style="list-style-type: none"> Press Left ALT > Press and Release 5 > Release Left ALT
Switch between ports	Switch from target port 5 to port 11: <ul style="list-style-type: none"> Press Left ALT > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port GUI	Disconnect from target port 11 and return to the local port GUI (the page from which you connected to target): <ul style="list-style-type: none"> Double Click Scroll Lock

Special Sun Key Combinations

The following key combinations for Sun™ Microsystems server's special keys operate on the local port. These special are available from the Keyboard menu when you connect to a Sun target server:

Sun key	Local port key combination
Again	Ctrl+ Alt +F2
Props	Ctrl + Alt +F3
Undo	Ctrl + Alt +F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Mute	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *

Sun key	Local port key combination
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	No key combination
Power	No key combination

Returning to the LX Local Console Interface

Important: The LX Local Console default hot key is to press the Scroll Lock key twice rapidly. This key combination can be changed in the Local Port Settings page. See [Configuring LX Local Port Settings from the Local Console](#).

- ▶ **To return to the LX Local Console from the target server:**
 - Press the hot key twice rapidly (the default hot key is Scroll Lock). The video display switches from the target server interface to the LX Local Console interface.

Local Port Administration

The LX can be managed by either the LX Local Console or the LX Remote Console. Note that the LX Local Console also provides access to:

- Factory Reset
- Local Port Settings(available in the Remote Console, as well)

Note: Only users with administrative privileges can access these functions.

Configuring LX Local Console Local Port Settings

From the Local Port Settings page, you can customize many settings for the LX Local Console including keyboard, hot keys, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

Note: Only users with administrative privileges can access these functions.

► **To configure the local port settings:**

Note: Some changes you make to the settings on the Local Port Settings page will restart the browser you are working in. If a browser restart will occur when a setting is changed, it is noted in the steps provided here.

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.
2. Select the checkbox next to the Enable Standard Local Port to enable it. Deselect the checkbox to disable it. By default, the standard local port is enabled but can be disabled as needed. If you are using the tiering feature, this feature will be turned off since both features cannot be used at the same time.
3. If you are using the tiering feature, select the Enable Local Port Device Tiering checkbox and enter the tiered secret word in the Tier Secret field. In order to configure tiering, you must also configure the base device on the Device Services page. See **Configuring and Enabling Tiering** (on page 121) for more information on tiering.
4. If needed, configure the Local Port Scan Mode settings. These settings apply to Scan Settings feature, which is accessed from the Port page. See **Scanning Ports** (on page 45).
 - 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.
 - In the "Interval Between Ports (10 - 255 sec):" field, specify the interval at which the device should pause between ports.
5. Choose the appropriate keyboard type from among the options in the drop-down list. The browser will be restarted when this change is made.
 - US
 - US/International
 - United Kingdom
 - French (France)
 - German (Germany)

- JIS (Japanese Industry Standard)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangeul (Korean)
- German (Switzerland)
- Portuguese (Portugal)
- Norwegian (Norway)
- Swedish (Sweden)
- Danish (Denmark)
- Belgian (Belgium)

Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for LX Local Console functions.

Note: 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.

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

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

7. Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target. You can then use the hot key to disconnect from the target and return to the local port GUI. Once the local port connect key is created, it will appear in the Navigation panel of the GUI so you can use it as a reference. See Connect Key Examples for examples of connect key sequences.
8. Click OK.

LX Local Console Factory Reset

Note: This feature is available only on the LX Local Console.

The LX offers several types of reset modes from the Local Console user interface.

*Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, see **Audit Log** (on page 149).*

► **To perform a factory reset:**

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.
2. Choose the appropriate reset option from the following options:
 - Full Factory Reset - Removes the entire configuration and resets the device completely to the factory defaults. Note that any management associations with CommandCenter will be broken. Because of the complete nature of this reset, you will be prompted to confirm the factory reset.
 - Network Parameter Reset - Resets the network parameters of the device back to the default values (click Device Settings > Network Settings to access this information):
 - IP auto configuration
 - IP address
 - Subnet mask
 - Gateway IP address
 - Primary DNS server IP address
 - Secondary DNS server IP address
 - Discovery port
 - Bandwidth limit
 - LAN interface speed & duplex
3. Click Reset to continue. You will be prompted to confirm the factory reset because all network settings will be permanently lost.
4. Click OK proceed. Upon completion, the LX device is automatically restarted.

Resetting the LX Using the Reset Button

On the back panel of the device, there is a Reset button. It is recessed to prevent accidental resets (you will need a pointed object to press this button).

The actions that are performed when the Reset button is pressed are defined in the graphical user interface. See **Encryption & Share** (on page 144).

*Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged on the audit log. For more information about saving the audit log, see **Audit Log** (on page 149).*

► **To reset the device:**

1. Power off the LX.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the LX device back on.
4. Continue holding the Reset button for 10 seconds. Once the device has been reset, two short beeps signal that the reset is complete.



Appendix A Specifications

In This Chapter

LX Specifications	184
LED Indicators	186
Supported Operating Systems (Clients).....	186
Supported Browsers	187
Supported CIMS and Operating Systems	188
Supported Video Resolutions.....	189
Certified Modems	190
Remote Connection.....	190
Supported Keyboard Languages.....	191
TCP and UDP Ports Used.....	193
Events Captured in the Audit Log and Syslog.....	194
Network Speed Settings.....	195

LX Specifications

Dominion LX Model	Description	Product Dimension (WxDxH), Shipping Weight and Power	Environment
DLX-108	Economical, extensible 8-port KVM-over-IP switch, 1 remote, 1 local user, virtual media, single power and single LAN	11.45" x 10.63 " x1.73 " ; 291 mm x 270mm x 44mm 8.82 lbs ; 4.0kg	Operating Temperature: 0° – 40° C (32° – 104° F) Humidity: 20% – 85% RH
DLX-116	Economical, extensible 16-port KVM-over-IP switch, 1 remote, 1 local user, virtual media, single power and single LAN	Single Power 100-240V AC, 50-60Hz, 0.5A, 30 Watts, 25.794 kcal/h	
DLX-216	Economical, extensible 16-port KVM-over-IP switch, 2 remote, 1 local user, virtual media, single power and single LAN		

Hardware Supported	
Form Factor	1U, rack mountable (brackets included)
Local Access Port	Video: HD15(F) VGA; Keyboard/Mouse : USB(F); 3 USB rear
Sample Video Resolutions	PC text mode: 640x350, 640x480, 720x400 PC graphic mode: 640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1440x900, 1680x1050, 1600x1200, 1920x1080 Sun video mode: 1024x768, 1152x864, 1152x900, 1280x1024
Remote Connection	
Ports	8(DLX-108) or 16 (DLX-116, DLX-216)
Users	Local user; 1 or 2 remote users (model dependent)
Network	Single 10/100/1000 gigabit Ethernet access, dual-stack: IPv4 and IPv6
Protocols	TCP/IP; HTTP; HTTPS; UDP; RADIUS; SNMP; DHCP; PAP; CHAP
Computer Interface Modules (CIMs) and Cat5 Cables	
Dominion CIMs	Available for USB, Dual USB, Universal Virtual Media/Absolute Mouse Synchronization, PS2, Sun, Serial Devices Dimensions (WxDxH) = 1.7" x 3.5" x 0.8"; 43mm x 90mm x 19mm (Dual USB) and 1.3" x 3.0" x 0.6"; 33mm x 76mm x 15mm (other DCIMs)
Cat5 MCUTP Cables	KVM UTP cable for PS/2, USB, Sun – lengths from 0.6m (2 ft.) – 6m (20 ft.). Specifications: RJ45 <-> HDB-15M, mini-din 6 x 2 (PS/2), USB type A (USB/Sun)
Service and Support	
Warranty	Two years standard with advanced replacement

LED Indicators

Front Panel LED

- Boot-up - Blue and Red LED = ON
- Operational - Solid blue
- Firmware upgrade - Blue LED blinks

Rear Panel LED

- 10 Mbps/Half - Both LEDs blink
- 10 Mbps/Full - Both LEDs blink
- 100 Mbps/Half - Yellow LED blinks
- 1 Gbps/Full - Green LED blinks

Supported Operating Systems (Clients)

The following operating systems are supported on the Virtual KVM Client and Multi-Platform Client (MPC):

Client operating system	Virtual media (VM) support on client?
Windows 7®	Yes
Windows XP®	Yes
Windows 2008®	Yes
Windows Vista®	Yes
Windows 2000® SP4 Server	Yes
Windows 2003® Server	Yes
Windows 2008® Server	Yes
Red Hat® Desktop 5.0	Yes
Red Hat Desktop 4.0	Yes
Open SUSE 10, 11	Yes
Fedora® 13 and 14	Yes
Mac® OS	Yes
Solaris™	No
Linux®	Yes

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®	<ul style="list-style-type: none"> Internet Explorer® 6.0 SP1+ or 7.0, IE 8 Firefox® 1.06 - 3
	Windows Server 2003®	<ul style="list-style-type: none"> Internet Explorer 6.0 SP1++, IE 7, IE 8 Firefox 1.06 - 3
	Windows Vista®	<ul style="list-style-type: none"> Internet Explorer 7.0 or 8.0
	Windows 7®	<ul style="list-style-type: none"> Internet Explorer 9.0 Firefox 1.06 - 3
Windows x64 64-bit mode	Windows XP	64bit OS, 32bit browsers:
	Windows XP Professional®	<ul style="list-style-type: none"> Internet Explorer 6.0 SP1+, 7.0 or 8.0 Firefox 1.06 - 3
	Windows XP Tablet®	
	Windows Vista	64bit mode, 64bit browsers:
	Windows Server 2003	<ul style="list-style-type: none"> Internet Explorer 7.0 or 8.0
	Windows Server 2008	
	Windows 7	

Supported Browsers

LX supports the following browsers:

- Internet Explorer® 6 through 9
- Firefox® 1.5, 2.0, 3.0 (up to build 3.6.17) and 4.0
- Safari® 3 or later

Supported CIMs and Operating Systems

In addition to the D2CIMs, most Dominion CIMs are supported. The following table displays the supported target server operating systems, CIMs, virtual media, and mouse modes.

Note: D2CIM-VUSB is not supported on Sun™ (Solaris™) targets.

Supported LX D2CIMs	Target server and remote rack PDUs (where applicable)	Virtual media	Absolute Mouse mode	Intelligent Mouse mode	Standard Mouse mode
D2CIM-VUSB	<ul style="list-style-type: none"> • Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora Core 3 and above • Mac OS 	✓	✓	✓	✓
	<ul style="list-style-type: none"> • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 	✓		✓	✓
D2CIM-DVUSB	<ul style="list-style-type: none"> • Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS 	✓	✓	✓	✓

Supported LX D2CIMs	Target server and remote rack PDUs (where applicable)	Virtual media	Absolute Mouse mode	Intelligent Mouse mode	Standard Mouse mode
	<ul style="list-style-type: none"> Red Hat Enterprise Linux 4 ES Red Hat Enterprise Linux 5 	✓		✓	✓

Supported Video Resolutions

Ensure that each target server's video resolution and refresh rate are supported by the LX and that the signal is noninterlaced.

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. See **Target Server Connection Distance and Video Resolution** (on page 190).

The LX supports these resolutions:

Resolutions	
640x350 @70Hz	1024x768@85
640x350 @85Hz	1024x768 @75Hz
640x400 @56Hz	1024x768 @90Hz
640x400 @84Hz	1024x768 @100Hz
640x400 @85Hz	1152x864 @60Hz
640x480 @60Hz	1152x864 @70Hz
640x480 @66.6Hz	1152x864 @75Hz
640x480 @72Hz	1152x864 @85Hz
640x480 @75Hz	1152x870 @75.1Hz
640x480 @85Hz	1152x900 @66Hz
720x400 @70Hz	1152x900 @76Hz
720x400 @84Hz	1280x720@60Hz
720x400 @85Hz	1280x960 @60Hz
800x600 @56Hz	1280x960 @85Hz
800x600 @60Hz	1280x1024 @60Hz
800x600 @70Hz	1280x1024 @75Hz
800x600 @72Hz	1280x1024 @85Hz
800x600 @75Hz	1360x768@60Hz

Resolutions	
800x600 @85Hz	1366x768@60Hz
800x600 @90Hz	1368x768@60Hz
800x600 @100Hz	1400x1050@60Hz
832x624 @75.1Hz	1440x900@60Hz
1024x768 @60Hz	1600x1200 @60Hz
1024x768@70	1680x1050@60Hz
1024x768@72	1920x1080@60Hz

Target Server Connection Distance and Video Resolution

The maximum supported distance is a function of many factors including the type/quality of the Cat5 cable, server type and manufacturer, video driver and monitor, environmental conditions, and user expectations. For the 1600x1200 and 1920x1080 video resolutions, the refresh rate is 60 and the maximum connection distance is 50 ft. (15 m).

Note: Due to the multiplicity of server manufacturers and types, OS versions, video drivers, and so forth and the subjective nature of video quality, Raritan cannot guarantee performance across all distances in all environments.

See the **Supported Video Resolutions** (on page 13) for the video resolutions supported by the LX.

Certified Modems

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

Remote Connection

Remote connection	Details
Network	10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet

Remote connection	
	Details
Protocols	TCP/IP, UDP, SNMP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Supported Keyboard Languages

The LX provides keyboard support for the languages listed in the following table.

*Note: You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for the LX Local Console functions. For more information about non-US keyboards, see **Informational Notes** (on page 205).*

Note: Raritan strongly recommends that you use system-config-keyboard to change languages if you are working in a Linux environment.

Language	Regions	Keyboard layout
US English	United States of America and most of English-speaking countries: for example, Canada, Australia, and New Zealand.	US Keyboard layout
US English International	United States of America and most of English-speaking countries: for example, Netherlands	US Keyboard layout
UK English	United Kingdom	UK layout keyboard
Chinese Traditional	Hong Kong S. A. R., Republic of China (Taiwan)	Chinese Traditional
Chinese Simplified	Mainland of the People's Republic of China	Chinese Simplified
Korean	South Korea	Dubeolsik Hanguk
Japanese	Japan	JIS Keyboard
French	France	French (AZERTY) layout keyboard.
German	Germany and Austria	German keyboard (QWERTZ layout)
French	Belgium	Belgian
Norwegian	Norway	Norwegian
Danish	Denmark	Danish

Appendix A: Specifications

Language	Regions	Keyboard layout
Swedish	Sweden	Swedish
Hungarian	Hungary	Hungarian
Slovenian	Slovenia	Slovenian
Italian	Italy	Italian
Spanish	Spain and most Spanish speaking countries	Spanish
Portuguese	Portugal	Portuguese

TCP and UDP Ports Used

Port	Description
HTTP, Port 80	This port can be configured as needed. See HTTP and HTTPS Port Settings (on page 120). By default, all requests received by the LX via HTTP (port 80) are automatically forwarded to HTTPS for complete security. The LX responds to Port 80 for user convenience, relieving users from having to explicitly type in the URL field to access the LX, while still preserving complete security.
HTTPS, Port 443	This port can be configured as needed. See HTTP and HTTPS Port Settings (on page 120). By default, this port is used for multiple purposes, including the web server for the HTML client, the download of client software (MPC/VKC) onto the client's host, and the transfer of KVM and virtual media data streams to the client.
LX (Raritan KVM-over-IP) Protocol, Configurable Port 5000	This port is used to discover other Dominion devices and for communication between Raritan devices and systems. By default, this is set to Port 5000, but you may configure it to use any TCP port not currently in use. For details on how to configure this setting, see Network Settings (on page 115).
SNTP (Time Server) on Configurable UDP Port 123	The LX offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation. Optional
LDAP/LDAPS on Configurable Ports 389 or 636	If the LX is configured to remotely authenticate user logons via the LDAP/LDAPS protocol, ports 389 or 636 will be used, but the system can also be configured to use any port of your designation. Optional
RADIUS on Configurable Port 1812	If the LX is configured to remotely authenticate user logons via the RADIUS protocol, either port 1812 will be used, but the system can also be configured to use any port of your designation. Optional
RADIUS Accounting on Configurable Port 1813	If the LX is configured to remotely authenticate user logons via the RADIUS protocol, and also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation will be used to transfer log notifications.
SYSLOG on Configurable UDP Port 514	If the LX is configured to send messages to a Syslog server, then the indicated port(s) will be used for communication - uses UDP Port 514.
SNMP Default UDP Ports	Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps. Optional
TCP Port 21	Port 21 is used for the LX command line interface (when you are working with Raritan Technical Support).

Events Captured in the Audit Log and Syslog

Following is a list of the events that are captured by the LX audit log and syslog:


- System Startup
- System Shutdown
- Network Parameter Changed
- Port Status Changed
- Network Failure
- Communication Error
- Factory Reset
- Device Update Started
- Device Update Completed
- Device Update Failed
- Firmware Update Failed
- Firmware File Discarded
- Firmware Validation Failed
- Configuration Backed Up
- Configuration Restored
- Port Connection Denied
- Active USB Profile
- Certificate Update
- Date/Time Settings Changed
- Password Settings Changed
- Login Failed
- Password Changed
- User Blocked
- Port Connected
- Port Disconnected
- Access Login
- Access Logout
- Connection Lost
- Session Timeout
- VM Image Connected
- VM Image Disconnected
- CIM Update Started

- CIM Update Completed
- CIM Connected
- CIM Disconnected
- Duplicate CIM Serial
- Forced User Logout
- Scan Started
- Scan Stopped
- User Added
- User Changed
- User Deleted
- Group Added
- Group Changed
- Group Deleted


Network Speed Settings

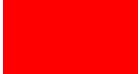
LX network speed setting						
Network switch port setting	Auto	1000/Full	100/Full	100/Half	10/Full	10/Half
Auto	Highest Available Speed	1000/Full	LX: 100/Full Switch: 100/Half	100/Half	LX: 10/Full Switch: 10/Half	10/Half
1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
100/Full	LX: 100/Half Switch: 100/Full	LX: 100/Half Switch: 100/Full	100/Full	LX: 100/Half Switch: 100/Full	No Communication	No Communication
100/Half	100/Half	100/Half	LX: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
10/Full	LX: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	LX: 10/Half Switch: 10/Full
10/Half	10/Half	No Communication	No Communication	No Communication	LX: 10/Full Switch: 10/Half	10/Half


Legend:

 Does not function as expected

 Supported

 Functions; not recommended

 NOT supported by Ethernet specification; product will communicate, but collisions will occur

 Per Ethernet specification, these should be “no communication,” however, note that the LX behavior deviates from expected behavior

Note: For reliable network communication, configure the LX and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure both the LX and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100MB/s/Full.

Appendix B Updating the LDAP Schema

Note: The procedures in this chapter should be attempted only by experienced users.

In This Chapter

Returning User Group Information	197
Setting the Registry to Permit Write Operations to the Schema	198
Creating a New Attribute	198
Adding Attributes to the Class	199
Updating the Schema Cache.....	201
Editing rcusergroup Attributes for User Members	201

Returning User Group Information

Use the information in this section to return User Group information (and assist with authorization) once authentication is successful.

From LDAP/LDAPS

When an LDAP/LDAPS authentication is successful, the LX determines the permissions for a given user based on the permissions of the user's group. Your remote LDAP server can provide these user group names by returning an attribute named as follows:

rcusergroup attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user group information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

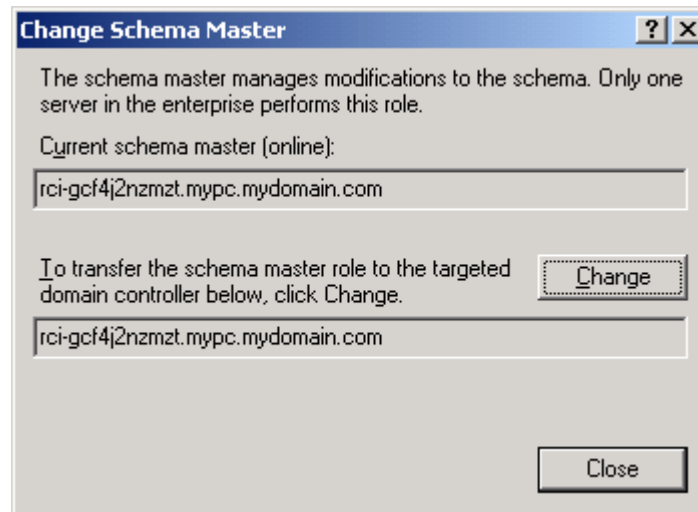
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

► **To permit write operations to the schema:**

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.



2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

Creating a New Attribute

► **To create new attributes for the rcigroup class:**

1. Click the + symbol before Active Directory® Schema in the left pane of the window.
2. Right-click Attributes in the left pane.

- Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

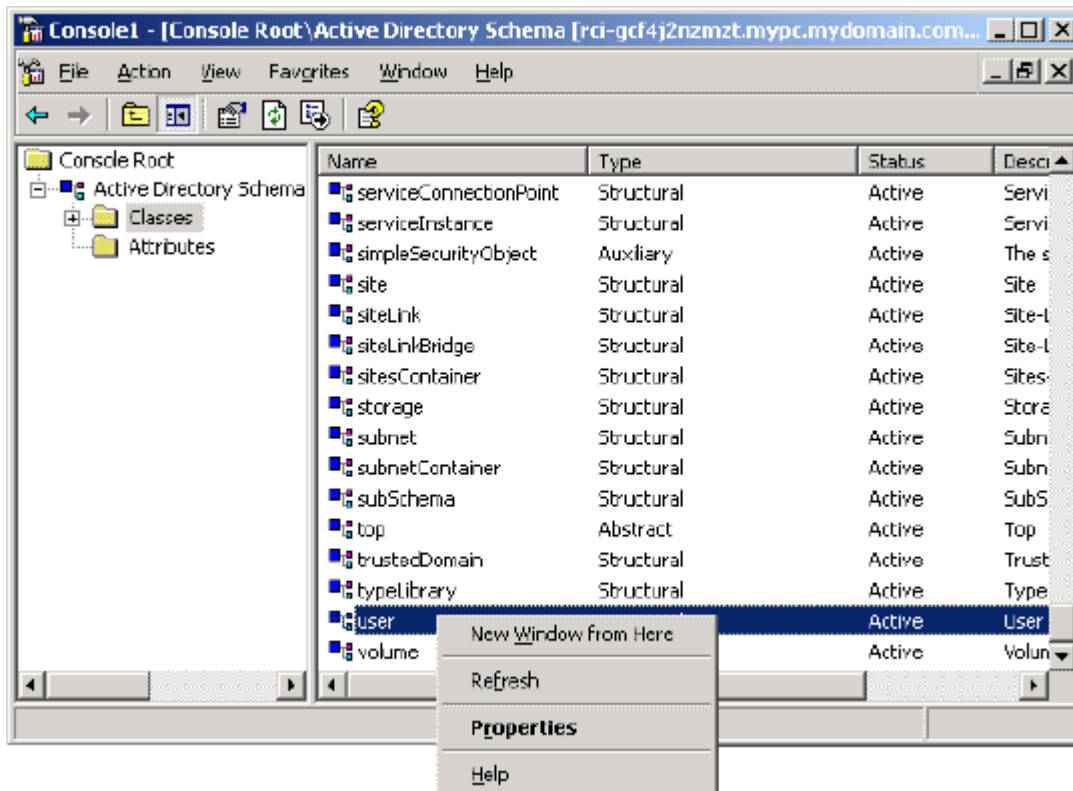
- Type *rciusergroup* in the Common Name field.
- Type *rciusergroup* in the LDAP Display Name field.
- Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
- Type a meaningful description in the Description field.
- Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
- Type *1* in the Minimum field.
- Type *24* in the Maximum field.
- Click OK to create the new attribute.

Adding Attributes to the Class

► **To add attributes to the class:**

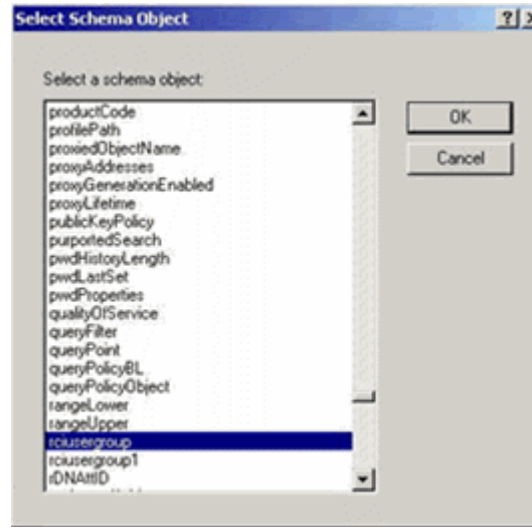
- Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.

- Choose rcusergroup from the Select Schema Object list.



- Click OK in the Select Schema Object dialog.
- Click OK in the User Properties dialog.

Updating the Schema Cache

► **To update the schema cache:**

- Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
- Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

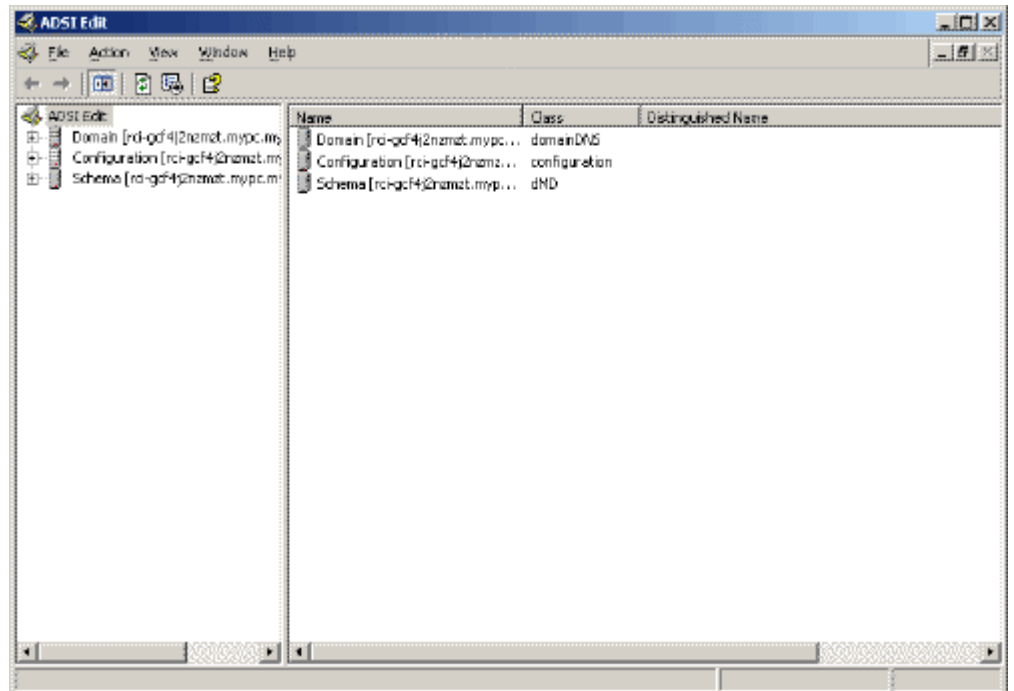
Editing rcusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

► **To edit the individual user attributes within the group rcusergroup:**

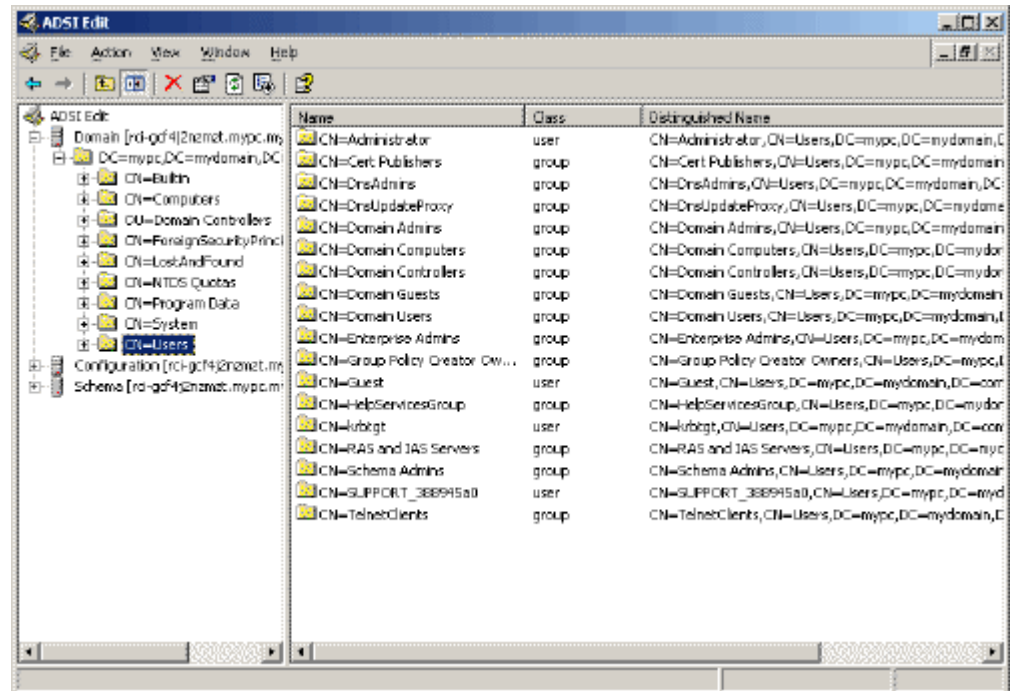
- From the installation CD, choose Support > Tools.
- Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run `adsiedit.msc`. The ADSI Edit window opens.



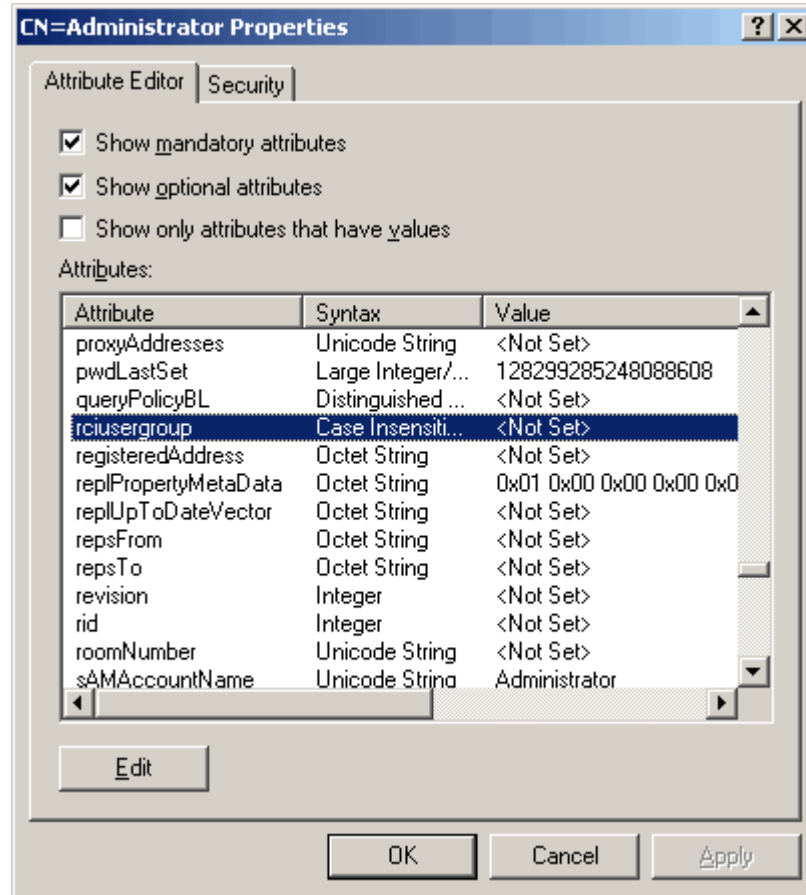
4. Open the Domain.

- In the left pane of the window, select the CN=Users folder.

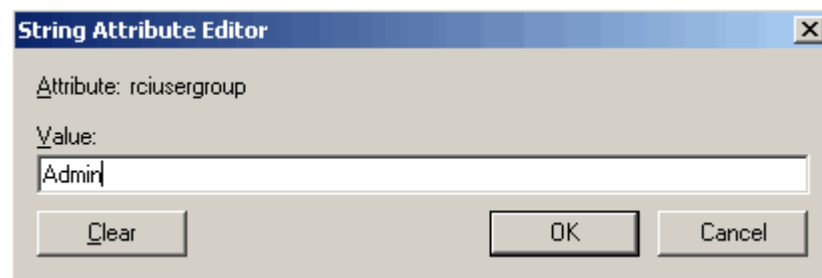


- Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

- Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



- Click Edit. The String Attribute Editor dialog appears.
- Type the user group (created in the LX) in the Edit Attribute field. Click OK.



Appendix C Informational Notes

In This Chapter

Overview	205
Java Runtime Environment (JRE)	205
IPv6 Support Notes	206
Keyboards	207
Fedora	210
Video Modes and Resolutions.....	211
VM-CIMs and DL360 USB Ports	211
MCUTP	212
Virtual Media.....	213
CIMs	215

Overview

This section includes important notes on LX usage. Future updates will be documented and available online through the Help link in the LX Remote Console interface.

Note: Some topics in this section reference other multiple Raritan devices because various devices are impacted by the information.

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 1.6 for optimum performance, but the Remote Console and MPC will 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

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)

Java 5.0 and above supports the IPv6 for the following:

- Solaris 10 (and later)
- Linux kernel 2.1.2 (and later), kernel 2.4.0 (and later) recommended for better IPv6 support
- Windows XP® SP1 and Windows 2003®, Windows Vista® operating systems

The following IPv6 configurations *are not* supported by Java:

- J2SE 1.4 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.

Mac Leopard

- IPv6 is not supported in KX II version 2.0.20 for Mac® Leopard®.

Samba

- IPv6 is not supported for use with virtual media when using Samba.

Keyboards

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.

Macintosh Keyboard

When a Macintosh® 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

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.

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 libnjp2.so Java™ plug-in on the server.

Video Modes and Resolutions

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 LX, 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 will be used and will correspond exactly with the VESA video mode timing, resulting in the proper video display on the LX.

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.

VM-CIMs and DL360 USB Ports

HP® DL360 servers have one USB port on the back of the device and another on the front of the device. With the DL360, both ports cannot be used at the same time. Therefore, a dual VM-CIM cannot be used on DL360 servers.

However, as a workaround, a USB2 hub can be attached to the USB port on the back of the device and a dual VM-CIM can be attached to the hub.

MCUTP

The serial number and CIM name provided on the MCUTP are not stored in the device. As such, MCUTP ports behave differently than others. Specifically:

- No storage of name on the CIM, port name is a label associated with the port as long as the port type doesn't change because a different CIM type is connected to it
- Power associations cannot be made to ports of this type
- Target Settings cannot be applied to ports of this type
- The serial number will be shown as 'N/A' on displays showing CIM serial number or in log entries
- Ports of this type cannot be associated with Port Groups
- Ports of this type cannot be associated with Connect Scripts

Virtual Media

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: <ul style="list-style-type: none"> • Fixed drives and fixed drive partitions • Removable drives • CD/DVD drives • ISO images • Remote ISO images 	Access to: <ul style="list-style-type: none"> • Removable drives • CD/DVD drives • ISO images • Remote ISO images

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
 - Windows FAT and NTFS 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.

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.

Active System Partitions

You cannot mount active system partitions from a Mac or 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
- Windows FAT and NTFS 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.

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.

Mac and Linux Locked, Mapped Drives

Mapped drives from Mac® and 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), which provides support for Mac and Linux.

Accessing Virtual Media on a Windows 2000 Server Using a D2CIM-VUSB

A virtual media local drive cannot be accessed on a Windows 2000® server using a D2CIM-VUSB.

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.

CIMs

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.

MCUTP CIM Behavior

There is no storage of CIM serial number or CIM name provided on the MCUTP, so ports with this type behave different than other CIMS, specifically:

- The CIM name is not stored
- The port name is a label associated with the port as long as the port type doesn't change because a different CIM type is connected to it
- Target Settings cannot be applied to ports of this type
- The serial number will be shown as 'N/A' on displays showing CIM serial number or in log entries

Appendix D Frequently Asked Questions

In This Chapter

LX FAQs	218
---------------	-----

Chapter 12

LX FAQs

Question	Answer
What is the Dominion LX?	The Dominion LX is a family of economical KVM-over-IP switches with single power, single LAN and virtual media. Targeted towards small and midsize businesses with less than 75 servers under management, they provide BIOS-level, IP control of 8 or 16 servers with one or two user remote access.
Can you describe the typical LX customer?	The typical customer, usually an IT administrator or software developer/tester, works for a small or midsize business that needs full-featured, remote KVM-over-IP access at an economical price. LX customers want productivity-enhancing features such as virtual media, Absolute Mouse Synchronization™ and common remote and local user interfaces.
What's so special about the Dominion LX?	The LX provides a full-featured, high-quality KVM-over-IP switch at an affordable price. Unlike other products in its price range, it supports productivity-enhancing features such as virtual media, Absolute Mouse Synchronization and a common browser-based user interface.
What types of IT equipment can the LX manage?	LX can manage computer and serially-controlled equipment, including computer servers and equipment, telecommunications gear and networking devices.
What types of remote management functions are supported?	Dominion LX provides reliable, out-of-band, remote management. This includes BIOS-level KVM-over-IP control, remote virtual media and optional modem access. LX provides anytime, anywhere remote management, regardless of the target device's state. You can enter at the BIOS level, run hardware diagnostics, reboot a hung server, install software from DVDs and even reimage a server – all from a remote location.
How does the Dominion LX compare to the competition?	The competition is typically an entry-level KVM-over-IP switch with limited features and an old-school OSD user interface. The competition lacks standard features such as virtual media, Absolute Mouse Synchronization, 1920x1080 remote video resolution and standard security features.

Question	Answer
What is the LX's value proposition?	<p>A high-quality KVM-over-IP switch, at an economy price, for the IT and development staffs of small and midsize businesses.</p> <p>The LX's value proposition is based on anytime/anywhere, remote access and control of servers and other IT devices.</p> <p>LX customers benefit from:</p> <ul style="list-style-type: none"> • Reduced travel expenses • Increased productivity • Decreased mean time to repair • Higher quality services
Technical Questions	
What LX models are available?	The Dominion LX family includes three KVM-over-IP models. The DLX-108 is an 8-port switch supporting one remote user session and one local user. The DLX-116 is a 16-port switch supporting one remote user session and one local user. The DLX-216 is a 16-port switch supporting two remote user sessions and one local user.
What are the hardware features?	The Dominion LX has a 1U-sized, compact case with 8 or 16 server ports, single power supply, single gigabit LAN, USB-based local port with optional modem access.
How does the Dominion LX compare to the Dominion KX II?	<p>The Dominion KX II is Raritan's, top-of-the line, enterprise-class, secure KVM-over-IP switch. With models supporting up to 64 remote servers and up to 8 remote users, the KX II is targeted at enterprise and midsize customers managing hundreds or even thousands of servers. The Dominion KX II is the industry's most reliable and secure switch, featuring dual power supplies, dual LAN, FIPS 140-2 encryption module and smart card/CAC authentication.</p> <p>The Dominion LX is a family of economical KVM-over-IP switches targeted towards small and midsize businesses with less than 75 servers to manage. The LX provides BIOS-level, IP control of 8 or 16 servers with one or two user remote access.</p>

Question	Answer
<p>What are the standard features of the Dominion LX?</p>	<p>Standard Dominion LX features include:</p> <ul style="list-style-type: none"> • Virtual media • Absolute Mouse Synchronization • Common browser-based remote/local user interface • 1920x1080 remote video resolution • Local and remote authentication (LDAP/AD/Radius) • Port and administrator permissions • Dual stack IPv6/IPv4 • Port scanning and thumbnail views • Tiering (cascading) with other LX switches • Modem access • Basic security features <p>See the Dominion LX Features and Benefits document for more information.</p>
<p>What KX II features are not available in the LX?</p>	<p>The following KX II features are not available in the LX:</p> <ul style="list-style-type: none"> • CommandCenter® Secure Gateway (CC-SG) centralized management • Mobile access via iPad® and iPhone® (CC-SG required) • Blade server support • Digital audio over IP • FIPS 140-2 encryption module • Smart card/CAC support • Secure login banner • Integrated remote power control • Dual monitor and KVM client launch options
<p>What CIMs (server dongles) can the LX use?</p>	<p>The Dominion LX can use: (1) the standard and virtual media Dominion CIMs, (2) the economical MCUTP cable-CIMs, and (3) the P2CIM-SER serial CIMs.</p>
<p>What is a MCUTP cable-CIM, and why would I want one?</p>	<p>For customers who don't plan to use virtual media or Absolute Mouse Synchronization, MCUTP cable-CIMs provide an economical alternative to the Dominion CIMs. The cable CIM is an integrated CIM and Cat5 cable available in several different lengths.</p>
<p>Is centralized management available for the Dominion LX?</p>	<p>Centralized management is not available as a standard feature for the Dominion LX.</p>

Question	Answer
What is virtual media?	Virtual media is a powerful feature that enables a user to mount drives and media from the user's desktop to remote servers during a KVM connection. This is ideal to install software, run hardware diagnostics, transfer files and even remotely reimage a server.
What types of virtual media does the Dominion LX support?	Dominion LX supports the following types of virtual media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives and local and remote ISO images.
What is Absolute Mouse Synchronization?	This is a technology developed by Raritan in which the local and remote mouse cursors stay in synch right out of the box. It eliminates the cumbersome need to manually change the mouse settings on each target server.

Index

A

- A. AC Power • 27
- About the Active KVM Client • 53
- About the Virtual KVM Client • 53
- Absolute Mouse Mode • 74
- Access and Control Target Servers Remotely • 34
- Accessing a Target Server • 34, 175
- Accessing the LX Using CLI • 164
- Accessing Virtual Media on a Windows 2000 Server Using a D2CIM-VUSB • 215
- Active System Partitions • 214
- Adding a New User • 100, 101
- Adding a New User Group • 95, 100
- Adding Attributes to the Class • 199
- Adding, Deleting and Editing Favorites • 50
- Adjusting Video Settings • 66
- Administering the LX Console Server
 - Configuration Commands • 169
- AKC Supported .NET Framework, Operating Systems and Browsers • 54
- Apple Macintosh Settings • 26
- Assigning an IP Address • 30
- Audit Log • 149, 182, 183
- Authentication Settings • 102
- Auto-Sense Video Settings • 65

B

- B. Network Port • 27
- Backup and Restore • 151
- Building a Keyboard Macro • 62

C

- C. Local Access Port (Local PC) • 28
- Cabling Example in Tiered Configurations • 123
- Calibrating Color • 66
- Certified Modems • 127, 190
- Changing a Password • 114
- Changing the Default GUI Language Setting • 136
- Changing the Default Password • 29
- Changing the Keyboard Layout Code (Sun Targets) • 35
- Changing the Maximum Refresh Rate • 70
- Checking Your Browser for AES Encryption • 144, 146

- CIMs • 215
- Cisco ACS 5.x for RADIUS Authentication • 110
- CLI Commands • 163, 168
- CLI Prompts • 168
- CLI Syntax -Tips and Shortcuts • 166
- Client Launch Settings • 77
- Command Line Interface (CLI) • 163
- Common Commands for All Command Line Interface Levels • 166
- Completion of Commands • 165
- Conditions when Read/Write is Not Available • 88, 90
- Configuring and Enabling Tiering • 43, 97, 98, 99, 121, 134, 174, 180
- Configuring Date/Time Settings • 127
- Configuring Date/Time Settings (Optional) • 32
- Configuring Event Management - Settings • 129
- Configuring KVM Switches • 121, 132
- Configuring LX Local Console Local Port Settings • 180
- Configuring LX Local Port Settings • 134
- Configuring Modem Settings • 29, 126
- Configuring Network • 169
- Configuring Ports • 131
- Configuring Standard Target Servers • 132
- Connect Key Examples • 178
- Connecting to Virtual Media • 90
- Connection Information • 59
- Connection Properties • 57
- Create User Groups and Users • 34
- Creating a New Attribute • 198
- Ctrl+Alt+Del Macro • 64

D

- D. Target Server Ports • 28
- Default Login Information • 12
- Desktop Background • 13
- Device Diagnostics • 161
- Device Information • 150
- Device Management • 36, 115
- Device Services • 119
- Diagnostics • 157
- Disconnecting a Target Server • 35
- Disconnecting Virtual Media • 88, 93
- Discovering Devices on the Local Subnet • 49
- Discovering Devices on the LX Subnet • 50

Drive Partitions • 214

E

E. Modem Port (Optional) • 29
 Editing rcusergroup Attributes for User Members • 201
 Enabling Direct Port Access via URL • 53, 124
 Enabling SSH • 119
 Enabling the AKC Download Server Certificate Validation • 125
 Enabling Tiering • 122
 Encryption & Share • 138, 144, 183
 Entering the Discovery Port • 120
 Event Management • 128
 Events Captured in the Audit Log and Syslog • 149, 194

F

Favorites List Page • 49, 50
 Fedora • 210
 French Keyboard • 207
 Frequently Asked Questions • 217
 From LDAP/LDAPS • 197
 From Microsoft Active Directory • 197
 Full Screen Mode • 79

G

General Settings • 75
 Getting Started • 13, 167

H

Hardware • 8
 Help Options • 80
 Hot Keys and Connect Keys • 177
 HTTP and HTTPS Port Settings • 120, 193

I

IBM AIX 5.3 Settings • 25
 Implementing LDAP/LDAPS Remote Authentication • 103, 107
 Implementing RADIUS Remote Authentication • 108
 Import/Export Keyboard Macros • 60
 Informational Notes • 191, 205
 Initial Configuration Using CLI • 167
 Installation and Configuration • 12
 Intelligent Mouse Mode • 73
 Interface and Navigation • 40
 Interface Command • 170
 Introduction • 1

IPv6 Command • 171
 IPv6 Support Notes • 206

J

Java Runtime Environment (JRE) • 205

K

Keyboard Language Preference (Fedora Linux Clients) • 208
 Keyboard Limitations • 76
 Keyboard Macros • 59
 Keyboard Options • 59
 Keyboards • 207

L

LAN Interface Settings • 118
 Launching MPC from a Web Browser • 80
 Launching the LX Remote Console • 38
 LED Indicators • 186
 Left Panel • 41
 Linux Settings (Red Hat 4) • 20
 Linux Settings (Red Hat 9) • 18
 Local Port Administration • 179
 Logging a User Off (Force Logoff) • 101
 Logging In • 164, 165
 Logging Out • 51
 Login Limitations • 138, 139
 LX Client Applications • 7
 LX Console Navigation • 42
 LX FAQs • 218
 LX Help • 9
 LX Interface • 40
 LX Interfaces • 37
 LX Local Console • 172
 LX Local Console Factory Reset • 182
 LX Local Console Interface
 LX Devices • 38, 173
 LX Overview • 2
 LX Photos • 4
 LX Remote Console Interface • 38
 LX Specifications • 184

M

Mac and Linux Locked, Mapped Drives • 215
 Macintosh Keyboard • 209
 Maintenance • 149
 Make Linux Settings Permanent • 22
 Make UNIX Settings Permanent • 26
 Manage Favorites Page • 49
 Managing Favorites • 42, 48

MCUTP • 212
 MCUTP CIM Behavior • 216
 Modifying an Existing User • 101
 Modifying and Existing User Group • 99
 Modifying and Removing Keyboard Macros • 64
 Mounting CD-ROM/DVD-ROM/ISO Images • 89, 91
 Mounting Local Drives • 90
 Mouse Modes • 14
 Mouse Options • 70
 Mouse Pointer Synchronization • 71
 Mouse Pointer Synchronization (Fedora) • 210
 Multi-Platform Client (MPC) • 80

N

Name Command • 171
 Naming Target Servers • 32
 Navigation of the CLI • 165
 Network Basic Settings • 115, 116
 Network Interface Page • 157
 Network Settings • 30, 32, 115, 116, 118, 193
 Network Speed Settings • 119, 195
 Network Statistics Page • 158
 Non-US Keyboards • 207
 Note on Microsoft Active Directory • 33

O

Overview • 12, 83, 163, 172, 205

P

Package Contents • 7
 Ping Host Page • 160
 Port Access Page • 40, 43, 121
 Port Access Page (Local Console Server Display) • 174
 Port Action Menu • 44
 Prerequisites for Using AKC • 54
 Prerequisites for Using Virtual Media • 85, 88
 Proxy Server Configuration for Use with MPC, VKC and AKC • 51

R

RADIUS Communication Exchange Specifications • 111
 Rebooting the LX • 155
 Refreshing the Screen • 65
 Related Documentation • 10
 Relationship Between Users and Groups • 95
 Remote Authentication • 33, 136
 Remote Connection • 191

Resetting the LX Using the Reset Button • 145, 183
 Resolving Fedora Core Focus • 210
 Resolving Issues with Firefox Freezing when Using Fedora • 210
 Returning to the LX Local Console Interface • 179
 Returning User Group Information • 197
 Returning User Group Information from Active Directory Server • 107
 Returning User Group Information via RADIUS • 111
 Running a Keyboard Macro • 64

S

Scaling • 79
 Scan Settings • 45, 78
 Scanning Ports • 40, 43, 45, 78, 134, 180
 Scanning Ports - Local Console • 45, 176
 Security and Authentication • 173
 Security Issues • 169
 Security Management • 138
 Security Settings • 138
 Setting CIM Keyboard/Mouse Options • 65
 Setting Network Parameters • 167
 Setting Parameters • 167
 Setting Permissions • 96, 99
 Setting Permissions for an Individual Group • 98, 101
 Setting Port Permissions • 98, 99
 Setting the Registry to Permit Write Operations to the Schema • 198
 Simultaneous Users • 172
 Single Mouse Mode • 74
 Software • 9
 Special Sun Key Combinations • 178
 Specifications • 29, 184
 SSH Access from a UNIX/Linux Workstation • 164
 SSH Access from a Windows PC • 164
 SSH Connection to the LX • 164
 SSL Certificates • 147
 Standard Mouse Mode • 72
 Step 1
 Configure the KVM Target Servers • 12, 13
 Step 2
 Configure Network Firewall Settings • 12, 26
 Step 3
 Connect the Equipment • 12, 27, 132
 Step 4

Index

- Configure the LX • 12, 29
- Step 5
 - Launch the LX Remote Console • 12, 34
- Step 6
 - Configure the Keyboard Language (Optional) • 12, 35
- Step 7
 - Configure Tiering (Optional) • 12, 36
- Strong Passwords • 114, 138, 140
- Sun Solaris Settings • 22
- Supported Browsers • 187
- Supported CIMs and Operating Systems • 188
- Supported Keyboard Languages • 191
- Supported Operating Systems (Clients) • 28, 186
- Supported Protocols • 33
- Supported Video Resolutions • 13, 189, 190
- Supported Video Resolutions - Local Console • 174
- Supported Video Resolutions Not Displaying • 211
- SUSE Linux 10.1 Settings • 21
- SUSE/VESA Video Modes • 211
- Switching between Target Servers • 35

T

- Target BIOS Boot Time with Virtual Media • 215
- Target Server Connection Distance and Video Resolution • 13, 174, 189, 190
- TCP and UDP Ports Used • 193
- Terminology • 10
- Tiering - Target Types, Supported CIMs and Tiering Configurations • 121, 122
- Tool Options • 75, 79
- Toolbar • 55
- Trace Route to Host Page • 160

U

- Unsupported and Limited Features on Tiered Targets • 122
- Updating the LDAP Schema • 107, 197
- Updating the Schema Cache • 201
- Upgrade History • 155
- Upgrading CIMs • 153
- Upgrading Firmware • 153
- User Authentication Process • 113
- User Blocking • 138, 142
- User Group List • 95

- User Groups • 94
- User List • 100
- User Management • 34, 94, 173
- Users • 99
- Using Scan Options • 47, 177
- Using Screenshot from Target • 69
- Using Virtual Media • 88

V

- Video Modes and Resolutions • 211
- Video Properties • 65
- View Options • 78
- View Status Bar • 79
- View Toolbar • 78
- Virtual KVM Client (VKC) and Active KVM Client (AKC) • 39, 53
- Virtual Media • 82, 213
- Virtual Media Connection Failures Using High Speed for Virtual Media Connections • 215
- Virtual Media File Server Setup (File Server ISO Images Only) • 88, 89
- Virtual Media in a Linux Environment • 86
- Virtual Media Linux Drive Listed Twice • 215
- Virtual Media Not Refreshed After Files Added • 214
- Virtual Media via VKC and AKC in a Windows Environment • 213
- VM-CIMs and DL360 USB Ports • 211

W

- Windows 2000 Composite USB Device Behavior for Virtual Media • 216
- Windows 2000 Settings • 18
- Windows 3-Button Mouse on Linux Targets • 215
- Windows 7 and Windows Vista Settings • 16
- Windows XP, Windows 2003 and Windows 2008 Settings • 15
- Working with Target Servers • 7, 37

▶ **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