Raritan®

A brand of legrand®

Dominion LX II

User Guide

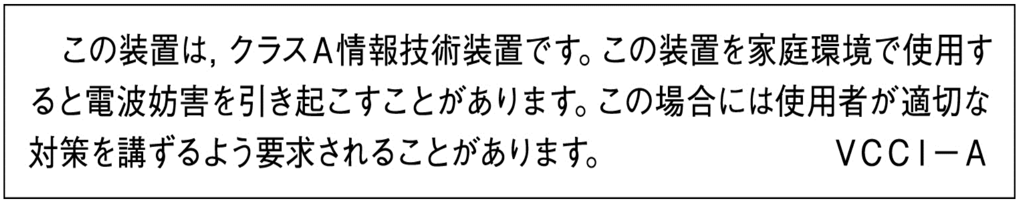
Release 3.0.0

LX2-v3.0.0-0B-E
June 2020

FCC Information

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

VCCI Information (Japan)



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

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

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

1F61
I.T.E.

- 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** in User Guide.
- 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.

Welcome

Contents

Dominion LX II Release 3.0.0

User Guide

What's New in LX II Release 3.0.0

- New models: ***Dominion LX II Integrated Switch/LED Drawers*** (on page 2)

Chapter 7 Command Line Interface (CLI) 133

Chapter 8 Virtual Media 139

Chapter 1 Introduction

Raritan's Dominion LX II KVM-over-IP switches give one or two remote users and one local user, Java-free, BIOS-level access and control of 8 or 16 servers (expandable to 256 servers with tiering), and virtual media. Three LX II switch models and three integrated switch / LCD drawer combination models support 8 or 16 KVM ports, 1-2 remote users, 1 local user and up to 8 serial ports.

LX II appliances, designed for small to midsize businesses (SMBs), support a wide variety of computer and serial devices with VGA, DVI, HDMI, USB-C and DisplayPort video. Productive, KVM-over-IP connections up to 15 frames-per second with video resolutions up to 1080p and 1200p are supported for digital and analog video.

In This Chapter

Features

- Java-free, BIOS-level, IP remote access
- One or two remote users. One local user. 8 or 16 KVM ports. Up to 8 serial ports.
- Integrated Switch / LCD drawer models
- Single power supply and LAN port
- VGA, DVI, HDMI, USB-C and DisplayPort
- Second generation platform with 1080p and 1200p video at 15 frames/second
- Universal Virtual Media™
- Absolute Mouse Synchronization™
- Manage up to 8 serial devices (DSAM)
- VGA/USB Local port
- RADIUS, LDAP and Active Directory
- Tiering support up to 256 servers

Dominion LX II Switches

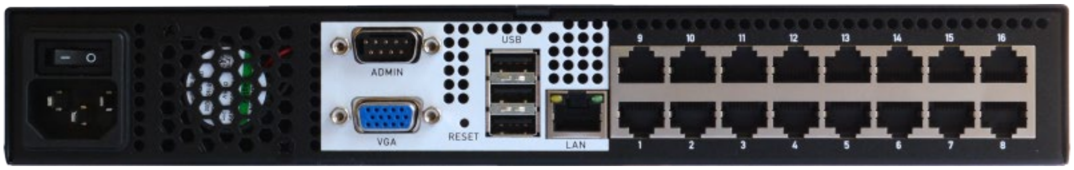
There are 3 Dominion LX II switch-only models.

- **DLX2-108**: 8-port KVM-over-IP switch, 1 remote and 1 local user, virtual media, single power and single LAN
- **DLX2-116**: 16-port KVM-over-IP switch, 1 remote and 1 local user, virtual media, single power and single LAN
- **DLX2-216**: 16-port KVM-over-IP switch, 2 remote and 1 local user, virtual media, single power and single LAN

Product Photos

▶ **Front View:**

▶ **Rear View:**



Dominion LX II Integrated Switch/LED Drawers

These models combine a Dominion LX II KVM-over-IP Switch with a T1700-LED style keyboard drawer. This 1U unit supports local, at-the-rack access via the integrated screen, keyboard and touchpad, as well as remote IP access. The Dominion LX II local port functions are available and you can locally access target servers connected to the Dominion LX II. The unit also provides buttons and an OSD to control the embedded video display.

There are 3 Dominion LX II integrated switch/LED drawer models.

DLX2-108-LED:1 User, 8 Ports, 256 Managed Servers (Cascaded), 1920 x 1080@60Hz (VGA) Video Resolution, > 30,000 Hours MTBF

DLX2-208-LED: 1 User, 16 Ports, 256 Managed Servers (Cascaded), 1920 x 1080@60Hz (VGA) Video Resolution, > 30,000 Hours MTBF

DLX2-216-LED: 2 Users, 16 Ports, 256 Managed Servers (Cascaded), 1920 x 1080@60Hz (VGA) Video Resolution, > 30,000 Hours MTBF

Product Photos

Front View:

Rear View:

Chapter 2 Installation and Initial Configuration

Thank for choosing the Dominion LX II, Raritan's economical, Java-free line of KVM-over-IP switches for small and medium businesses.

This chapter contains a high-level, quick setup guide to installation and initial configuration.

In This Chapter

Package Contents

Switch-only models: DLX2-108, DLX2-116, DLX2-216

- 1 - LX II switch-only device
- 1 - Rackmount kit
- 1 - AC power cord
- 1 - Set of 4 rubber feet for desktop use

Integrated switch/LED drawer models: DLX2-108-LED, DLX2-116-LED, DLX2-216-LED

- 1 - LX II integrated switch/LED drawer device
- 1 - Rackmount kit with sliding rails
- 1 - AC power cord

- 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** in User Guide.
- 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.

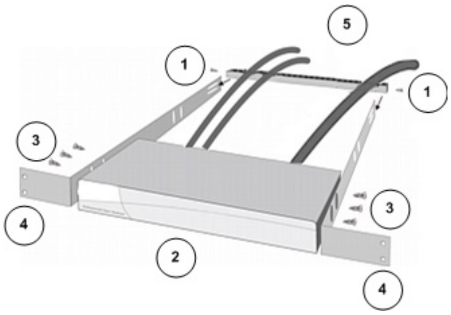
Rack Mounting - Switch-Only Models - DLX2-108, DLX2-116, DLX2-216

LX II switch-only models can be mounted in 1U (1.73", 44 mm) of vertical space in a standard 19" equipment rack, facing the front of the rack or facing the rear of the rack.

Use the brackets and screws shipped with the device.

Forward Mount - Switch-Only Models - DLX2-108, DLX2-116, DLX2-216

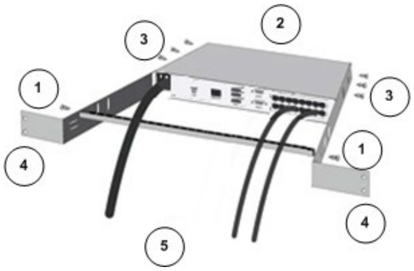
Numbered steps correspond to the numbers in the diagram.



1. Secure the cable-support bar to the back end of the side brackets using two of the included screws.
2. Slide the LX II between the side brackets, with its rear panel facing the cable-support bar, until its front panel is flush with the "ears" of the side brackets.
3. Secure the LX II to the side brackets using the remaining included screws (three on each side).
4. Mount the entire assembly in your rack and secure the side brackets' ears to the rack's front rails with your own fasteners.
5. When connecting cables to the rear panel, drape them over the cable-support bar.

Rear Mount - Switch-Only Models - DLX2-108, DLX2-116, DLX2-216

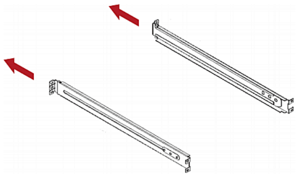
Numbered steps correspond to the numbers in the diagram.



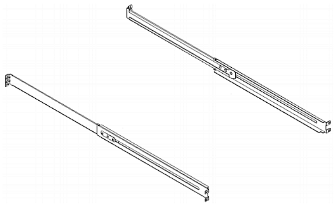
1. Secure the cable-support bar to the front end of the side brackets, near the side brackets' "ears," using two of the included screws.
2. Slide the LX II between the side brackets, with its rear panel facing the cable-support bar, until its front panel is flush with the back edges of the side brackets.
3. Secure the LX II to the side brackets using the remaining included screws (three on each side).
4. Mount the entire assembly in your rack and secure the side brackets' ears to the rack's front rails with your own fasteners.
5. When connecting cables to the rear panel, drape them over the cable-support bar.

Rack Mounting - Integrated Switch/LED Drawer Models - DLX2-108-LED, DLX2-116-LED, DLX2-216-LED

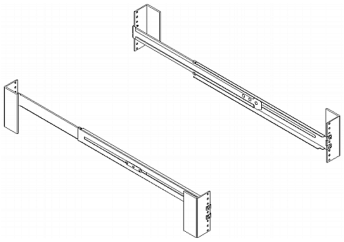
1. Adjust the length of the brackets to match the mounting depth of your rack. Brackets are labeled Left Front and Right Front.



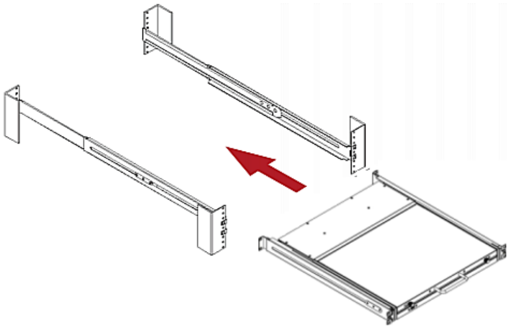
Now the brackets look similar to the following.



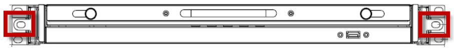
2. Fasten the brackets to the rack rails securely with your own screws or cage nuts.



3. Slide the LX II between the brackets.



4. Fasten the LX II to the rack using screws.



Step 1: Configuring Network Firewall Settings

- TCP Port 5000: Allow network and firewall communication to enable remote access.
- TCP Port 443: Allow access to the standard HTTPS port to enable access via web browser.
- TCP Port 80: Allow access to the standard HTTP port to enable redirection of HTTP requests.

TCP Port 5000

Enable remote access to LX II by allowing network and firewall communication on TCP Port 5000.

TCP Port 443

Allow access to TCP Port 443 (Standard HTTPS) so you can access LX II via a web browser.

TCP Port 80

Allow access to TCP Port 80 (Standard HTTP) to enable automatic redirection of HTTP requests to HTTPS.

Step 2: Configuring KVM Target Servers

Mouse Settings

Absolute Mouse Synchronization is recommended to minimize mouse settings on target servers.

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

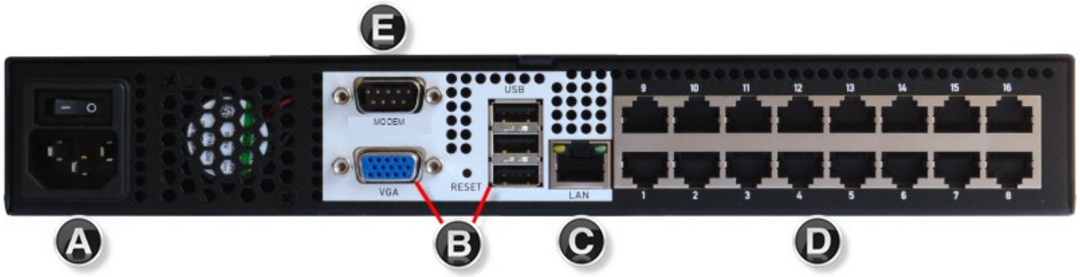
- Absolute Mouse Synchronization requires the use of a virtual media CIM - D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP, D2CIM-VUSB-USBC

Target Server Video Resolutions

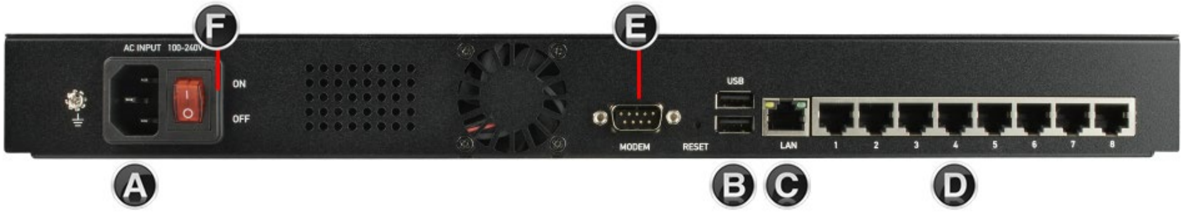
See **Supported Target Server Video Resolutions** in Online Help.

Step 3: Connecting the Equipment

▶ **LX II switch-only models: DLX2-108, DLX2-116, DLX2-216**



▶ **LX II integrated switch/LED drawer models: DLX2-108-LED, DLX2-116-LED, DLX2-216-LED**



A. AC Power

▶ **To connect the power supply:**

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

B: USB Ports and Additional Local Access Port on Switch-Only Models

▶ **To connect a local console to a Switch-Only Model:**

Attach a multi-sync VGA monitor, and USB mouse and keyboard. Note: VGA Port not available on integrated switch/LED drawer models.

C: Network Port

▶ **To connect the network:**

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

D: Target Server Ports

▶ **To connect target servers:**

1. Connect the keyboard, mouse and video plugs on the CIM to the corresponding ports on the target server.
2. Connect the CIM to an available target server port on the back of the LX II via a Cat5/5e/6 cable.

E: Modem Port (Optional)

See ***Configuring Modem Settings*** (on page 94), in the Online Help.

F: Power Switch (Integrated Switch/LED Drawer Models Only)

Use the On/Off switch to operate the integrated LED screen.

Step 4: Configuring the LX II

For the following steps, you must change the default password and assign the LX II its IP address at the Local Console. All other steps can be performed either from the Local Console, or the LX II Remote Console in a web browser using the LX II's IP address.

Default Login - Change the Password

The LX II device is shipped with the following default settings. You are forced to change the password at first login. Up to 64 English alphanumeric and special characters allowed.

- Username = `admin`
- Password = `raritan`
- IP address = `192.168.0.192`

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

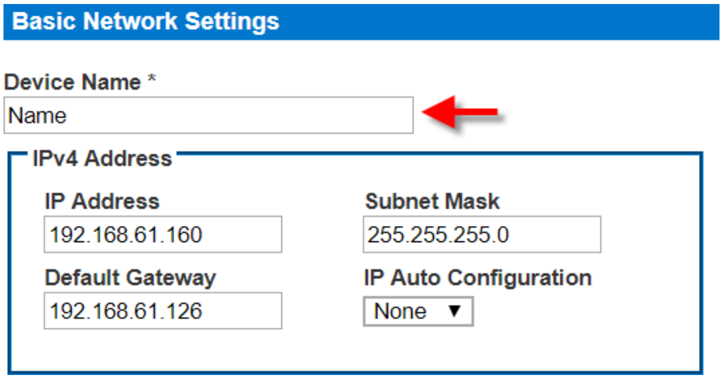
Change the Default Password

The first time you start the LX II device, you are required to change the default password.

1. Once the unit has booted, enter the default username `admin` and password `raritan`.
2. Click Login.
3. Enter the old password `raritan`, then enter and reenter a new password.
   - Up to 64 English alphanumeric and special characters.
4. Click Apply, then click OK on the Confirmation page.

Assign the LX II a Device Name

Choose Device Settings > Network to go to the Basic Network Settings page in the LX II Remote client.



Basic Network Settings

Device Name * Name

IPv4 Address

IP Address 192.168.61.160

Subnet Mask 255.255.255.0

Default Gateway 192.168.61.126

IP Auto Configuration None

- Specify a meaningful Device Name for your LX II device.
  - Up to 32 alphanumeric and valid special characters, no spaces between characters.

Next, configure the IP address and DNS settings.

Configure the Network: IPv4 and IPv6 Settings

1. Set the IP Auto Configuration to None in the IPv4 section.
2. Enter the IP address you want to use to connect to the LX II LAN1. The default IP address is 192.168.0.192.
3. Enter the IPv4 Subnet Mask. The default subnet mask is 255.255.255.0.
4. Complete the IPv6 sections, if applicable.
5. Select the IP Auto Configuration. If None is selected, you must manually specify -
   - Global/Unique IP Address - this is the IP address assigned to LX II.
   - Prefix Length - this is the number of bits used in the IPv6 address.
   - Gateway IP Address.

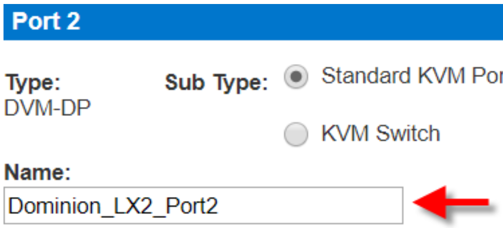
   Select Router Discovery to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

   Note that the following additional, read-only information appears in this section -
   - Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.
   - Zone ID - Identifies the device the address is associated with. Read-Only
6. Select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary addresse is used if the primary DNS server connection is lost due to an outage.

   Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when LX II is configured in DHCP mode
7. When finished, click OK. Your LX II device is now accessible via the LAN IP address.

Name Your Target Servers

1. Connect all of the target servers if you have not already done so.
2. Select Device Settings > Port Configuration, then click the Port Name of the target server you want to name.



Port 2

Type: DVM-DP

Sub Type: ● Standard KVM Port ○ KVM Switch

Name: Dominion_LX2_Port2

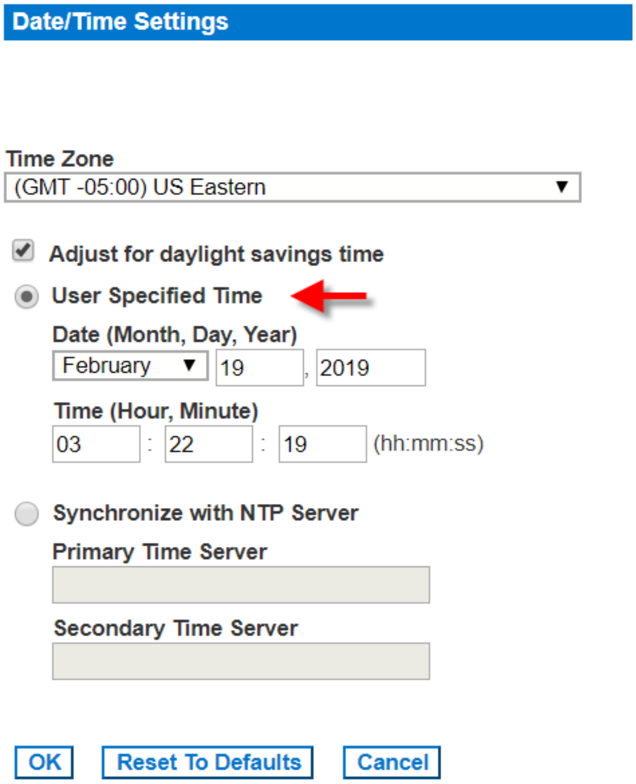
3. Enter a name for the server. Up to 32 alphanumeric and special characters. Click OK.

Configure Date/Time Settings

The date and time settings impact SSL certificate validation if LDAPS is enabled. Configuring the date and time also ensures your audit logs will be timestamped correctly.

There are two ways to do this:

- Manually set the date and time.



Date/Time Settings

Time Zone: (GMT -05:00) US Eastern ▼

☑ Adjust for daylight savings time

● User Specified Time

Date (Month, Day, Year): February ▼ 19 , 2019

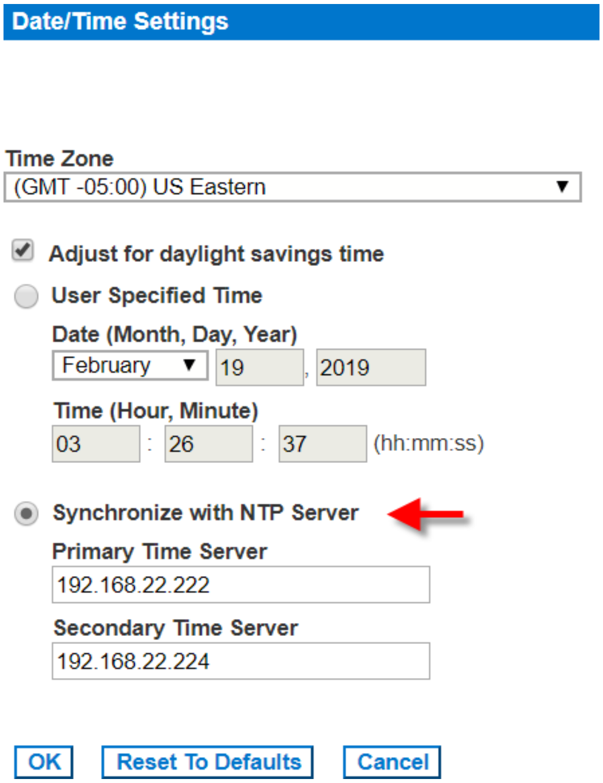
Time (Hour, Minute): 03 : 22 : 19 (hh:mm:ss)

○ Synchronize with NTP Server

Primary Time Server:

Secondary Time Server:

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



Date/Time Settings

Time Zone
(GMT -05:00) US Eastern

☑ Adjust for daylight savings time

○ User Specified Time

Date (Month, Day, Year)
February 19, 2019

Time (Hour, Minute)
03 : 26 : 37 (hh:mm:ss)

● Synchronize with NTP Server

Primary Time Server
192.168.22.222

Secondary Time Server
192.168.22.224

To configure date/time settings:

1. Choose Device Settings > Date/Time to open the Date/Time Settings page.
2. Choose your time zone from the Time Zone drop-down list.
3. Adjust for daylight savings time by checking the "Adjust for daylight savings time" checkbox.
4. Choose the method to use to set the date and time:
   - User Specified Time - use 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 - use this option to synchronize the date and time with the Network Time Protocol (NTP) Server.

     For the Synchronize with NTP Server option:
     - Enter the IP address or hostname of the Primary Time server.
     - Enter the IP address or hostname of the Secondary Time server.

       Optional

Note: If DHCP is selected for the Network Settings on the Network page, the NTP server IP address is automatically retrieved from the DHCP server by default. Manually enter the NTP server IP address by selecting the Override DHCP checkbox.

5. Click OK.

Step 5: Launching the Remote Console

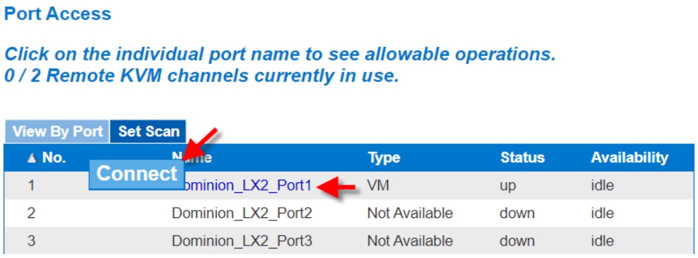
1. Launch a supported web browser, and enter the IP address assigned to the LX II. A default client is launched based on your pc and browser settings. See the online help for details about clients.
2. Enter your username and password, then click Login.
3. Accept the user agreement (if applicable).
4. If security warnings appear, click to accept.

Access and Control Target Servers Remotely

The LX II Port Access page provides a list of all LX II ports.

The page also lists all of the target servers connected to the LX II along with their status and availability.

Access a Target Server from the LX II



Port Access

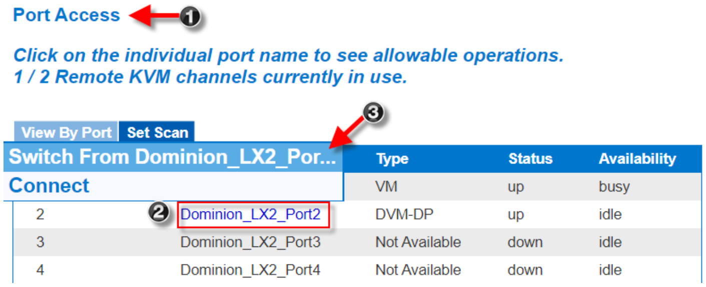
Click on the individual port name to see allowable operations.
0 / 2 Remote KVM channels currently in use.

▲ No.	Name	Type	Status	Availability
1	ominion_LX2_Port1	VM	up	idle
2	Dominion_LX2_Port2	Not Available	down	idle
3	Dominion_LX2_Port3	Not Available	down	idle

1. On the Port Access page, 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.

Switch between Target Servers



Port Access

Click on the individual port name to see allowable operations.
1 / 2 Remote KVM channels currently in use.

No.	Name	Type	Status	Availability
		VM	up	busy
2	Dominion_LX2_Port2	DVM-DP	up	idle
3	Dominion_LX2_Port3	Not Available	down	idle
4	Dominion_LX2_Port4	Not Available	down	idle

While already using a target server, access the LX II Port Access page.

Click the port name of the target you want to access. The Port Action menu appears.

Choose Switch From. The new target server you selected is displayed.

Disconnect from a Target Server

▶ To disconnect a target:

- On the Port Access page, click the port name of the target you want to disconnect from, then click Disconnect on the Port Action menu when it appears.

Or

- Close the client window.

Step 6: Configuring the Keyboard Language (Optional)

If you are using a non-US language, the keyboard must be configured for the appropriate language. Also, the keyboard language for the client machine and the KVM target servers must match. Consult your operating system documentation for information about changing the keyboard layout.

Chapter 3 Using the Integrated Switch/LED Drawer

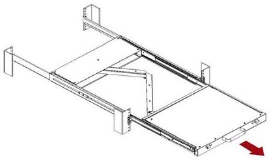
This chapter describes using the functions of the LED drawer itself, at the rack, including physical operation of the LED drawer and on-screen display functions.

In This Chapter

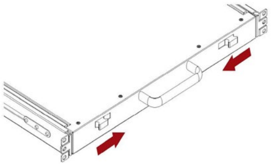
Using the LED Drawer

▶ **To open the drawer:**

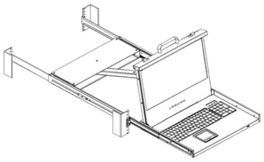
1. Pull out the LED drawer.



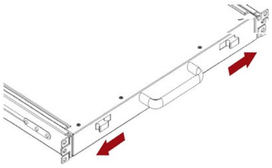
2. Push the locking latches toward the center to unlock the display.



3. Flip up the display, and press Power.

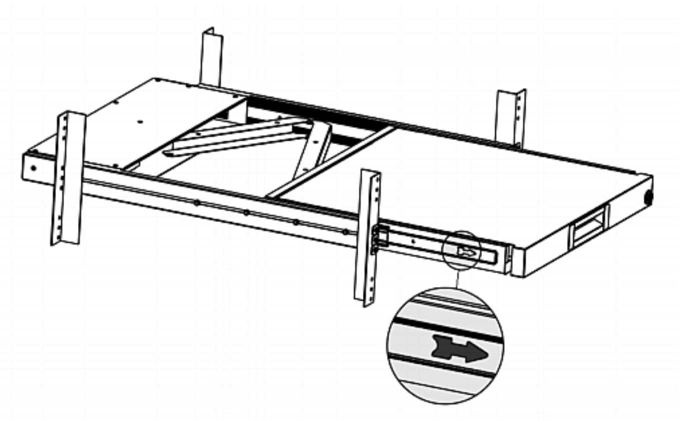


4. After completing operation, close the display, and push the locking latches toward two sides to lock it.



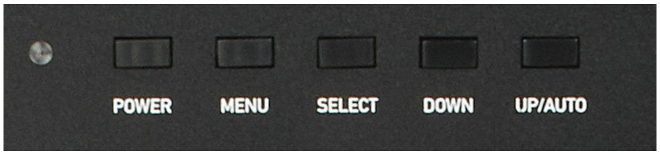
To close the drawer:

1. Locate the gray-arrow release buttons on each side of the LED drawer.



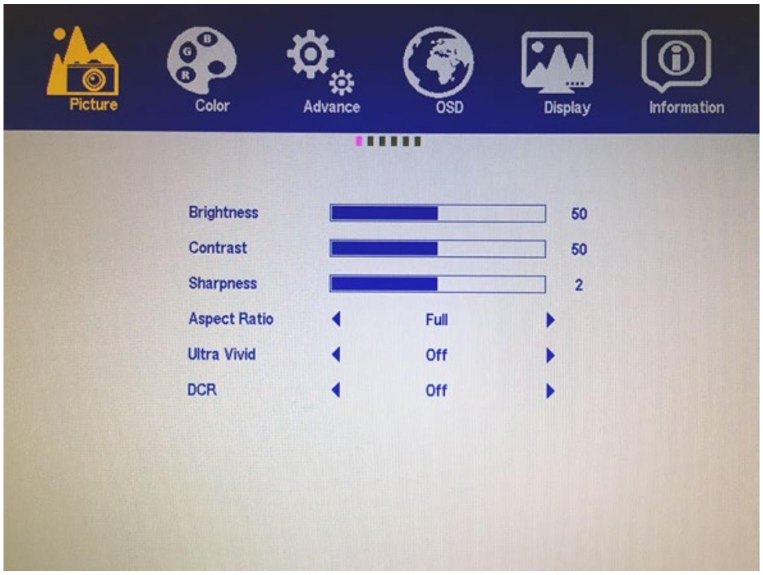
2. Push both gray-arrow buttons in the direction as indicated by the arrow head before pushing the LX II into the rack.
3. Keep pushing the gray-arrow buttons until completely moved into the rack.

Using the LED On-Screen Display (OSD)



Buttons	Function
POWER	Power on/off the built-in LED display. The LED indicator lamp indicates the current power on/off status. ▪ Light off = LED display power off ▪ Light on = LED display power on
MENU	This button has two functions: ▪ When OSD is not displayed, pressing this button triggers the OSD menu. ▪ When the OSD is displayed, this button functions as the Back key for going back to the last action.
SELECT	▪ This button is used as the Enter key and can be used to confirm the selection.
DOWN	▪ When the OSD is displayed, pressing this button moves down (or left) the selection.
UP/AUTO	This button has two functions: ▪ When OSD is not displayed, pressing this button optimizes the visual settings. ▪ When the OSD is displayed, pressing this button moves up (or right) the selection.

Picture



Brightness 50

Contrast 50

Sharpness 2

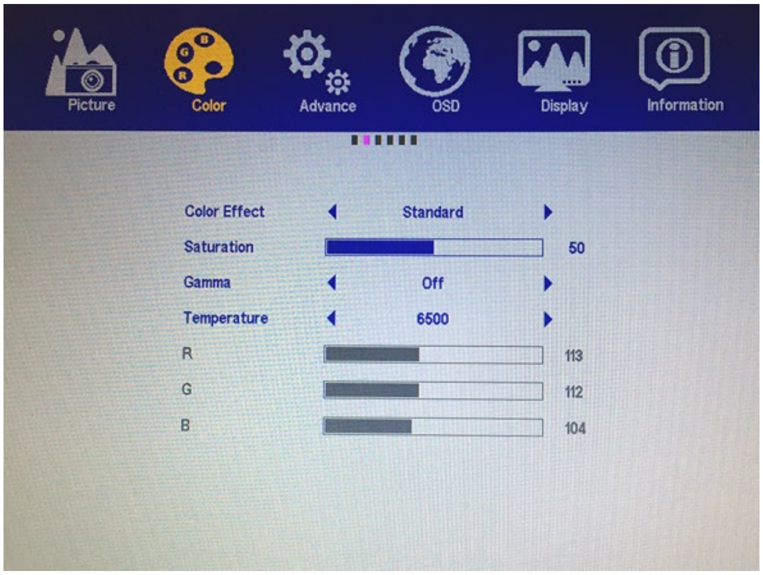
Aspect Ratio Full

Ultra Vivid Off

DCR Off

- Brightness: Make the screen image brighter or darker.
- Contrast: Adjust the difference between the background black level and the foreground white level.
- Sharpness: Fine tune the sharpness of the screen image.
- Aspect Ratio: Set the Aspect Ratio
- Ultra Vivid: On/off the Ultra Vivid function.
- DCR: On/off the Dynamic Contrast Ratio function.

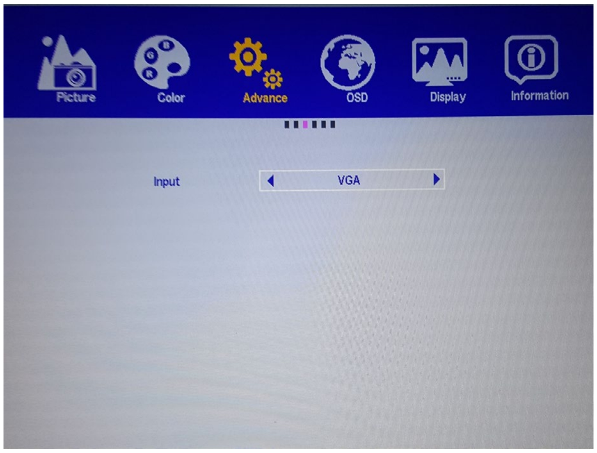
Color



Color Effect ◀ Standard ▶
Saturation 50
Gamma ◀ Off ▶
Temperature ◀ 6500 ▶
R 113
G 112
B 104

- Color Effect: Choose the Color Effect.
- Saturation: Adjusts the Saturation setting.
- Gamma: On/off the Gamma function.
- Temperature: Select the screen color temperatures.
- R/G/B: Adjust red, green, and blue colors respectively. (The adjustments are available for user define)

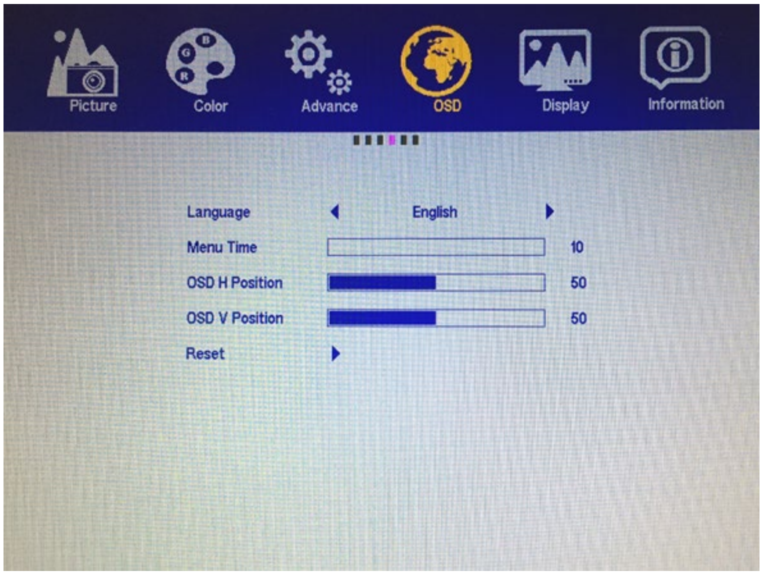
Advance



Input ◄ VGA ►

- Input: The video input is VGA only.

OSD



Language ◄ English ►

Menu Time 10

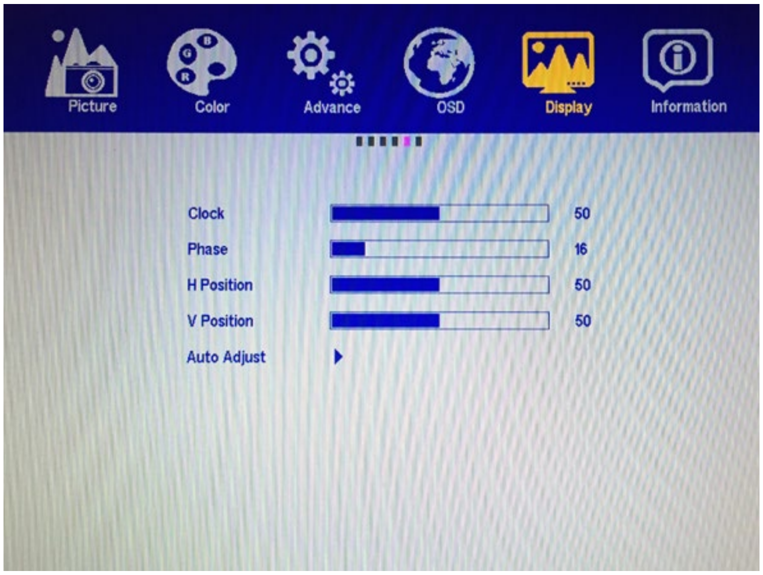
OSD H Position 50

OSD V Position 50

Reset ►

- Language: Select the language in which the OSD menu is displayed.
- Menu Time: Set the time duration in seconds for which the OSD remains visible after the last button is pressed.
- OSD H Position: Adjust the horizontal position of the OSD
- OSD V Position: Adjust the vertical position of the OSD
- Reset: Reset all settings to factory defaults.

Display



Clock 50

Phase 16

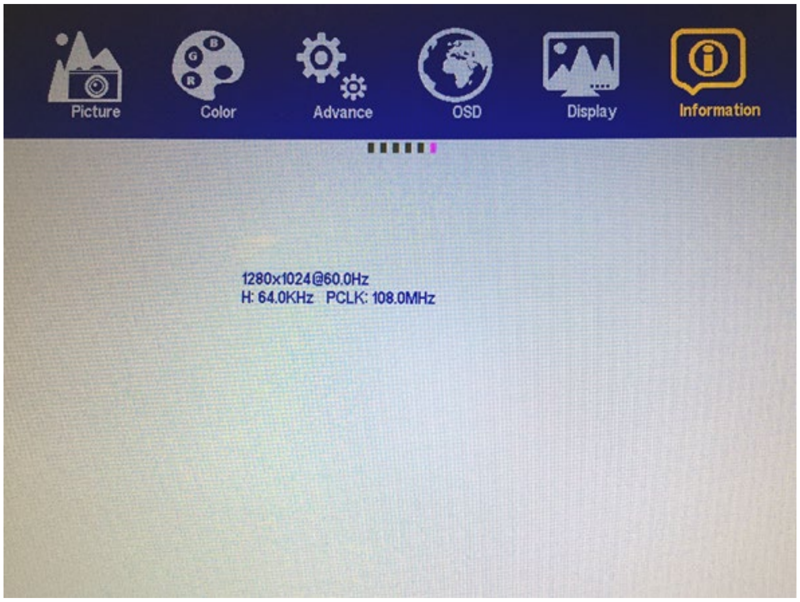
H Position 50

V Position 50

Auto Adjust ▶

- Clock: Adjust the clock to synchronize the sampling clock of the display with the pixel clock of the connected equipment.
- Phase: Adjust the phase to synchronize the frequency settings of the display with the frequency output of the connected equipment.
- H Position: Move the screen image left or right.
- V Position: Move the screen image up or down.
- Auto Adjust: Optimize the visual settings.

Information



1280x1024@60.0Hz
H: 64.0KHz   PCLK: 108.0MHz

- Display the current video input information on the screen.

Chapter 4 Getting Started Using LX II

This section walks you through some high-level tasks you should complete to start using LX II.

In This Chapter

Install and Configure LX II

If you have not already done so, install and configure LX II.

See ***Installation and Initial Configuration*** (on page 4), or follow the Quick Setup Guide shipped with your LX II. You can download all LX II documentation from the Raritan Support page.

Default Login - Change the Password

The LX II device is shipped with the following default settings. You are forced to change the password at first login. Up to 64 English alphanumeric and special characters allowed.

- Username = `admin`
- Password = `raritan`
- IP address = `192.168.0.192`

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

Allow Pop-Ups

Regardless of the browser you are using, you must allow pop-ups in order to launch the LX II Remote Console.

Security Warnings and Validation Messages

When logging in to LX II, security warnings and application validation messages may appear.

These include -

- Additional security warnings based on your browser and security settings

  See ***Additional Security Warnings*** (on page 24)

- If you choose to use the Virtual KVM Client (VKC/VKCS), you may see Java™ security warnings and requests to validate LX II.

  See ***Java Validation and Access Warning*** (on page 184) and ***Installing a Certificate*** (on page 24).

Note! Use the HTML KVM Client (HKC) instead to avoid Java. The HKC is Java-Free. See **KVM Client Launching** *(on page 148).*

Additional Security Warnings

Even after an SSL certificate is installed in the LX II, depending on your browser and security settings, additional security warnings may be displayed when you log in to LX II.

It is necessary to accept these warnings to launch the LX II Remote Console.

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

Installing a Certificate

You may be prompted by the browser to accept and validate the LX II's SSL certificate.

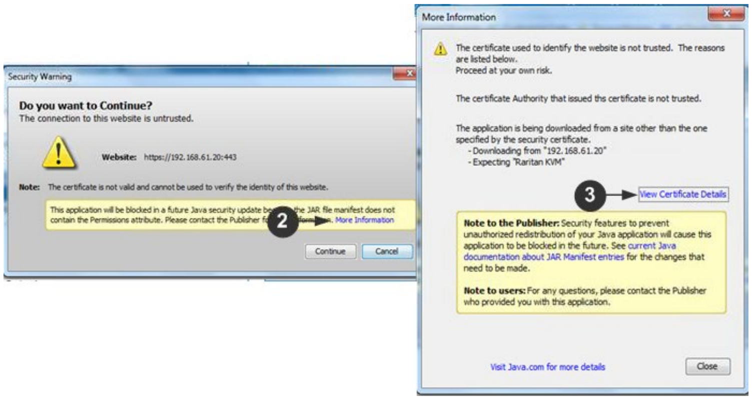
Depending on your browser and security settings, additional security warnings may be displayed when you log in to LX II.

It is necessary to accept these warnings to launch the LX II Remote Console. For more information, see ***Security Warnings and Validation Messages*** (on page 24).

Two sample methods on how to install an SSL Certificate in the browser are provided here. Specific methods and steps depend on your browser and operating system. See your browser and operating system help for details.

Example 1: Import the Certificate into the Browser

In this example, you import the Certificate into the browser.



Do you want to Continue?
The connection to this website is untrusted.

Website: https://192.168.61.20:443

Note: The certificate is not valid and cannot be used to verify the identity of this website.

This application will be blocked in a future Java security update be... the JAR file manifest does not contain the Permissions attribute. Please contact the Publisher f... More Information

More Information

The certificate used to identify the website is not trusted. The reasons are listed below.
Proceed at your own risk.

The certificate Authority that issued ths certificate is not trusted.

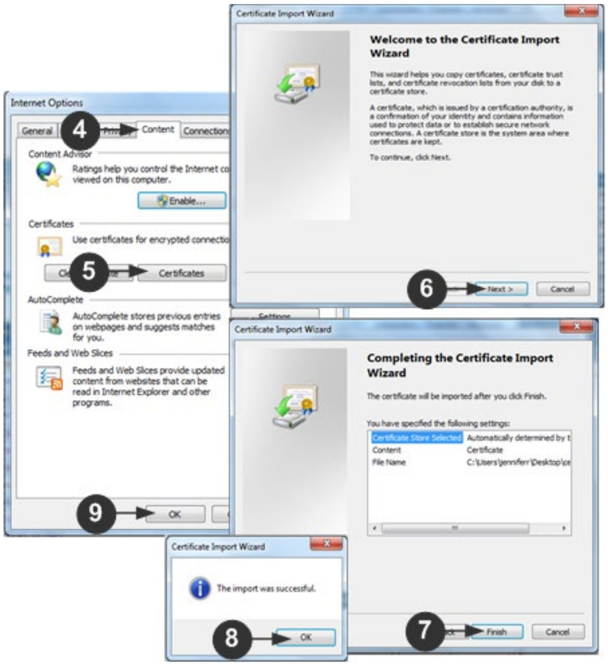
The application is being downloaded from a site other than the one specified by the security certificate.
- Downloading from "192.168.61.20"
- Expecting "Raritan KVM"

Note to the Publisher: Security features to prevent unauthorized redistribution of your Java application will cause this application to be blocked in the future. See current Java documentation about JAR Manifest entries for the changes that need to be made.

Note to users: For any questions, please contact the Publisher who provided you with this application.

1. Open a browser, then log in to LX II.
2. Click More Information on the first warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

Note: If you are not prompted by the browser, manually select the Settings or Options for your browser, and import the certificate. The following example shows the IE > Tools > Internet Options method.



Ratings help you control the Internet co... viewed on this computer.

Use certificates for encrypted connectio...

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate
File Name	C:\Users\jennifer\Desktop\ce

The import was successful.

1. Click the Content tab.
2. Click Certificates.

The Certificate Import Wizard opens and walks you through each step.

- File to Import - Browse to locate the Certificate
- Certificate Store - Select the location to store the Certificate

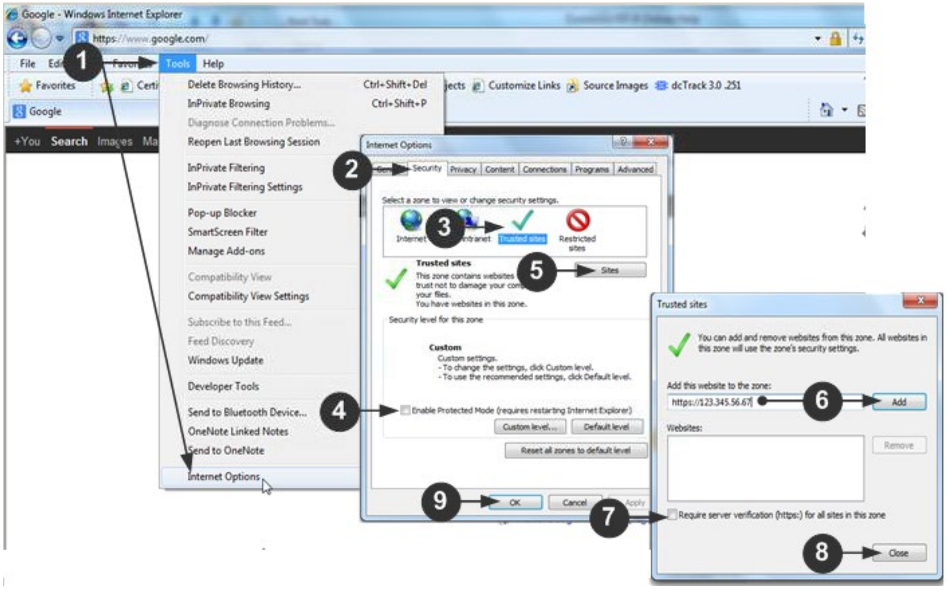
3. Click Finish on the last step of the Wizard.

   The Certificate is imported. Close the success message.

4. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

Example 2: Add the LX II to Trusted Sites and Import the Certificate

In this example, the LX II's URL is added as a Trusted Site, and the Self Signed Certificate is added as part of the process.



Select a zone to view or change security settings.

Trusted sites
This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

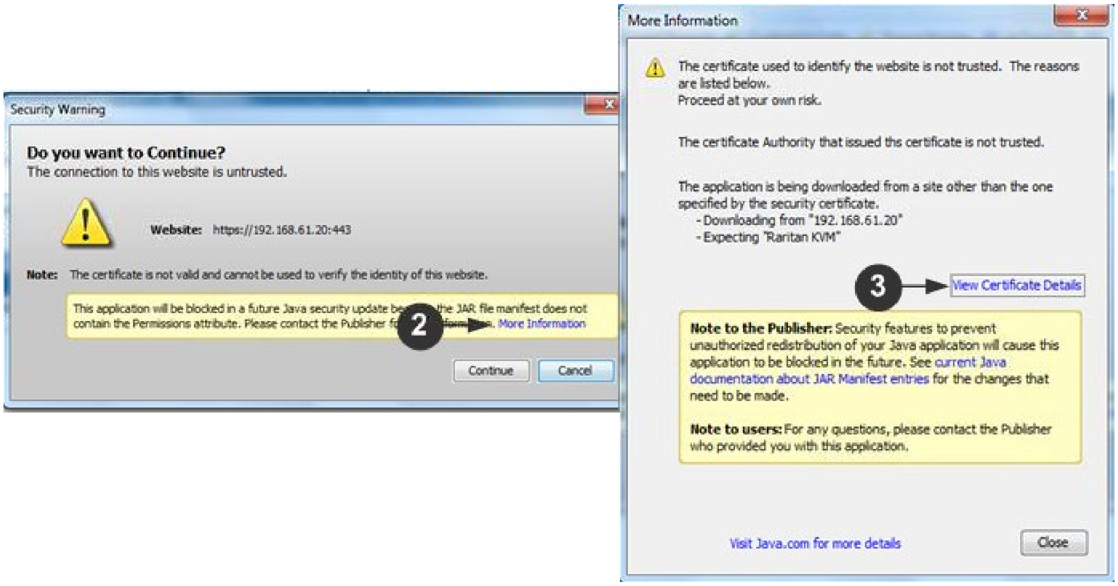
Add this website to the zone: https://123.345.56.67

Websites:

□ Require server verification (https:) for all sites in this zone

1. Open an IE browser, then select Tools > Internet Options to open the Internet Options dialog
2. Click the Security tab.
3. Click on Trusted Sites.
4. Disable Protected Mode, and accept any warnings.
5. Click Sites to open the Trusted Sites dialog.
6. Enter the LX II URL, then click Add.
7. Deselect server verification for the zone (if applicable).
8. Click Close.
9. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

Next, import the Certificate.



Do you want to Continue?
The connection to this website is untrusted.

Website: https://192.168.61.20:443

Note: The certificate is not valid and cannot be used to verify the identity of this website.

This application will be blocked in a future Java security update be the JAR file manifest does not contain the Permissions attribute. Please contact the Publisher f formation. More Information

The certificate used to identify the website is not trusted. The reasons are listed below.
Proceed at your own risk.

The certificate Authority that issued ths certificate is not trusted.

The application is being downloaded from a site other than the one specified by the security certificate.
- Downloading from "192.168.61.20"
- Expecting "Raritan KVM"

Note to the Publisher: Security features to prevent unauthorized redistribution of your Java application will cause this application to be blocked in the future. See current Java documentation about JAR Manifest entries for the changes that need to be made.

Note to users: For any questions, please contact the Publisher who provided you with this application.

1. Open an IE browser, then log in to LX II.
2. Click More Information on the first Java™ security warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

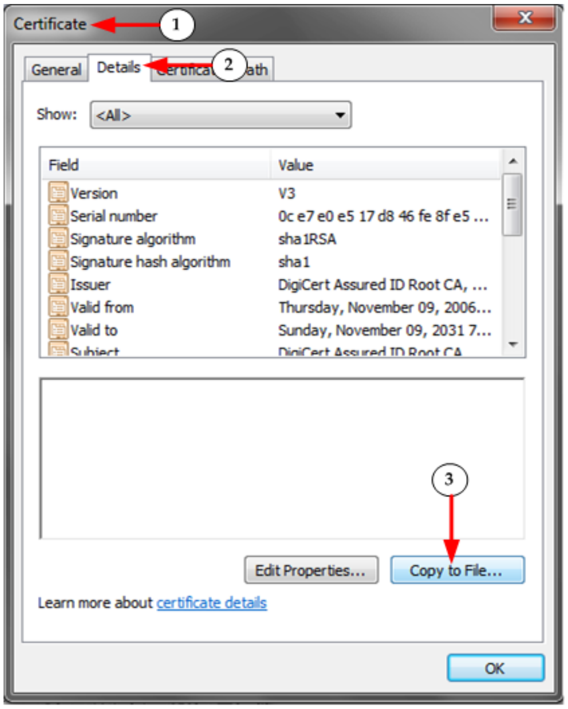
For details see, ***Example 1: Import the Certificate into the Browser*** (on page 25).

Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)

LX II requires an SSL certificate in either Base64-Encoded DER format or PEM format.

If you are using an SSL certificate in binary format, you cannot install it.

However, you can convert your binary SSL certificate.



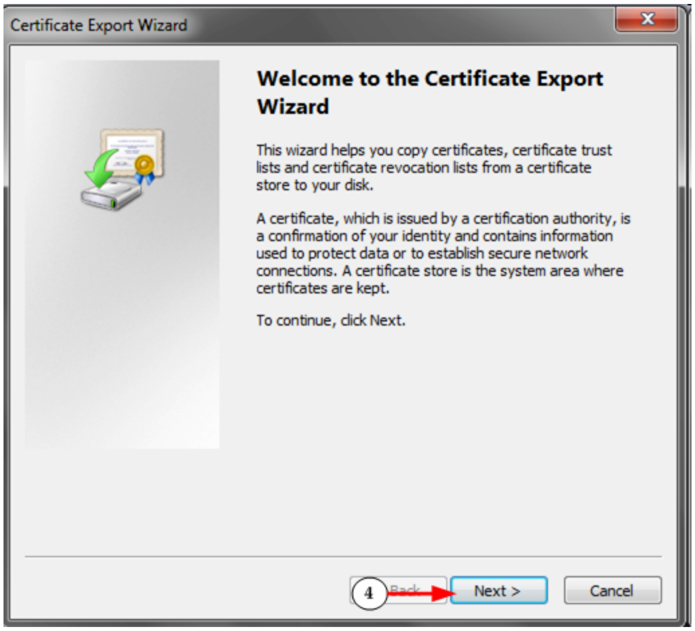
Field	Value
Version	V3
Serial number	0c e7 e0 e5 17 d8 46 fe 8f e5 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	DigiCert Assured ID Root CA, ...
Valid from	Thursday, November 09, 2006...
Valid to	Sunday, November 09, 2031 7...
Subject	DigiCert Assured ID Root CA

1. Locate the DEGHKVM0001.cer binary file on your Windows machine.

   Double-click on the DEGHKVM0001.cer file to open its Certificate dialog.

2. Click the Detail tab.

3. Click "Copy to File...".



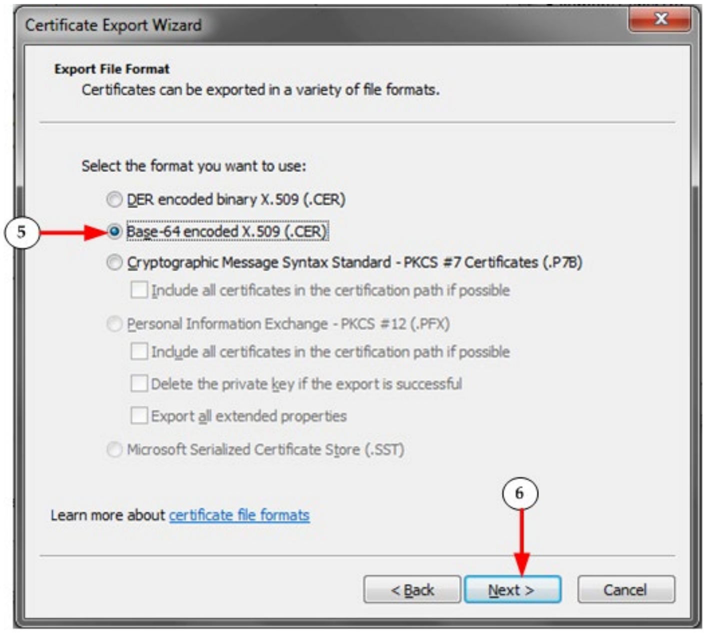
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4. The Certificate Export Wizard opens. Click Next to start the Wizard.



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

5. Select "Base-64 encoded X.509" in the second Wizard dialog.

6. Click Next to save the file as a Base-64 encoded X.509.

You can now install the certificate on your LX II.

Logging In to LX II

Log in to your LX II Remote Console from any workstation with network connectivity. See the Release Notes for supported browser versions.

Logging in and using LX II requires you to allow pop-ups.

For information on security warnings and validation messages, and steps to reduce or eliminate them, see ***Security Warnings and Validation Messages*** (on page 24).

▶ To log in via Remote Console:

1. Launch a supported web browser, and enter the IP address assigned to the LX II.
2. A default client is launched based on your PC and browser settings. See ***KVM Clients*** (on page 148). You can also choose a client by entering the URL directly. See ***KVM Client Launching*** (on page 148).
3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable). If security warnings appear, click to accept.

Chapter 5 Interface and Navigation

The LX II Remote Console and the LX II Local Console are web-based graphical user interfaces.

Use the Remote Console interface to configure and manage the LX II over a network connection.

Use the Local Console interface to access the LX II while at the rack.

Access targets from either the Remote or Local console from one of the supported KVM clients.

In This Chapter

LX II Remote Console Interface

The LX II 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 II and to remotely administer the LX II.

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

There are many similarities among the LX II Local Console and the LX II 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 II Remote Console but not the LX II Local Console:

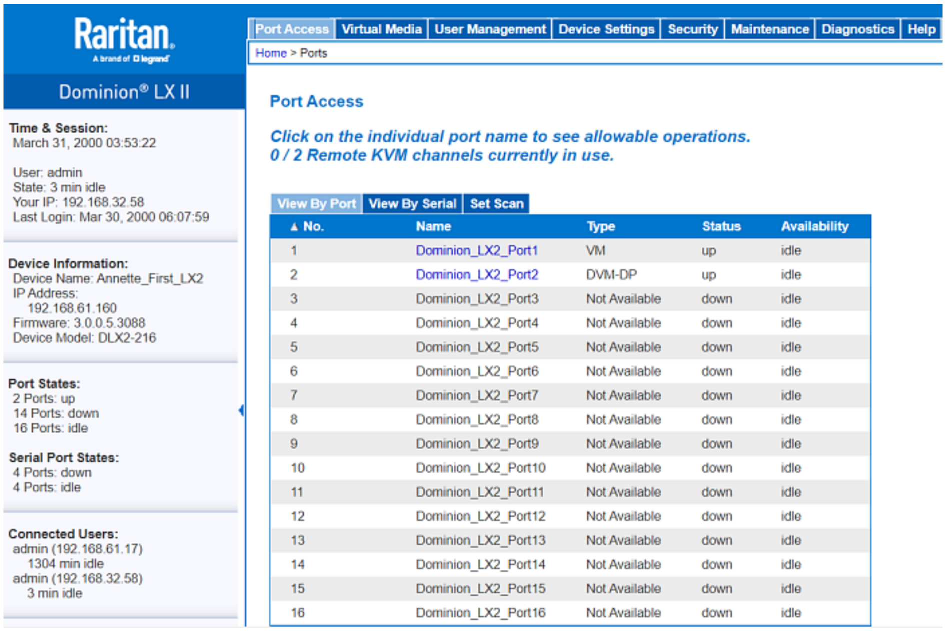
- Virtual Media
- Favorites
- Backup/Restore
- Firmware Upgrade
- SSL Certificates

Port Access Page (Remote Console Display)

After a successful login, the Port Access page opens listing all ports along with their status and availability.

Ports connected to KVM target servers are displayed in blue. Right-click on any of these ports to open the Port Action menu.

If a port has no CIM connected or is connected to a CIM with no name, a default port name of Dominion_LX2_PortNumber is assigned to the port. PortNumber is the number of the LX II physical port.



Time & Session:
March 31, 2000 03:53:22

User: admin
State: 3 min idle
Your IP: 192.168.32.58
Last Login: Mar 30, 2000 06:07:59

Device Information:
Device Name: Annette_First_LX2
IP Address:
192.168.61.160
Firmware: 3.0.0.5.3088
Device Model: DLX2-216

Port States:
2 Ports: up
14 Ports: down
16 Ports: idle

Serial Port States:
4 Ports: down
4 Ports: idle

Connected Users:
admin (192.168.61.17)
1304 min idle
admin (192.168.32.58)
3 min idle

Port Access

Click on the individual port name to see allowable operations.
0 / 2 Remote KVM channels currently in use.

▲ No.	Name	Type	Status	Availability
1	Dominion_LX2_Port1	VM	up	idle
2	Dominion_LX2_Port2	DVM-DP	up	idle
3	Dominion_LX2_Port3	Not Available	down	idle
4	Dominion_LX2_Port4	Not Available	down	idle
5	Dominion_LX2_Port5	Not Available	down	idle
6	Dominion_LX2_Port6	Not Available	down	idle
7	Dominion_LX2_Port7	Not Available	down	idle
8	Dominion_LX2_Port8	Not Available	down	idle
9	Dominion_LX2_Port9	Not Available	down	idle
10	Dominion_LX2_Port10	Not Available	down	idle
11	Dominion_LX2_Port11	Not Available	down	idle
12	Dominion_LX2_Port12	Not Available	down	idle
13	Dominion_LX2_Port13	Not Available	down	idle
14	Dominion_LX2_Port14	Not Available	down	idle
15	Dominion_LX2_Port15	Not Available	down	idle
16	Dominion_LX2_Port16	Not Available	down	idle

Two tabs are provided on the page allowing you to view by port or scan ports. A View by Serial tab is available when an optional DSAM is connected.

You can sort by Port Number, Port Name, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading.

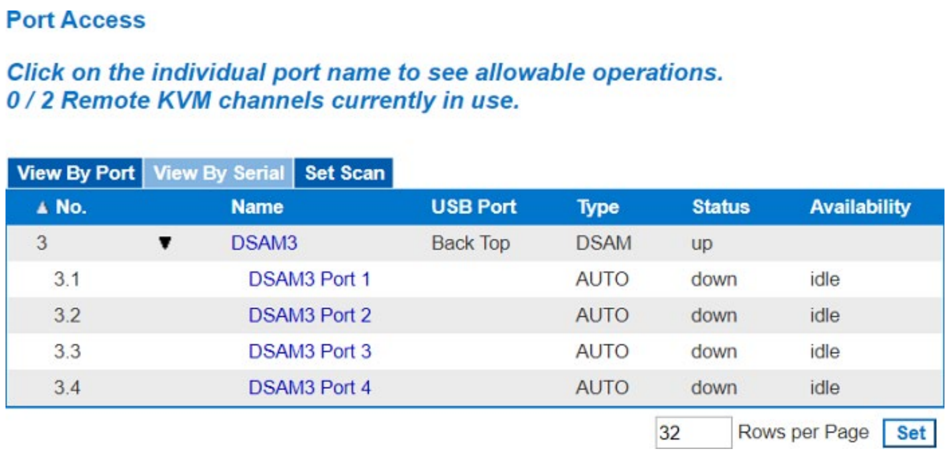
Use the Set Scan tab to scan for the targets that are connected to the LX II. See Scanning Ports - Remote Console

Tiered Devices - Port Access Page

If you are using a tiered configuration in which a base LX II 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.

View by Serial

The View By Serial tab is visible when a Dominion Serial Access Module (DSAM) is connected by USB. Up to 4 serial targets can be connected to the DSAM by USB.



Port Access

Click on the individual port name to see allowable operations.
0 / 2 Remote KVM channels currently in use.

▲ No.		Name	USB Port	Type	Status	Availability
3	▼	DSAM3	Back Top	DSAM	up	
3.1		DSAM3 Port 1		AUTO	down	idle
3.2		DSAM3 Port 2		AUTO	down	idle
3.3		DSAM3 Port 3		AUTO	down	idle
3.4		DSAM3 Port 4		AUTO	down	idle

32 Rows per Page

Set Scan Tab

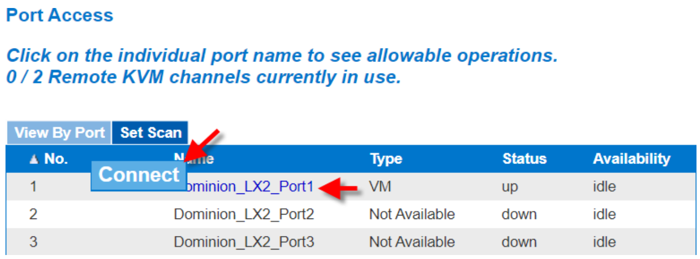
The port scanning feature is accessed from the Set Scan tab on the Port Access page. The feature allows you to define a set of KVM targets to be scanned. Thumbnail views of the scanned targets are also available. Select a thumbnail to open that target in its Virtual KVM Client window.

See Scanning Ports - Remote Console for more information.

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.



Port Access

Click on the individual port name to see allowable operations.
0 / 2 Remote KVM channels currently in use.

▲ No.	Name	Type	Status	Availability
1	ominion_LX2_Port1	VM	up	idle
2	Dominion_LX2_Port2	Not Available	down	idle
3	Dominion_LX2_Port3	Not Available	down	idle

Connect

- Connect - Creates a new connection to the target server

  For the LX II Remote Console, a new KVM Client page appears.

  For the LX II Local Console, the display switches to the target server, and switches away from the local user interface.

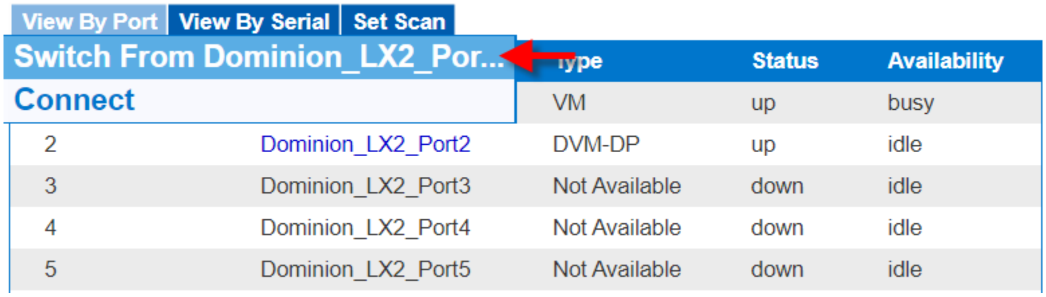
  On the local port, the LX II Local Console interface must be visible in order to perform the switch.

  Hot key switching is also available from the local port.

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

Switch From

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

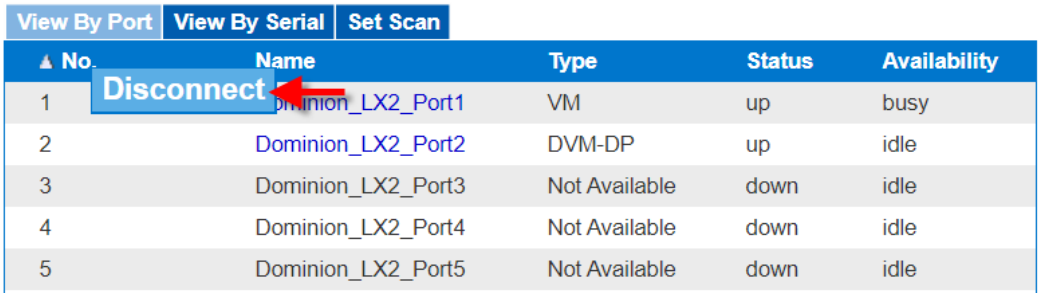


		Type	Status	Availability
		VM	up	busy
2	Dominion_LX2_Port2	DVM-DP	up	idle
3	Dominion_LX2_Port3	Not Available	down	idle
4	Dominion_LX2_Port4	Not Available	down	idle
5	Dominion_LX2_Port5	Not Available	down	idle

Disconnect

- Disconnect - Disconnects this port and closes the 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 II Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.

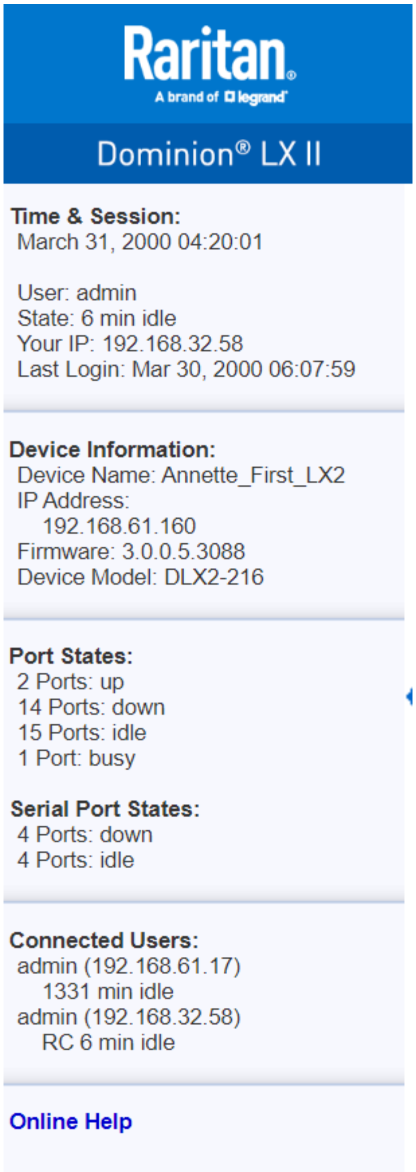


▲ No.	Name	Type	Status	Availability
1	Dominion_LX2_Port1	VM	up	busy
2	Dominion_LX2_Port2	DVM-DP	up	idle
3	Dominion_LX2_Port3	Not Available	down	idle
4	Dominion_LX2_Port4	Not Available	down	idle
5	Dominion_LX2_Port5	Not Available	down	idle

Left Panel

The left panel of the LX II interface contains the following information.

Note that some information is conditional - meaning it is displayed based on your role, features being used and so on. Conditional information is noted here.



Time & Session:
March 31, 2000 04:20:01

User: admin
State: 6 min idle
Your IP: 192.168.32.58
Last Login: Mar 30, 2000 06:07:59

Device Information:
Device Name: Annette_First_LX2
IP Address:
192.168.61.160
Firmware: 3.0.0.5.3088
Device Model: DLX2-216

Port States:
2 Ports: up
14 Ports: down
15 Ports: idle
1 Port: busy

Serial Port States:
4 Ports: down
4 Ports: idle

Connected Users:
admin (192.168.61.17)
1331 min idle
admin (192.168.32.58)
RC 6 min idle

Online Help

Information	Description	When displayed?
Time & Session	The date and time the current session started	Always

Information	Description	When displayed?
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 II	Always
Last Login	The last login date and time	Always
Device Information	Information specific to the LX II you are using	Always
Device Name	Name assigned to the device	Always
IP Address	The IP address of the LX II	Always
Firmware	Current version of firmware	Always
Device Model	Model of the LX II	Always
Configured As Base or Configured As Tiered	If you are using a tiering configuration, this indicates if the LX II you are accessing is the base device or a tiered device.	When the LX II is part of a tiered configuration
Port States	The statuses of the ports being used by the LX II	Always
Connected Users	The users, identified by their username and IP address, who are currently connected to the LX II	Always
Online Help	Links to online help	Always

LX II Local Console Interface

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

For details on using the Local Console see ***LX II Local Console*** (on page 240).

Chapter 6 LX II Administrator Help

Administrator Help contains information specific to LX II functions typically performed by LX II application administrators, such as installing and configuring LX II, managing user groups and users, managing security, and so on.

Administrator functions are typically performed in the LX II Remote Console and/or from the Local Console.

Functions typically performed by end users rather than administrators, and some functions performed from the Remote Console or Local Console are described in their own sections of help.

These functions include using virtual media, configuring mouse settings, using the scan port feature, configuring video options and so on.

In This Chapter

USB Profiles

Overview

To broaden the LX II's compatibility with different KVM target servers, Raritan provides a standard selection of USB configuration profiles for a wide range of operating system and BIOS-level server implementations.

The Generic (default) USB profile meets the needs of the vast majority of deployed KVM target server configurations.

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

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

USB profiles are configured on the Device Settings > Port Configuration > Port page of the LX II Remote and Local Consoles.

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

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

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

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

CIM Compatibility

In order to make use of USB profiles, you must use a virtual media CIM with updated firmware. For a list of virtual media CIMs, see ***Supported Computer Interface Module (CIMs) Specifications*** (on page 253).

Available USB Profiles

The current release of the LX II comes with the selection of USB profiles described in the following table. New profiles may be included with each firmware upgrade provided by Raritan.

USB profile	Description
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS Use either this profile or 'Generic' profile for Dell PowerEdge 1950/2950/2970/6950/R200 BIOS. Restrictions:

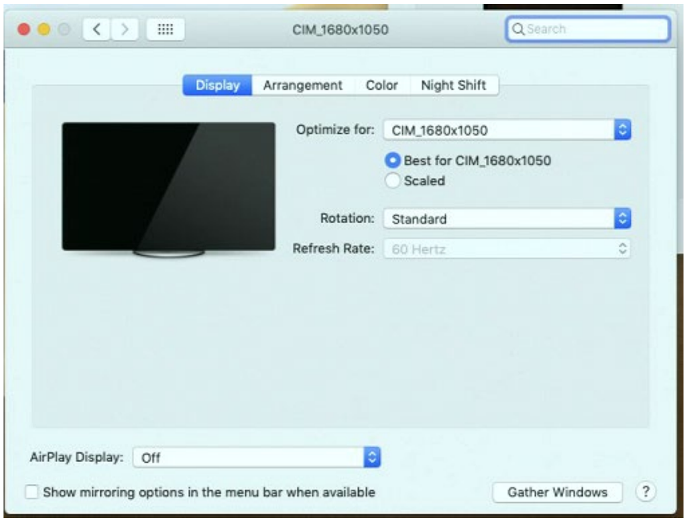
USB profile	Description
	▪ None
BIOS Dell OptiPlex ™ Keyboard and Mouse Only	Dell OptiPlex BIOS Access (Keyboard and Mouse Only) Use this profile to have keyboard functionality for the Dell OptiPlex BIOS when using D2CIM-VUSB. When using the new D2CIM-DVUSB, use 'Generic' profile. Notice: ▪ Optiplex 210L/280/745/GX620 requires D2CIM-DVUSB with 'Generic' profile to support virtual media Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ No virtual media support
BIOS Dell Optiplex 790	Use this profile for Dell Optiplex 790 during BIOS operations. Warning: ▪ USB enumeration will trigger whenever Virtual Media is connected or disconnected Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Absolute mouse synchronization not supported ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS Dell Optiplex 790 Keyboard Only	Use this profile for Dell Optiplex 790 when using Keyboard Macros during BIOS operations. Only keyboard is enabled with this profile. Restrictions: ▪ Mouse is disabled. ▪ Virtual CD-ROM and disk drives are disabled.

USB profile	Description
BIOS DellPowerEdge Keyboard and Mouse Only	Dell PowerEdge BIOS Access (Keyboard and Mouse Only) Use this profile to have keyboard functionality for the Dell PowerEdge BIOS when using D2CIM-VUSB. When using the new D2CIM-DVUSB, use 'Generic' profile. Notice: ▪ PowerEdge 650/1650/1750/2600/2650 BIOS do not support USB CD-ROM and disk drives as a bootable device ▪ PowerEdge 750/850/860/1850/2850/SC1425 BIOS requires D2CIM-DVUSB with 'Generic' profile to support virtual media ▪ Use 'BIOS Dell PowerEdge 1950/2950/2970/6950/R200' or 'Generic' profile for PowerEdge 1950/2950/2970/6950/R200 when operating in the BIOS Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Absolute mouse synchronization™ not supported ▪ No virtual media support
BIOS ASUS P4C800 Motherboard	Use this profile to access BIOS and boot from Virtual Media on Asus P4C800-based systems. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS Generic	BIOS Generic Use this profile when Generic OS profile does not work on the BIOS. WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Absolute mouse synchronization™ not supported ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS Use this profile for HP Proliant DL145 PhoenixBIOS during OS installation. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Use this profile to boot the HP Compaq DC7100/DC7600 series desktops from virtual media.

USB profile	Description
	Restrictions: ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS Use this profile for the IBM® Thinkcentre Lenovo system board (model 828841U) during BIOS operations. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
IBM BladeCenter H with Advanced Management Module	Use this profile to enable virtual media functionality when D2CIM-VUSB or D2CIM-DVUSB is connected to the Advanced Management Module. Restrictions: ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 and X61 (boot from virtual media) Use this profile to boot the T61 and X61 series laptops from virtual media. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s)
Generic	The generic USB profile can be used for Windows 2000® operating system, Windows XP® operating system, Windows Vista® operating system and later. Note: Microsoft no longer supports some legacy Windows OS, and using them may be a security risk. Restrictions: ▪ None
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) Use this profile for the HP Proliant DL360/DL380 G4 series server when installing OS using HP SmartStart CD. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Absolute mouse synchronization™ not supported
HP Proliant DL360/DL380 G4 (Windows 2003® Server Installation)	HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation) Use this profile for the HP Proliant DL360/DL380 G4 series server when installing Windows 2003 Server without the help of HP SmartStart CD. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s)
Linux®	Generic Linux profile This is the generic Linux profile; use it for Redhat Enterprise Linux, SuSE

USB profile	Description
	Linux Enterprise Desktop and similar distributions. Restrictions: ▪ Absolute mouse synchronization™ not supported
BIOS Mac®	BIOS Mac Use this profile for Mac BIOS. Restrictions: ▪ Absolute mouse synchronization™ is not supported ▪ Virtual CD-ROM and disk drives cannot be used simultaneously If you use this USB profile, see ***Mouse Modes when Using the Mac Boot Menu*** (on page 46) for information mouse modes when using the Mac Boot Menu
MAC OS X® 10.4.9 (and later)	Mac OS X version 10.4.9 (and later) This profile compensates the scaling of mouse coordinates introduced in recent versions of Mac OS X. Select this if the remote and local mouse positions get out of sync near the desktop borders. Restrictions: ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
RUBY Industrial Mainboard (AwardBIOS)	RUBY Industrial Mainboard (AwardBIOS) Use this profile for the RUBY-9715VG2A series industrial mainboards with Phoenix/AwardBIOS v6.00PG. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro Mainboard Phoenix AwardBIOS Use this profile for the Supermicro series mainboards with Phoenix AwardBIOS. Restrictions: ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
Suse 9.2	SuSE Linux 9.2 Use this for SuSE Linux 9.2 distribution. Restrictions: ▪ Absolute mouse synchronization™ not supported ▪ USB bus speed limited to full-speed (12 MBit/s)
Troubleshooting 1	Troubleshooting Profile 1 ▪ Mass Storage first ▪ Keyboard and Mouse (Type 1) ▪ USB bus speed limited to full-speed (12 MBit/s)

USB profile	Description
	▪ Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.
Troubleshooting 2	Troubleshooting Profile 2 ▪ Keyboard and Mouse (Type 2) first ▪ Mass Storage ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.
Troubleshooting 3	Troubleshooting Profile 3 ▪ Mass Storage first ▪ Keyboard and Mouse (Type 2) ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.
Use Full Speed for Virtual Media CIM	Use Full Speed for virtual media CIM This profile can be useful for BIOS that cannot handle High Speed USB devices. Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s)
Use Full Speed for Keyboard and Mouse USB	This profile will set the Keyboard and Mouse USB interface on the Dual-VM CIM to Full Speed. Useful for devices that cannot operate properly with the Low Speed USB settings. Restrictions: ▪ USB bus speed set to full-speed (12 MBit/s) on Keyboard and Mouse USB interface

USB profile	Description
Mac USB-C	Use this profile with the D2CIM-VUSB-USBC CIM on Mac targets. ▪ Make sure the resolution on Mac Notebook targets is set to "Best for CIM" instead of "Scaled CIM".  CIM_1680x1050 Search Display Arrangement Color Night Shift Gather Windows ? Optimize for: CIM_1680x1050 ● Best for CIM_1680x1050 ○ Scaled Rotation: Standard Refresh Rate: 60 Hertz AirPlay Display: Off □ Show mirroring options in the menu bar when available

Mouse Modes when Using the Mac Boot Menu

When working with the "BIOS Mac" USB profile, to use the mouse in the Mac Boot Menu, you must use Single Mouse mode since Absolute Mouse Mode is not supported in the BIOS.

▶ To configure the mouse to work at the Boot menu:

1. Reboot the Mac and press the Option key during the reboot to open the Boot menu. The mouse will not respond at this point.
2. Select Single Mouse mode. The mouse now responds.

   Note: Mouse speed may be slow while in Single Mouse mode.

3. Once you are out of the Boot menu and back to the OS X, exit Single Mouse mode and switch back to Absolute Mouse mode.

Selecting Profiles for a KVM Port

The LX II comes with a set of USB profiles that you can assign to a KVM port based on the characteristics of the KVM target server it connects to. You assign USB profiles to a KVM port in the Device Settings > Port Configuration > Port page in either the Remote or Local Console.

Administrators designate the profiles that are most likely to be needed for a specific target. These profiles are then available for selection. If a profile has not been made available, you can access any of the available profiles by selecting USB Profile > Other Profiles.

Assigning USB profiles to a KVM port makes those profiles available to a user when connected to a KVM target server. If required, the user can select a USB profile from the USB Profile menu.

For information about assigning USB profiles to a KVM port, see ***Configuring USB Profiles (Port Page)*** (on page 81).

User Management

User Groups

The LX II stores an internal list of all user profiles and user groups to determine access authorization and permissions. This information is stored internally in an encrypted format.

All users must be authenticated to access LX II.

LX II can be configured to authenticate users locally and/or remotely using LDAP/LDAPS or RADIUS. Remote user authentication is processed before local authentication if remote authentication is enabled.

Every LX II 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	An individual group is essentially a “group” of one. That is,

User	Description
Group	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 II.

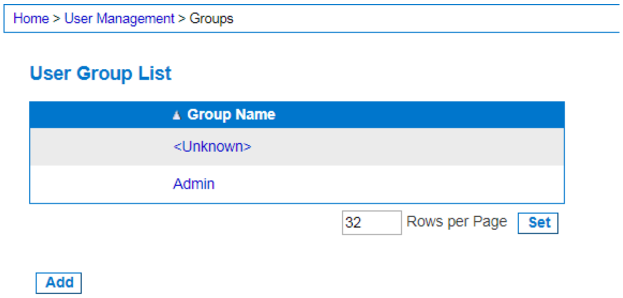
User Group List

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 II 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 appliance uses group information to determine the user's permissions, such as which server ports are accessible, whether rebooting the appliance 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
4. Specify the server ports and the type of access for each user belonging to this group. See Setting Port Permissions
5. Click OK.

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 Access While Under CC-SG Management	▪ Not applicable on LX II
Device Settings	Network settings, date/time settings, port configuration, device services, event management (SNMP, Syslog), virtual media file server setups.
Diagnostics	Network interface status, network statistics, ping host, trace route to host, LX II diagnostics.
Hide Client Toolbar and Menu Bar	Removes toolbars and menu bars from AKC, VKC, and HKC so that users can only use the Scale Video and Exit functions.
Maintenance	Backup and restore database, firmware upgrade, reboot. Factory reset is available from the local console only.
Modem Access	Permission to use the modem to connect to the LX II device.

Permission	Description
PC-Share	Simultaneous access to the same target by multiple users. If you are using a tiered configuration in which a base LX II device is used to access multiple, additional tiered devices, all devices must share the same PC-Share setting.
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL.
User Management	User and group management, remote, authentication (LDAP/LDAPS/RADIUS), login settings. If you are using a tiered configuration in which a base LX II device is used to access multiple other tiered devices, user, user group and remote authentication settings must be consistent across all devices.

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. 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 and power control access will also be granted. 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. Control access must be granted for audio or smart card related controls to be active.

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.

Note: If you are using a tiered configuration in which a base LX II device is used to access multiple other tiered devices, the tiered device enforces individual port control levels. See ***Configuring and Enabling Tiering*** (on page 87) 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 a 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.
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.
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, then click OK to confirm.

Users

Users must be granted user names and passwords to gain access to the LX II. This information is used to authenticate users attempting to access your LX II.

Up to 254 users can be created for each user group.

If you are using a tiered configuration in which a base LX II 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's access to the tiered device's ports is controlled by the user groups and permissions set on the tiered device. See ***Configuring and Enabling Tiering*** (on page 87)for more information on tiering. See ***User Permissions in Tiered Configurations*** (on page 88) for examples.

Adding a New User

*Note: Since you must assign a user to an existing user group when you add them, it is a good idea to define user groups before creating LX II users. See **Adding a New User Group**.*

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

*Note: A user 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 51).

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

View the LX II Users List

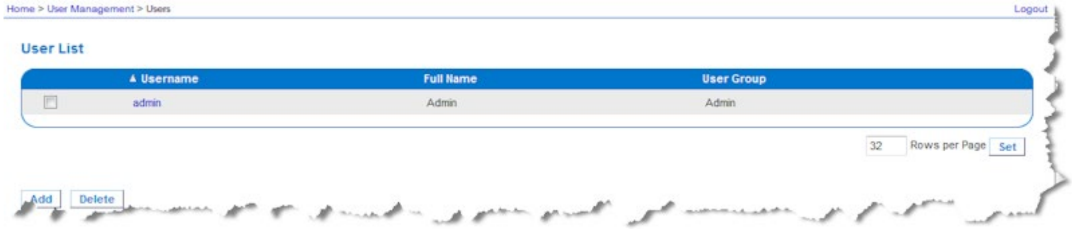
The User List page displays a list of all users including their user name, full name, and user group. The list can be sorted on any of the columns by clicking on the column name. From the User List page, you can add, modify, or delete users.

LX II users with User Management privileges can disconnect users from ports or log them off (force log off) as needed. See ***Disconnecting Users from Ports*** (on page 54) and ***Logging Users Off the LX II (Force Logoff)*** (on page 54) respectively.

To view the target ports each user is connected to, see ***View Users by Port*** (on page 53).

To view the list of users:

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



User List

	▲ Username	Full Name	User Group
□	admin	Admin	Admin

32 Rows per Page

View Users by Port

The User By Ports page lists all authenticated local and remote users and ports they are being connected to. Only permanent connections to ports are listed. Ports being accessed when scanning for ports are not listed.

If the same user is logged on from more than one client, their username appears on the page for each connection they have made. For example, if a user has logged on from two (2) different clients, their name is listed twice.

This page contains the following user and port information:

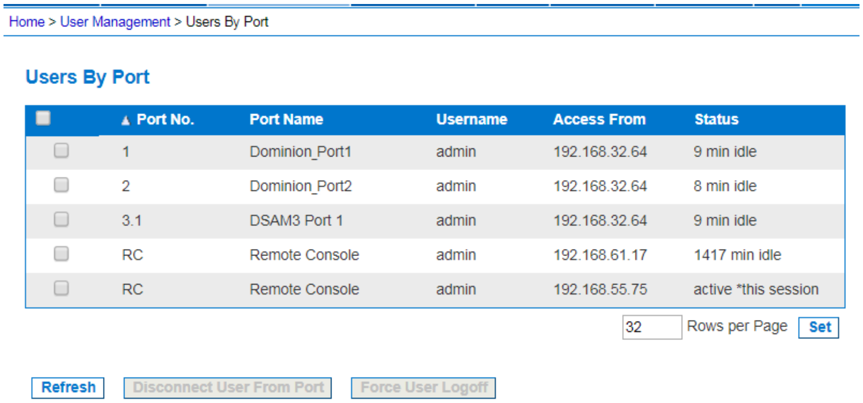
- Port Number - port number assigned to the port the user is connected to
- Port Name - port name assigned to the port the user is connected to

Note: If user is not connected to a target, 'Local Console' or 'Remote Console' is displayed under the Port Name.

- Username - username for user logins and target connections
- Access From - IP address of client PC accessing the LX II
- Status - current Active or Inactive status of the connection

▶ To view users by port:

- Choose User Management > User by Port. The Users by Port page opens.


Home > User Management > Users By Port
Users By Port
32
Rows per Page
Set
Refresh
Disconnect User From Port
Force User Logoff

□	▲ Port No.	Port Name	Username	Access From	Status
□	1	Dominion_Port1	admin	192.168.32.64	9 min idle
□	2	Dominion_Port2	admin	192.168.32.64	8 min idle
□	3.1	DSAM3 Port 1	admin	192.168.32.64	9 min idle
□	RC	Remote Console	admin	192.168.61.17	1417 min idle
□	RC	Remote Console	admin	192.168.55.75	active *this session

Disconnecting Users from Ports

Disconnecting users disconnects them from the target port *without* logging them off of LX II.

This is unlike the force user logoff LX II function that disconnects users from the target port and logs them off of LX II. See ***Logging Users Off the LX II (Force Logoff)*** (on page 54) for information.

If the "Disconnect User from Port" is disabled, the user is not logged on to the port at the current time.

1. Choose User Management > Users by Port. The Users by Port page opens.
2. Select the checkbox next to the username of the person you want to disconnect from the target.
3. Click "Disconnect User from Port".
4. Click OK on the confirmation message to disconnect the user.
5. A confirmation message is displayed to indicate that the user was disconnected.

Logging Users Off the LX II (Force Logoff)

If you are an administrator, you are able to log off any authenticated user who is logged on to the LX II. Users can also be disconnected at the port level. See ***Disconnecting Users from Ports*** (on page 54).

▶ To log a user off the LX II:

1. Choose User Management > Users by Port. The Users by Port page opens.

2. Select the checkbox next to the username of the person you want to disconnect from the target.
3. Click Force User Logoff.
4. Click OK on the Logoff User confirmation message.

Modifying an Existing User

▶ **To modify an existing user:**

1. Open the User List page by choosing User Management > User List.
2. Locate the user from among those listed on the User List page.
3. Click the user name. The User page opens.
4. On the User page, change the appropriate fields. See ***Adding a New User*** (on page 52) for information about how to get access the User page.
5. To delete a user, click Delete. You are prompted to confirm the deletion.
6. Click OK.

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 II 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 II 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 II.

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:**

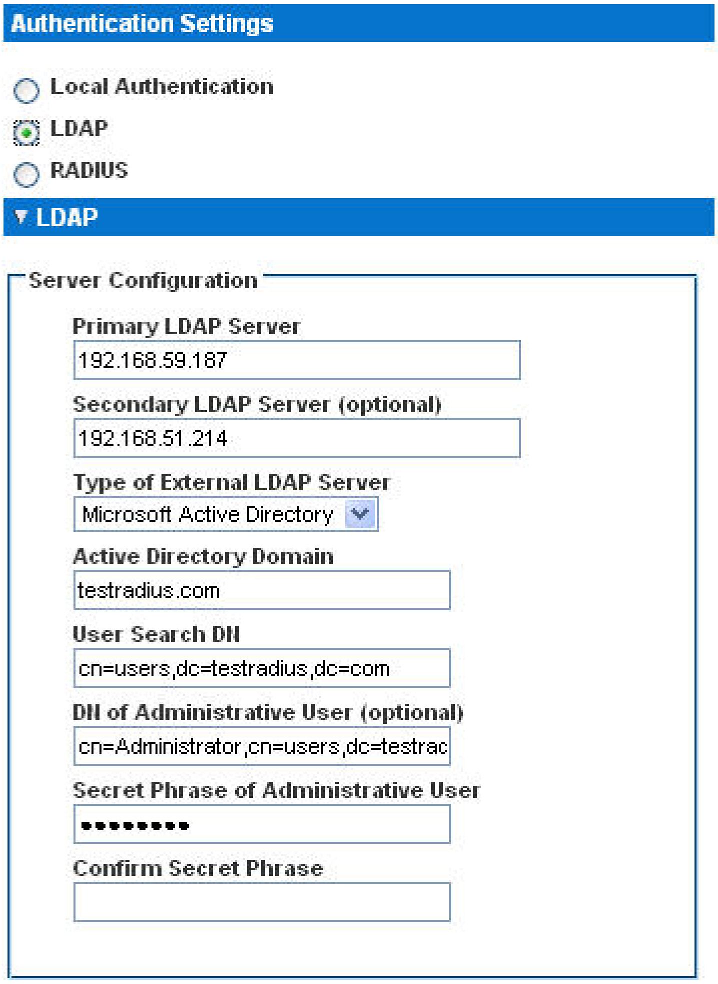
1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Select the LDAP radio button to enable the LDAP section of the page.
3. Click the ► LDAP icon to expand the LDAP section of the page.

   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: 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.

7. Type the name of the Active Directory Domain if you selected Microsoft Active Directory. For example, *acme.com*. Consult your Active Directive Administrator for a specific domain name.
8. 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=company,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.
9. 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**

10. 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: 192.168.59.187

Secondary LDAP Server (optional): 192.168.51.214

Type of External LDAP Server: Microsoft Active Directory

Active Directory Domain: testradius.com

User Search DN: cn=users,dc=testradius,dc=com

DN of Administrative User (optional): cn=Administrator,cn=users,dc=testrac

Secret Phrase of Administrative User: ●●●●●●●●●

Confirm Secret Phrase:

LDAP/Secure LDAP

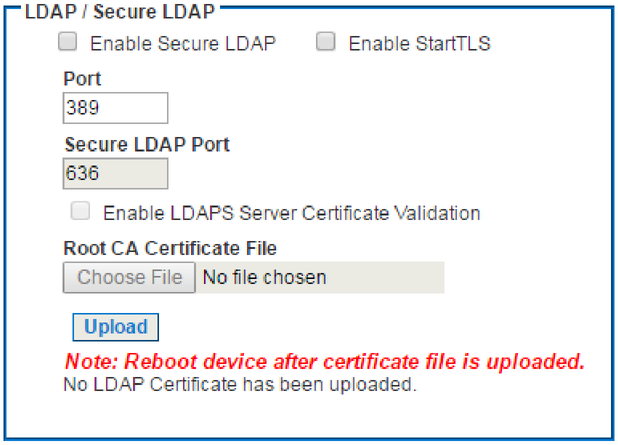
11. For an encrypted connection, select the Enable Secure LDAP checkbox to use SSL, or select the Enable StartTLS checkbox to use StartTLS. Both options enable the Enable LDAPS Server Certificate Validation checkbox.
    - For an unsecured connection, do not enable Secure LDAP or StartTLS. The default port for unsecured connections is 389. Use the standard LDAP TCP port or specify another port.

- SSL is a cryptographic protocol that allows LX II to communicate securely with the LDAP/LDAPS server. The default Secure LDAP port is 636, or you may specify another port. This field is used only when Enable Secure LDAP is selected.
- StartTLS is a command that upgrades an unsecured connection to a secure connection using SSL/TLS. StartTLS does not require a specific port. The standard LDAP port 389 is default.

12. 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.

13. If needed, upload the Root CA Certificate File. This field is enabled for secured connections only. 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 II in order for the new certificate to take effect.



LDAP / Secure LDAP

☐ Enable Secure LDAP ☐ Enable StartTLS

Port

389

Secure LDAP Port

636

☐ Enable LDAPS Server Certificate Validation

Root CA Certificate File

Choose File No file chosen

Upload

Note: Reboot device after certificate file is uploaded.

No LDAP Certificate has been uploaded.

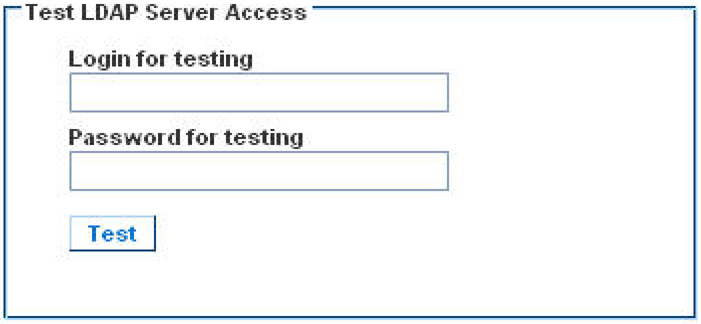
Test LDAP Server Access

14. To test the LDAP configuration, enter the login name and password in the "Login for testing" and "Password for testing" fields. Click Test.

    The test login name and password should be the pair you entered to access the LX II. It is also username and password the LDAP server uses to authenticate you.

The LX II then tests the LDAP configuration from the Authentication Settings page. This is helpful due to the complexity sometimes encountered when configuring the LDAP server and LX II for remote authentication.

Once the test is completed, you will see a success message or a detailed error message. In a successful test, group information retrieved from the remote LDAP server is also displayed.



Returning User Group Information from Active Directory Server

The LX II supports user authentication to Active Directory® (AD) without requiring that users be defined locally on the LX II. 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 II policies and user group privileges that are applied locally to AD user groups.

IMPORTANT: If you are an existing user, and have already configured the Active Directory server by changing the AD schema, the LX II still supports this configuration and you do not need to perform the following operations. See Updating the LDAP Schema for information about updating the AD LDAP/LDAPS schema.

▶ To enable your AD server on the LX II:

1. Using the LX II, 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 II users to the groups created in step 2.
4. From the LX II, enable and configure your AD server properly. See Implementing LDAP/LDAPS Remote Authentication.

Important Notes

- Group Name is case sensitive.
- The LX II 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 II group configuration, the LX II 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:**

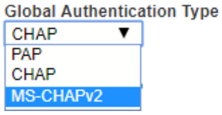
1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Click the RADIUS radio button to enable the RADIUS section of the page.
3. Click the ► RADIUS icon to expand the RADIUS section of the page.
4. In the Primary Radius Server and Secondary Radius Server fields, 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 II 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 II 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 II will send an authentication request to the RADIUS server.

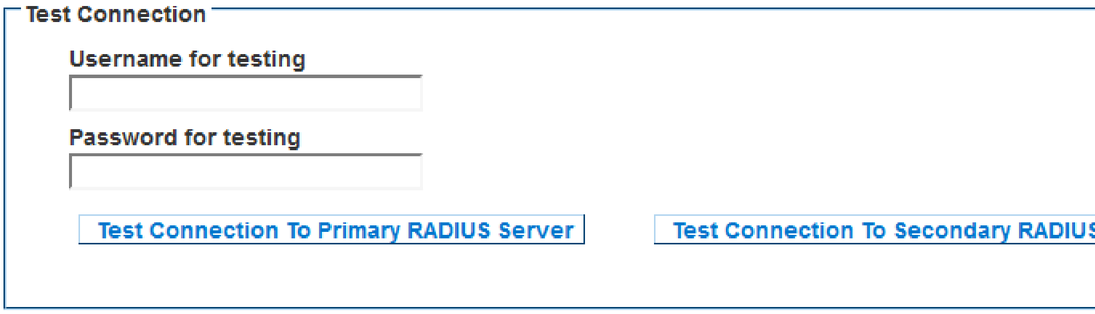
10. Choose the Global Authentication Type in the drop-down list:



- 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.
- MSCHAPv2 - Provides mutual authentication of server and client. Both client and server issue challenges and verify the responses. Considered to be more secure than PAP or CHAP.

11. Click OK to save.

Test Connection:


Test Connection
Username for testing
Password for testing
Test Connection To Primary RADIUS Server
Test Connection To Secondary RADIUS

1. Enter the login name and password in the "Login for testing" and "Password for testing" fields.
   - The test login name and password should be the pair you entered to access the LX II that the RADIUS server uses to authenticate you.
   - The LX II then tests the configuration from the Authentication Settings page. This is helpful due to the complexity sometimes encountered when configuring the RADIUS server and LX II for remote authentication.
2. Once the test is completed, you will see a success message or a detailed error message. In a successful test, group information retrieved from the remote RADIUS server is also displayed.

Cisco ACS 5.x for RADIUS Authentication

If you are using a Cisco ACS 5.x server, after you have configured the LX II 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 II 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 LX II). 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 II 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 II modem will use to dial back to the user account.

RADIUS Communication Exchange Specifications

The LX II 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 II.
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 II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
Log out	
Accounting-Request(4)	
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 II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

RADIUS Using RSA SecurID Hardware Tokens

LX II supports RSA SecurID Hardware Tokens used with a RADIUS server for two factor authentication

Users will specify their RADIUS password followed by the token ID without a delimiter between.

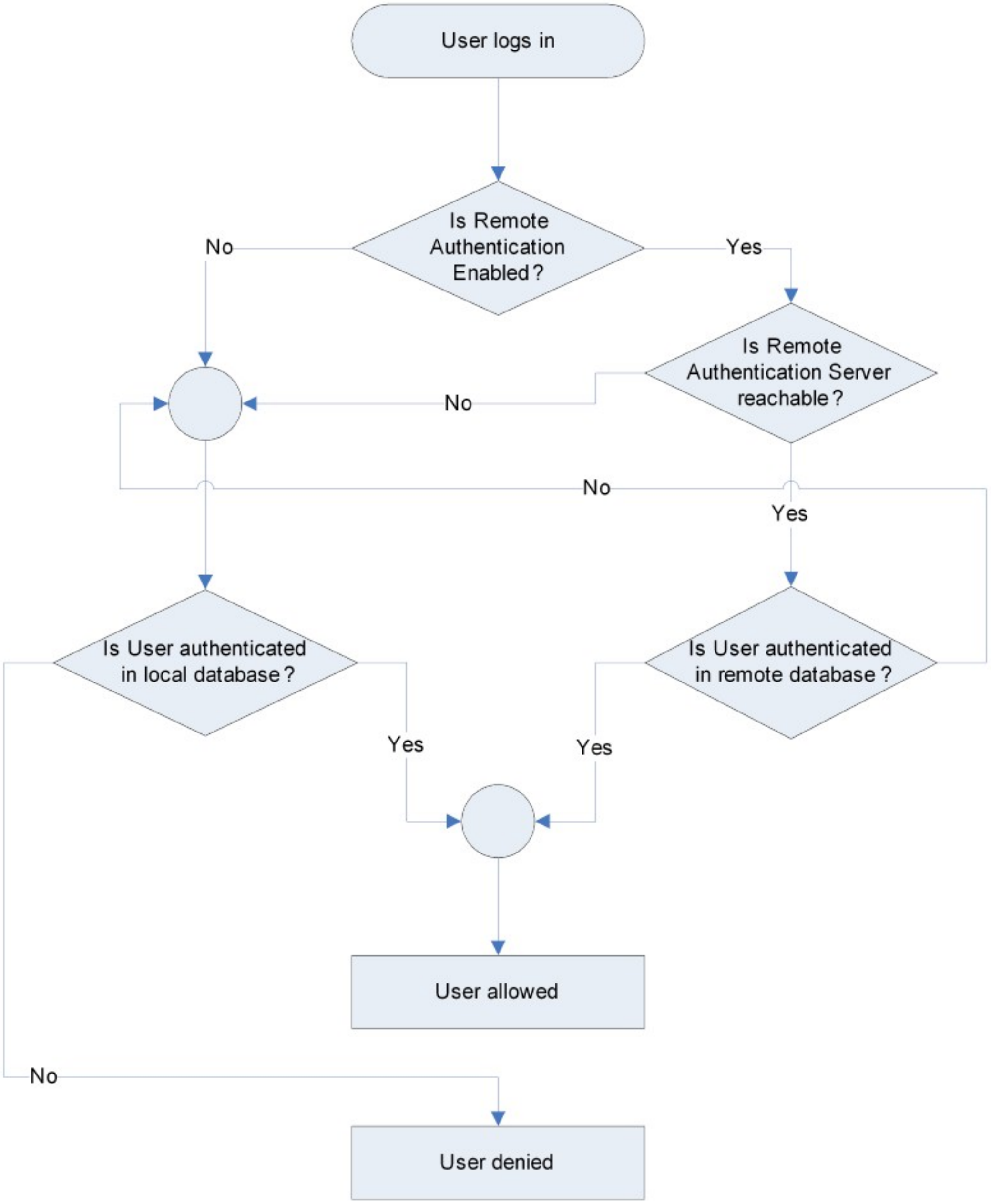
For example:

- password = apple
- token = 1234
- User enters: apple1234

Or, configure the RADIUS server to use only hardware token and no passwords. Users will specify the token ID only.

User Authentication Process

Remote authentication follows the process specified in the flowchart below:

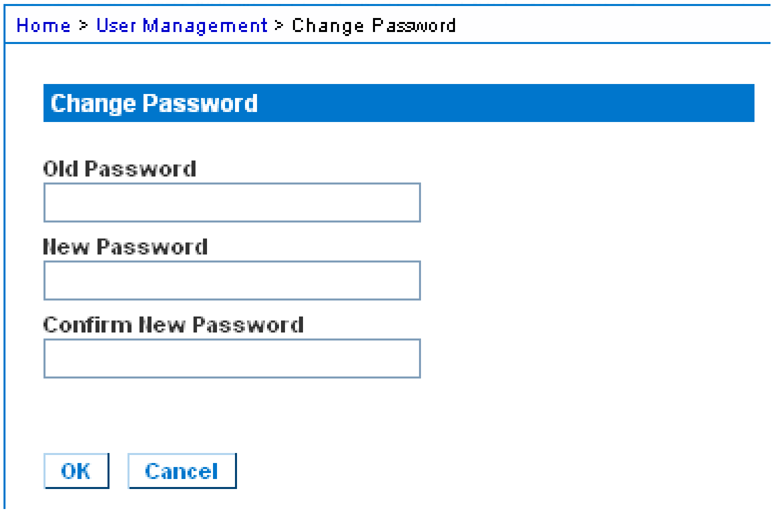

User logs in
Is Remote Authentication Enabled ?
No
Yes
Is Remote Authentication Server reachable ?
No
No
Yes
Is User authenticated in local database ?
Is User authenticated in remote database ?
Yes
Yes
User allowed
No
User denied

Changing a Password

To change your LX II 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 107).*



Device Settings

Network Settings

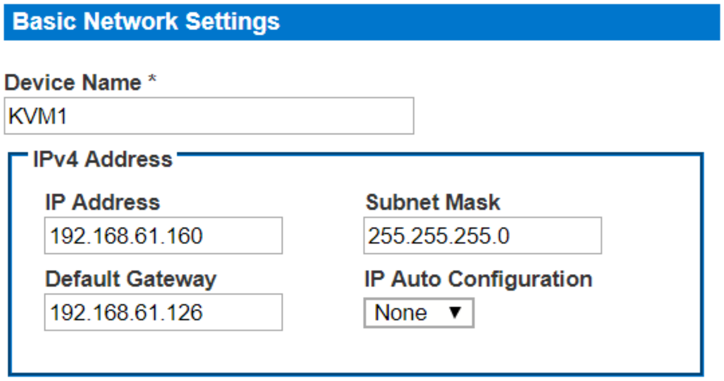
Basic Network Settings - Static IP Address

It is recommended to set a static IP address, rather than using DHCP. DHCP is disabled by default.

If you must use DHCP, see ***Configure the DNS Settings*** (on page 69).

To set a static IP address:

1. Select Device Settings > Network to open the Device Network Settings page.
2. Set the IP Auto Configuration to None in the IPv4 section.
3. If needed, manually specify the network parameters by entering the Default Gateway and then complete the steps that follow.
4. Enter the IP address you want to use to connect to the LX II LAN. The default IP address is 192.168.0.192.
5. Enter the IPv4 Subnet Mask. The default subnet mask is 255.255.255.0.



Basic Network Settings

Device Name *
KVM1

IPv4 Address

IP Address: 192.168.61.160

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.61.126

IP Auto Configuration: None ▼

6. Complete the IPv6 sections, if applicable.
7. Select the IP Auto Configuration.

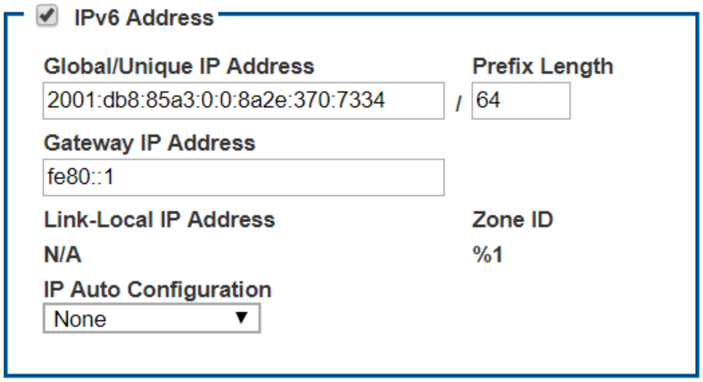
   If *None* is selected, you must manually specify -

   - Global/Unique IP Address - this is the IP address assigned to LX II.
   - Prefix Length - this is the number of bits used in the IPv6 address.
   - Gateway IP Address.

   Select *Router Discovery* to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

   Note that the following additional, read-only information appears in this section -

- Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.
- Zone ID - Identifies the device the address is associated with. Read-Only



☑ IPv6 Address

Global/Unique IP Address: 2001:db8:85a3:0:0:8a2e:370:7334 / Prefix Length: 64

Gateway IP Address: fe80::1

Link-Local IP Address: N/A

Zone ID: %1

IP Auto Configuration: None

8. Select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary address is used if the primary DNS server connection is lost due to an outage.

   Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when LX II is configured in DHCP mode

9. When finished, click OK.

   Your LX II device is now accessible via the configured IP address.

Configure the DNS Settings

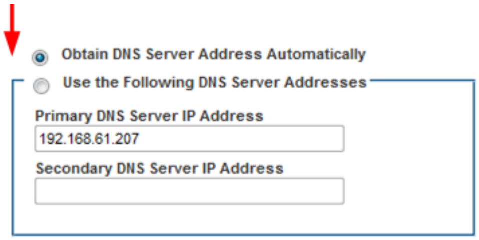
It is recommended to set a static IP address. See ***Basic Network Settings - Static IP Address*** (on page 68).

If you must use DHCP, enable it in the Basic Network Settings, then configure the DNS settings.

▶ To configure the DNS settings:

1. Select Device Settings > Network to open the Device Network Settings page. Select DHCP in the IP Auto Configuration field.
2. Do one of the following to configure DNS -
   - "Obtain DNS Server Address Automatically"

- "Use the Following DNS Server Addresses"

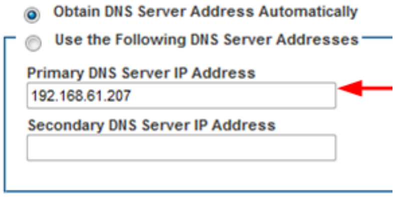


● Obtain DNS Server Address Automatically

○ Use the Following DNS Server Addresses

Primary DNS Server IP Address: 192.168.61.207

Secondary DNS Server IP Address:



● Obtain DNS Server Address Automatically

○ Use the Following DNS Server Addresses

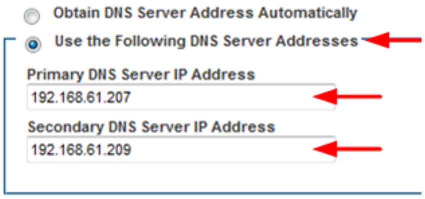
Primary DNS Server IP Address: 192.168.61.207

Secondary DNS Server IP Address:

a. Select "Obtain DNS Server Address Automatically" if DHCP is selected.

The DNS information is then provided by the DHCP server that is used.

When finished, click OK. Your LX II device is now network accessible.



○ Obtain DNS Server Address Automatically

● Use the Following DNS Server Addresses

Primary DNS Server IP Address: 192.168.61.207

Secondary DNS Server IP Address: 192.168.61.209

b. Enter the following information if the "Use the Following DNS Server Addresses" is selected -

   - Primary DNS Server IP Address
   - Secondary DNS Server IP Address

   These secondary DNS address is used if the primary DNS server connection is lost due to an outage.

   Even if DHCP is selected in the IPv4 section, enter the primary and secondary addresses since these addresses are used to connect to the DNS server.

When finished, click OK.

LAN Interface Settings

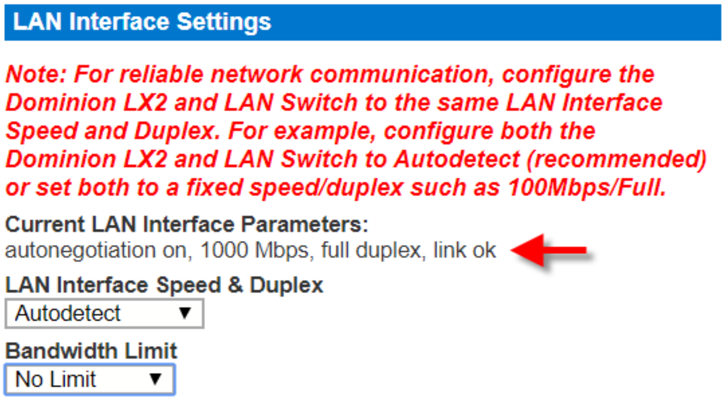
The LAN interface settings include speed and duplex mode and bandwidth limit options.

For reliable network communication, configure the LX II and the LAN switch to the same LAN interface speed and duplex. For example, configure both the LX II and LAN switch to Autodetect, the recommended setting. Or, set both to a fixed speed and duplex setting such as 100Mbps/Full.

To configure LAN interface settings:

1. Choose Device Settings > Network.

The current parameters are listed above the settings.



LAN Interface Settings

Note: For reliable network communication, configure the Dominion LX2 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion LX2 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

Current LAN Interface Parameters:
autonegotiation on, 1000 Mbps, full duplex, link ok

LAN Interface Speed & Duplex: Autodetect

Bandwidth Limit: No Limit

2. Choose the LAN Interface Speed & Duplex from the following options:
   - Autodetect (default option)
   - 10 Mbps/Half - Both LX II device LEDs blink
   - 10 Mbps/Full - Both LX II device LEDs blink
   - 100 Mbps/Half - Yellow LX II device LED blinks
   - 100 Mbps/Full - Yellow LX II device LED blinks
   - 1000 Mbps/Full (gigabit) - Green LX II device 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 258) for more information.

   Click OK to apply the setting.

1. Change the Bandwidth Limit, if needed. The default is No Limit.

   This sets the maximum amount of bandwidth that can be consumed by the LX II device (for all sessions).

   Note: Lower bandwidth may result in slower performance.

   Click OK to apply the setting.

Reset Network Settings to Factory Defaults

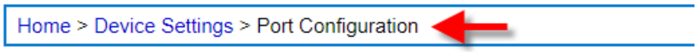
1. Select Device Management > Network to open the Network Settings page.
2. Click "Reset to Defaults" at the bottom of the page.

Configuring Ports

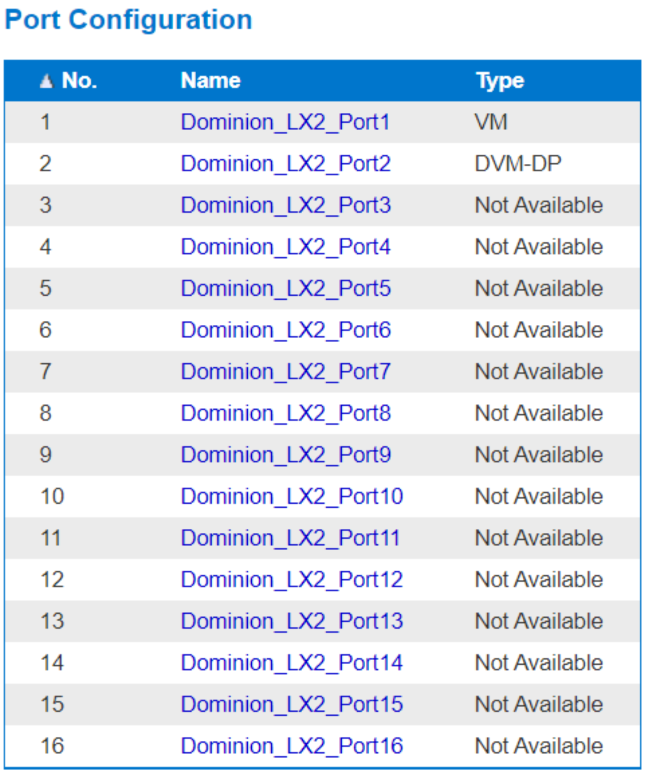
Access the Port Configuration Page

To access a port configuration:

1. Choose Device Settings > Port Configuration. The Port Configuration Page displays a list of the LX II ports. .



Home > Device Settings > Port Configuration



Port Configuration

No.	Name	Type
1	Dominion_LX2_Port1	VM
2	Dominion_LX2_Port2	DVM-DP
3	Dominion_LX2_Port3	Not Available
4	Dominion_LX2_Port4	Not Available
5	Dominion_LX2_Port5	Not Available
6	Dominion_LX2_Port6	Not Available
7	Dominion_LX2_Port7	Not Available
8	Dominion_LX2_Port8	Not Available
9	Dominion_LX2_Port9	Not Available
10	Dominion_LX2_Port10	Not Available
11	Dominion_LX2_Port11	Not Available
12	Dominion_LX2_Port12	Not Available
13	Dominion_LX2_Port13	Not Available
14	Dominion_LX2_Port14	Not Available
15	Dominion_LX2_Port15	Not Available
16	Dominion_LX2_Port16	Not Available

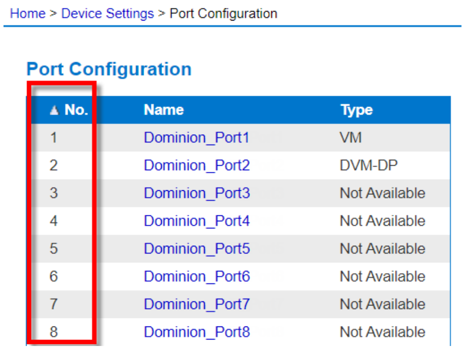
- This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.
- When a port's status is down, Not Available is displayed as its status. A port may be down when the port's CIM is removed or powered down.

2. Click the Port Name for the port you want to edit. The Port page for KVM ports opens.

Port Number

Ports are numbered from 1 up to the total number of ports available for the LX II.

For example, Port_1 - Port_16.



Home > Device Settings > Port Configuration

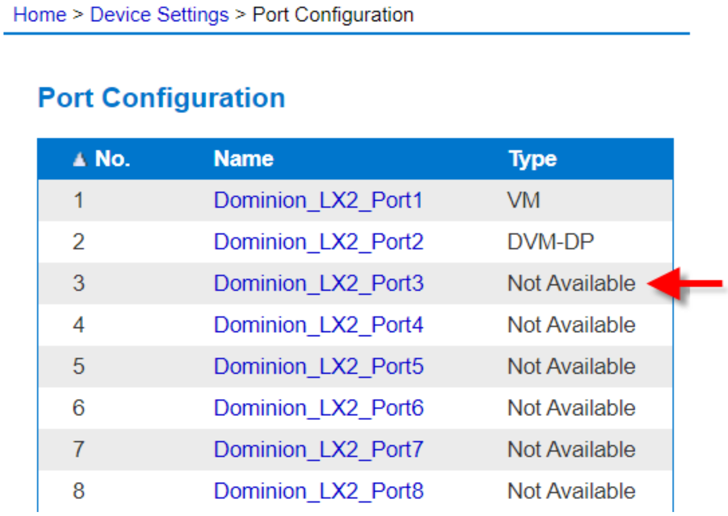
Port Configuration

▲ No.	Name	Type
1	Dominion_Port1	VM
2	Dominion_Port2	DVM-DP
3	Dominion_Port3	Not Available
4	Dominion_Port4	Not Available
5	Dominion_Port5	Not Available
6	Dominion_Port6	Not Available
7	Dominion_Port7	Not Available
8	Dominion_Port8	Not Available

Port Name

If a LX II port has no CIM connected or is connected to a CIM with no name, a default port name of Dominion_LX2_PortNumber is assigned to the port. PortNumber is the number of the LX II physical port.

When a CIM is attached to the LX II, the CIM name will be used for the port.



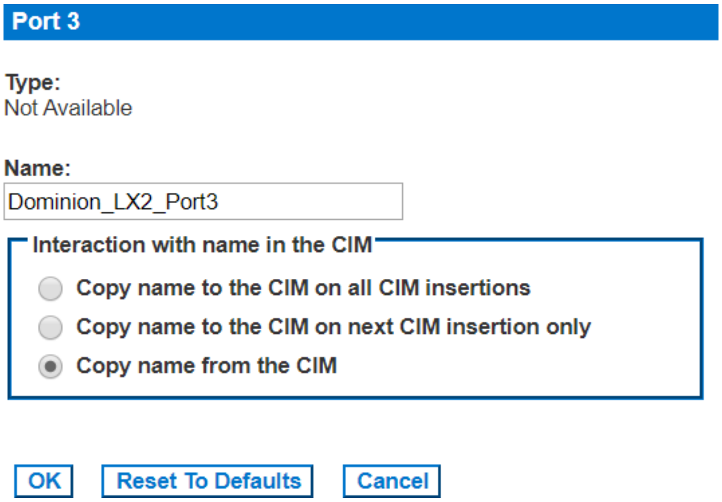
Home > Device Settings > Port Configuration

Port Configuration

▲ No.	Name	Type
1	Dominion_LX2_Port1	VM
2	Dominion_LX2_Port2	DVM-DP
3	Dominion_LX2_Port3	Not Available
4	Dominion_LX2_Port4	Not Available
5	Dominion_LX2_Port5	Not Available
6	Dominion_LX2_Port6	Not Available
7	Dominion_LX2_Port7	Not Available
8	Dominion_LX2_Port8	Not Available

There are several options to control how the name of the port interacts with the name of the CIM. Click a port of type "Not Available" to select an option:

- **Copy name to the CIM on all CIM insertions**: Enter a port name, and select "Copy name to the CIM on all CIM insertions" to keep the port name and copy it to any CIM that is inserted. This option keeps the port name permanently even if the CIM changes.
- **Copy name to the CIM on next CIM insertion only**: Enter a port name, and select "Copy name to the CIM on next CIM insertion only" to keep the port name and copy it once only to the next CIM. After that CIM insertion, the port name will be updated with the CIM name for all future CIM changes.
- **Copy name from the CIM**: Enter a port name or keep the default, and select "Copy name from the CIM" to allow this port name to update with the CIM name for all future CIM changes.


Port 3

Type:
Not Available

Name:
Dominion_LX2_Port3

Interaction with name in the CIM

○ Copy name to the CIM on all CIM insertions
○ Copy name to the CIM on next CIM insertion only
● Copy name from the CIM

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

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

When you reset a port name to its default, any existing power associations are removed and, if the port is a part of a port group, it is removed from the group.

Port Type

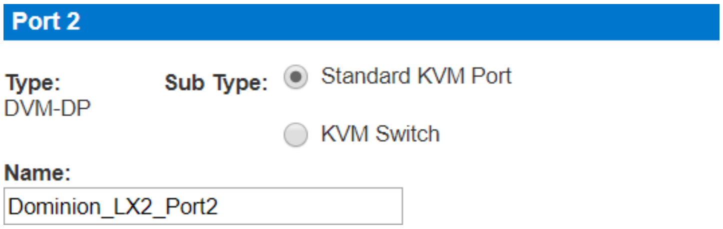
Port type includes:

- DCIM - Dominion CIM
- TierDevice - Tiered device
- Not Available - No CIM connected
- DVM-DP - Display Port CIM
- DVM-HDMI - HDMI CIM
- DVM-DVI - DVI CIM
- VM - D2CIM - VUSB CIM
- Dual - VM - D2CIM-DVUSB CIM
- VM-USBC - USB-C CIM
- KVM Switch - Generic KVM Switch connection

Configuring Standard Target Servers

▶ To name the target servers:

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 Standard KVM Port as the subtype for the port.
4. 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.
5. Click OK.



Port 2

Type: DVM-DP

Sub Type: ● Standard KVM Port ○ KVM Switch

Name: Dominion_LX2_Port2

Configuring KVM Switches

The LX II also supports use of hot key sequences to switch between targets on a KVM switch. KVM switching is supported by blade chassis and in tiered configurations.

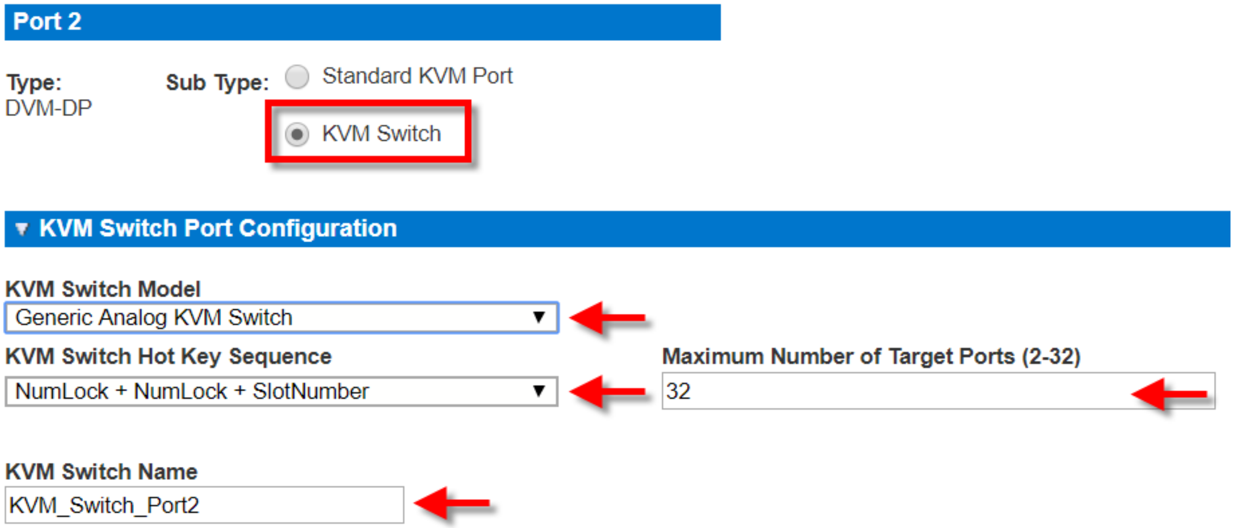
> Important: For user groups to see the KVM switch that you create, you must first create the switch and then create the group. If an existing user group needs to see the KVM switch you are creating, you must recreate the user group.

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 the 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.



Port 2

Type: DVM-DP

Sub Type: ○ Standard KVM Port ● KVM Switch

▼ KVM Switch Port Configuration

KVM Switch Model: Generic Analog KVM Switch

KVM Switch Hot Key Sequence: NumLock + NumLock + SlotNumber

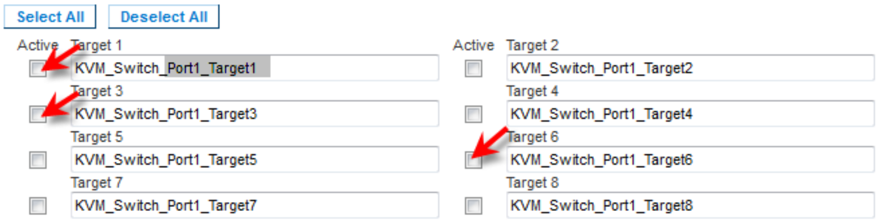
Maximum Number of Target Ports (2-32): 32

KVM Switch Name: KVM_Switch_Port2

8. Activate the targets that the KVM switch hot key sequence will be applied to.

Indicate that the KVM switch ports have targets attached by selecting 'Active' for each of the ports. Use Select All and Deselect All to select and deselect the Active checkboxes accordingly.

Change the port names as need.



Active		Active	
	Target 1		Target 2
□	KVM_Switch_Port1_Target1	□	KVM_Switch_Port1_Target2
	Target 3		Target 4
□	KVM_Switch_Port1_Target3	□	KVM_Switch_Port1_Target4
	Target 5		Target 6
□	KVM_Switch_Port1_Target5	□	KVM_Switch_Port1_Target6
	Target 7		Target 8
□	KVM_Switch_Port1_Target7	□	KVM_Switch_Port1_Target8

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. Select Active to activate the link once it is entered.

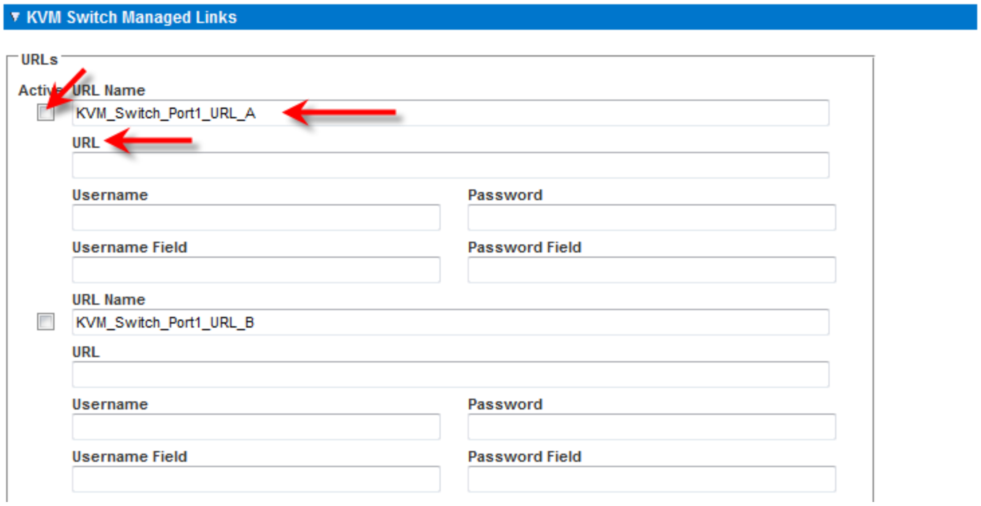
       Leave the checkbox deselected to keep the link inactive.

       You can enter information into the link fields and save without activating the links.

       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.



▾ KVM Switch Managed Links

URLs

Active

□ URL Name: KVM_Switch_Port1_URL_A

URL

Username

Password

Username Field

Password Field

□ URL Name: KVM_Switch_Port1_URL_B

URL

Username

Password

Username Field

Password Field

10. Click OK.

To change the active status/deactivate 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 deactivate. The Port Page opens.
3. Deselect the Active checkbox next to the KVM switch target port or URL to deactivate them.
4. Click OK.

Configuring CIM Ports

The LX II supports the use of standard and virtual media CIMs to connect a server to the LX II.

To access a CIM to configure:

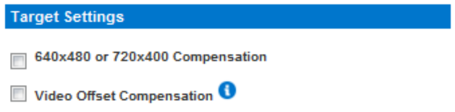
1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name of the target server you want to rename. The Port Page opens.
3. Next -
   - ***Configure the CIM Settings*** (on page 80)
   - ***Configure the CIM Target Settings*** (on page 80)
   - ***Apply Selected Profiles to Other CIMs*** (on page 80)
   - ***Apply a Native Display Resolution to Other CIMs*** (on page 81)

Configure the CIM Settings

1. Select Standard KVM Port as the subtype for the port.
2. 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.

Configure the CIM Target Settings

1. In the Target Settings section, select "640x480 or 720x400 Compensation" if you are experiencing display issues when the target is using this resolution.
2. In the Target Settings section, select "Video Offset Compensation" if the video appears off center on your target.

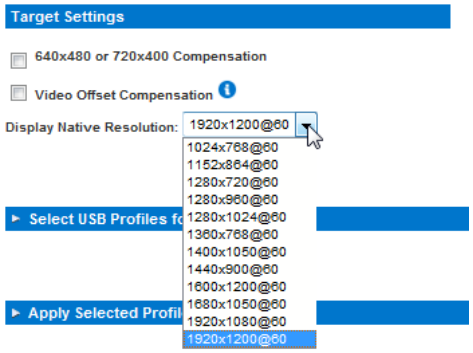


Target Settings

□ 640x480 or 720x400 Compensation

□ Video Offset Compensation

3. For digital CIMs, to set the target's video resolution to match your monitor's native display resolution, select the resolution from the Display Native Resolution drop-down.



Target Settings

□ 640x480 or 720x400 Compensation

□ Video Offset Compensation

Display Native Resolution: 1920x1200@60

For a complete list of supported video resolutions from the remote console, see ***Supported Target Server Video Resolutions*** (on page 251).

Note: To ensure the configured native resolution will display on Mac notebooks, you must select the"Best for CIM" option instead of "Scaled CIM" on the Mac target.

---

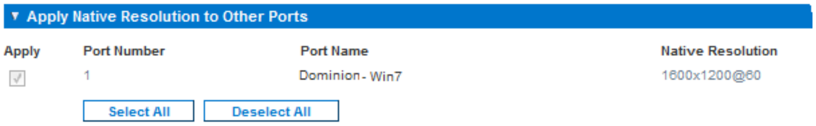
4. If you are using an HDMI CIM, some operating system/video card combinations may offer a limited range of RGB values. Improve the colors by selecting the DVI Compatibility Mode checkbox under the Target Settings section.

Apply Selected Profiles to Other CIMs

1. Apply the profile to other CIMs by selecting them from the list in the Apply Selected Profiles to Other Ports section of the Port Configuration page.

Apply a Native Display Resolution to Other CIMs

1. Apply the native display resolution to the CIM or to other CIMs of the same type by selecting the ports other CIMs are connected to from the list in the Apply Native Resolutions to Other Ports section of the Port Configuration page.



Apply	Port Number	Port Name	Native Resolution
☑	1	Dominion - Win7	1600x1200@60

Configuring USB Profiles (Port Page)

You choose the available USB profiles for a port in the Select USB Profiles for Port section of the Port page. The USB profiles chosen in the Port page become the profiles available to the user in VKC when connecting to a KVM target server from the port. For information about USB profiles, see ***USB Profiles*** (on page 40, on page 191).

Note: To set USB profiles for a port, you must have a supported CIM connected with firmware compatible with the current firmware version of the LX II. See **Upgrading CIMs** *(on page 121).*

The profiles available to assign to a port appear in the Available list on the left. The profiles selected for use with a port appear in the Selected list on the right. When you select a profile in either list, a description of the profile and its use appears in the Profile Description field.

In addition to selecting a set of profiles to make available for a KVM port, you can also specify the preferred profile for the port and apply the settings from one port to other KVM ports.

▶ To open the Port page:

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name for the KVM port you want to edit. The Port page opens.

▶ To select the USB profiles for a KVM port:

1. In the Select USB Profiles for Port section, select one or more USB profiles from the Available list.
   - Shift-Click and drag to select several continuous profiles.
   - Ctrl-Click to select several discontinuous profiles.
2. Click Add. The selected profiles appear in the Selected list. These are the profiles that can be used for the KVM target server connected to the port.

To specify a preferred USB profile:

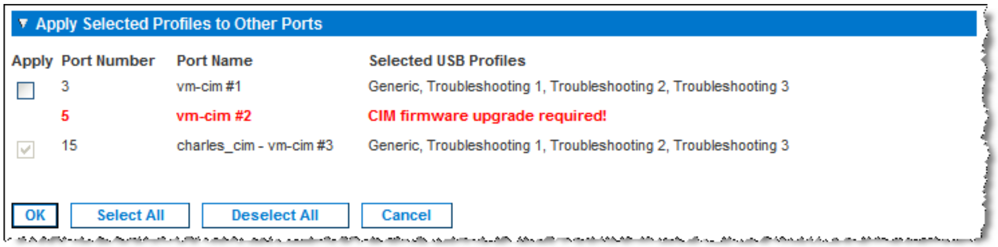
1. After selecting the available profiles for a port, choose one from the Preferred Profile for Port menu. The default is Generic. The selected profile is used when connecting to the KVM target server. You can change to any other USB profile as necessary.
2. If check box Set Active Profile As Preferred Profile is selected, this preferred USB is also used as active profile.

To remove selected USB profiles:

1. In the Select USB Profiles for Port section, select one or more profiles from the Selected list.
   - Shift-Click and drag to select several continuous profiles.
   - Ctrl-Click to select several discontinuous profiles.
2. Click Remove. The selected profiles appear in the Available list. These profiles are no longer available for a KVM target server connected to this port.

To apply a profile selection to multiple ports:

1. In the Apply Selected Profiles to Other Ports section, select the Apply checkbox for each KVM port you want to apply the current set of selected USB profiles to.



▼ Apply Selected Profiles to Other Ports

Apply	Port Number	Port Name	Selected USB Profiles
☐	3	vm-cim #1	Generic, Troubleshooting 1, Troubleshooting 2, Troubleshooting 3
	5	vm-cim #2	CIM firmware upgrade required!
☑	15	charles_cim - vm-cim #3	Generic, Troubleshooting 1, Troubleshooting 2, Troubleshooting 3

   - To select all KVM ports, click Select All.
   - To deselect all KVM ports, click Deselect All.

Configuring LX II Local Port Settings

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

To configure the local port settings:

- Choose Device Settings > Local Port Settings. The Local Port Settings page opens.

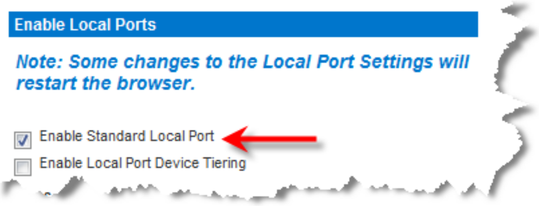
Enable Standard Local Port

1. 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.

The browser is restarted when this change is made.

Note: If you are using the tiering feature, the Standard Local Port feature will be turned off since both features cannot be used at the same time.



Enable Local Ports

Note: Some changes to the Local Port Settings will restart the browser.

☑ Enable Standard Local Port

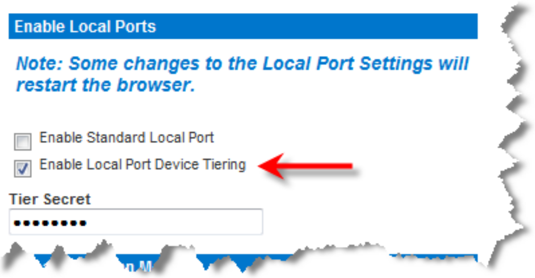
□ Enable Local Port Device Tiering

Enable Local Port Device Tiering

1. 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 87) for more information on tiering.



Enable Local Ports

Note: Some changes to the Local Port Settings will restart the browser.

□ Enable Standard Local Port

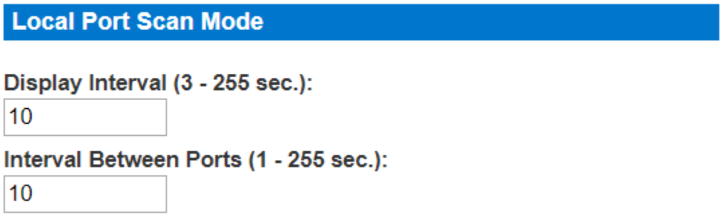
☑ Enable Local Port Device Tiering

Tier Secret

••••••••

Configure the Local Port Scan Mode Settings

1. If needed, configure the Local Port Scan Mode settings. These settings apply to Scan Settings feature, which is accessed from the Port page.
   - In the "Display Interval" 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 (1 - 255 sec):" field, specify the interval at which the device should pause between ports.



Local Port Scan Mode

Display Interval (3 - 255 sec.):

10

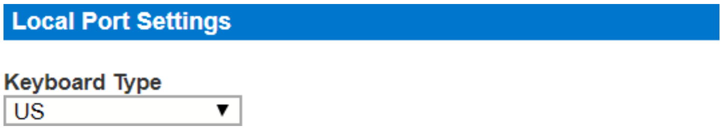
Interval Between Ports (1 - 255 sec.):

10

Select the Local Console Keyboard Type

1. Choose the appropriate keyboard type from among the options in the drop-down list.

   The browser will be restarted when this change is made.



Local Port Settings

Keyboard Type

US ▼

- US
- US/International
- United Kingdom
- French (France)
- German (Germany)
- German (Switzerland)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangul (Korean)
- JIS (Japanese Industry Standard)
- Portuguese (Portugal)
- Norwegian (Norway)
- Swedish (Sweden)
- Danish (Denmark)
- Belgian (Belgium)
- Hungarian
- Spanish
- Italian
- Slovenian

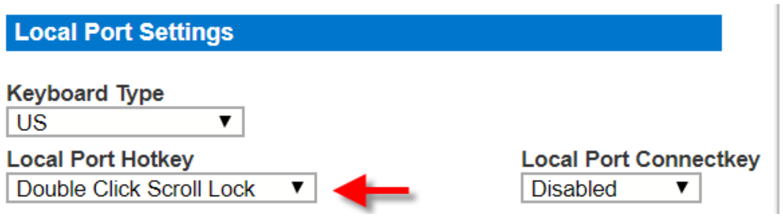
Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for LX II Local Console functions.

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

Select the Local Port Hotkey

1. Choose the local port hotkey. The local port hotkey is used to return to the LX II 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



Local Port Settings

Keyboard Type
US

Local Port Hotkey
Double Click Scroll Lock

Local Port Connectkey
Disabled

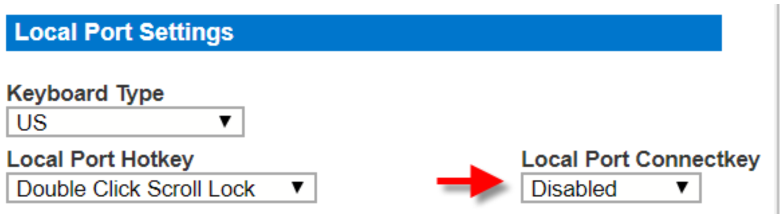
Select the Local Port Connect Key

Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target without returning to the GUI.

Then use the hot key to disconnect 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*** (on page 241) for examples of connect key sequences.

The connect key works for both standard servers and blade chassis.



Local Port Settings

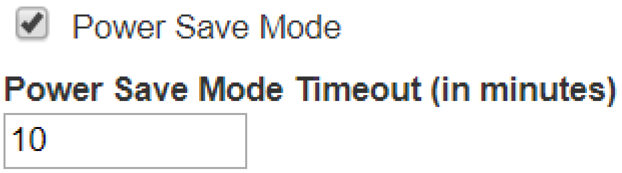
Keyboard Type
US

Local Port Hotkey
Double Click Scroll Lock

Local Port Connectkey
Disabled

Configure the Power Save Feature (Optional)

1. 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.



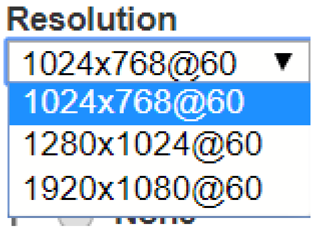
☑ Power Save Mode

Power Save Mode Timeout (in minutes)
10

Select the Local Port Video Resolution

Select the local port video resolution.

Choose Device Settings > Local Port Settings.



Resolution

1024x768@60 ▼

1024x768@60

1280x1024@60

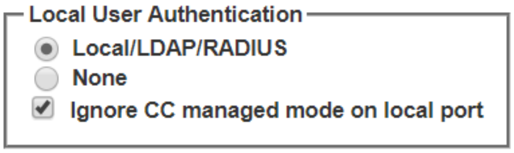
1920x1080@60

Select the Local User Authentication

1. Choose the type of local user authentication.
   - Local/LDAP/RADIUS. This is the recommended option.
   - None. There is no authentication for Local Console access.

     This option is recommended for secure environments only.

Note: Ignore CC managed mode on local port function is not supported on Dominion LX II.



Local User Authentication

● Local/LDAP/RADIUS

○ None

☑ Ignore CC managed mode on local port

Device Services

Enabling SSH

Enable SSH access to allow administrators to access the LX II 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 II. 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.

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

LX II 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 LX II from beyond a firewall, your firewall settings must enable two-way communication through the default Port 5000 or a non-default port configured on this page.

via Remote Console or command line interface (CLI).

▶ **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

The tiering feature allows you to access LX II targets and PDUs through one base LX II device.

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

When setting up the devices, you will use specific CIMS for specific 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.

Tiering also supports the use of KVM switches to switch between servers. See Configuring KVM Switches.

Once configured, base and tiered devices are displayed on the Port Access Page. See Tiered Devices - Port Access Page

Before Creating a Tiering Configuration

Before creating a tiering configuration, review Permitted Tiering Configurations and Unsupported and Limited Features on Tiered Targets.

Before adding tiered devices to a tiering configuration:

- Base and tiered devices must all be operating with the same firmware revision.
- Enable base devices on the Device Settings page. See Configuring Standard Target Servers
- Enable tiered devices on the Local Port Settings page. See ***Configuring LX II Local Port Settings*** (on page 82), then ***Enable Local Port Device Tiering*** (on page 83)
- Enable tiering for the base device, and the tiered devices. See ***Enabling Tiering*** (on page 89)

Permitted Tiering Configurations

Before tiering devices, review ***Before Creating a Tiering Configuration*** (on page 88).

LX II only supports tiering with other LX II devices.

User Permissions in Tiered Configurations

The user must have a valid user account on the tiered device. The group that the user belongs to on the tiered device controls the user's permissions to the ports on the tiered device.

These examples illustrate how various user permissions work in tiered configurations.

▶ Example 1:

Base unit and tiered units have the same user with permissions to all ports. The base user will be able to access all ports on the base and tiered device.

▶ Example 2:

The base and tiered devices have the same user but different port permissions. The base user will have different tiered port access.

▶ Example 3:

The base and tiered devices do not have the same user. The user at the base device will not be able to access ports at the tiered device.

Unsupported and Limited Features on Tiered Targets

The following features are not supported on tiered targets:

- Virtual media tiered devices
- DSAM on tiered devices

Tiered LX II Connection Example

The following diagram illustrates the cabling configurations between LX II base and tiered devices.

▶ To connect LX II devices in a tiered configuration:

- Connect a Cat5/5e/6 cable to a target server port on the LX IIbase device, and connect the other end to a D2CIM-DVUSB CIM.
- Connect the D2CIM-DVUSB CIM to the Local Access video/keyboard/mouse ports on the tiered device.

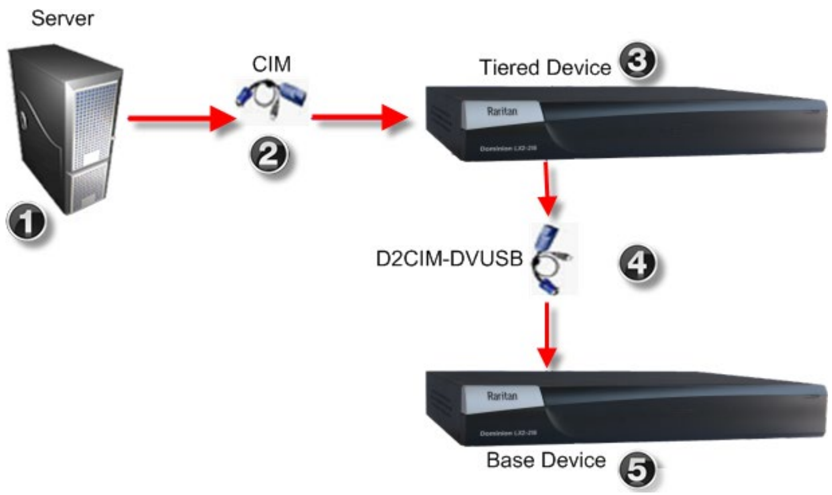


Diagram key	
❶	Target server
❷	CIM from target server to the LX II tiered device
❸	LX II tiered device
❹	D2CIM-DVUSB CIM from the LX II tiered device to the LX II base device
❺	LX II base device

Enabling Tiering

	From the base LX II tier device, select Device Settings > Device Services to open the Device Service Settings page.
	Select Enable Tiering as Base.

	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. Enter the same secret word for the tiered device. Click OK.
	Enable the tiered devices. From the tiered device, choose Device Settings > Local Port Settings.
	In the Enable Local Ports section of the page, select Enable Local Port Device Tiering.
	In the Tier Secret field, enter the same secret word you entered for the base device on the Device Settings page. Click OK.

Once devices are enabled and configured, they appear on the Port Access page.

When the LX II 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 II interface for base devices.
- 'Configured As Tier Device' in the Device Information section of the left panel of the LX II 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.

Remote and Local Access from Tiered Devices

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.

Enabling Direct Port Access via URL

Direct Port Access allows users to bypass having to use the LX II's Login dialog and Port Access page.

This feature also provides the ability to enter a username and password directly to proceed to the target, if the username and password is not contained in the URL.

Enable Direct Port Access

▶ **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 through the LX II by passing in the necessary parameters in the URL.
3. Click OK.

Direct Port Access URL Syntax for the HKC

Follow the syntax described to create direct port access URLs for HKC.

If you are using the HKC and direct port access, use:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=hkc

  Or

- https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=hkc

Username and password are optional.

If username and password are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.

The port may be a port number or port name.

If you are using a port name, the name must be unique or an error is reported.

If the port is omitted altogether, an error is reported.

Direct Port Access URL Syntax for the VKC

If you are using the VKC and direct port access, use one of the following syntaxes for standard ports:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=vkc

  Or

- https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=vkc

Username and password are optional.

If username and password are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.

The port may be a port number or port name.

If you are using a port name, the name must be unique or an error is reported.

If the port is omitted altogether, an error is reported.

Direct Port Access URL Syntax for the AKC

Follow the syntax described to create direct port access URLs for AKC. If you are using Chrome on Windows, you must also enable the "Enable AKC Download Server Certificate Validation" option in Device Settings > Device Services.

If you are using the AKC and direct port access, use:

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

  Or

- https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=akc

Username and password are optional.

If username and password are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.

The port may be a port number or port name.

If you are using a port name, the name must be unique or an error is reported.

If the port is omitted altogether, an error is reported.

Configuring SNMP Agents

See ***Viewing the LX II MIB*** (on page 103) for information on viewing the LX II MIB.

LX II supports SNMP logging for SNMP v2c and/or v3. SNMP v2c defines message formats and protocol operations when SNMP logging is enabled. SNMP v3 is a security extension of SNMP that provides user authentication, password management and encryption.

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Provide the following SNMP agent identifier information for the MIB-II System Group objects:
   - System Name - the SNMP agent's name/appliance name
   - System Contact - the contact name related to the appliance

   a. System Location - the location of the appliance
3. Select either or both Enable SNMP v1/v2c and Enable SNMP v3. At least one option must be selected. **Required**
4. Complete the following fields for SNMP v2c (if needed):
   - Community - the appliance's community string

   a. Community Type - grant either Read-Only or Read-Write access to the community users

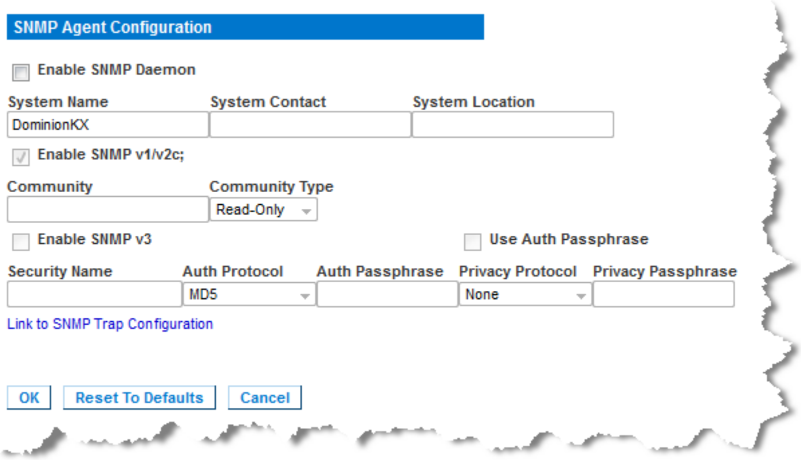
> *Note: An SNMP community is the group to which appliances and management stations running SNMP belong. It helps define where information is sent. The community name is used to identify the group. The SNMP device or agent may belong to more than one SNMP community.*

5. Complete the following fields for SNMP v3 (if needed):
   - Select Use Auth Passphrase if one is needed. If the Privacy Passphrase is required, the 'Use Auth Passphrase' allows you to have the same passphrase for both without having to re-enter the Auth Passphrase.
   - Security Name - the username or service account name of the entity communicating with the SNMP agent (up to 32 characters).
   - Authentication Protocol - the MD5 or SHA authentication protocol used by the SNMP v3 agent. Note: When FIPS is enabled, SHA must be used for v3 traps for FIPS compliance.
   - Authentication Passphrase - the pass phrase required to access the SNMP v3 agent (up to 64 characters).
   - Privacy Protocol - if applicable, the AES or DES algorithm used to encrypt data.

   a. Privacy Passphrase - if applicable, the pass phrase used to access the privacy protocol algorithm (up to 64 characters).
6. Click OK to start the SNMP agent service.

Configure SNMP traps on the Event Management - Settings page, which can be quickly accessed by clicking the SNMP Trap Configuration link. See ***Configuring SNMP Notifications*** (on page 98)for information on creating SNMP traps and ***SNMP Notifications*** (on page 100) for a list of available LX II SNMP traps.

The events that are captured once an SNMP trap or inform is configured are selected on the Event Management - Destination page. See ***Configuring Event Management - Destinations*** (on page 103).



SNMP Agent Configuration

☐ Enable SNMP Daemon

System Name	System Contact	System Location
DominionKX		

☑ Enable SNMP v1/v2c;

Community	Community Type
	Read-Only

☐ Enable SNMP v3 ☐ Use Auth Passphrase

Security Name	Auth Protocol	Auth Passphrase	Privacy Protocol	Privacy Passphrase
	MD5		None	

Link to SNMP Trap Configuration

► To reset to factory defaults:

- Click Reset To Defaults. All items on the page are set back to their defaults.

> WARNING: When using SNMP notifications over UDP, it is possible for the LX II and the router that it is attached to fall out of synchronization when the LX II is rebooted, preventing the reboot completed SNMP notification from being logged.

Configuring Modem Settings

See ***Certified Modems*** (on page 259) for information on certified modems that work with the LX II.

For information on settings that will give you the best performance when connecting to the LX II via modem, see ***Configuring Connection Properties*** (on page 186).

► To configure modem settings:

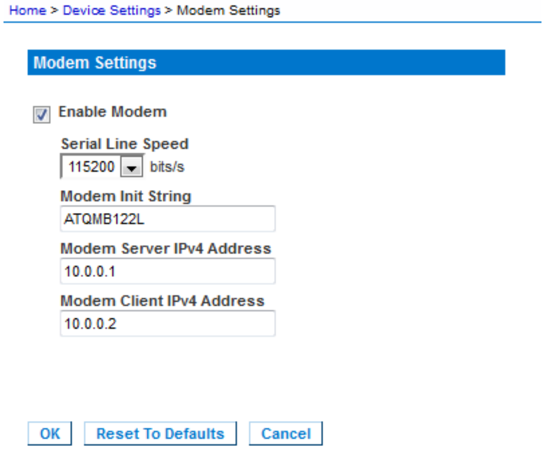
1. Click Device Settings > Modem Settings to open the Modem Settings page.
2. Select the Enable Modem checkbox. This will enable the Serial Line Speed and Modem Init String field.
3. The Serial Line Speed of the modem is set to 115200.
4. Enter the initial modem string in the Modem Init String field. 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.

6. 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
ATQMB122L

Modem Server IPv4 Address
10.0.0.1

Modem Client IPv4 Address
10.0.0.2

Connect and Enable Global Access to an External USB-Connected Broadband Modem

Users who need access to LX II via the Sierra Wireless modem must be assigned to a user group with Modem Access permissions. This is a security measure that helps control who can access LX II via the modem. For example, create a user group called Sierra Wireless Users and give the group Modem Access permissions, then assign only users who need access to the modem to that group.

The Enable Broadband Modem feature must be enabled in LX II in order for users to access LX II via the Sierra Wireless modem. This is a global-level feature, so it is disabled by default in order to prevent all users from being able to access LX II via the modem.

Sierra Wireless Software and Firmware Versions

Sierra Wireless must have at least ALEOS Software Version 4.4.1.014

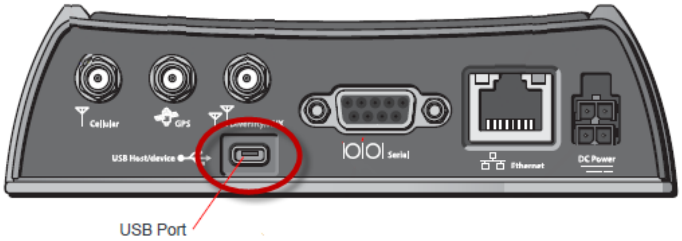
This configuration has been tested with the Verizon Wireless MC7750 Radio Module using firmware version 3.05.10.13.

Connect the External, Wireless Modem

USB Connection

Use either a Micro A or Micro B to USB Type A cable to connect the Sierra Wireless to the LX II.

- Connect the Sierra Wireless USB port to any of the USB ports on back of the LX II or to the USB port on the front of the LX II.



Note: Only USB connections are supported for this modem.

Configure the Sierra Wireless Modem

Configure the Sierra Wireless modem for use with LX II using these connections. These settings are configured on the Sierra Wireless modem, not LX II.

Configure the Sierra Wireless Modem for a Cellular Connection

- A SIM card must be purchased from your service provider and installed in the Sierra Wireless modem.
- Get a static IP address from your service provider, then assign it to the Sierra Wireless modem.
- Sierra Wireless must be configured for Public mode.
- Host Connection Mode must be set to "USB Uses Public IP".
- USB Device Mode must be set to "USBNET".

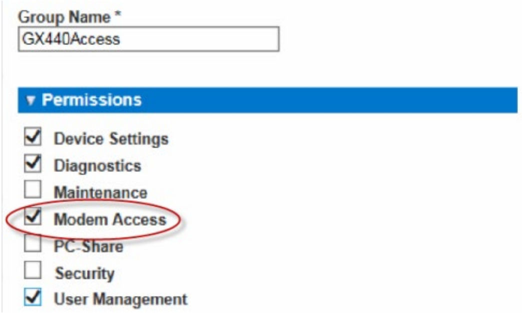
Change Default Username

For security reasons, change the default Admin account username to a new name before using the Sierra Wireless .

Assign User Groups Modem Access Permissions

Following are settings applied in LX II.

- Modem Access permission is assigned to a user group on the Group page, and the user is then assigned to the group on the User page. For more information, see Configure and Manage Users and Groups from the Remote Console.



Group Name *
GX440Access

☑ Device Settings
☑ Diagnostics
□ Maintenance
☑ Modem Access
□ PC-Share
□ Security
☑ User Management

Configuring Date/Time Settings

Use the Date/Time Settings page to specify the date and time for the LX II. 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:

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. Adjust for daylight savings time by checking the "Adjust for daylight savings time" checkbox.
4. Choose the method to use to set the date and time:
   - User Specified Time - use 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 - use 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**

   Note: If DHCP is selected for the Network Settings on the Network page, the NTP server IP address is automatically retrieved from the DHCP server by default. Manually enter the NTP server IP address by selecting the Override DHCP checkbox.

6. Click OK.

Event Management

The LX II Event Management feature allows you to enable and disable the distribution of system events to SNMP Managers, SMTP, the Syslog and the audit log. These events are categorized, and for each event you can determine whether you want the event sent to one or several destinations.

Configuring Event Management - Settings

Configure SNMP notifications and the syslog configuration from the Event Management - Settings page. See ***Configuring SNMP Notifications*** (on page 98).

Once configured, enable the SNMP notifications on the Event Management - Destinations page. See ***Configuring Event Management - Destinations*** (on page 103).

Configuring SNMP Notifications

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions.

SNMPv2 provides for both traps and informs to be sent out over a network to gather information. The basic difference between traps and informs is that when the remote application receives an inform it sends back an acknowledgment, while traps are not acknowledged. In SNMPv3, there are further capabilities and restrictions on how the messages are handled.

The traps and informs are configured on the Event Management - Settings page. See ***SNMP Notifications*** (on page 100) for a list of supported traps and informs.

SNMP agents are configured on the Device Services page. See ***Configuring SNMP Agents*** (on page 92) for information on configuring SNMP agents and ***Viewing the LX II MIB*** (on page 103) for information on viewing the LX II MIB.

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Select the SNMP Logging Enabled checkbox to enable to remaining checkboxes in the section. **Required**
3. Select either or both SNMP v2c Notifications Enabled and SNMP v3 Notifications Enabled. At least one option must be selected.

   Once selected, all related fields are enabled. **Required**
4. Complete the following fields for SNMP v2c (if needed):
   - Destination IP/Hostname - the IP or hostname of the SNMP manager. Up to five (5) SNMP managers can be created

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

   a. Port Number - the port number used by the SNMP manager

   b. Community String - the appliance's community string

Note: An SNMP community is the group to which appliances 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.

c. Type - notification type, either Trap or Inform

d. Retries and Timeout - for Informs, enter the number of retries to be attempted, and the timeout period in seconds.

WARNING: Non-responding destinations may significantly slow system response if informs are configured with large values for retries and/or timeouts.

5. If it is not already, select the SNMPv3 Notifications Enabled checkbox to enable the following fields. Complete the following fields for SNMP v3 (if needed):

   - Destination IP/Hostname - the IP or hostname of the SNMP manager. Up to five (5) SNMP managers can be created

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

a. Port Number - the port number used by the SNMP manager

- Security Name - the username or service account name of the entity communicating with the SNMP agent (up to 32 characters).
- Authentication Protocol - the MD5 or SHA authentication protocol used by the SNMP v3 agent. Note: When FIPS is enabled, SHA must be used for v3 traps for FIPS compliance.
- Authentication Passphrase - the pass phrase required to access the SNMP v3 agent (up to 64 characters).
- Privacy Protocol - if applicable, the AES or DES algorithm used to encrypt data.

a. Privacy Passphrase - if applicable, the pass phrase used to access the privacy protocol algorithm (up to 64 characters).

Note: If you are accessing the Event Management - Settings page from the local console and are using a screen resolution lower than 1280x1024, the Privacy Passphrase column may not be displayed on the page. If this occurs, hide the LX II's left panel. See Left Panel

b. Type - notification type, either Trap or Inform.

c. Retries and Timeout - for Informs, enter the number of retries to be attempted, and the timeout period in seconds.

6. Click OK to create the notifications.

Use the Link to SNMP Agent Configuration link to quickly navigate to the Devices Services page from the Event Management - Settings page.

The events that are captured once an SNMP trap or inform is configured are selected on the Event Management - Destination page. See ***Configuring Event Management - Destinations*** (on page 103).

LX II supports SNMP logging for SNMP v2c and/or v3. SNMP v2c defines message formats and protocol operations when SNMP logging is enabled. SNMP v3 is a security extension of SNMP that provides user authentication, password management and encryption.

To edit existing SNMP notifications:

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Make changes as needed and click OK to save the changes.

Note: If you disable SNMP settings at any time, the SNMP information is retained so you do not have to reenter if you re-enable the settings.

To delete SNMP notifications:

- Clear all of the SNMP fields and save.
- Use the reset to factory defaults feature to remove the SNMP configuration and set the LX II to its original factory default.

To reset to factory defaults:

- Click Reset To Defaults.

WARNING: When using SNMP notifications over UDP, it is possible for the LX II and the router that it is attached to fall out of synchronization when the LX II is rebooted, preventing the reboot completed SNMP notification from being logged.

SNMP Notifications

SNMP provides the ability to send notifications, to advise an administrator when one or more conditions have been met.

The following table lists the LX II SNMP notifications

Trap Name	Description
bladeChassisCommError	A communications error with blade chassis device connected to this port was detected.
cimConnected	The CIM is connected.
cimDisconnected	The CIM is disconnected.
cimUpdateStarted	The CIM update start is underway.

Trap Name	Description
cimUpdateCompleted	The CIM update is complete.
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The LX II has completed update via an RFP file.
deviceUpgradeStarted	The LX II has begun update via an RFP file.
factoryReset	The device has been reset to factory defaults.
firmwareFileDiscarded	Firmware file was discarded.
firmwareUpdateFailed	Firmware update failed.
firmwareValidationFailed	Firmware validation failed.
groupAdded	A group has been added to the LX II system.
groupDeleted	A group has been deleted from the system.
groupModified	A group has been modified.
ipConflictDetected	An IP Address conflict was detected.
ipConflictResolved	An IP Address conflict was resolved.
networkFailure	An Ethernet interface of the product can no longer communicate over the network.
networkParameterChanged	A change has been made to the network parameters.
passwordSettingsChanged	Strong password settings have changed.
portConnect	A previously authenticated user has begun a KVM session.
portConnectionDenied	A connection to the target port was denied.
portDisconnect	A user engaging in a KVM session closes the session properly.
portStatusChange	The port has become unavailable.
powerNotification	The power outlet status notification: 1=Active, 0=Inactive.
powerOutletNotification	Power strip device outlet status notification.
rebootCompleted	The LX II has completed its reboot.
rebootStarted	The LX II has begun to reboot, either through cycling power to the system or by a warm reboot from the

Trap Name	Description
	OS.
scanStarted	A target server scan has started.
scanStopped	A target server scan has stopped.
securityBannerAction	Security banner was accepted or rejected.
securityBannerChanged	A change has been made to the security banner.
securityViolation	Security violation.
setDateTime	The date and time for the device has been set.
setFIPSMode	FIPS mode has been enabled.
startCCManagement	The device has been put under CommandCenter Management.
stopCCManagement	The device has been removed from CommandCenter Management.
userAdded	A user has been added to the system.
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userForcedLogout	A user was forcibly logged out by Admin
userLogin	A user has successfully logged into the LX II and has been authenticated.
userLogout	A user has successfully logged out of the LX II properly.
userModified	A user account has been modified.
userPasswordChanged	This event is triggered if the password of any user of the device is modified.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
userUploadedCertificate	A user uploaded a SSL certificate.
userUploadedCACertificate	A user uploaded a CA Certificate for 802.1X authentication.
userUploadedClientCertificate	A user uploaded a client certificate for 802.1X authentication.

Trap Name	Description
userUploadedClientKey	A user uploaded a Client Key for 802.1X authentication.
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media. For every attempt on device/image mapping (mounting) this event is generated.
vmImageDisconnected	User attempted to unmount a device or image on the target using Virtual Media.

Viewing the LX II MIB

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Click the 'Click here to view the 'SNMP MIB' link. The MIB file opens in a browser window.

SysLog Configuration

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Select Enable Syslog Forwarding to log the appliance's messages to a remote Syslog server.
3. Type the IP Address/Hostname of your Syslog server in the IP Address field.
4. Click OK.

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

- Click Reset to Defaults at the bottom of the page to remove the setting.

Configuring Event Management - Destinations

If system events are enabled, SNMP notification events (traps and informs) are generated. The events can be logged to the syslog or audit log.

Events and where the event information is sent is configured on the Event Management - Destinations page.

Note: SNMP, Syslog, and SMTP logging only works when enabled in the Event Management - Settings page.

▶ To select events and their destinations:

1. Choose Device Settings > Event Management - Destinations. The Event Management - Destinations page opens.

   System events are categorized by Device Operation, Device Management, Security, User Activity, and User Group Administration.

2. Select the checkboxes for those event line items you want to enable or disable, and where you want to send the information.

   Tip: Enable or disable entire categories by checking or clearing the Category checkboxes, respectively.

3. Click OK.

▶ **To reset to factory defaults:**

- Click Reset To Defaults.

WARNING: When using SNMP notifications over UDP, it is possible for the LX II and the router that it is attached to fall out of synchronization when the LX II is rebooted, preventing the reboot completed SNMP notification from being logged.

Security Management

Security Settings

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

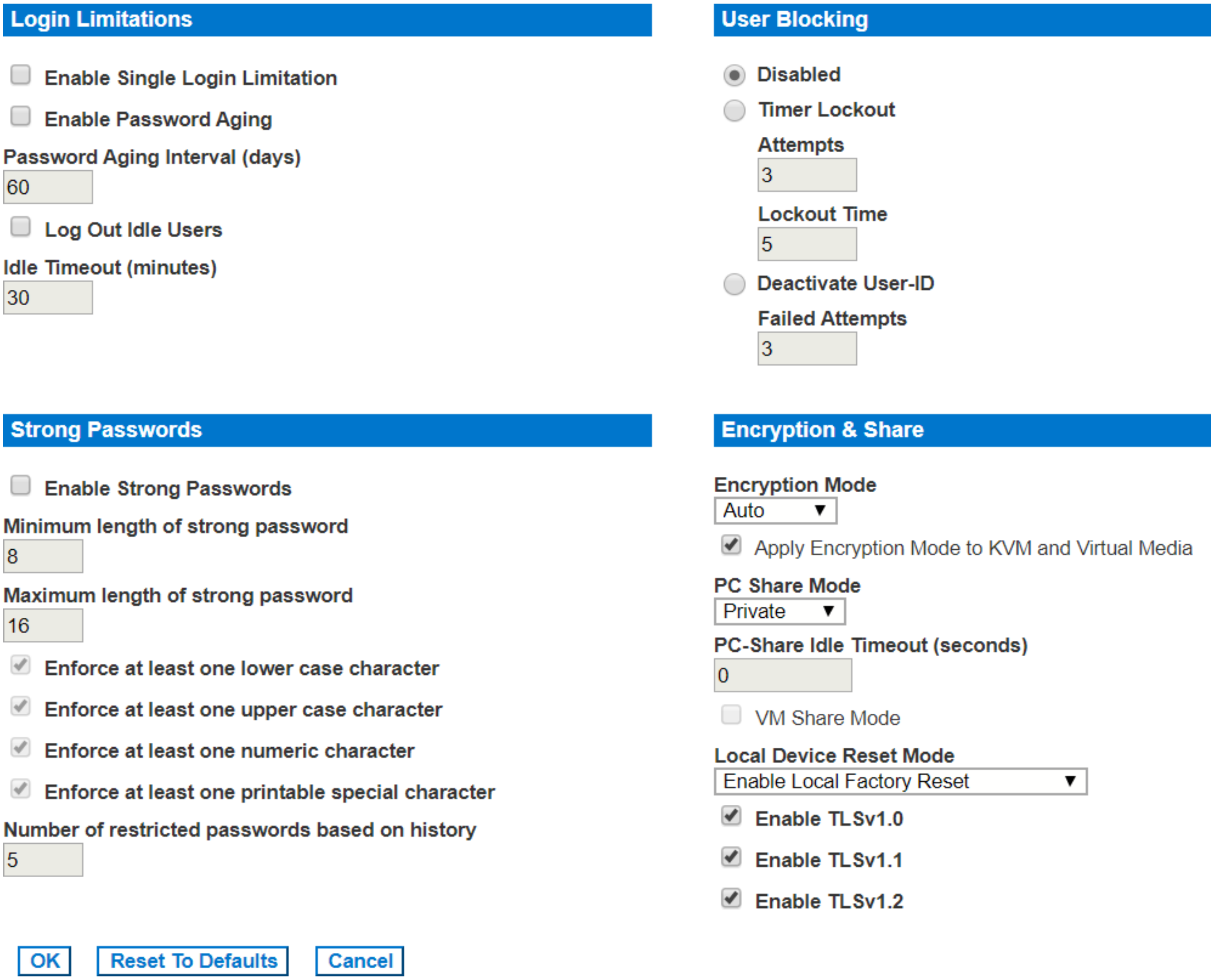
SSL certificates are used for public and private key exchanges, and provide an additional level of security. The web server certificates are self-signed. Java applet certificates are signed by a VeriSign certificate. Encryption guarantees that your information is safe from eavesdropping and these certificates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

▶ **To configure the security settings:**

1. Choose Security > Security Settings. The Security Settings page opens.
2. Update the ***Login Limitations*** (on page 105) settings as appropriate.
3. Update the ***Strong Passwords*** (on page 107) settings as appropriate.
4. Update the ***User Blocking*** (on page 108) settings as appropriate.
5. Update the Encryption & Share settings as appropriate.
6. Click OK.

To reset back to defaults:

- Click Reset to Defaults.



Login Limitations

□ Enable Single Login Limitation

□ Enable Password Aging

Password Aging Interval (days): 60

□ Log Out Idle Users

Idle Timeout (minutes): 30

User Blocking

● Disabled

○ Timer Lockout

Attempts: 3

Lockout Time: 5

○ Deactivate User-ID

Failed Attempts: 3

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

Encryption & Share

Encryption Mode: Auto

☑ Apply Encryption Mode to KVM and Virtual Media

PC Share Mode: Private

PC-Share Idle Timeout (seconds): 0

□ VM Share Mode

Local Device Reset Mode: Enable Local Factory Reset

☑ Enable TLSv1.0

☑ Enable TLSv1.1

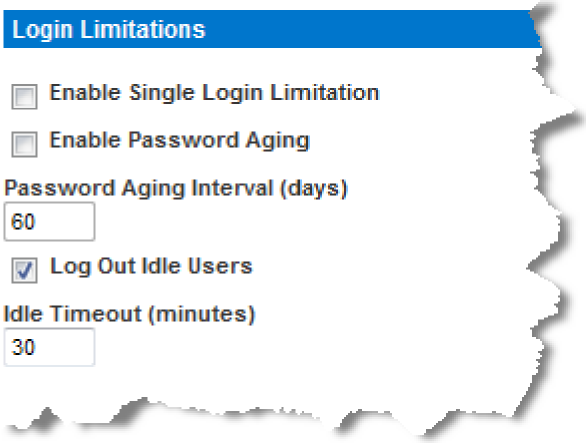
☑ Enable TLSv1.2

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 any time. When deselected, a given user name/password combination can be connected into the appliance from several client workstations

Limitation	Description
	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 Out 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, however, the session does not timeout. 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



Login Limitations

☐ Enable Single Login Limitation

☐ Enable Password Aging

Password Aging Interval (days)
60

☑ Log Out Idle Users

Idle Timeout (minutes)
30

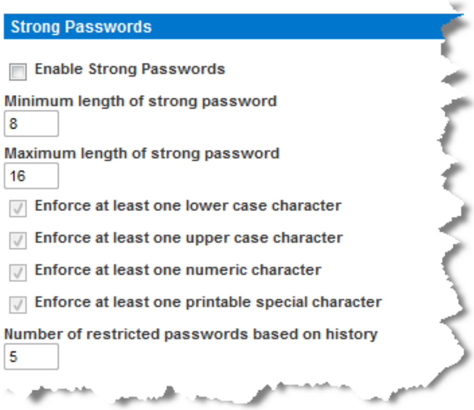
Strong Passwords

Strong passwords provide more secure local authentication for the system. Using strong passwords, you can specify the format of valid LX II 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 administrators can change the minimum to 63 characters.
Maximum length of strong password	The default minimum length is 8, but administrators can set the maximum to a default of 16 characters. The maximum length of strong passwords is 64 characters.
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

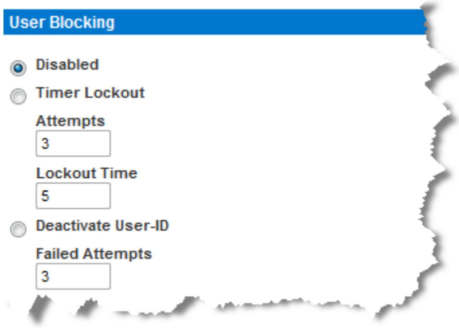
User Blocking

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.
Timer Lockout	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: ▪ 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. *Note: Users in the role of Administrator are exempt from the timer lockout settings.*
Deactivate User-ID	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: ▪ Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the

Option	Description
	Deactivate User-ID option is selected. The valid range is 1 - 10. 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.



User Blocking

● Disabled

○ Timer Lockout

Attempts

3

Lockout Time

5

○ Deactivate User-ID

Failed Attempts

3

Encryption and 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 II 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 II from your browser.

Note that video performance may be impacted once encryption is applied. The extent of the performance impact varies based on the encryption mode.

For the best possible video performance and throughput, disable encryption mode to KVM and Virtual Media if your security policy permits this.

▶ 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 II.

   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 II."

Auto

This is the recommended option. The LX II autonegotiates to the highest level of encryption possible.

You must select Auto in order for the device and client to successfully negotiate the use of FIPS compliant algorithms.

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 111) for more information.

AES-256

The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology 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 111) for more information.

1. PC Share Mode - Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one LX II 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. Selecting PC Share enables PC Share Timeout. Enter from 0 seconds to 600 seconds (10 minutes). The default timeout value is 0, so there is no exclusive keyboard/mouse control. If a user has not moved the mouse or entered keyboard input and the timeout period expires, the user relinquishes control, and another user can join.
2. 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 and audio among multiple users, that is, several users can access the same virtual media or audio session. The default is disabled.
3. 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 II Using the Reset Button. Choose one of the following options:

Local device reset mode	**Description**
Enable Local Factory	Returns the LX II device to the factory defaults.

Local device reset mode	Description
Reset (default)	
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

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.

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

- Firefox®
- Internet Explorer®
- Chrome®
- Safari®

In addition to browser support, AES 256-bit encryption requires the installation of Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files if you are using VKC/VKCS

Jurisdiction files for various JREs™ are available at the “other downloads” section the Java download website.

Enabling TLS Protocols

To meet your security policies, enable the specific TLS protocol versions you require. Disabled protocols will not be used by the device.

To enable TLS protocols:

1. Choose Security > Security Settings. In the Encryption and Share section, all TLS versions are listed.
2. Select the checkboxes of each TLS protocol version you want to enable. All versions are enabled by default. Unchecked protocols are not used. At least one protocol must be enabled.
3. Click OK to apply the settings.

SSL and TLS Certificates

LX II uses the Transport Layer Security (TLS) for any encrypted network traffic between itself and a connected client.

When establishing a connection, LX II has to identify itself to a client using a cryptographic certificate.

LX II can generate a Certificate Signing Request (CSR) or a self-signed certificate using SHA-2.

The CA verifies the identity of the originator of the CSR.

The CA then returns a certificate containing its signature to the originator. The certificate, bearing the signature of the well-known CA, is used to vouch for the identity of the presenter of the certificate.

Important: Make sure your LX II date/time is set correctly.

When a self-signed certificate is created, the LX II date and time are used to calculate the validity period. If the LX II date and time are not accurate, the certificate's valid from - to date range may be incorrect, causing certificate validation to fail. See ***Configuring Date/Time Settings*** (on page 97).

Note: The CSR must be generated on the LX II.

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

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

1. Select Security > Certificate.
2. Complete the following fields:
    a. Common name - The network name of the LX II once it is installed on your network (usually the fully qualified domain name). The common name is identical to the name used to access the LX II with a web browser, but without the prefix “http://”. In case the name given here and the actual network name differ, the browser displays a security warning when the LX II is accessed using HTTPS.
    b. Organizational unit - This field is used for specifying to which department within an organization the LX II belongs.
    c. Organization - The name of the organization to which the LX II 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. Email - The email address of a contact person that is responsible for the LX II and its security.

h. Subject Alternative Name (SAN) - Optional. Add up to ten SANs, which may include alternate hostnames. Maximum of 64 characters. This allows devices that are reachable under different names to pass the TLS hostname validation for each name registered in the TLS certificate. Enter the SAN in the Enter Hostname/IP address field, then click Add to create the list of SANs. Select a SAN and click Remove to delete.

i. Challenge Password - Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). Applicable when generating a CSR for CA Certification.

j. Confirm Challenge Password - Confirmation of the Challenge Password. Applicable when generating a CSR for CA Certification.

k. Key length - The length of the generated key in bits. 1024 is the default. Up to 4096 is supported.

3. To generate, do one of the following:

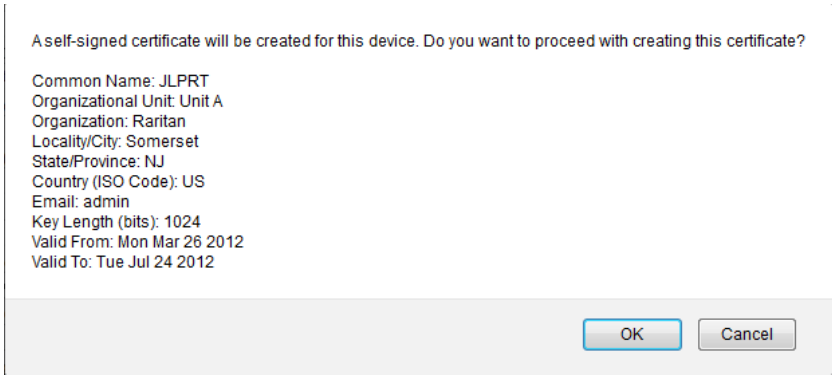
- To generate self-signed certificate, do the following:

a. Select the Create a Self-Signed Certificate checkbox if you need to generate a self-signed certificate. When you select this option, the LX II generates the certificate based on your entries, and acts as the signing certificate authority. The CSR does not need to be exported and used to generate a signed certificate.

b. Specify the number of days for the validity range. Ensure the LX II date and time are correct. If the date and time are not correct, the certificate's valid date range may not be calculated correctly.

c. Click Create.

d. A confirmation dialog is displayed. Click OK to close it.



A self-signed certificate will be created for this device. Do you want to proceed with creating this certificate?

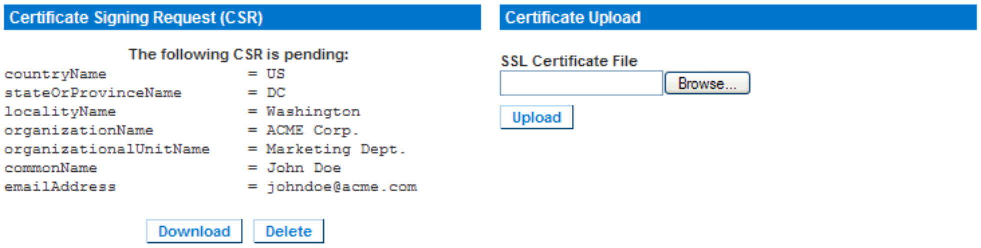
Common Name: JLPRT
Organizational Unit: Unit A
Organization: Raritan
Locality/City: Somerset
State/Province: NJ
Country (ISO Code): US
Email: admin
Key Length (bits): 1024
Valid From: Mon Mar 26 2012
Valid To: Tue Jul 24 2012

e. Reboot the LX II to activate the self-signed certificate.

- To generate a CSR to send to the CA for certification:

a. Click Create.

b. A message containing all of the information you entered appears.



The following CSR is pending:

```
countryName                  = US
stateOrProvinceName          = DC
localityName                 = Washington
organizationName             = ACME Corp.
organizationalUnitName       = Marketing Dept.
commonName                   = John Doe
emailAddress                 = johndoe@acme.com
```

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

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

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

- Once you get the certificate from the CA, upload it to the LX II by clicking Upload.
- Reboot the LX II to activate the certificate.

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

Important: If you destroy the CSR on the LX II 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.

Maintenance

Audit Log

A log is created of LX II 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 for information on what is captured in the audit log and syslog.

▶ To view the audit log for your LX II:

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 II 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 II device and the CIMs in use. This information is helpful should you need to contact Technical Support.

▶ To view information about your LX II and CIMs:

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

The following information is provided about the LX II:

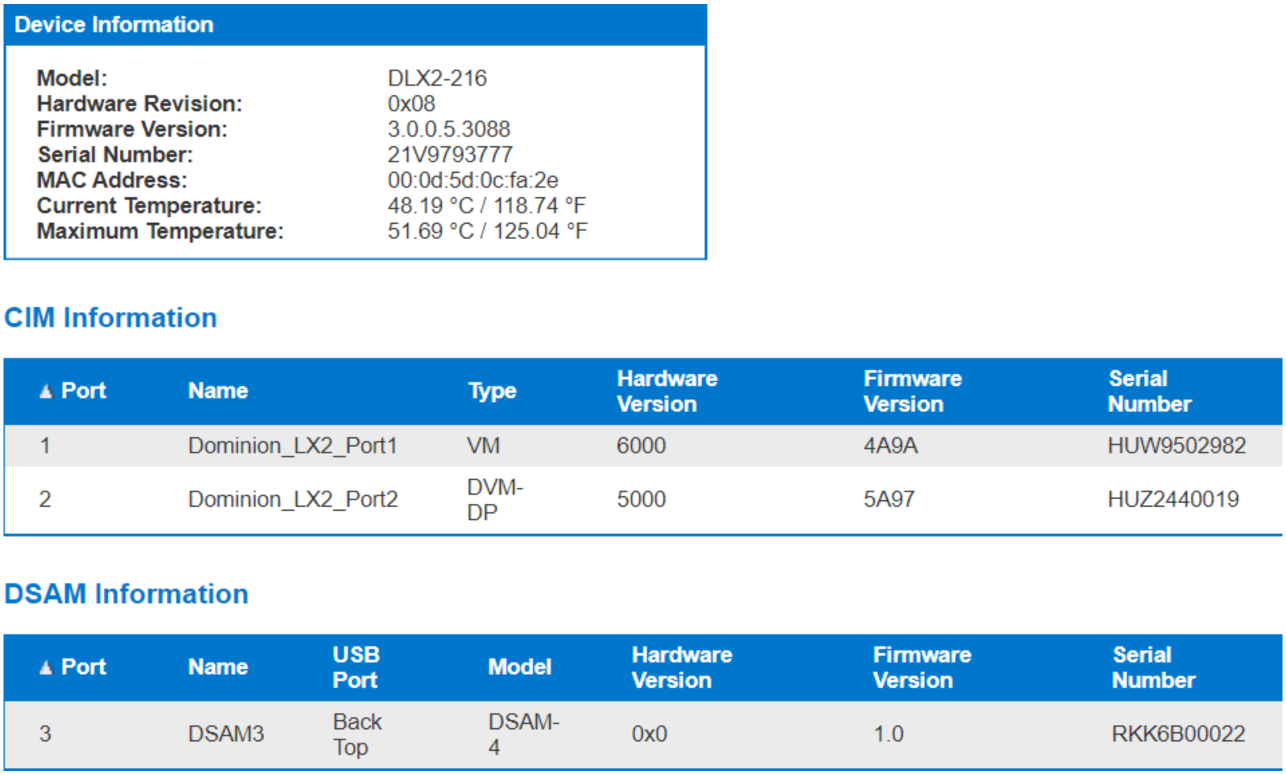
- Model
- Hardware Revision
- Firmware Version
- Serial Number
- MAC Address

The following information is provided about the CIMs in use:

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

The following information about connected DSAM units:

- Port number
- Name
- USB Port where DSAM unit is connected
- Model
- Hardware version
- Firmware version
- Serial number



Device Information

Model:	DLX2-216
Hardware Revision:	0x08
Firmware Version:	3.0.0.5.3088
Serial Number:	21V9793777
MAC Address:	00:0d:5d:0c:fa:2e
Current Temperature:	48.19 °C / 118.74 °F
Maximum Temperature:	51.69 °C / 125.04 °F

CIM Information

▲ Port	Name	Type	Hardware Version	Firmware Version	Serial Number
1	Dominion_LX2_Port1	VM	6000	4A9A	HUW9502982
2	Dominion_LX2_Port2	DVM-DP	5000	5A97	HUZ2440019

DSAM Information

▲ Port	Name	USB Port	Model	Hardware Version	Firmware Version	Serial Number
3	DSAM3	Back Top	DSAM-4	0x0	1.0	RKK6B00022

Creating a Backup and Restore File

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

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 II by backing up the user configuration settings from the LX II in use and restoring those configurations to the new LX II.

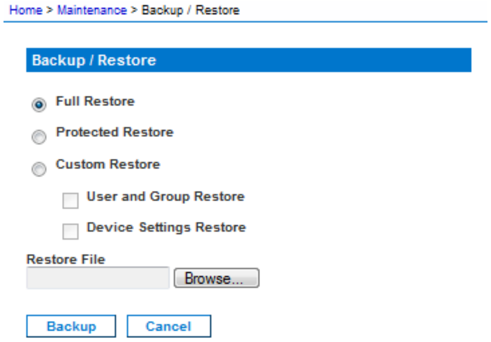
You can also set up one LX II and copy its configuration to multiple LX II appliances.

Create a Backup File

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

To create a backup file:

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



Home > Maintenance > Backup / Restore

Backup / Restore

● Full Restore

○ Protected Restore

○ Custom Restore

□ User and Group Restore

□ Device Settings Restore

Restore File

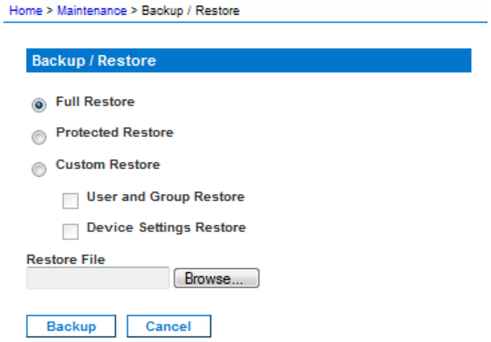
2. Click Backup. The backup file is created and displays as a downloaded file in your browser. Download location varies based on browser.

Restore Your LX II Using a Restore File

> WARNING: Exercise caution when restoring your LX II 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 II.
>
> 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.

To restore your LX II:

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



Home > Maintenance > Backup / Restore

Backup / Restore

● Full Restore
○ Protected Restore
○ Custom Restore
□ User and Group Restore
□ Device Settings Restore

Restore File

2. 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 appliance-specific information such as IP address, name, and so forth. With this option, you can setup one LX II and copy the configuration to multiple LX II appliances.
    - 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 II.
        - Device Settings Restore - This option includes only appliance settings such as USB profiles. Use this option to quickly copy the appliance information.
3. Click Browse. A Choose File dialog appears.
4. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.

5. Click Restore. The configuration is restored based on the type of restore selected.

USB Profile Management

From the USB Profile Management page, you can upload custom profiles provided by technical support. These profiles are designed to address the needs of your target server's configuration, in the event that the set of standard profiles does not already address them. Technical support will provide the custom profile and work with you to verify the solution for your target server's specific needs.

▶ To access the USB Profile Management page:

- Choose Maintenance > USB Profile Management. The USB Profile Management page opens.

▶ To upload a custom profile to your LX II:

1. Click Browse. A Choose File dialog appears.
2. Navigate to and select the appropriate custom profile file and click Open. The file selected is listed in the USB Profile File field.
3. Click Upload. The custom profile will be uploaded and displayed in the Profile table.

Note: If an error or warning is displayed during the upload process (for example. overwriting an existing custom profile), you may continue with the upload by clicking Upload or cancel it by clicking on Cancel.

▶ To delete a custom profile to your LX II:

1. Check the box corresponding to the row of the table containing the custom profile to be deleted.
2. Click Delete. The custom profile will be deleted and removed from the Profile table.

As noted, you may delete a custom profile from the system while it is still designated as an active profile. Doing so will terminate any virtual media sessions that were in place.

Handling Conflicts in Profile Names

A naming conflict between custom and standard USB profiles may occur when a firmware upgrade is performed. This may occur if a custom profile that has been created and incorporated into the list of standard profiles has the same name as a new USB profile that is downloaded as part of the firmware upgrade.

Should this occur, the preexisting custom profile will be tagged as 'old_'. For example, if a custom profile called GenericUSBProfile5 has been created and a profile with the same name is downloaded during a firmware upgrade, the existing file will then be called 'old_GenericUSBProfile5'.

You can delete the existing profile if needed. See ***USB Profile Management*** (on page 120) for more information.

Upgrading CIMs

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

▶ **To upgrade CIMs using the LX II 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.

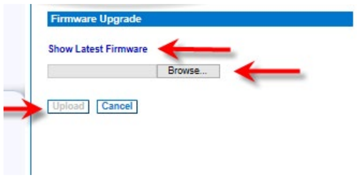
2. Check the Selected checkbox for each CIM you want to upgrade.
3. Click Upgrade. You are prompted to confirm the upgrade.
4. Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes or less per CIM.

Upgrading the LX II Firmware

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

Firmware Upgrade

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



▶ To upgrade your LX II appliance:

1. Click the Show Latest Firmware link to locate the appropriate file (*.RFP) on the ***Raritan website http://www.raritan.com***.
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. 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.

6. 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 appliance reboots (1 beep sounds to signal that the reboot has completed).
7. As prompted, close the browser and wait approximately 5 minutes before logging in to the LX II again.

Upgrade History

The LX II provides information about upgrades performed.

To view the upgrade history:

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

Information is provided about the LX II 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)

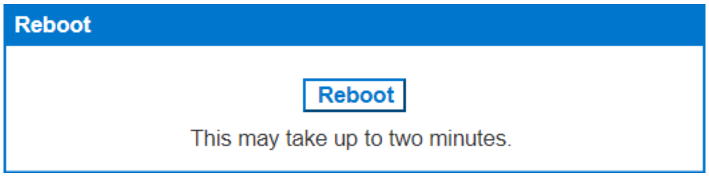
Rebooting the LX II

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

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

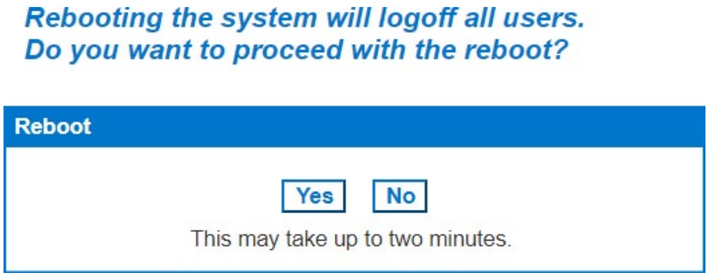
To reboot your LX II:

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



This may take up to two minutes.

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



Rebooting the system will logoff all users.
Do you want to proceed with the reboot?

This may take up to two minutes.

Diagnostics

Network Interface Page

The LX II 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:**

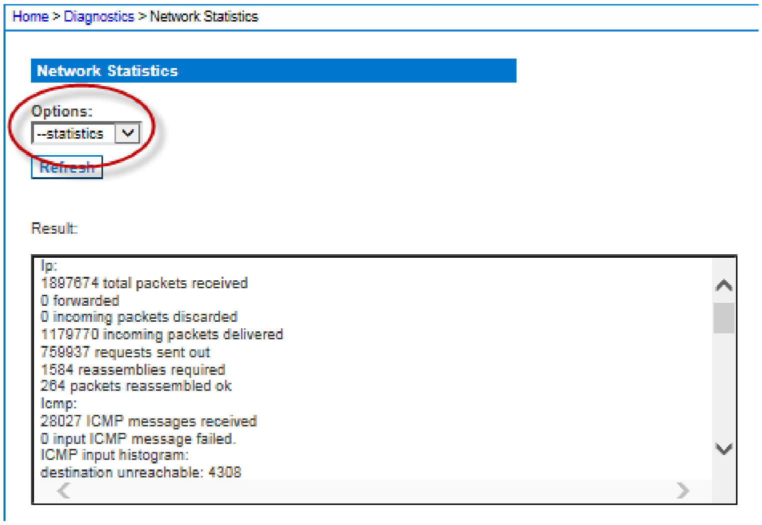
- Click Refresh.

Network Statistics Page

The LX II provides statistics about your network interface.

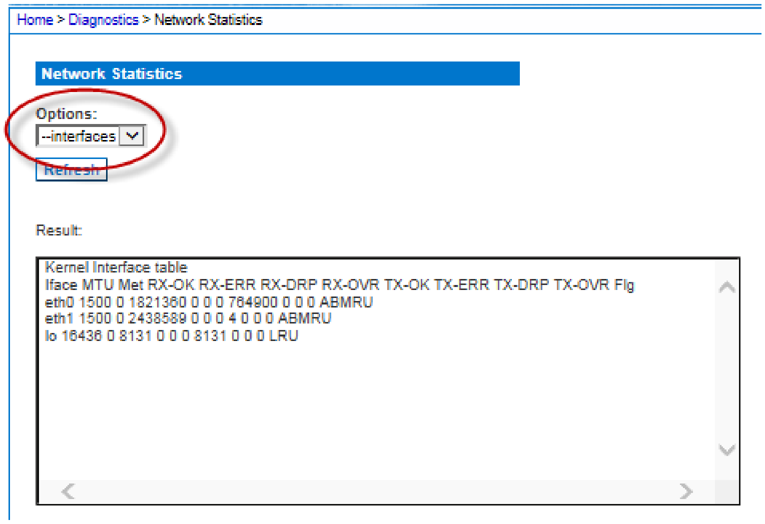
1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
2. Choose the appropriate option from the Options drop-down list.
3. Click Refresh. The relevant information is displayed in the Result field. See examples.

- Statistics



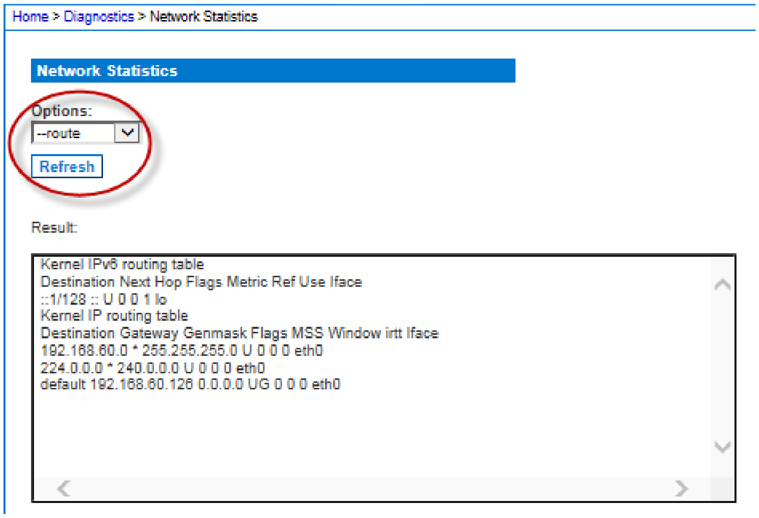
```
Ip:
1897674 total packets received
0 forwarded
0 incoming packets discarded
1179770 incoming packets delivered
759937 requests sent out
1584 reassemblies required
264 packets reassembled ok
Icmp:
28027 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
destination unreachable: 4308
```

- Interfaces:



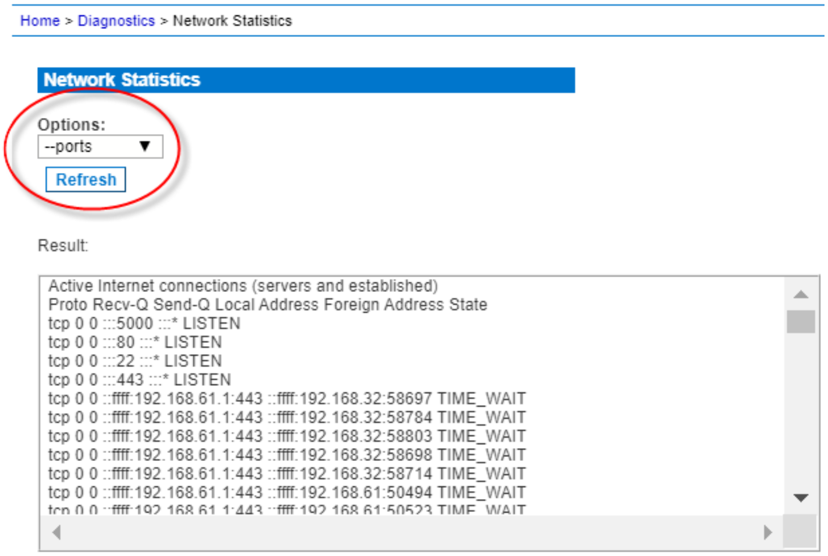
```
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0 1500 0 1821360 0 0 0 764900 0 0 0 ABMRU
eth1 1500 0 2438589 0 0 0 4 0 0 0 ABMRU
lo 16436 0 8131 0 0 0 8131 0 0 0 LRU
```

- Route:



```
Kernel IPv6 routing table
Destination Next Hop Flags Metric Ref Use Iface
::1/128 :: U 0 0 1 lo
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.60.0 * 255.255.255.0 U 0 0 0 eth0
224.0.0.0 * 240.0.0.0 U 0 0 0 eth0
default 192.168.60.126 0.0.0.0 UG 0 0 0 eth0
```

- Ports:



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 :::5000 :::* LISTEN
tcp 0 0 :::80 :::* LISTEN
tcp 0 0 :::22 :::* LISTEN
tcp 0 0 :::443 :::* LISTEN
tcp 0 0 ::ffff:192.168.61.1:443 ::ffff:192.168.32:58697 TIME_WAIT
tcp 0 0 ::ffff:192.168.61.1:443 ::ffff:192.168.32:58784 TIME_WAIT
tcp 0 0 ::ffff:192.168.61.1:443 ::ffff:192.168.32:58803 TIME_WAIT
tcp 0 0 ::ffff:192.168.61.1:443 ::ffff:192.168.32:58698 TIME_WAIT
tcp 0 0 ::ffff:192.168.61.1:443 ::ffff:192.168.32:58714 TIME_WAIT
tcp 0 0 ::ffff:192.168.61.1:443 ::ffff:192.168.61:50494 TIME_WAIT
tcp 0 0 ::ffff:192.168.61.1:443 ::ffff:192.168.61:50523 TIME_WAIT
```

Ping Host Page

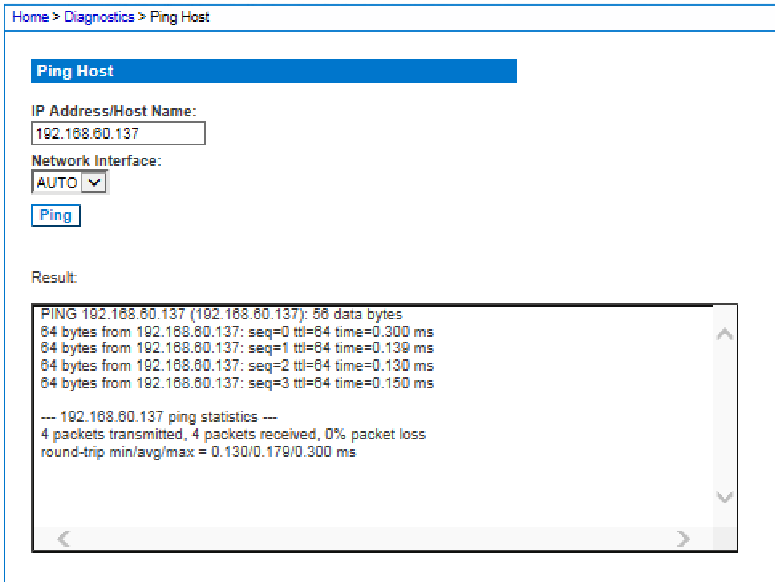
Ping is a network tool used to test whether a particular host or IP address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another LX II is accessible.

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.

4. Select the interface in the Network Interface drop-down box to ping on a specified interface. **Optional**



IP Address/Host Name: 192.168.60.137

Network Interface: AUTO

```
PING 192.168.60.137 (192.168.60.137): 56 data bytes
64 bytes from 192.168.60.137: seq=0 ttl=64 time=0.300 ms
64 bytes from 192.168.60.137: seq=1 ttl=64 time=0.139 ms
64 bytes from 192.168.60.137: seq=2 ttl=64 time=0.130 ms
64 bytes from 192.168.60.137: seq=3 ttl=64 time=0.150 ms

--- 192.168.60.137 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.130/0.179/0.300 ms
```

Trace Route to Host Page

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

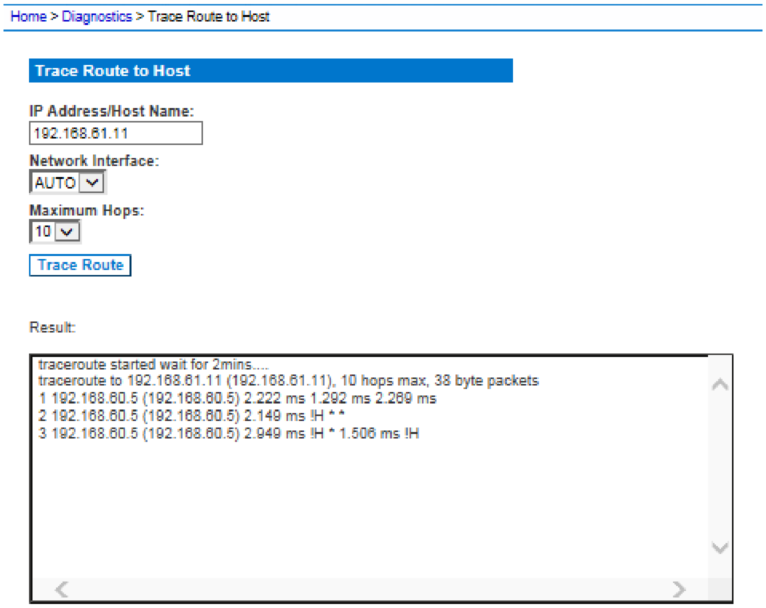
▶ To trace the route to the host:

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.

5. Select the interface in the Network Interface drop-down box to trace route on a specified interface. **Optional**



IP Address/Host Name: 192.168.61.11

Network Interface: AUTO

Maximum Hops: 10

Result:

```
traceroute started wait for 2mins....
traceroute to 192.168.61.11 (192.168.61.11), 10 hops max, 38 byte packets
1 192.168.60.5 (192.168.60.5) 2.222 ms 1.292 ms 2.269 ms
2 192.168.60.5 (192.168.60.5) 2.149 ms !H * *
3 192.168.60.5 (192.168.60.5) 2.949 ms !H * 1.506 ms !H
```

Device Diagnostics

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

Use this feature to download diagnostic information from the LX II 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 appliance 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 II appliance 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.

1. Choose Diagnostics > LX II Diagnostics. The LX II Diagnostics page opens.
2. To execute a diagnostics script file emailed to you from Raritan Technical Support, retrieve the diagnostics file supplied by Raritan using the browse function.
3. Click Run Script. Send this file to Raritan Technical Support.
4. To create a diagnostics file to send to Raritan Technical Support, click Save to File and save the file locally from the Save As dialog.

5. Email this file as directed by Raritan Technical Support.

LX II Local Console - Administration Functions

The LX II provides at-the-rack access and administration via its local port. Access to LX II features are provided via the Local Console.

The majority of administrative functions performed from the LX II Remote Console are also performed from the Local Console.

This section is specific to Administrator tasks. For end user tasks performed from the Local Console, see ***LX II Local Console*** (on page 240).

Security and Authentication

In order to use the LX II Local Console, you must first authenticate with a valid username and password.

The LX II provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port.

In either case, the LX II allows access only to those servers to which a user has access permissions. See ***User Management*** (on page 47) for additional information on specifying server access and security settings.

If your LX II 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 II Local Console:**

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

Configuring Local Port Settings from the Local Console

The standard local port can be configured from the Remote Console on the Port Configuration page, or from the Local Console on the Local Port Settings page.

From the Local Port Settings page, you can customize many settings for the LX II 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.

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

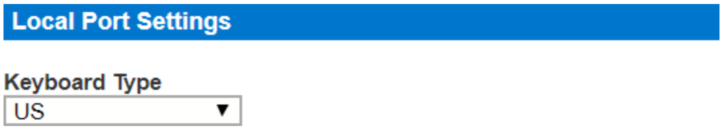
▶ To configure the local port settings:

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.

Select the Local Console Keyboard Type

1. Choose the appropriate keyboard type from among the options in the drop-down list.

   The browser will be restarted when this change is made.



Local Port Settings

Keyboard Type

US ▼

- US
- US/International
- United Kingdom
- French (France)
- German (Germany)
- German (Switzerland)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangul (Korean)
- JIS (Japanese Industry Standard)
- Portuguese (Portugal)
- Norwegian (Norway)
- Swedish (Sweden)
- Danish (Denmark)
- Belgian (Belgium)
- Hungarian
- Spanish
- Italian
- Slovenian

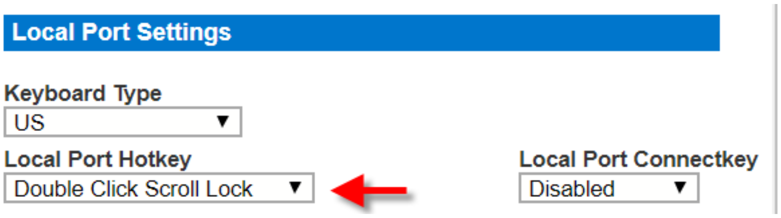
Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for LX II Local Console functions.

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

Select the Local Port Hotkey

1. Choose the local port hotkey. The local port hotkey is used to return to the LX II 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


Local Port Settings

Keyboard Type: US

Local Port Hotkey: Double Click Scroll Lock

Local Port Connectkey: Disabled

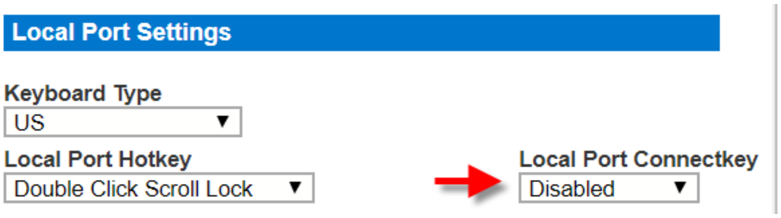
Select the Local Port Connect Key

Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target without returning to the GUI.

Then use the hot key to disconnect 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*** (on page 241) for examples of connect key sequences.

The connect key works for both standard servers and blade chassis.


Local Port Settings

Keyboard Type: US

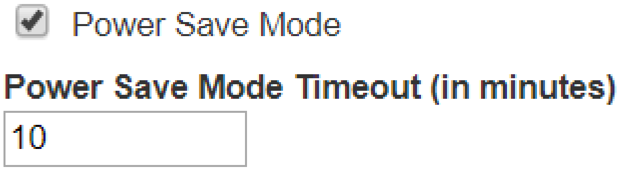
Local Port Hotkey: Double Click Scroll Lock

Local Port Connectkey: Disabled

Configure the Power Save Feature (Optional)

1. 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.



☑ Power Save Mode

Power Save Mode Timeout (in minutes)

10

Select the Local User Authentication

1. Choose the type of local user authentication.
   - Local/LDAP/RADIUS. This is the recommended option.
   - None. There is no authentication for Local Console access.

     This option is recommended for secure environments only.

Chapter 7 Command Line Interface (CLI)

In This Chapter

Overview

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

There is a limited set of CLI commands. See ***CLI Commands*** (on page 137) for a list of all the commands, definitions and links to examples.

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

Accessing the LX II Using CLI

Access the LX II 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.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client - ***www.openssh.org http://www.openssh.org***

SSH Connection to the LX II

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

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

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 II 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.

SSH Access from a UNIX/Linux Workstation

▶ **To open an SSH session from a UNIX®/Linux® workstation:**

1. Log in as the user `admin`, enter the following command:

```
ssh -l admin 192.168.30.222
```

Enter your password when the `Password` prompt appears.

See Logging In.

Navigating 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 a single word without an 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 II 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. The same configuration can be done via the Remote or Local Console.

LX II 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 II devices are shipped with the same default password. To avoid security breaches you must change the admin password from raritan to a custom password for the administrators who will manage the LX II 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.

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 II will need to be reset to the factory default from the Reset button on the back of the LX II. The initial configuration tasks will need to be performed again if this is done.

The LX II 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 II.

CLI Prompts

The Command Line Interface prompt indicates the current command level.

The root portion of the prompt is the login name.

`admin` is the root portion of a command when you establish a direct admin serial port connection via a terminal emulation application.

```
admin >
```

CLI Commands

- Enter `admin > help`.

Command	Description
config	Change to config sub menu.
connect	Connect to a port. (Only when DSAM is attached.)
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.
password	Set the current user's password.

- Enter `admin > config > network`.

Command	Description
dns	Display DNS information
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.
top	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 LX II.
- Providing authentication and authorization for users.
- Security profile.

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

Chapter 8 Virtual Media

In This Chapter

Overview

All LX II models support virtual media. Virtual media extends KVM capabilities by enabling target servers to remotely access media from a client PC and network file servers.

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

Each LX II comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, audio devices, internal and remote drives, and images.

Virtual media sessions are secured using 128 or 256 bit AES encryption.

HKC does not support all virtual media features. See ***HTML KVM Client (HKC)*** (on page 149) for details

Prerequisites for Using Virtual Media

LX II Virtual Media Prerequisites

- For users requiring access to virtual media, the LX II permissions must be set to allow access to the relevant port, as well as virtual media access (VM Access port permission) for the port. Port permissions are set at the group-level.
- If you want to use PC-Share, Security Settings must also be enabled in the Security Settings page. **Optional**
- A USB connection must exist between the device and the target server.
- You must choose the correct USB connection settings for the KVM target server you are connecting to.

Remote PC VM Prerequisites

- Certain virtual media options require administrative privileges on the PC (for example, drive redirection of complete drives).

Note: If you are using Windows, disable User Account Control or select Run as Administrator when starting Internet Explorer. To do this, click the Start Menu, locate IE, right-click and select Run as Administrator.

Target Server VM Prerequisites

- KVM target servers must support USB connected drives.

CIMs Required for Virtual Media

You must use one of the following CIMs is to use virtual media:

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP
- D2CIM-VUSB-USBC

The black USB connector on the DVUSB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media.

For CIMs with two USB plugs, keep both connected to the device.

The device may not operate properly if both plugs are not connected to the target server.

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.

Supported Tasks Via Virtual Media

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

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

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

Supported Virtual Media Types

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

- Internal and external hard drives
- Internal and USB-mounted CD and DVD drives
- USB mass storage devices
- PC hard drives
- ISO images (disk images)
- ISO9660 is the standard supported. However, other ISO standards can be used.

Note: Due to browser limitations, HKC supports a different set of virtual media types.

Conditions when Read/Write is Not Available

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

- For Linux® and Mac® clients
- When the drive is write-protected
- When the user does not have Read/Write permission:
  - Port Permission Access is set to None or View
  - Port Permission VM Access is set to Read-Only or Deny

Supported Virtual Media Operating Systems

The following client operating systems are supported:

- Windows ® 10
- Windows® 7
- openSUSE 15
- Fedora® 28
- RHEL® 7.4
- OSX Sierra

The Active KVM Client (AKC) can be used to mount virtual media types but only for Windows operating systems.

Number of Supported Virtual Media Drives

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

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

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

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

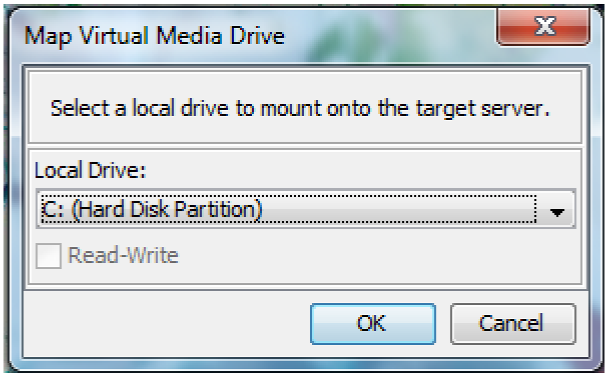
Virtual Media

Access a Virtual Media Drive on a Client Computer

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

To access a virtual media drive on the client computer:

1. From the KVM client, choose Virtual Media > Connect Drive, or click the Connect Drive... button . The Map Virtual Media Drive dialog appears.



Map Virtual Media Drive

Select a local drive to mount onto the target server.

Local Drive: C: (Hard Disk Partition)

□ Read-Write

2. Choose the drive from the Local Drive drop-down list.

   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 141) 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.

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

Mounting CD-ROM/DVD-ROM/ISO Images

This option mounts CD-ROM, DVD-ROM, and ISO images.

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

To access a CD-ROM, DVD-ROM, or ISO image:

1. From the KVM client, choose Virtual Media > Connect CD-ROM/ISO Image, or click the Connect CD ROM/ISO button . The Map Virtual Media CD/ISO Image dialog appears.
2. For internal and external CD-ROM or DVD-ROM drives:
   a. Choose the Local CD/DVD Drive option.
   b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.

   c. Click OK.

3. For ISO images:
   a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
   b. Click Browse.
   c. Navigate to the path containing the disk image you want to use and click Open. The path is populated in the Image Path field.
   d. Click OK.
4. For remote ISO images on a file server:
   a. Choose the Remote Server ISO Image option.
   b. Choose Hostname and Image from the drop-down list. The file servers and image paths available are those that you configured using the Virtual Media Shared Images page. Only items you configured using the Virtual Media Shared Images page will be in the drop-down list.
   c. File Server Username - User name required for access to the file server. The name can include the domain name such as mydomain/username.
   d. File Server Password - Password required for access to the file server (field is masked as you type).
   e. Click OK.

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

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

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

Disconnect from Virtual Media Drives

▶ To disconnect the virtual media drives:

- For local drives, choose Virtual Media > Disconnect Drive.
- For CD-ROM, DVD-ROM, and ISO images, choose Virtual Media > Disconnect CD-ROM/ISO Image.

Note: In addition to disconnecting the virtual media using the Disconnect command, simply closing the KVM connection closes the virtual media as well.

Virtual Media in a Linux Environment

Active System Partitions

You cannot mount active system partitions from a Linux client.

Linux Ext3/4 drive partitions need to be unmounted via umount /dev/<device label> prior to a making a virtual media connection.

Mapped Drives

Mapped drives from Linux clients are not locked when mounted onto connected targets.

Drive Partitions

The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows and Linux cannot read Mac formatted partitions
- Only Windows Fat partitions are supported by Linux

Root User Permission Requirement

Your virtual media connection can be closed if you mount a CD ROM from a Linux client to a target and then unmount the CD ROM.

To avoid these issues, you must be a root user.

Connect Drive Permissions (Linux)

Linux users must have read-only permissions for the removable device they wish to connect to the target. For /dev/sdb1 run the following as root user:

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

The drive is then available to connect to the target.

Virtual Media in a Mac Environment

Active System Partition

You cannot use virtual media to mount active system partitions for a Mac client.

Drive Partitions

The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows cannot read Mac formatted partitions
- Windows FAT and NTFS are supported by Mac
- Mac users must unmount any devices that are already mounted in order to connect to a target server. Use >diskutil umount /dev/disk1s1 to unmount the device and diskutil mount /dev/disk1s1 to remount it.

Connect Drive Permissions (Mac)

For a device to be available to connect to a target from a Mac® client, you must have read-only permissions to the removable device, and also unmount the drive after doing so.

For /dev/sdb1, run the following commands as root user:

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
root@admistrator-desktop:~# diskutil umount /dev/sdb1
```

Virtual Media File Server Setup (File Server ISO Images Only)

This feature is only required when using virtual media to access file server ISO images. ISO9660 format is the standard supported. However, other CD-ROM extensions may also work.

Note: SMB/CIFS support is required on the file server.

Use the 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 143).

► 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.

Chapter 9 KVM Clients

LX II can be accessed with a variety of KVM clients that support your individual configuration.

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

KVM Client	Name	Platforms	Features
HTML KVM Client	**HKC**	▪ Linux ▪ Mac ▪ Windows ▪ HTML and Javascript	▪ Java-Free ▪ Supports most features ▪ See HTML KVM Client (HKC) for supported features
Active KVM Client	**AKC**	▪ Windows ▪ Requires Microsoft .NET	▪ Full-featured KVM Client ▪ Java-Free
Virtual KVM Client	**VKC**	▪ Linux ▪ Mac ▪ Windows	▪ Full-featured KVM Client ▪ Requires Java

In This Chapter

KVM Client Launching

KVM Client	Name	URL to Force Launch
HTML KVM Client - Java-Free	HKC	<LX II IP Address>**/hkc**
Active KVM Client - Requires .NET	AKC	<LX II IP Address>**/akc**
Virtual KVM Client - Requires Java	VKCs	<LX II IP Address>**/vkcs**

HTML KVM Client (HKC)

The HTML KVM client (HKC) provides KVM over IP access that runs in the browser without the need for applets or browser plugins. HKC is HTML5-based and does not use Java.

HKC runs on Linux and Mac clients, and on Windows clients in Internet Explorer 11 (not supported in IE 10 or lower), Edge, Firefox, Chrome and Safari browsers.

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

▶ Supported Features:

- Connection Properties
- USB Profiles
- Video Settings
- Input Settings
- Virtual Media: HKC supports a different set of virtual media features than the other KVM clients
- Keyboard Macros
- Import and Export of Keyboard Macros
- Send Text to Target
- Keyboard and Mouse Settings
- Single Mouse Mode - not available on IE browser
- Port Scanning

▶ Not supported:

- Audio
- Smartcard
- Tools Menu for setting client launch settings, setting disconnect from target hotkey, or configuring toolbar display.
- Limited keyboard support: US-English, UK-English, French, German, Swiss-German, and Japanese are supported
- Hotkeys for keyboard macros
- Pre-populated keyboard macros for Sun targets
- Can only create Macros from keys that exist on the client PC (US-English, UK-English, French, German), no special function keys except for delay key.
- Single Mouse mode - not available on IE
- Virtual Media write not supported
- Local file transfer supported by Chrome, Firefox, and Safari browsers only
- USB drive connects
- Favorites

- Dual video targets

Known Issues:

- When Single Mouse Mode in the Edge browser is selected for the first time, the user is prompted to turn off the local mouse pointer. Select the bottom part of the Yes button.
- Target connections from Chrome 61 running on Fedora requires HardWare Acceleration to be enabled.
- If erratic mouse response is seen in Single Mouse mode on Fedora clients using the default Gnome desktop, use the Gnome classic desktop.
- To enable scrollbars on Mac Browser target connections: On the OS menu bar, choose System Preferences > General > Show scroll bars: Always.
- Internet Explorer and Edge support only 6 sessions at a time. The error displayed when attempting to connect to a seventh target is "Error could not connect to target." For IE11, you can increase the sessions allowed in the Group policy editor. See https://jwebsocket.org/documentation/reference-guide/internet-explorer-tips.
- For IE11 and Edge IPv6 device connections, either use device hostname or literal IPv6 as UNC. See https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names
- For Mac/Safari IPv6 device connections, use device hostname.
- Client Keyboard input selection should be set for each device individually.
- If encountering issues on browsers that have previously connected to an older version, it may be necessary to clear the Cache Web Content from the browser.
- To launch HKC automatically in Safari browser: Use http://<IP Address>/hkc, OR use http://<IP Address>/ if "Java content on browser" is disabled in Java Control Panel, and "Java Plugin" is disabled in the browser.
- From Chrome running on Linux, to get ´ ` or ^, the key needs to be hit three times, or twice followed by a space.
- For Mac Client browsers, ensure that the device certificate is installed and trusted. The certificate Common name should match the IP address/Hostname used to connect to the device. See SSL and TLS Certificates for information on creating and installing certificates
- On a default build of Redhat 7/Firefox ESR 24.5, there is no target video displayed on HKC connections. Older versions of Firefox lack HTML5 functions needed to support HKC. Upgrade Firefox to the latest available version.
- If HKC does not load, but rather displays a white screen, your browser memory may be full. Close all browser windows and try again.

Connection Properties

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

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

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

▶ **To view connection properties:**

- Choose File > Connection Properties.

Default Connection Properties

The LX II comes configured to provide optimal performance for the majority of video streaming conditions.

Default connection settings are:

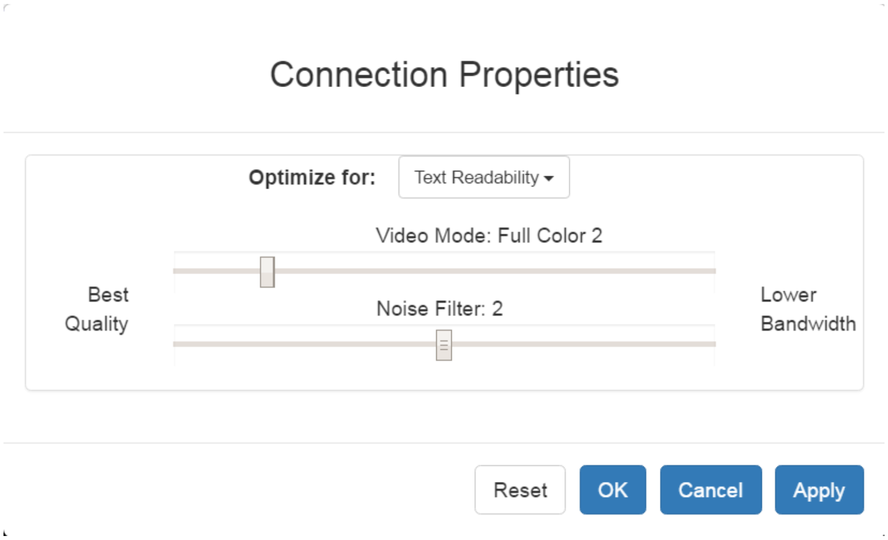
- Optimized for: Text Readability - video modes are designed to maximize text readability.

  This setting is ideal for general IT and computer applications, such as performing server administration.
- Video Mode - defaults to Full Color 2.

  Video frames transmit in high-quality, 24-bit color. This setting is suitable where a high-speed LAN is used.
- Noise Filter - defaults to 2.

  The noise filter setting does not often need to be changed.

Click Reset to regain the default connection properties.



Connection Properties

Optimize for: Text Readability

Video Mode: Full Color 2

Noise Filter: 2

Text Readability

Text Readability is designed to provide video modes with lower color depth but text remains readable. Greyscale modes are even available when applying lower bandwidth settings.

This setting is ideal when working with computer GUIs, such as server administration.

When working in full color video modes, a slight contrast boost is provided, and text is sharper.

In lower quality video modes, bandwidth is decreased at the expense of accuracy.

Color Accuracy

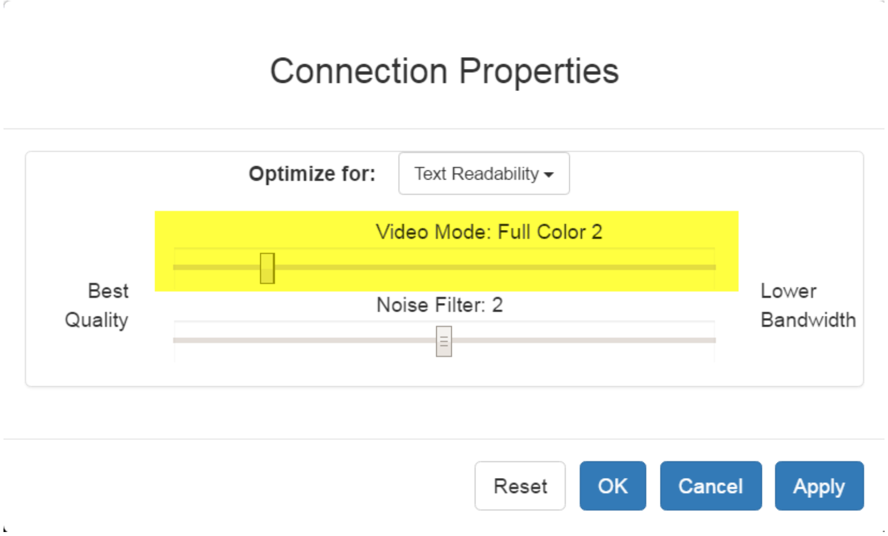
When Color Accuracy is selected, all video modes are rendered in full 24-bit color with more compression artifacts.

This setting applies to viewing video streams such as movies or other broadcast streams.

In lower quality video modes, sharpness of fine detail, such as text, is sacrificed.

Video Mode

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



Connection Properties

Optimize for: Text Readability

Video Mode: Full Color 2

Noise Filter: 2

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

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

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

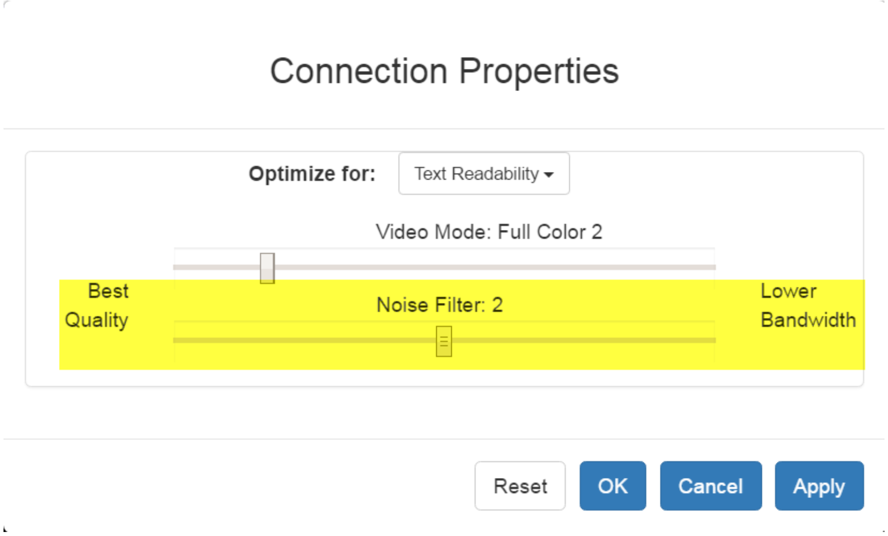
When Text Readability is selected as the Optimized setting, the four rightmost modes provide reduced color resolution or no color at all.

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

Noise Filter

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

The Noise Filter controls how much interframe noise is absorbed by the LX II.



Connection Properties

Optimize for: Text Readability

Video Mode: Full Color 2

Noise Filter: 2

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

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

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

Connection Info

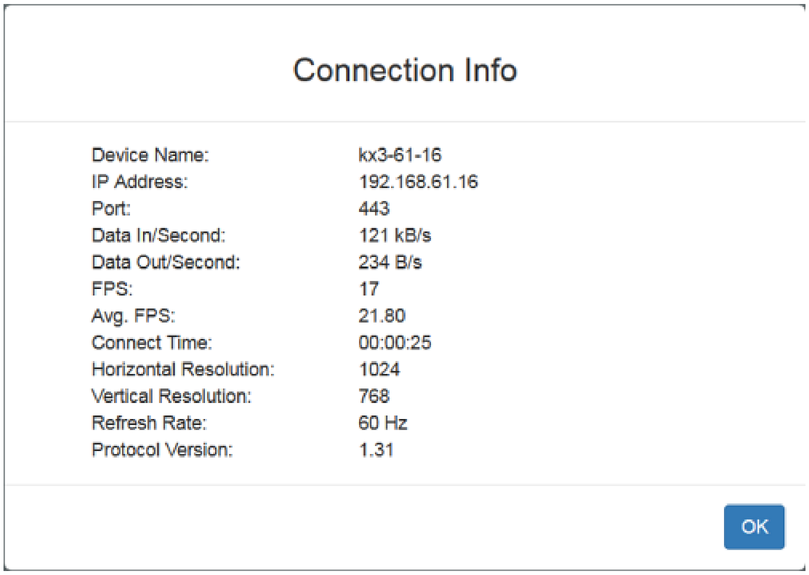
Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See ***Default Connection Properties*** (on page 151) for help configuring the connection properties.

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

To view connection info:

- Choose File > Connection Info.



Connection Info

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

USB Profile

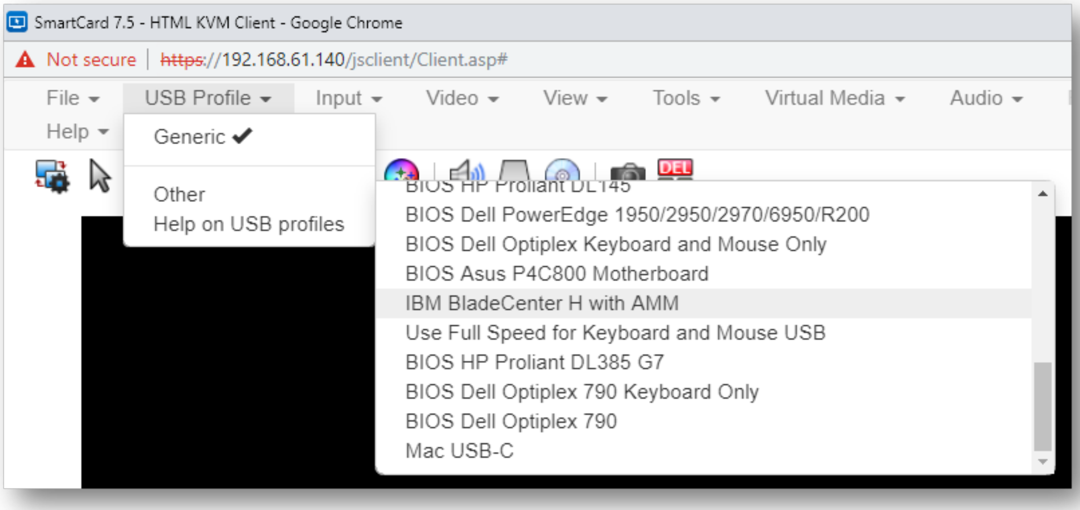
Select a USB profile that best applies to the KVM target server.

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

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

▶ To set a USB profile for a target server:

- Choose USB Profile, then choose Generic, or choose Other Profiles to select from a menu.


SmartCard 7.5 - HTML KVM Client - Google Chrome
Not secure | https://192.168.61.140/jsclient/Client.asp#
File
USB Profile
Input
Video
View
Tools
Virtual Media
Audio
Help
Generic ✔
Other
Help on USB profiles
BIOS HP Proliant DL145
BIOS Dell PowerEdge 1950/2950/2970/6950/R200
BIOS Dell Optiplex Keyboard and Mouse Only
BIOS Asus P4C800 Motherboard
IBM BladeCenter H with AMM
Use Full Speed for Keyboard and Mouse USB
BIOS HP Proliant DL385 G7
BIOS Dell Optiplex 790 Keyboard Only
BIOS Dell Optiplex 790
Mac USB-C
DEL

Note: When using the D2CIM-VUSB-USBC on Mac targets, you must select the "Mac USB-C" profile.

▶ To view details on USB profiles:

Choose USB Profile > Help on USB Profiles.

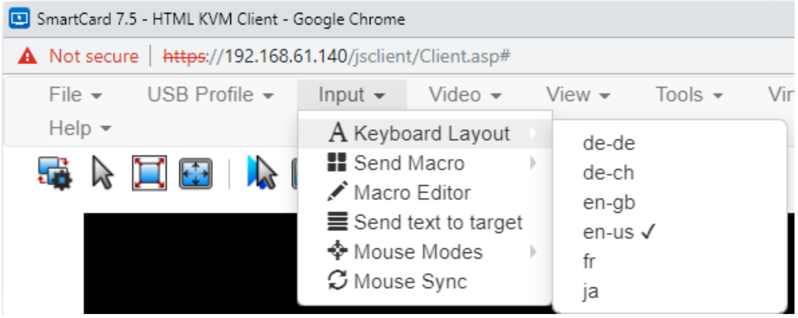
Input Menu

Keyboard Layout

▶ To set your keyboard type.

- Choose Input > Keyboard Layout, then select your keyboard type.
  - de-de
  - de-ch
  - en-gb

  - en-us
  - fr
  - ja

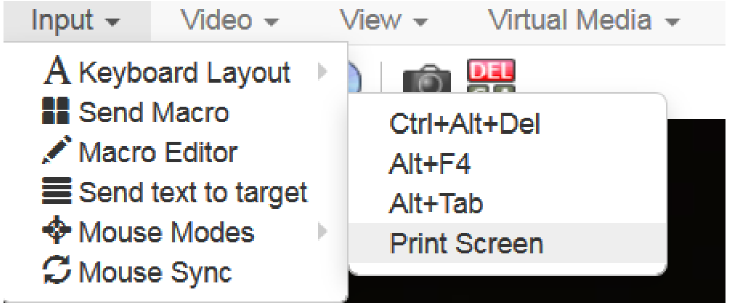


Send Macro

Due to frequent use, several keyboard macros are preprogrammed.

To send a preprogrammed macro:

- Choose Input > Send Macro, then select the macro:
  - Ctrl+Alt+Del: Sends the key sequence to the target without affecting the client.
  - Alt+F4: Closes a window on a target server.
  - Alt+Tab: Switch between open windows on a target server.
  - Print Screen: Take a screenshot of the target server.



Macro Editor

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

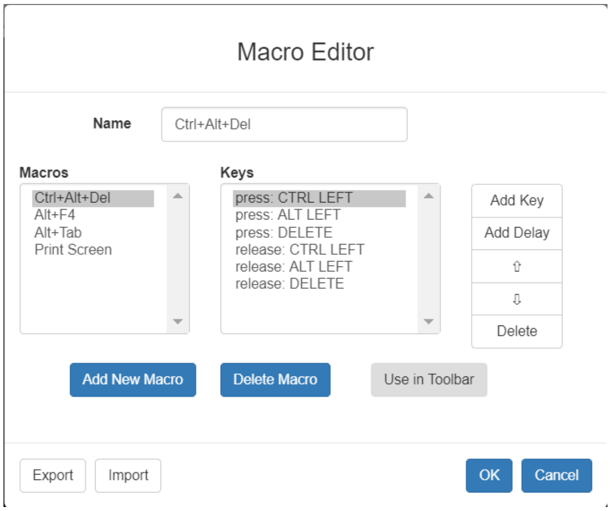
Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

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

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one LX II, your macros will only be available on the browser and LX II where they were created. To reuse your macros in another LX II device, you can import and export the macro files. See ***Import and Export Macros*** (on page 161).

To access the Macro Editor:

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



Macro Editor

Name: Ctrl+Alt+Del

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

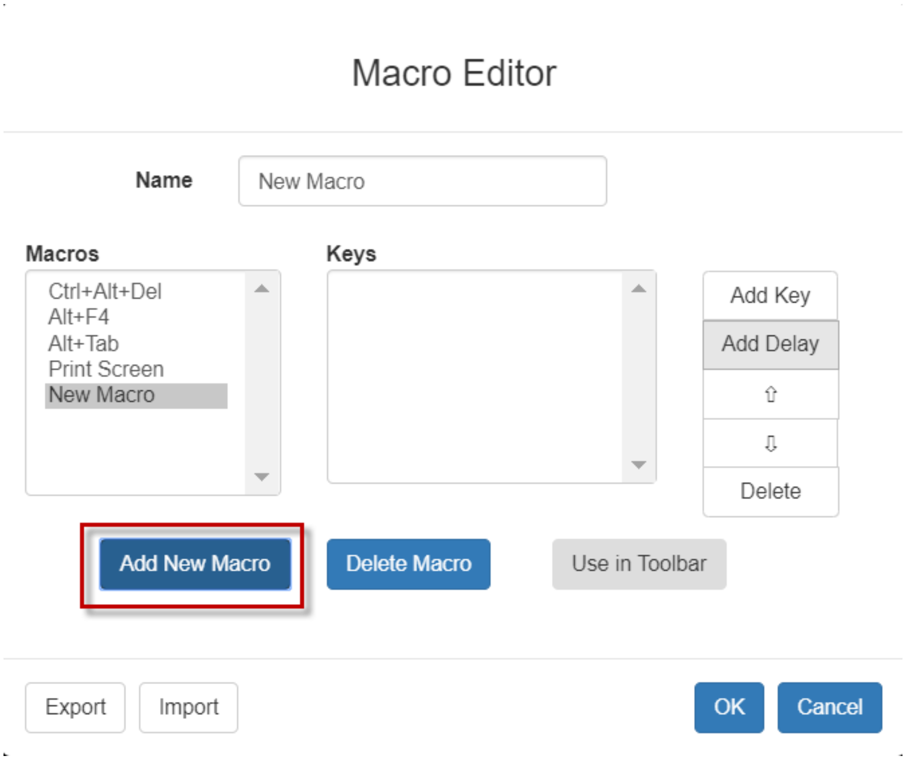
Keys:
press: CTRL LEFT
press: ALT LEFT
press: DELETE
release: CTRL LEFT
release: ALT LEFT
release: DELETE

Add New Macro

To add a new macro:

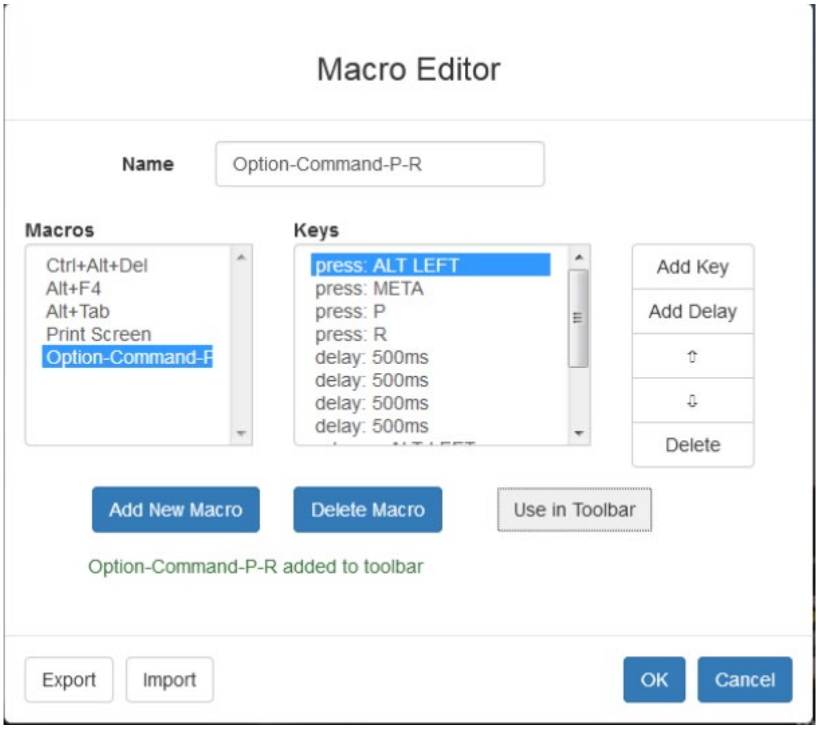
1. Choose Inputs > Macro Editor.

2. Click Add New Macro.



3. Enter a Name for the new macro. The name will appear in the Send Macro menu once the macro is saved.
4. Click Add Key, then press the key you want to add to the macro. The key press and key release appear in the Keys list.
   - To add more keys, click Add Key again, and press another key.
   - To remove a key, select it in the Keys list and click Delete Key
5. To put the keys in the correct sequence, click to select a key in the Keys list, then click the up and down arrows.
6. To add a 500 ms delay to a key sequence, click Add Delay. A delay in the middle of a press-and-release key sequence indicates holding down a key. Add multiple delays to indicate a longer press-and-hold of a key. Click the up and down arrows to move the delays into the correct sequence.

7. Click OK to save. To use this macro from your toolbar, click Use in Toolbar. See ***Add a Macro to the Toolbar*** (on page 160) for more details.



Name: Option-Command-P-R

Macros:
- Ctrl+Alt+Del
- Alt+F4
- Alt+Tab
- Print Screen
- Option-Command-P

Keys:
- press: ALT LEFT
- press: META
- press: P
- press: R
- delay: 500ms
- delay: 500ms
- delay: 500ms
- delay: 500ms

Option-Command-P-R added to toolbar

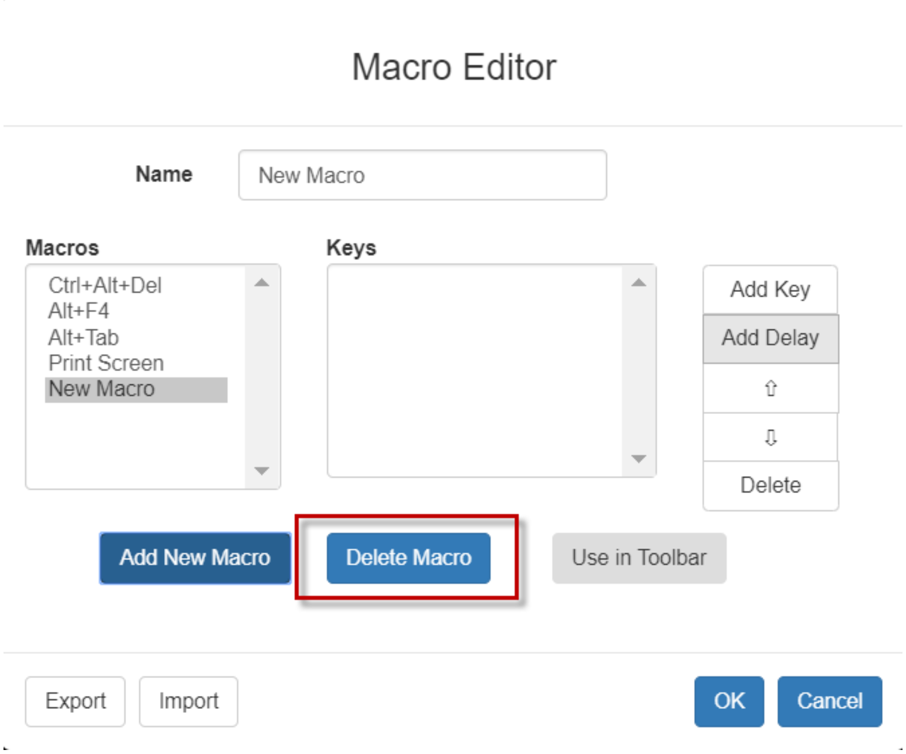
This example shows a macro for a Mac bootup sequence that requires a 2-second delay.

Delete a Macro

To delete a macro:

1. Choose Inputs > Macro Editor.
2. Select the macro, then click Delete Macro.

3. Click OK.



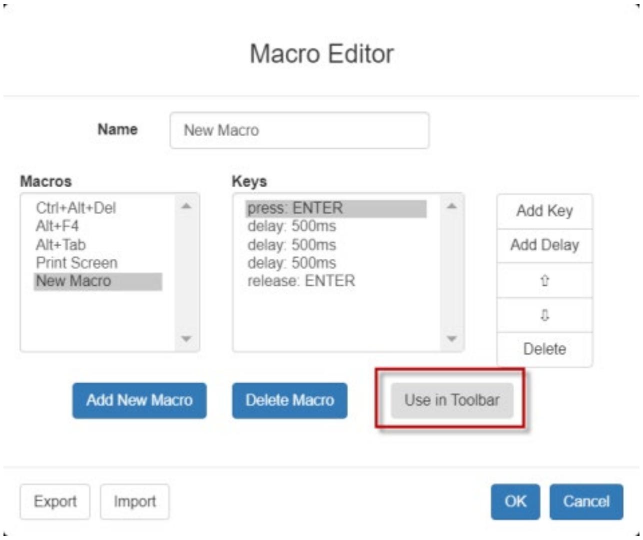
Add a Macro to the Toolbar

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

▶ To add a macro to the toolbar:

1. Choose Inputs > Macro Editor.
2. Select a macro from the Macros list.

3. Click Use in Toolbar.



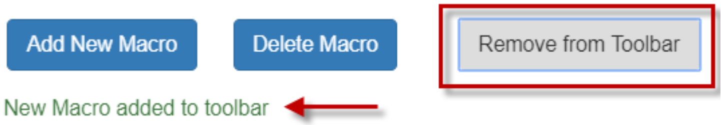
Macro Editor

Name: New Macro

Macros
Ctrl+Alt+Del
Alt+F4
Alt+Tab
Print Screen
New Macro

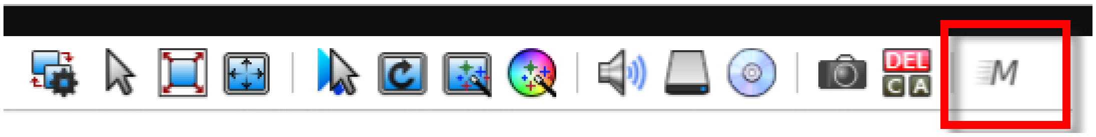
Keys
press: ENTER
delay: 500ms
delay: 500ms
delay: 500ms
release: ENTER

4. A message appears to confirm the macro is added to the toolbar.
   - To remove the macro from the toolbar, click Remove from Toolbar, or select a different macro and click Use in Toolbar.



New Macro added to toolbar

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



Import and Export Macros

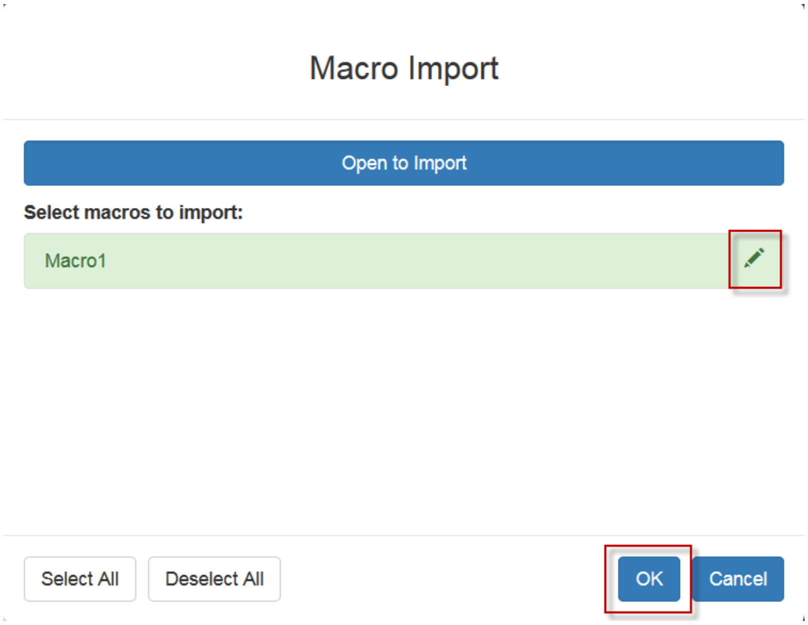
Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one LX II, your macros will only be available on the browser and LX II where they were created. To reuse your macros in another LX II device, you can import and export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

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

▶ To export and import macros:

1. Choose Input > Macro Editor. The list of macros created for your browser and LX II displays in the Macro Editor dialog.

2. To export the list, click the Export button, then save the file.
3. Log in to the LX II where you want to import the macros.
4. Choose Input > Macro Editor.
5. Click Import, then click Open to Import and select the usermacros.xml file, and click OK.
6. The macros found in the file display in the list. Select the macros you want to import, then click OK.
   - Macro names must be unique. If a macro with the same name already exists, an error message appears. Click the Edit icon to rename the macro, then click the checkmark to save the name.



Known Issues for Macros

- You cannot add the Command (Windows) key to a macro from Fedora browsers. The key is consumed by the OS.

Send Text to Target

Use the Send Text to Target function to send text directly to the target. If a text editor or command prompt is open and selected on the target, the text is pasted there.

To send text to target:

1. Choose Input > Send Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target. Supported keyboard characters only.
3. Click OK.

Mouse Modes

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

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

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

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

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

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when other modes don't work.

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

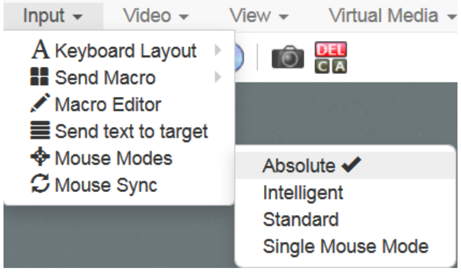
Absolute Mouse Synchronization

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

- Absolute Mouse Synchronization requires the use of a virtual media CIM - D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP, D2CIM-VUSB-USBC

▶ To enter Absolute Mouse Synchronization Mode:

- Choose Input > Mouse Modes > Absolute.

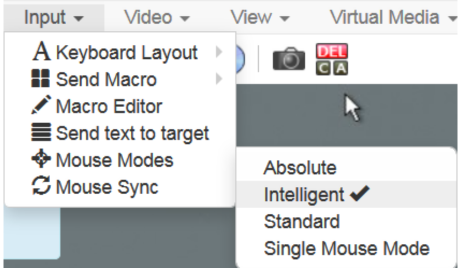


Intelligent

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

To enter Intelligent mouse mode:

- Choose Input > Mouse Mode > Intelligent. The mouse will synch. See ***Intelligent Mouse Synchronization Conditions*** (on page 166).



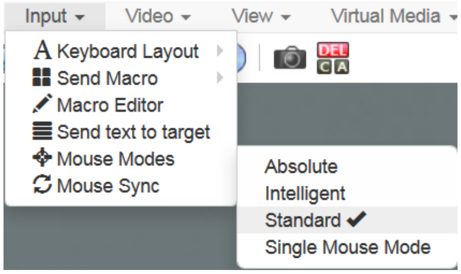
Standard

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

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

To enter Standard mouse mode:

- Choose Input > Mouse Modes > Standard.



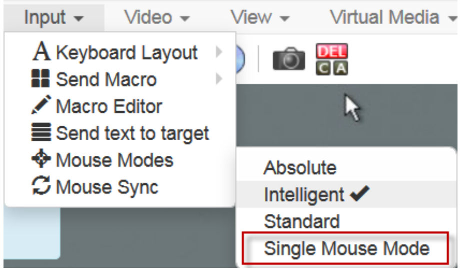
Single

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

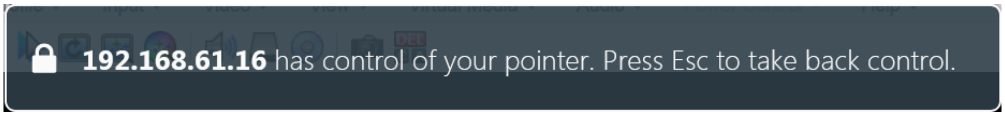
Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine. Single mouse mode is not available on Internet Explorer.

To enter Single mouse mode:

- Choose Inputs > Mouse Modes > Single.



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



192.168.61.16 has control of your pointer. Press Esc to take back control.

To exit Single mouse mode:

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

Mouse Sync

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

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

To synchronize the mouse cursors:

- Choose Inputs > Mouse Sync.

Intelligent Mouse Synchronization Conditions

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

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

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

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

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

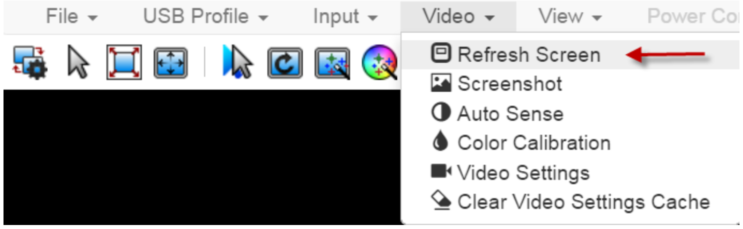
Video Menu

Refresh 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 command automatically detects the target server's video settings.
- The Color Calibration command calibrates the video to enhance the colors being displayed.
- In addition, you can manually adjust the settings using the Video Settings command.

To force a refresh of the video screen:

- Choose Video > Refresh Video.
- 

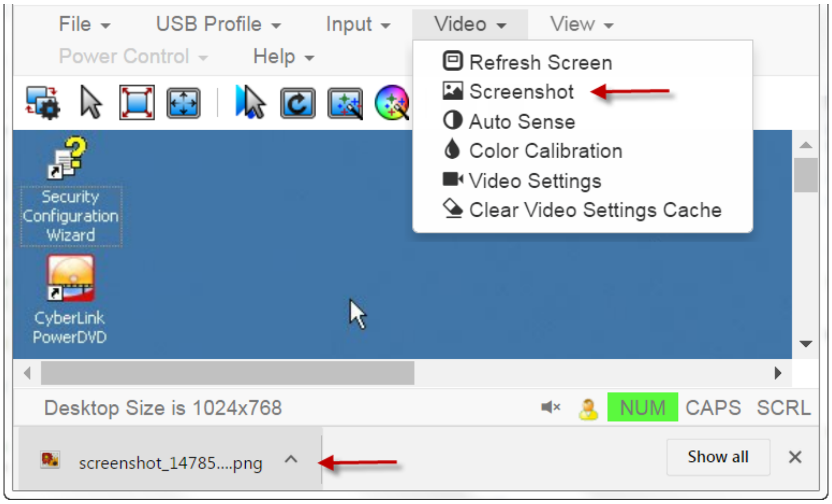
Screenshot

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

To take a screenshot of the target server:

1. Choose Video > Screenshot.

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



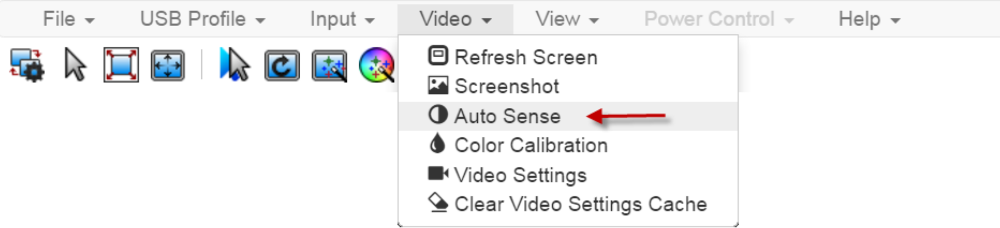
Auto Sense

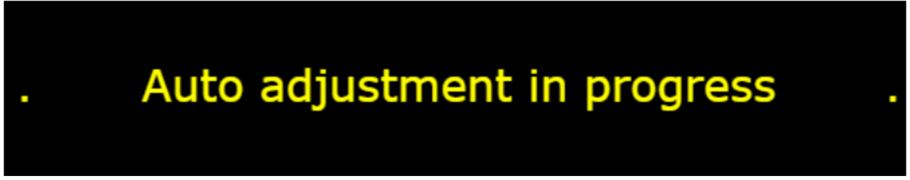
The Auto Sense command forces a re-sensing of the video settings, such as resolution and refresh rate, and redraws the video screen.

To automatically re-sense the video settings:

- Choose Video > Auto Sense .

  A message stating that the auto adjustment is in progress appears.





. Auto adjustment in progress .

Color Calibration

The Color Calibration command optimizes the color levels, such as hue, brightness, and saturation, of the transmitted video images.

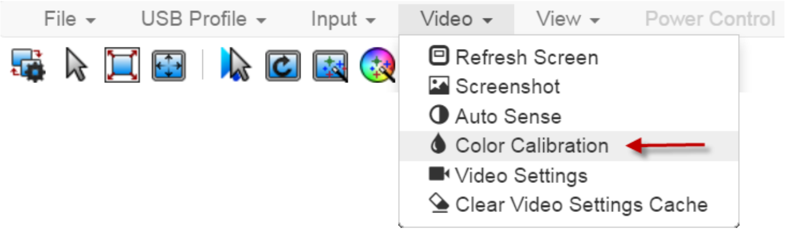
The color settings are on a target server-basis.

Note: When color is successfully calibrated, the values are cached and reused each time you switch to the target. Changes to the brightness and contrast in Video Settings are not cached. Changing resolution resets the video to the cached values again. You can clear the cached values in Video > Clear Video Settings Cache. See ***Clear Video Settings Cache*** (on page 196).

To calibrate color:

- Choose Video > Color Calibration.

  A message stating that the color calibration is in progress appears.



Video Settings

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

To change the video settings:

1. Choose Video > Video Settings to open the Video Settings dialog.
2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:
   a. 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.

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

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

      Brightness Green - Controls the brightness of the green signal.

Brightness Blue - Controls the brightness of the blue signal.

c. Contrast Red - Controls the red signal contrast.

Contrast Green - Controls the green signal.

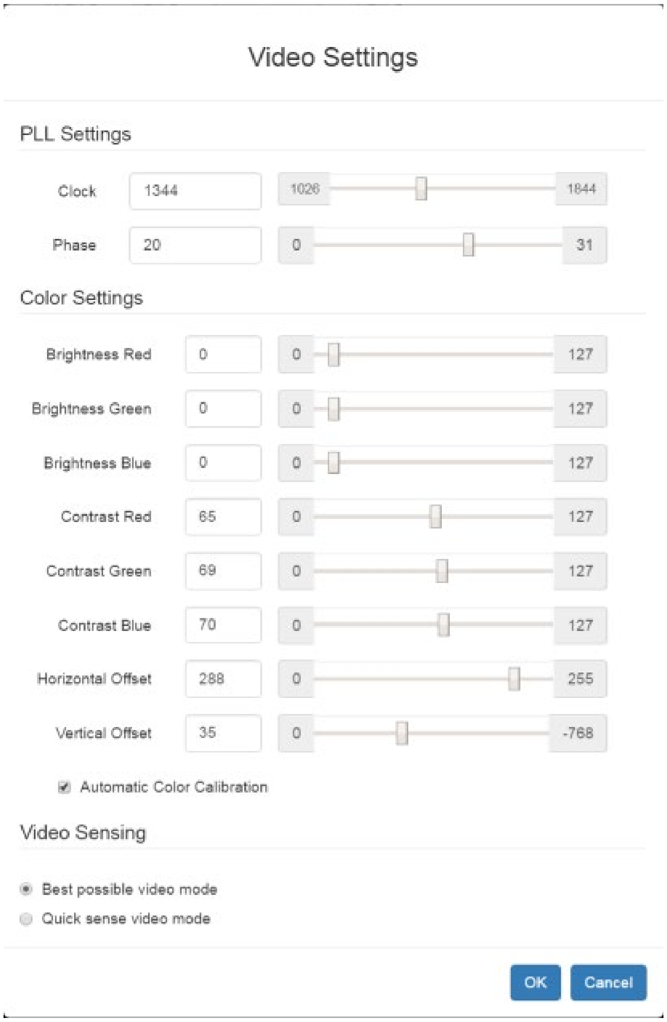
Contrast Blue - Controls the blue signal.

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 Technical Support before making any changes.

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

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



Video Settings

PLL Settings

Clock	1344	1026	1844
Phase	20	0	31

Color Settings

Brightness Red	0	0	127
Brightness Green	0	0	127
Brightness Blue	0	0	127
Contrast Red	65	0	127
Contrast Green	69	0	127
Contrast Blue	70	0	127
Horizontal Offset	288	0	255
Vertical Offset	35	0	-768

☑ Automatic Color Calibration

Video Sensing

● Best possible video mode

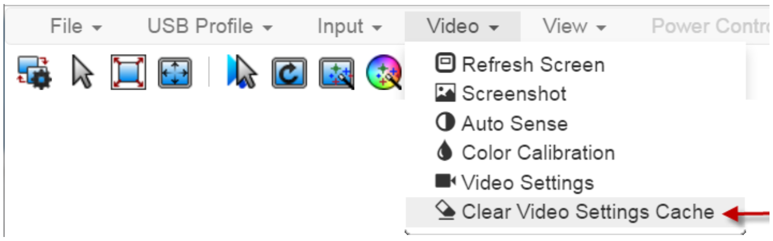
○ Quick sense video mode

Clear Video Settings Cache

You can clear the video settings cache to delete old settings that do not apply anymore, such as when a target server is replaced. When you clear the video settings cache, the server automatically does a video auto-sense and color calibration. The new values are cached and reused when the target is accessed again.

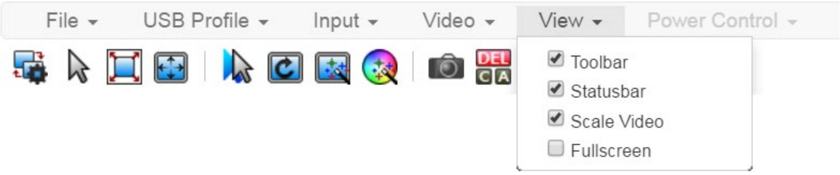
To clear the video settings cache:

- Choose Video > Clear Video Settings Cache in the toolbar.



View Menu

The View Menu contains options to customize your HKC display.



Toolbar and Statusbar:

The toolbar contains icons for some commands. The Statusbar displays screen resolution at the bottom of the client window.

Scale Video:

Scale Video scales your video to view the entire contents of the target server window in your HKC window. The scaling maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

Fullscreen:

Fullscreen sets the target window to the size of your full screen, removing your client from the view.

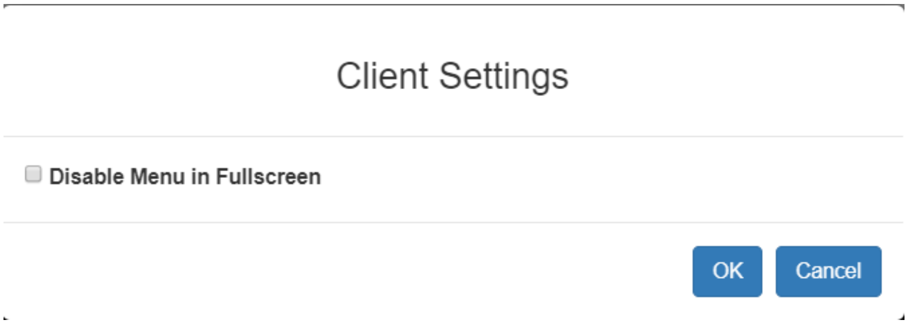
- Press Esc to exit fullscreen.

Tools Menu

The Tools menu contains options for settings that are helpful when accessing using a mobile device.

Client Settings:

- Choose Tools > Client Settings to access the Disable Menu in Fullscreen option.
- When selected, the menu bar will not be available in fullscreen mode. This setting is specific to the client, so it must be set for each client device and each browser used for access.



Client Settings

□ Disable Menu in Fullscreen

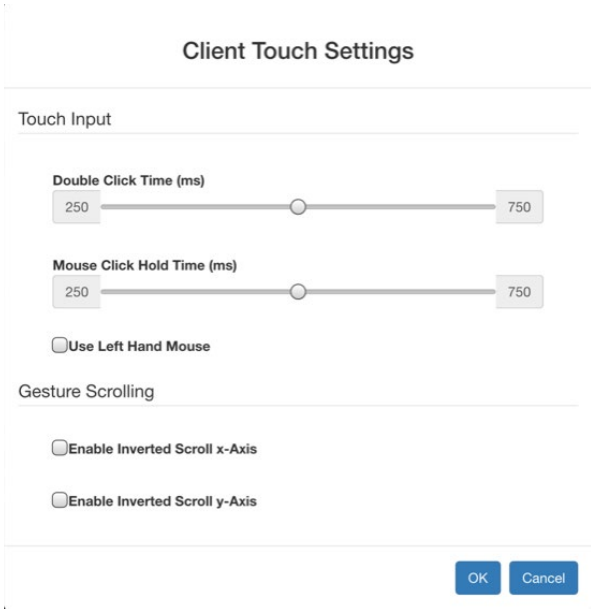
-

Launch Settings:

- Tap Tools > Launch Settings to access the Enable Scale Video option. When enabled, target video scales to the current KVM window size.

Touch Settings - enabled for iOS clients:

- Tap Tools > Touch Settings to access the Client Touch Settings. Customize the Touch Input and Gesture Scrolling settings for your mobile device.



Client Touch Settings

Touch Input

Double Click Time (ms)
250 750

Mouse Click Hold Time (ms)
250 750

☐ Use Left Hand Mouse

Gesture Scrolling

☐ Enable Inverted Scroll x-Axis

☐ Enable Inverted Scroll y-Axis

- Double Click Time: Time between two touch taps for the equivalent of a mouse double click.
- Mouse Click Hold Time: Time to hold after touch down for the equivalent of a mouse right click.
- Use Left Hand Mouse: Enable if the target OS's primary mouse button is set to Right.
- Enable Inverted Scroll x-Axis: If selected, two-finger movement to the right moves the screen to the left instead of the default right.
- Enable Inverted Scroll y-Axis: If selected, two-finger movement up moves the screen down instead of the default up.

Virtual Media Menu

Due to browser limitations, HKC supports a different set of virtual media functions than the other KVM Clients.

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

Connect Files and Folders

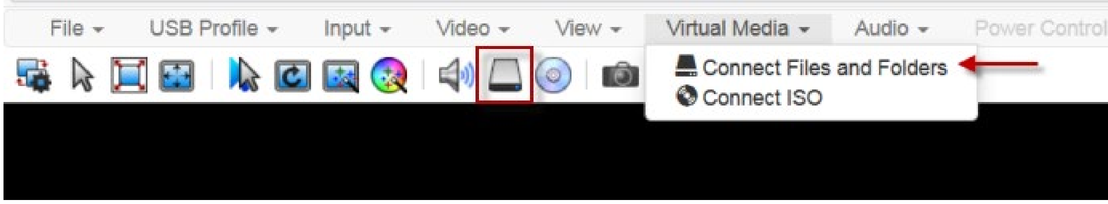
The Connect Files and Folders command provides an area to drag and drop files or folders that you want to connect to on virtual media.

Supported browsers: Chrome, Firefox, Safari

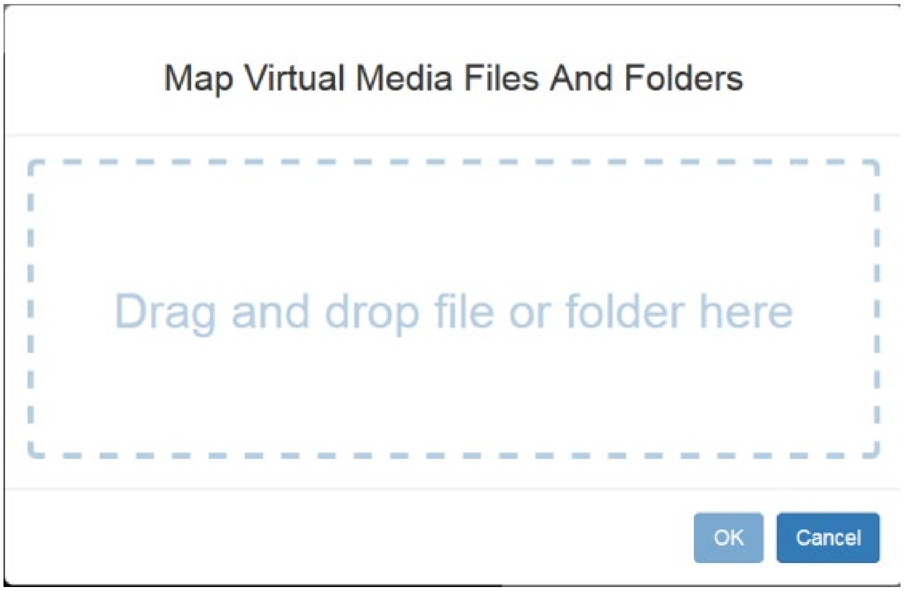
File size limit: 4GB per file

▶ **To connect files and folders:**

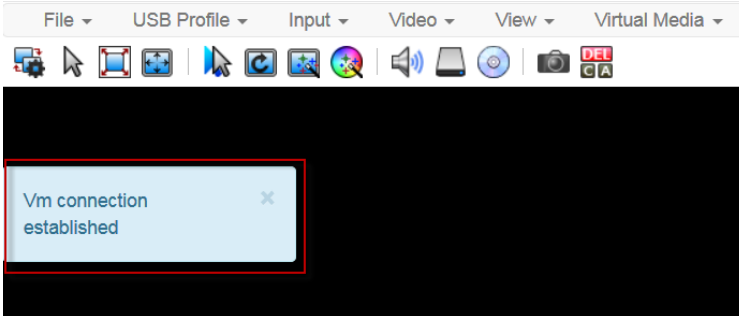
1. Choose Virtual Media > Connect Files and Folders. Or, click the matching icon in toolbar.



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


Map Virtual Media Files And Folders
Drag and drop file or folder here
OK
Cancel

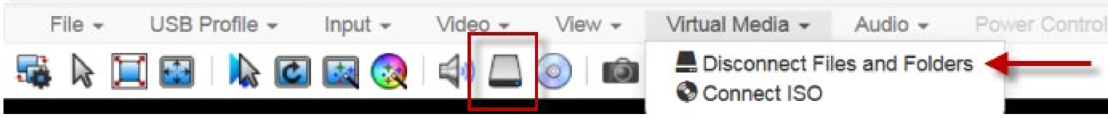
3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.



Vm connection established

To disconnect files and folders:

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



Connect ISO

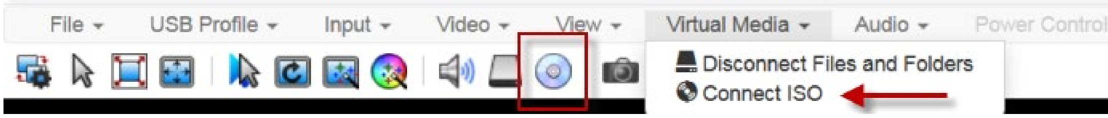
The Connect ISO command maps a virtual media ISO image to the target. You can connect to ISO images on your client or on remote servers.

File size limit: 4GB per file

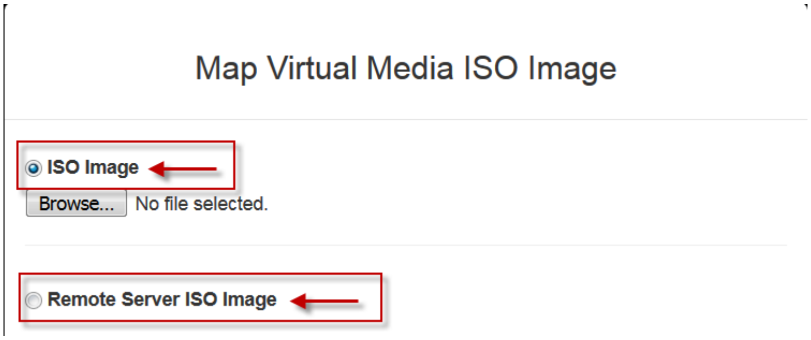
Note: If connection to your SAMBA server is lost while transferring files from your ISO to the target, keyboard and mouse control will be lost for several minutes, but will recover.

To map virtual media ISO images:

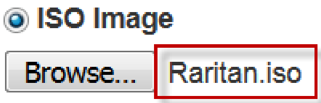
1. Choose Virtual Media > Connect ISO. Or, click the matching icon in the toolbar.



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

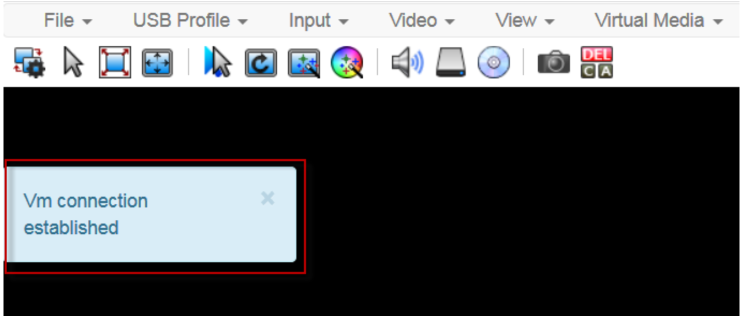


- Select ISO Image if the ISO file is directly accessible on your client. Click Browse, select the ISO file, and click OK. The filename appears next to the Browse button.



- Select Remote Server ISO Image if your ISO file is on a remote server. Remote ISO files must be pre-configured by an administrator for the mapping to appear here. See ***Virtual Media File Server Setup (File Server ISO Images Only)*** (on page 146). Select the Hostname, then select the ISO file from the Image list. Enter the file server's username and password.

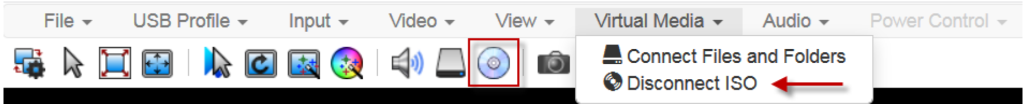
3. Click OK to map the selected file to the target. A message appears to show virtual media is connected.



Vm connection established

▶ To disconnect ISO:

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



Active KVM Client (AKC) Help

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

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

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

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

- Keyboard macros created in AKC cannot be used in any other client.
- Direct port access configuration
- AKC server certification validation configuration (see ***Prerequisites for Using AKC*** (on page 179))

For details on using the features, see ***Virtual KVM Client (VKC and VKCs) Help*** (on page 181).

Overview

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

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

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

- Keyboard macros created in AKC cannot be used in any other client.
- Direct port access configuration
- AKC server certification validation configuration (see ***Prerequisites for Using AKC*** (on page 179))

For details on using the features, see ***Virtual KVM Client (VKC and VKCs) Help*** (on page 181).

Recommended Minimum Active KVM Client (AKC) Requirements

It is recommended that the Active KVM Client (AKC) machines meet the following minimum requirements.

- Client machine with either a -
  - 'modern' dual-core CPU for a single connections, or
  - 'modern' quad core CPU for two or more simultaneous connections
- 4GB of RAM

AKC Supported Microsoft .NET Framework

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

AKC Supported Operating Systems

When launched from Internet Explorer®, the Active KVM Client (AKC) allows you to reach target servers via the LX II.

AKC is compatible with the following platforms:

- Windows 7® operating system (up to 64 bit)
- Windows 8® operating system (up to 64 bit)
- Windows 10 ® operating system (up to 64 bit)

AKC Supported Browsers

See the Release Notes for supported browser versions.

Prerequisites for Using AKC

Allow Cookies

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

Include LX II IP Address in 'Trusted Sites Zone'

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

Disable 'Protected Mode'

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

Enable AKC Download Server Certificate Validation

If the administrator has enabled the Enable AKC Download Server Certificate Validation option:

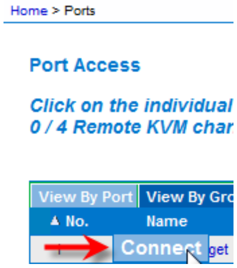
- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.
- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC)

Once you have logged on to the LX II Remote Console, access target servers via the Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC).

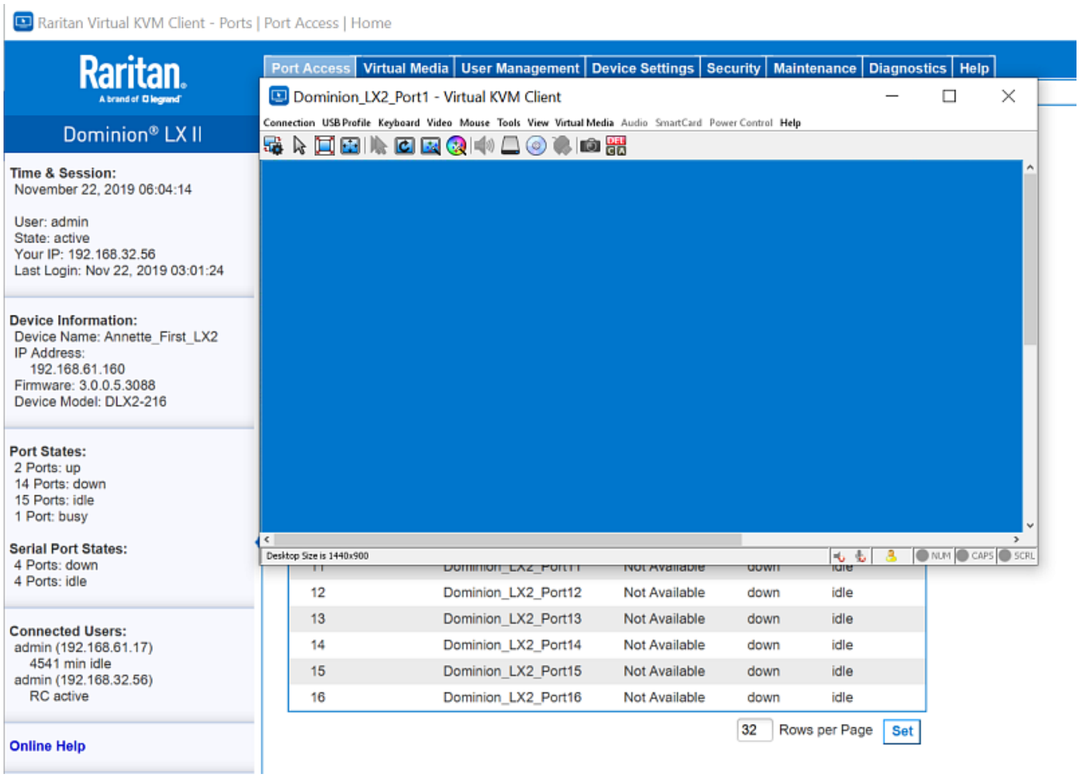
▶ To connect to an available server:

1. On the Port Access page, click on the port name of the target server you want to connect to. The Port Action menu opens.
2. Click Connect.



See Port Action Menu for details on additional available menu options.

Virtual KVM Client (VKC and VKCs) Help



Desktop Size is 1440x900

Time & Session:
November 22, 2019 06:04:14

User: admin
State: active
Your IP: 192.168.32.56
Last Login: Nov 22, 2019 03:01:24

Device Information:
Device Name: Annette_First_LX2
IP Address:
192.168.61.160
Firmware: 3.0.0.5.3088
Device Model: DLX2-216

Port States:
2 Ports: up
14 Ports: down
15 Ports: idle
1 Port: busy

Serial Port States:
4 Ports: down
4 Ports: idle

Connected Users:
admin (192.168.61.17)
4541 min idle
admin (192.168.32.56)
RC active

11	Dominion_LX2_Port11	Not Available	down	idle
12	Dominion_LX2_Port12	Not Available	down	idle
13	Dominion_LX2_Port13	Not Available	down	idle
14	Dominion_LX2_Port14	Not Available	down	idle
15	Dominion_LX2_Port15	Not Available	down	idle
16	Dominion_LX2_Port16	Not Available	down	idle

32 Rows per Page

Overview

There is one Virtual KVM Client for each target server connected.

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

IMPORTANT: Refreshing your browser closes the Virtual KVM Client connection.

Recommended Minimum Virtual KVM Client (VKC) Requirements

It is recommended that the Virtual KVM Client (VKC) machines meet the following minimum requirements.

- Client machine with either a -
  - 'modern' dual-core CPU for a single connections, or
  - 'modern' quad core CPU for two or more simultaneous connections
- 4GB of RAM
  - VKC requires 50MB of RAM per connection

Virtual KVM Client Java Requirements

A supported Java version is required. Check the release notes for latest supported version.

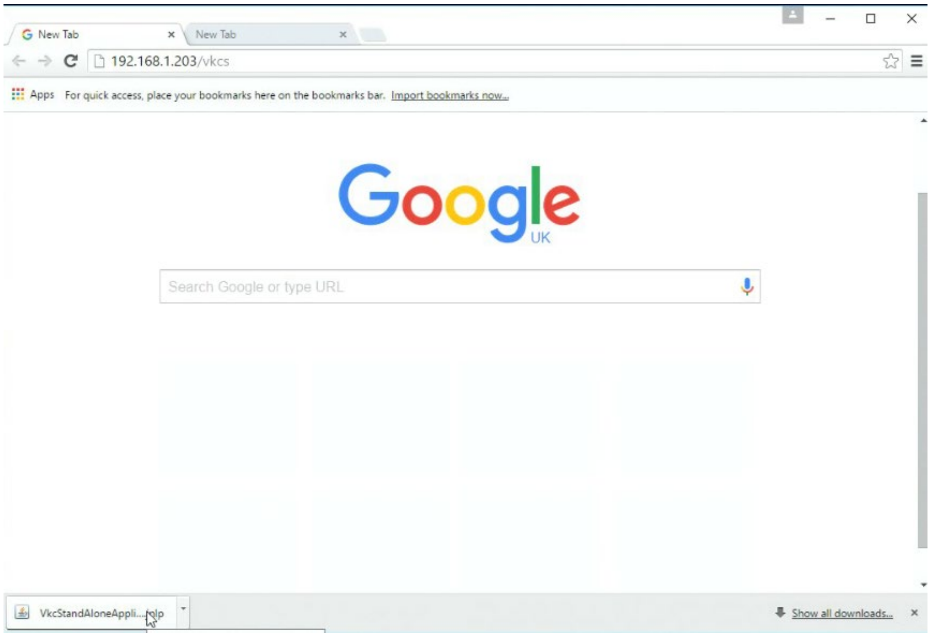
If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

Note: VKC cannot be launched from Safari, Edge, Chrome 45 or later, Firefox 42 or later. VKCS is recommended for these browsers.

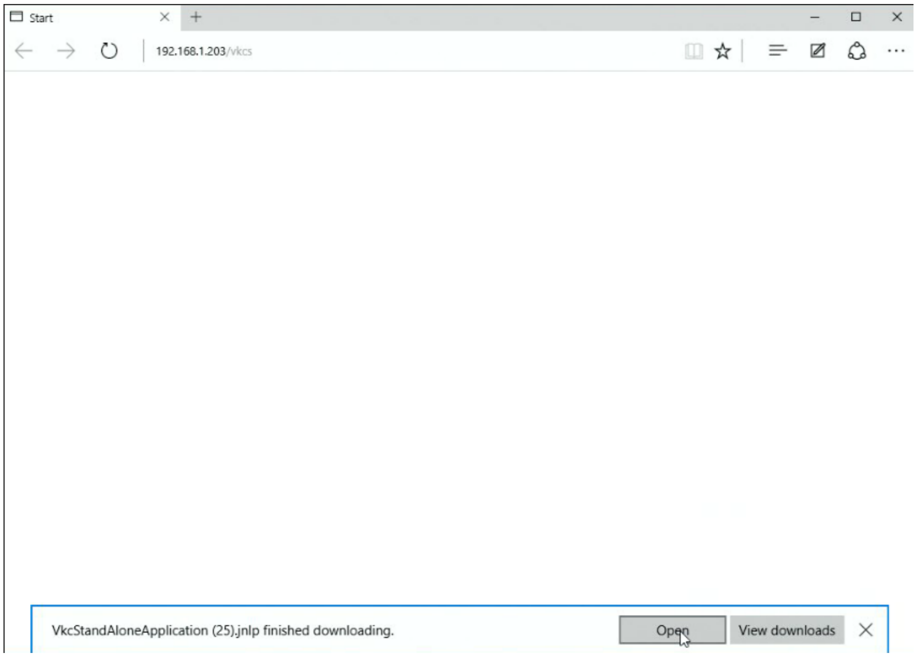
▶ VKCS Launching:

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

- Chrome: The downloaded VKCS jnlp file must always be clicked at bottom left corner of browser window to launch.


New Tab
New Tab
192.168.1.203/vkcs
Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Google
UK
Search Google or type URL
VkcStandAloneAppli....jnlp
Show all downloads...

- Edge: You must click Open at the bottom of the browser to launch.



VkcStandAloneApplication (25).jnlp finished downloading.

- Internet Explorer: Launches automatically.
- Safari: Save the jnlp file locally. Hold down the Ctrl key when selecting to open, then click Open in displayed prompt
- Firefox: The current default setting in Firefox on Windows saves the file and runs from the download. You can launch from the browser with this setting: Tools>Options>Applications, then select "Jnlp File" in the Content Type column, and change the Action from "Always ask" to "Use Java Web Launcher".

  When launched from the Firefox browser, an executable warning message is displayed. There are two methods to suppress this:

  - Launching via jnlp://<IP address>/vkcs

  For details, go to: https://superuser.com/questions/1441134/disable-firefoxs-open-executable-file-warning)

  OR

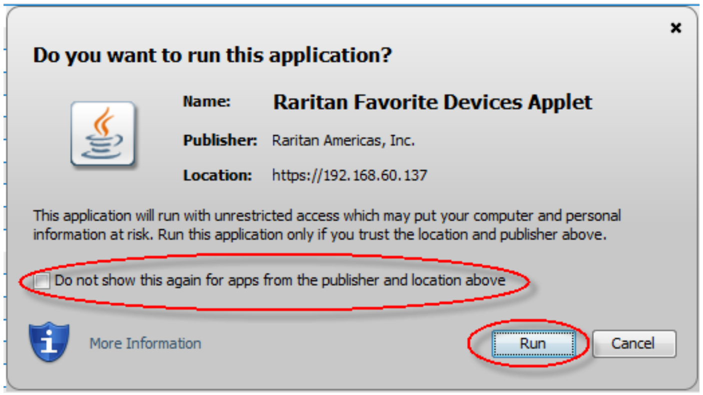
  - Add a new preference "browser.download.skipConfirmLaunchExecutable" to about:config.
- For details, go to https://support.mozilla.org/en-US/questions/1260307

Java Validation and Access Warning

When logging in to LX II using the Java-based client, Java prompts you to validate LX II, and to allow access to the application.

Installing an SSL certificate in each LX II device is recommended to reduce Java warnings, and enhance security.

See ***SSL and TLS Certificates*** (on page 112)



Do you want to run this application?

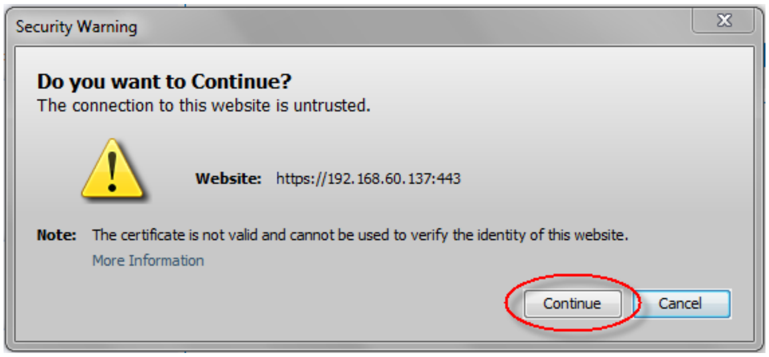
Name: Raritan Favorite Devices Applet

Publisher: Raritan Americas, Inc.

Location: https://192.168.60.137

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

□ Do not show this again for apps from the publisher and location above



Security Warning

Do you want to Continue?
The connection to this website is untrusted.

Website: https://192.168.60.137:443

Note: The certificate is not valid and cannot be used to verify the identity of this website.

Enable Standalone VKC Download Server Certificate Validation

On the Services page select the "Enable Standalone VKC Download Server Certificate Validation" checkbox to use HTTPS for download the VKCs application. JRE will perform a check to ensure the server certificate matches the designated device. If the certification does not match, a security warning message displays to give you the option to continue. Best practice for using VKCs is to select this option, and install a valid certificate on LX II.

When this option is not selected, the VKCs certificate is not validated.

Proxy Server Configuration

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

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

To configure the SOCKS proxy:

1. On the remote client PC, select Control Panel > Internet Options.
    a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.
    b. Select 'Use a proxy server for your LAN'.
    c. Click Advanced. The Proxy Settings dialog opens.
    d. Configure the proxy servers for all protocols.

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

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

    e. Click OK at each dialog to apply the settings.
2. Next, configure the proxy settings for the Java™ applets:
    a. Select Control Panel > Java.
    b. On the General tab, click Network Settings. The Network Settings dialog opens.
    c. Select "Use Proxy Server".
    d. Click Advanced. The Advanced Network Settings dialog opens.
    e. Configure the proxy servers for all protocols.

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

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

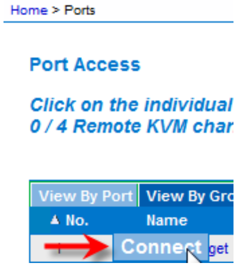
Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC)

Once you have logged on to the LX II Remote Console, access target servers via the Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC).

To connect to an available server:

1. On the Port Access page, click on the port name of the target server you want to connect to. The Port Action menu opens.

2. Click Connect.



Home > Ports

Port Access

Click on the individual
0 / 4 Remote KVM char

See Port Action Menu for details on additional available menu options.

Configuring Connection Properties

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

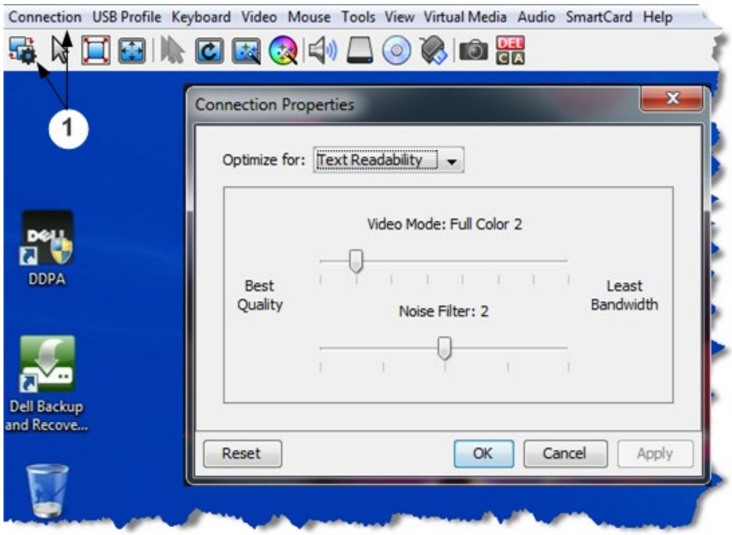
The properties are applied only to your connection - they do not impact the connection of other users accessing the same target servers.

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

Access Connection Properties

▶ **To access connection properties:**

1	Click Connection > Properties, or click the Connection... icon to open the Connection Properties dialog.



Connection Properties

Optimize for: Text Readability

Video Mode: Full Color 2

Noise Filter: 2

Default Connection Property Settings - Optimized for Best Performance

The LX II comes configured to provide optimal performance for the majority of video streaming conditions.

Default connection settings are:

- Optimized for: Text Readability - video modes are designed to maximize text readability.

  This setting is ideal for general IT and computer applications, such as performing server administration.

- Video Mode - defaults to Full Color 2.

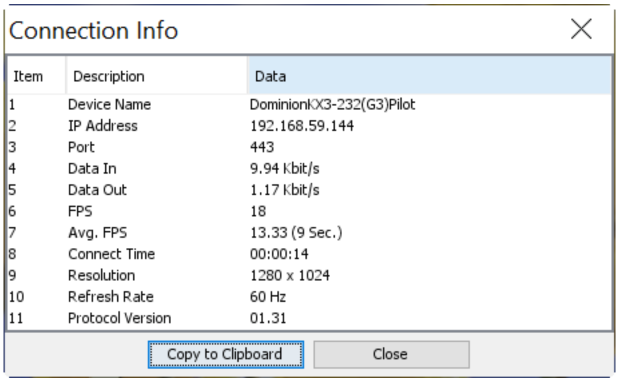
  Video frames transmit in high-quality, 24-bit color. This setting is suitable where a high-speed LAN is used.

- Noise Filter - defaults to 2.

  The noise filter setting does not often need to be changed.

Click Reset on the Connection Properties dialog at any time to return to the default settings.

Tip: Use the Connection Information dialog to monitor the connection in real-time. See **Access and Copy Connection Information** *(on page 190)*



Connection Info

Item	Description	Data
1	Device Name	DominionKX3-232(G3)Pilot
2	IP Address	192.168.59.144
3	Port	443
4	Data In	9.94 Kbit/s
5	Data Out	1.17 Kbit/s
6	FPS	18
7	Avg. FPS	13.33 (9 Sec.)
8	Connect Time	00:00:14
9	Resolution	1280 x 1024
10	Refresh Rate	60 Hz
11	Protocol Version	01.31

Optimize for: Selections

Text Readability

Text Readability is designed to provide video modes with lower color depth but text remains readable. Greyscale modes are even available when applying lower bandwidth settings.

This setting is ideal when working with computer GUIs, such as server administration.

When working in full color video modes, a slight contrast boost is provided, and text is sharper.

In lower quality video modes, bandwidth is decreased at the expense of accuracy.

Color Accuracy

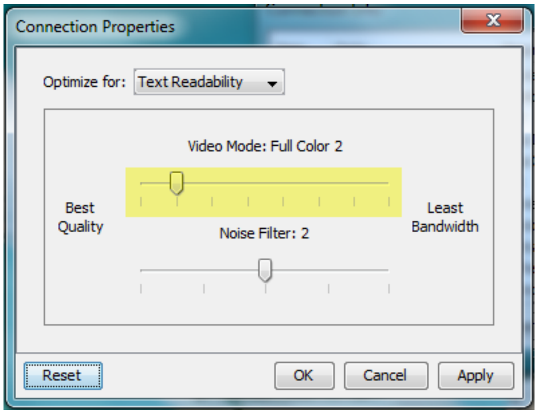
When Color Accuracy is selected, all video modes are rendered in full 24-bit color with more compression artifacts.

This setting applies to viewing video streams such as movies or other broadcast streams.

In lower quality video modes, sharpness of fine detail, such as text, is sacrificed.

Video Mode

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



Optimize for: Text Readability

Video Mode: Full Color 2

Noise Filter: 2

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

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

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

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

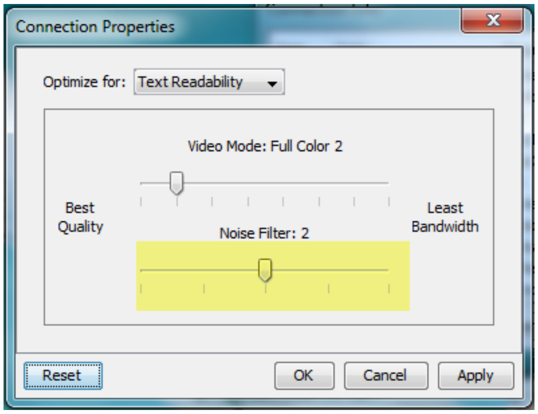
These modes are appropriate for administration work where text and GUI elements take priority, and bandwidth is at a premium.

Click Reset on the Connection Properties dialog at any time to return to the default settings.

Noise Filter

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

The Noise Filter controls how much interframe noise is absorbed by the LX II.



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

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

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

Click Reset on the Connection Properties dialog at any time to return to the default settings.

Connection Information

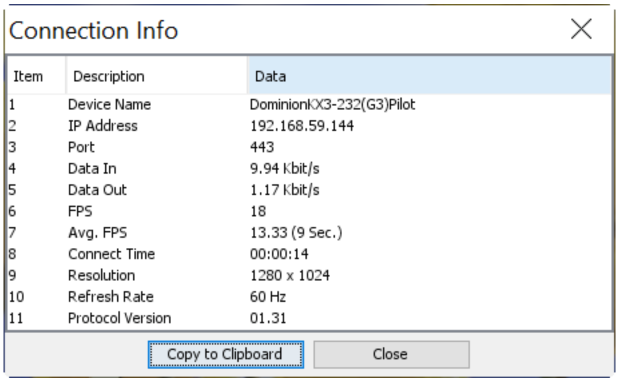
Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See ***Configuring Connection Properties*** (on page 186)

▶ To open connection info:

1. Click Connection > Info.

Note: Clicking Copy to Clipboard copies the information for pasting.



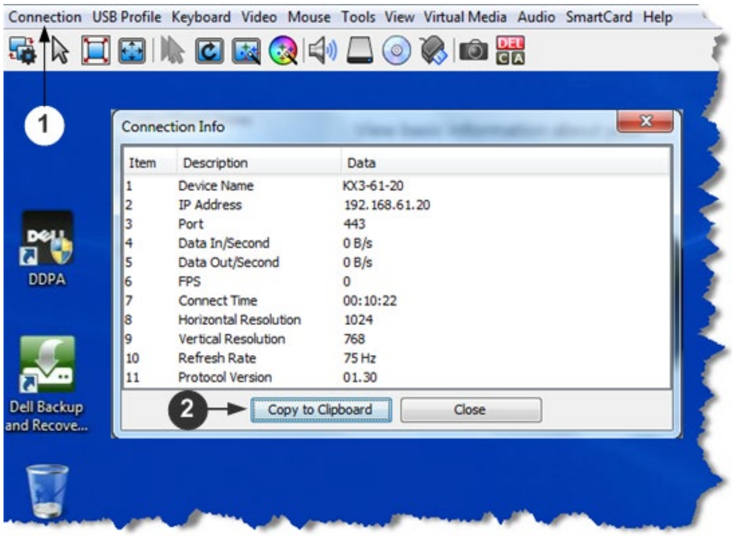
Connection Info

Item	Description	Data
1	Device Name	DominionKX3-232(G3)Pilot
2	IP Address	192.168.59.144
3	Port	443
4	Data In	9.94 Kbit/s
5	Data Out	1.17 Kbit/s
6	FPS	18
7	Avg. FPS	13.33 (9 Sec.)
8	Connect Time	00:00:14
9	Resolution	1280 x 1024
10	Refresh Rate	60 Hz
11	Protocol Version	01.31

Current connection information:

- Name of the LX II
- IP address of the LX II
- Port - The KVM communication TCP/IP port used to access LX II.
- Data In/Second - Data rate received from the LX II
- Data Out/Second - Data rate sent to the LX II.
- Connect Time - The duration of the current connection.
- FPS - Video frames per second transmitted received from the LX II.
- Average FPS - Average video frames per second.
- Resolution - The target server horizontal and vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - Communications protocol version.

Access and Copy Connection Information



Connection Info

Item	Description	Data
1	Device Name	KX3-61-20
2	IP Address	192.168.61.20
3	Port	443
4	Data In/Second	0 B/s
5	Data Out/Second	0 B/s
6	FPS	0
7	Connect Time	00:10:22
8	Horizontal Resolution	1024
9	Vertical Resolution	768
10	Refresh Rate	75 Hz
11	Protocol Version	01.30

Steps	
1	Click Connection > Info... to open the Connection Info dialog.
2	Click Copy to Clipboard. Paste the information as needed.

USB Profiles

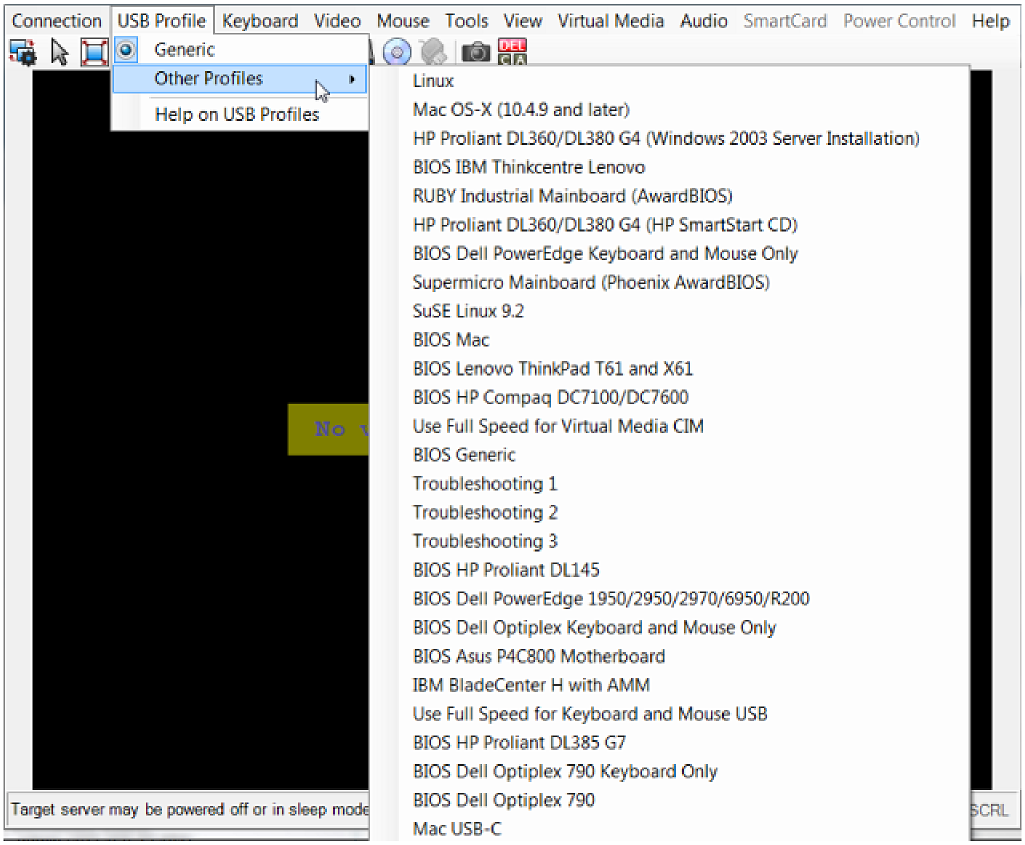
Select a USB profile that best applies to the KVM target server.

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

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

To set a USB profile for a target server:

- Choose USB Profile, then choose Generic, or choose Other Profiles to select from a menu.


Connection
USB Profile
Keyboard
Video
Mouse
Tools
View
Virtual Media
Audio
SmartCard
Power Control
Help
Generic
Other Profiles
Help on USB Profiles
Linux
Mac OS-X (10.4.9 and later)
HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation)
BIOS IBM Thinkcentre Lenovo
RUBY Industrial Mainboard (AwardBIOS)
HP Proliant DL360/DL380 G4 (HP SmartStart CD)
BIOS Dell PowerEdge Keyboard and Mouse Only
Supermicro Mainboard (Phoenix AwardBIOS)
SuSE Linux 9.2
BIOS Mac
BIOS Lenovo ThinkPad T61 and X61
BIOS HP Compaq DC7100/DC7600
Use Full Speed for Virtual Media CIM
BIOS Generic
Troubleshooting 1
Troubleshooting 2
Troubleshooting 3
BIOS HP Proliant DL145
BIOS Dell PowerEdge 1950/2950/2970/6950/R200
BIOS Dell Optiplex Keyboard and Mouse Only
BIOS Asus P4C800 Motherboard
IBM BladeCenter H with AMM
Use Full Speed for Keyboard and Mouse USB
BIOS HP Proliant DL385 G7
BIOS Dell Optiplex 790 Keyboard Only
BIOS Dell Optiplex 790
Mac USB-C
SCRL

Target server may be powered off or in sleep mode

To view details on USB profiles:

- Choose USB Profile > Help on USB Profiles.

Keyboard

Send Ctrl+Alt+Del Macro

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

Selecting Keyboard > Send Ctrl+Alt+Del, or clicking on the Ctrl+Alt+Delete button DEL C A in the toolbar sends this key sequence to the server or to the KVM switch to which you are currently connected.

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

Send LeftAlt+Tab (Switch Between Open Windows on a Target Server)

Select Keyboard > Send LeftAlt + Tab to switch between open windows on the target server.

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.

Send Text to Target

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

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

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

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

Keyboard Macros

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

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

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

Build a New Macro

► **To build a macro:**

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

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

   Press Left Alt

   Press F4

   Esc

   Release F4

   Esc

   Release Left Alt
6. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
   a. To remove a step in the sequence, select it and click Remove.
   b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.
7. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.

8. Click Close to close the Keyboard Macros dialog. The macro now appears on the Keyboard menu in the application.
9. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.

Importing and Exporting Macros

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

Import Macros

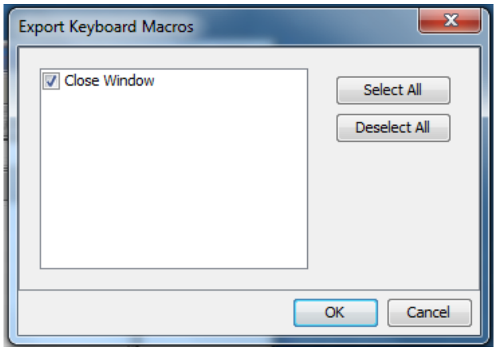
To import macros:

1. Choose Keyboard > Import Keyboard Macros to open the Import Macros dialog. Browse to the folder location of the macro file.
2. Click on the macro file and click Open to import the macro.
   a. If too many macros are found in the file, an error message is displayed and the import terminates once OK is selected.
   b. If the import fails, an error dialog appears and a message regarding why the import failed is displayed. Select OK to continue the import without importing the macros that cannot be imported.
3. Select the macros to be imported by checking their corresponding checkbox or using the Select All or Deselect All options.
4. Click OK to begin the import.
   a. If a duplicate macro is found, the Import Macros dialog appears. Do one of the following:
      - Click Yes to replace the existing macro with the imported version.
      - Click Yes to All to replace the currently selected and any other duplicate macros that are found.
      - Click No to keep the original macro and proceed to the next macro
      - Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are skipped as well.
      - Click Cancel to stop the import.
      - Alternatively, click Rename to rename the macro and import it. If Rename is selected, the Rename Macro dialog appears. Enter a new name for the macro in the field and click OK. The dialog closes and the process proceeds. If the name that is entered is a duplicate of a macro, an alert appears and you are required to enter another name for the macro.
   b. If during the import process the number of allowed, imported macros is exceeded, a dialog appears. Click OK to attempt to continue importing macros or click Cancel to stop the import process.

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

Export Macros

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



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

Video Properties

Refreshing the Screen

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

- 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: When color is successfully calibrated, the values are cached and reused each time you switch to the target. Changes to the brightness and contrast in Video Settings are not cached. Changing resolution resets the video to the cached values again. You can clear the cached values in Video > Clear Video Settings Cache. See **Clear Video Settings Cache** *(on page 196).*

▶ **To calibrate the color:**

- Choose Video > Calibrate Color, or click the Calibrate Color button in the toolbar.

  The target device screen updates its color calibration.

Clear Video Settings Cache

You can clear the video settings cache to delete old settings that do not apply anymore, such as when a target server is replaced. When you clear the video settings cache, the server automatically does a video auto-sense and color calibration. The new values are cached and reused when the target is accessed again.

▶ **To clear the video settings cache:**

- Choose Video > Clear Video Settings Cache in the toolbar.

Adjusting Video Settings

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

▶ **To change the video settings:**

1. Choose Video > Video Settings to open the Video Settings dialog.

2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:

   a. 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.

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

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

      Brightness Green - Controls the brightness of the green signal.

      Brightness Blue - Controls the brightness of the blue signal.

   c. Contrast Red - Controls the red signal contrast.

      Contrast Green - Controls the green signal.

      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 Technical Support before making any changes.

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

   e. 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

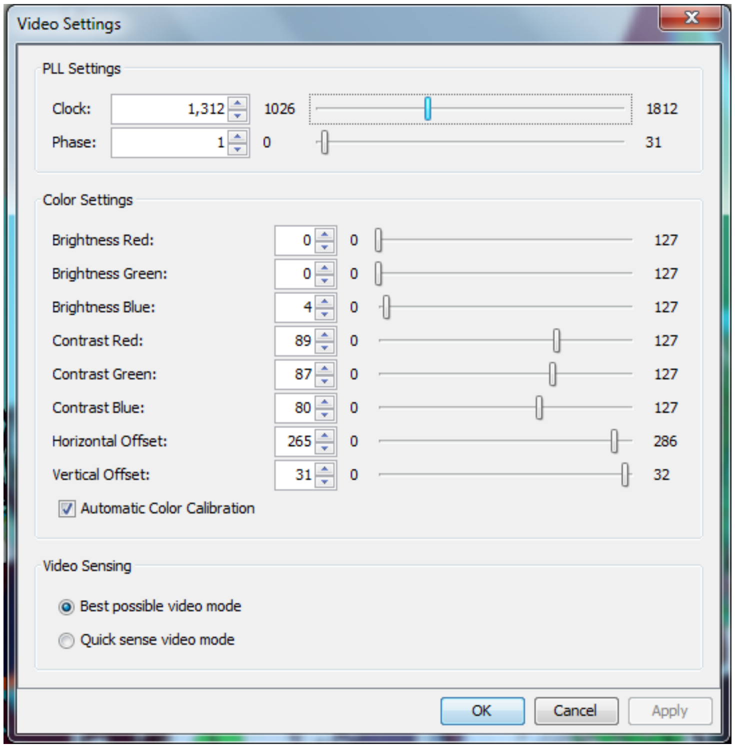
     The device will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.

   - 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.



Video Settings

PLL Settings

Clock:	1,312	1026	1812
Phase:	1	0	31

Color Settings

Brightness Red:	0	0	127
Brightness Green:	0	0	127
Brightness Blue:	4	0	127
Contrast Red:	89	0	127
Contrast Green:	87	0	127
Contrast Blue:	80	0	127
Horizontal Offset:	265	0	286
Vertical Offset:	31	0	32

☑ Automatic Color Calibration

Video Sensing

● Best possible video mode

○ Quick sense video mode

Screenshot from Target Command (Target Screenshot)

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

▶ To take a screenshot of the target server:

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

Mouse Options

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

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

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

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

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

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when other modes don't work.

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

Dual Mouse Modes

Absolute Mouse Synchronization

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

- Absolute Mouse Synchronization requires the use of a virtual media CIM - D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP, D2CIM-VUSB-USBC

To enter Absolute Mouse Synchronization:

- Choose Mouse > Absolute from the KVM client.

The black USB connector on the DVUSB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media.

For CIMs with two USB plugs, keep both connected to the device.

The device may not operate properly if both plugs are not connected to the target server.

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.

Enter Intelligent Mouse Mode

To enter intelligent mouse mode:

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

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

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

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

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

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

Standard Mouse Mode

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

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

▶ To enter Standard Mouse mode:

- Choose Mouse > Standard.

Mouse Synchronization Tips

If you have an issue with mouse synchronization:

1. Verify that the selected video resolution and refresh rate are among those supported by the device. The KVM Client Connection Info dialog displays the actual values that the device is seeing.
2. Force an auto-sense by clicking the KVM Client auto-sense button.
3. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
    a. Open a terminal window.
    b. Enter the following command: `xset mouse 1 1`
    c. Close the terminal window.
4. Click the "KVM Client mouse synchronization" button.

Synchronize Your Mouse

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

▶ To synchronize the mouse cursors, do one of the following:

- Click the Synchronize Mouse button in the KVM client toolbar, or select Mouse > Synchronize Mouse from the menu bar.

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

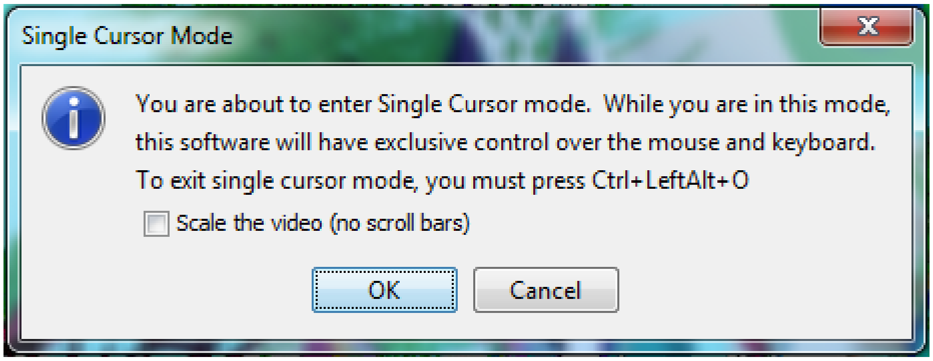
Single Mouse Mode

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

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

To enter single mouse mode, do one the following:

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



Single Cursor Mode

You are about to enter Single Cursor mode. While you are in this mode, this software will have exclusive control over the mouse and keyboard. To exit single cursor mode, you must press Ctrl+LeftAlt+O

□ Scale the video (no scroll bars)

To exit single mouse mode:

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

Tool Options

General Settings

To set the tools options:

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

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

   The options include:

   - US/International
   - French (France)
   - German (Germany)
   - Japanese
   - United Kingdom
   - Korean (Korea)

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

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

4. Configure hotkeys:
   - Toggle Full Screen Mode - Hotkey.

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

     This is the hot key used for toggling in and out of this mode.
   - Toggle Single Cursor Mode - Hotkey.

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

     This is the hot key used to toggle in and out of single cursor mode, removing and bringing back the client mouse cursor.
   - Toggle Scaling Mode - Hotkey.

     When you enter scaling mode, the target server scales to fit your display.

     This is the hot key used to toggle in and out of scaling mode.
   - Disconnect from Target - Hotkey.

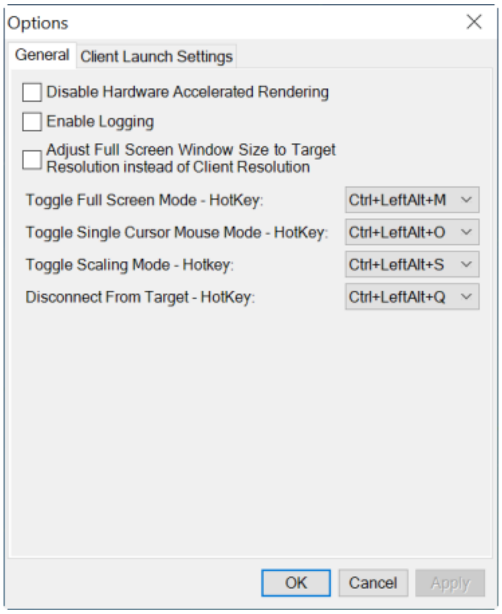
     Enable this hotkey to allow users to quickly disconnect from the target.

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

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

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

5. Click OK.



□ Disable Hardware Accelerated Rendering

□ Enable Logging

□ Adjust Full Screen Window Size to Target Resolution instead of Client Resolution

Toggle Full Screen Mode - HotKey: Ctrl+LeftAlt+M

Toggle Single Cursor Mouse Mode - HotKey: Ctrl+LeftAlt+O

Toggle Scaling Mode - Hotkey: Ctrl+LeftAlt+S

Disconnect From Target - HotKey: Ctrl+LeftAlt+Q

Keyboard Limitations

Turkish Keyboards

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

Slovenian Keyboards

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

Language Configuration on Linux

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

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

Language	Configuration method
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.

Configuring Port Scan Settings in VKC/VKCS and AKC

Configuring port scan options in VKC/VKCS and AKC applies to scanning from the Remote Console.

To configure port scan options for the Local Console, see ***Configure Local Console Scan Settings*** (on page 246)

Use the port scanning feature to search for selected targets, and display them in a slide show view, allowing you to monitor up to 32 targets at one time.

You can connect to targets or focus on a specific target as needed. Scans can include standard targets, blade servers, tiered devices, and KVM switch ports.

Configure scan settings from either the VKC/VKCS or AKC.

See ***Scanning Ports - Remote Console*** (on page 232)

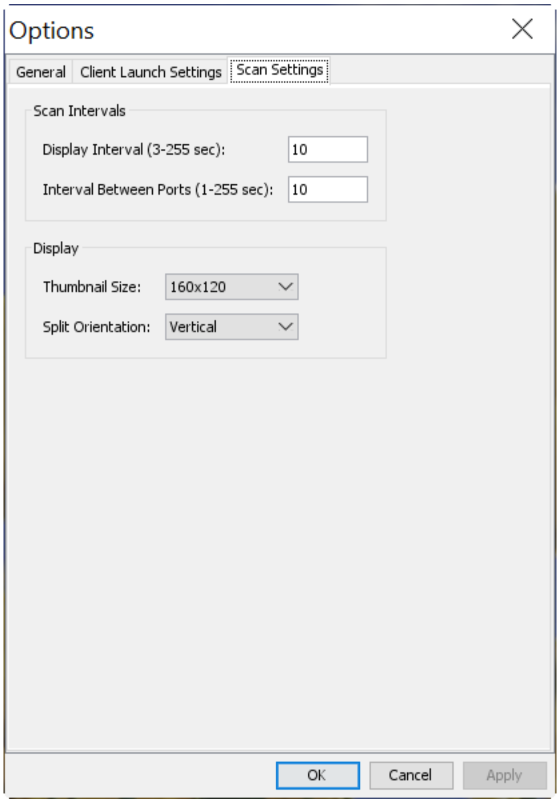
Use the Scan Settings tab to customize the scan interval and default display options.

Configure Port Scan

▶ **To set scan settings:**

1. Click Tools > Options. The Options dialog appears.
2. Select the Scan Settings tab.
3. In the "Display Interval" 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" 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.



Scan Intervals

Display Interval (3-255 sec): 10

Interval Between Ports (1-255 sec): 10

Display

Thumbnail Size: 160x120

Split Orientation: Vertical

Collecting a Diagnostic Snapshot of the Target

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

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

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

The following files are included in the zip file:

- screenshot_image.png

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

- raw_video_image.png:

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

- raw_video_ycbcr420.bin:

  Binary file of the raw snapshot.

- raw_video_ycbcr420.txt:

  Text file containing data used to help diagnose issues.

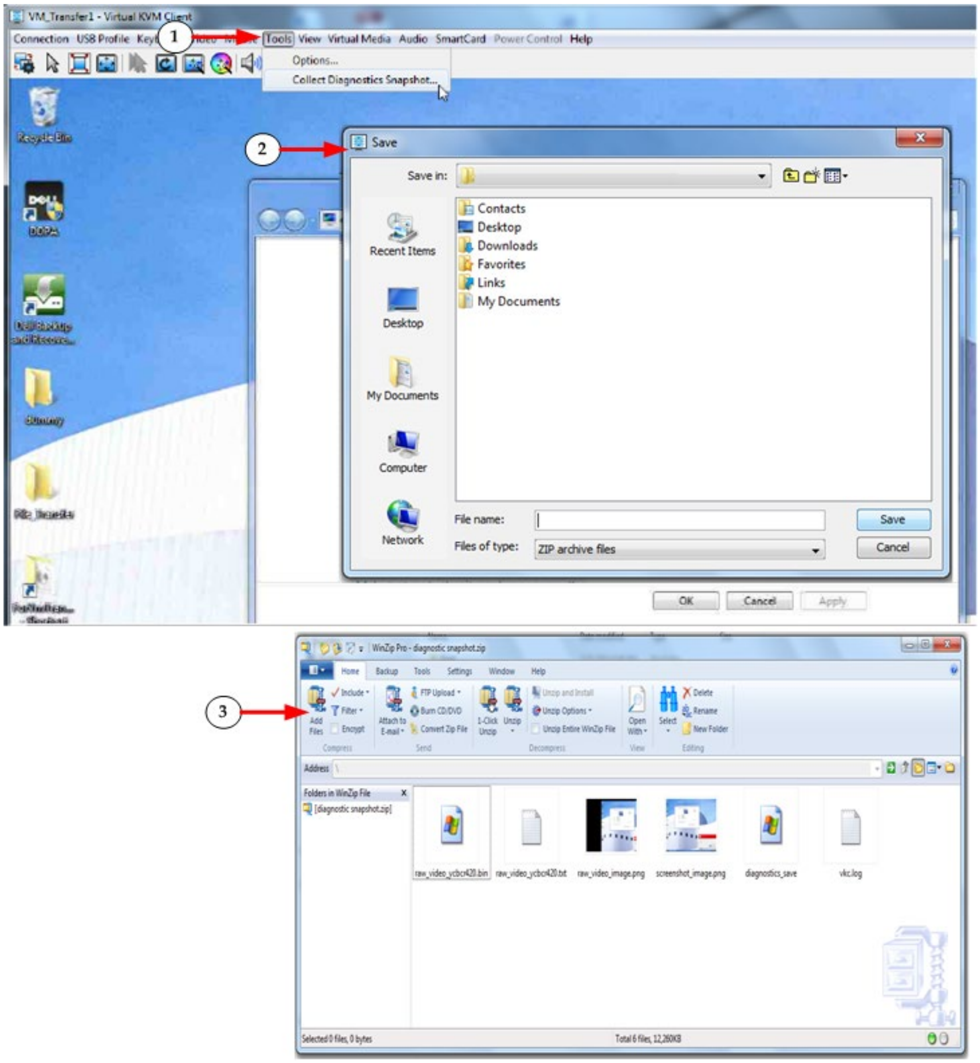
- Log.txt file:

  These are the client logs.

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

Collect a Diagnostic Snapshot

▶ To capture a diagnostic snapshot:



Files of type: ZIP archive files

Steps	
	Access a target, and then click Tools > Collect a Diagnostic Snapshot. Several messages are displayed as the information is collected.
	You are prompted to save the zip file containing the diagnostic files.
	The zip file containing the diagnostic files is saved.

View Options

View Toolbar

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

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

- Choose View > View Toolbar.

View Status Bar

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

▶ **To hide the status bar:**

- Click View > Status Bar to deselect it.

▶ **To restore the status bar:**

- Click View > Status Bar to select it.

Scaling

Scaling your target window allows you to view the entire contents of the target server window.

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

▶ **To toggle scaling (on and off):**

- Choose View > Scaling.

Full Screen Mode

When you enter Full Screen mode, the target's full screen is displayed and acquires the same resolution as the target server.

The hot key used for exiting this mode is specified in the Options dialog, see ***Tool Options*** (on page 202).

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

If you want the menu bar to remain visible while in Full Screen mode, enable the Pin Menu Toolbar option from the Tool Options dialog. See ***Tool Options*** (on page 202).

▶ To enter full screen mode:

- Choose View > Full Screen, or click the Full Screen button ⛶.

▶ To exit full screen mode:

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

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

▶ To set Full Screen mode as the default mode:

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

Connect to Virtual Media

See ***Virtual Media*** (on page 139)

Proxy Server Configuration

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

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

▶ To configure the SOCKS proxy:

1. On the remote client PC, select Control Panel > Internet Options.
   a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.
   b. Select 'Use a proxy server for your LAN'.
   c. Click Advanced. The Proxy Settings dialog opens.
   d. Configure the proxy servers for all protocols.

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

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

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

2. Next, configure the proxy settings for the Java™ applets:

a. Select Control Panel > Java.

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

c. Select "Use Proxy Server".

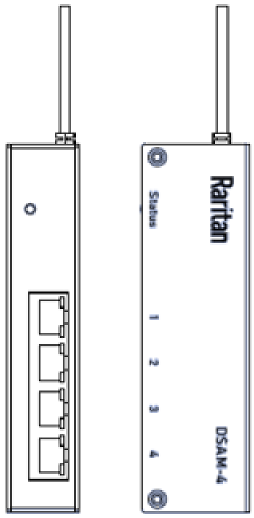
d. Click Advanced. The Advanced Network Settings dialog opens.

e. Configure the proxy servers for all protocols.

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

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

Chapter 10 Serial Access With Dominion Serial Access Module



Connecting a LX II and a Dominion Serial Access Module (DSAM) provides access to devices such as LAN switches and routers that have a RS-232 serial port.

The DSAM is a 2- or 4 port serial module that derives power from the LX II.

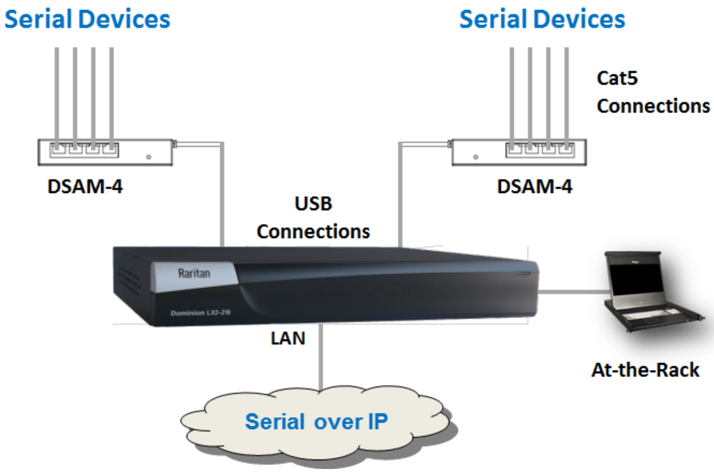
Connect a maximum of 2 DSAM modules to the LX II using USB cables. DSAM can be mounted in a 0U configuration.

In This Chapter

Only 1 DSAM unit can be connected to integrated switch/LED drawer models.

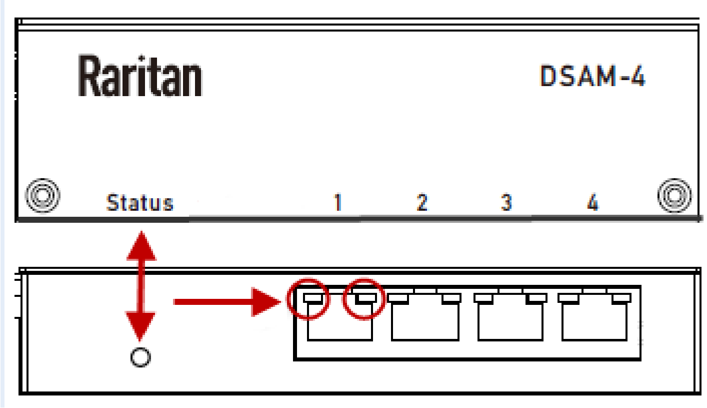
Connect DSAM

1. Connect the DSAM unit's USB cable to the **TOP USB port on the rear of LX II device.** Addtional DSAM units can be added at any other USB port.
2. Connect the serial devices to the serial ports on the DSAM unit.



DSAM LED Operation

The DSAM unit has one LED for status, and 2 LEDs on each port.



▶ Status LED:

The Status LED is labeled on the unit front. Light is on back. The Status LED gives information at bootup and upgrade.

- Green LED - Slow blink: DSAM booting up but not controlled by LX II.
- Blue LED - Slow blink: DSAM controlled by LX II.
- Blue LED - Fast blink: Firmware upgrade in progress.

▶ USB Port LEDs:

Each USB port has a left Green LED and a right Yellow LED.

- Green LED: Port is set as DCE
- Yellow LED: Port is set as DTE
- LEDs off: Port is set as AUTO

Supported USB Device Combinations

Each USB device draws from a fixed pool of USB resources. There are limits on the number of USB devices that can be connected to the LX II at the same time.

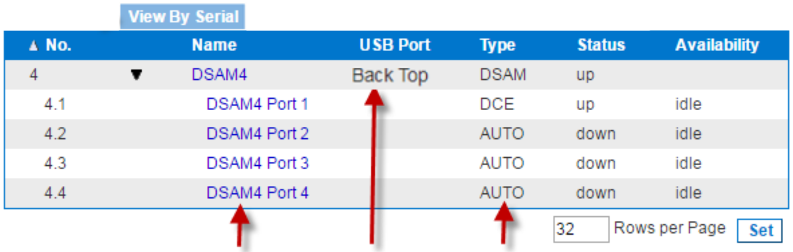
The following device combinations are supported for all LX II hardware versions.

If you have the latest 2020-released LX II hardware, which have a hardware revision number beginning with A or higher, the USB-combination in the last column is supported. Older hardware revision numbers begin with 0-9. To check your hardware version: Go to Maintenance > Device Information > Hardware Revision number.

Device	C1	C2	C3	C4	C5
4-Port DSAM	X			X	
4-Port DSAM	X	X	X		
2-Port DSAM		X	X		X
2-Port DSAM					
Keyboard and Mouse		X		X	X
Wireless Modem			X	X	X
DSAM Ports	8	6	6	4	2

View DSAM Serial Ports

When a DSAM unit is connected to the LX II, a new tab is available in the Ports page. The View by Serial tab shows all connected serial ports.



View By Serial

▲ No.		Name	USB Port	Type	Status	Availability
4	▼	DSAM4	Back Top	DSAM	up	
4.1		DSAM4 Port 1		DCE	up	idle
4.2		DSAM4 Port 2		AUTO	down	idle
4.3		DSAM4 Port 3		AUTO	down	idle
4.4		DSAM4 Port 4		AUTO	down	idle

32 Rows per Page Set

To view DSAM serial ports:

In the Port Access page, click the View By Serial tab.

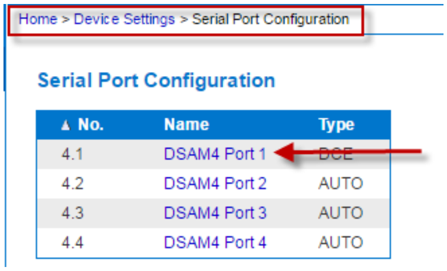
- Ports are listed by physical USB position on the DSAM unit.
- USB Port column indicates which LX II USB port DSAM is plugged into.
- Type column indicates port's DTE/DCE setting.

Configure DSAM Serial Ports

The serial port configuration options are available when a DSAM unit is connected.

To configure DSAM serial ports:

1. Choose Device Settings > Serial Port Configuration.
2. Click the Port Name for the port you want to configure.

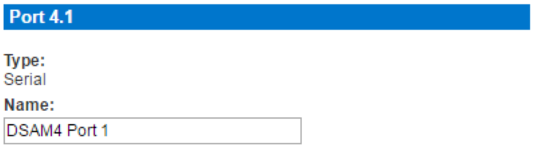


Home > Device Settings > Serial Port Configuration

Serial Port Configuration

▲ No.	Name	Type
4.1	DSAM4 Port 1	DCE
4.2	DSAM4 Port 2	AUTO
4.3	DSAM4 Port 3	AUTO
4.4	DSAM4 Port 4	AUTO

3. The Port Type is set to Serial only.
4. Enter a meaningful name for the serial target or leave the default name.



Port 4.1

Type:
Serial

Name:
DSAM4 Port 1

Serial Port Settings

Configure the remaining port settings.

1. Select the terminal emulation type from the drop-down menu in the Emulation field. This is the terminal emulation mode used to match the serial targets connected to the ports.
   - VT100
   - VT220
   - VT320
   - ANSI
2. Set Encoding if you want to always use a specific character encoding for this port. Encoding overrides the global setting for the port to whatever value you set.
   - DEFAULT
   - US-ASCII
   - ISO8859-1
   - ISO8859-15
   - UTF-8
   - Shift-JIS
   - EUC-JP
   - EUC-CN
   - EUC-KR
3. In the Equipment Type field, indicate whether you want the LX II to automatically detect a physical connection to the target. The default is Auto Detection.

   Force DTE causes LX II to act as a piece of data terminal detection equipment to detect targets connected to it.

   Force DCE causes LX II to act as a piece of data communications equipment to detect equipment connected to it.

   Note: If the target has the ability to autodetect either DTE or DCE, you must select either Force DTE or Force DCE for the port. LX II does not support autodetection of both DCE and DTE on the same port.
4. Select the value of Bits Per Second (BPS) from the BPS drop-down menu.
   - BPS options: 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
5. Select the Parity/Bits from the Parity Bits drop-down menu.
6. Select the Flow Control from the Flow Control drop-down menu.
7. Select the Stop Bits from the Stop Bits drop-down menu.
8. If you need to configure the delay between when individual characters are sent via the port, enter the time in milliseconds in the Char Delay field.

9. To configure the delay between when lines of text are sent via the port, enter it in the Line Delay field.
10. Configure the sendbreak duration by entering the send break time in the Send Break Duration field. The send break is configurable from 0ms - 1000ms.
11. Select an option to allow single or multiple writers on a port at one time in the Multiple Writers field.
12. Select Always Active if you want to log activities coming into a port even if no user is connected.

    The default option is to not maintain port access without a connected user, which means ignore data coming into a port when no user is connected.

    This option is for port data logs.

    Note: When no users are logged into a port session, port traffic, by default, is discarded .
13. If you do not want messages displayed to users connecting to LX II via Direct Port Access, select the Suppress Message checkbox.
14. Select the Escape Mode.

    The escape sequence affects only the CLI. When entering the escape mode, the user is given a menu of commands that can be performed (for example, gethistory, power commands, and so on), a command to return to the port session, and a command to exit the port connection.

    The default is None.

    Change as follows:

    - Select control from the drop-down menu in the Escape Mode field.
15. Type the character in the Escape Character field. The default for the LX II is] (closed bracket).

    Raritan recommends that you do not use [or Ctrl-[. Either of these may cause unintended commands, such as invoking the Escape Command unintentionally. This key sequence is also triggered by the arrow keys on the keyboard.
16. Type a command in the Exit Command field, such as `logout`.

    This is the command that is sent to your system when a user with write permission disconnects from the port.

    The main function of this command is to ensure that the user's session on the target machine is closed; however, it is not imperative to have an Exit command configured on a port.
17. Click OK.

Apply Settings to Other Ports

Once finished, you can apply the same port settings to other ports.

1. Select the ports from the Apply Serial Port Settings To Other Ports section of the page.

2. Click OK to apply the port configuration settings.

Configure Serial Port Keyword List

Port keywords work as a filter. You can create port keywords and associate them with -

- Events
- Local/remote syslog messages
- SNMP traps

If a keyword is detected -

- A corresponding message is logged in a local/NFS port log.
- A corresponding trap is sent via SNMP (if configured).

This feature is useful for notifying administrators if a particular event occurs on a port. Using port keywords to report events does not impact the NFS log size.

For keywords to trigger when no users are connected to a port, "Always Active" must be selected on the port's Port Configuration page.

A list of existing port keywords is displayed on the Port Configuration page as well.

To configure serial port keywords:

1. Choose Device Settings > Serial Port Keywords. The Serial Port Keyword List page opens.
2. Click Add at the bottom of list on the page. The Keyword page opens.
3. Type a keyword in the Keyword field.
4. Select the Port(s) you want to associate with that keyword.
5. Click Add to add them to the Selected box.

Click OK.

Upgrade DSAM Firmware

DSAM firmware is upgraded automatically during LX II device firmware upgrades if a new DSAM version is detected in the device firmware. You can also upgrade your DSAM firmware manually.

To upgrade the DSAM firmware manually:

1. Choose Maintenance > DSAM Firmware Upgrade.
2. Select the checkboxes for the DSAM units you want to upgrade to the Upgrade DSAM Version listed.
3. Click Upgrade, then click OK to confirm. A progress message appears.
4. When firmware upgrade completes, a success message appears.

Supported CLI Commands

Port Connect Commands

Connect to a serial port using port number or port name. Use double quotes around port names that contain space symbols. For example: "DSAM Port 1".

```
admin > connect <port number>
```

admin > connect <port name>

Port number example:

```
admin > connect 1.1
```

Port name example:

```
admin > connect "DSAM Port 1"
```

Port Sub-Menu Commands

The port sub-menu can be reached using the escape key sequence.

Clear history buffer for this port.

```
admin > [portname] > clearhistory
```

Close this target connection. When a target is disconnected, the appropriate disconnect message appears.

```
admin > [portname] > close, quit, q
```

Display the history buffer for this port.

```
admin > [portname] > gethistory
```

Get write access for the port.

```
admin > [portname] > getwrite
```

Return to the target session.

```
admin > [portname] > return
```

Send a break to the connected target.

```
admin > [portname] > sendbreak
```

Lock write access to this port.

```
admin > [portname] > writelock
```

Unlock write access to this port.

```
admin > [portname] > writeunlock
```

Display all users on the port.

```
admin > [portname] > clientlist
```

Display overview of commands

```
admin > [portname] > help
```

Display the current session's command line history

```
admin > [portname] > history
```

Close this target connection.

```
admin > [portname] > quit
```

Reset port

```
admin > [portname] > resetport
```

Configure Ports Commands

Enter `admin >` to access the menu.

Command	Description	Parameters
`listports`	List accessible ports	NA

Enter `admin > config > port` to access the menu.

Command	Description	Parameters
`keywordlist`	Display all configured keywords.	NA
keywordadd	Add a keyword to the port.	▪ port <number | range | *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) ▪ keyword <value> - When keyword is detected on target, notification is sent.
`keyworddelete`	Delete an existing keyword from the port.	▪ port <number | range | *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) ▪ keyword <value> - When keyword is detected on target, notification is sent.

Command	Description	Parameters
`config port`		■ port <number | range | *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) ■ name <port name> - Port name ■ bps <1200 | 1800 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 | 230400> - Port speed in bits-per-second ■ parity <none|even|odd> - Port parity type ■ flowcontrol <none|hw|sw> - Port flowcontrol type hw = hardware flow control sw =X on/X off) ■ eqtype <auto|dte|dce> - Equipment type (auto=>AUTO Detection, dte=>Force DTE, dce=>Force DCE) ■ Note: If the target has the ability to autodetect either DTE or DCE, you must select either Force DTE or Force DCE for the port. LX II does not support autodetection of both DCE and DTE on the same port. ■ escapemode <none|control> - Use Ctrl-key (escapemode=control) or single key (escapemode=none) as escape sequence; for example, Ctrl- => escapemode=control, escapechar= escapechar char-Escape character ■ Raritan recommends that you do not use or Ctrl- as the Escape command. Either of these may cause unintended commands, such as opening a menu, instead of invoking the Escape Command. ■ emulation <vt100 | vt220 | vt320 | ansi> - Target Emulation type ■ sendbreak <duration> - Duration of the sendbreak signal in milliseconds. ■ exitstring <cmd #delay; > - Execute exit string when port session closes, for example, config port 1 exitstring logout (execute logout on exit) config port 1 exitstring #0 (disable exit string for the port). The delay is the amount of time to wait after writing the command to the target. Number in seconds up to 60. ■ alwaysactive <true | false> - Determine whether data coming into a port is logged, for example, config port 1 alwaysactive true (always log activities coming into a port even if

Command	Description	Parameters
		no user is connected) config port 1 alwaysactive false (ignore data coming into a port when no user is connected) ▪ suppress - Determine whether none or all messages should be displayed during a DPA connection, such as "Authentication successful" ▪ encoding - Target Encoding type (DEFAULT|US-ASCII|ISO-8859-1|ISO-8859-15|UTF-8|Shift-JIS|EUC-JP|EUC-CN|EUC-KR) ▪ multiwrite - Port set in Multiple Writer Mode. ▪ chardelay delay - Delay inserted between writing characters (0-9999ms) ▪ linedelay delay - Delay inserted between writing lines (0-9999ms) ▪ stopbits - Number of bits used to signal the end of a character (usually 1) (1/2) ▪ stopbits <1/2> -Number of bits used to signal the end of a character ▪ chardelay - Delay inserted between characters (0-9999) in ms ▪ linedelay - Delay inserted between lines (0-9999) in ms ▪ escapechar - Escape character ▪ encoding - <DEFAULT/US-ASCII/ISO-8859-1/ISO-8859-15/UTF-8/Shift-JIS/EUC-JP/EUC-CN/EUC-KR> - Target encoding type ▪ multiwrite <true/false> - Port set in multiple writer mode ▪ suppress <true/false> - Suppress SX messages when connecting to this target(true/false) ▪ sendbreak - Duration of sendbreak signal in ms

Command Line Interface 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 on your keyboard to execute the command.
- Press Tab on your keyboard to complete a command. Tab also completes parameters and values (if the value is part of an enumerated set).

Command Line Interface High-Level Commands

The CLI is menu based. Some commands move to a menu with a different command set.

The following common commands can be used at all levels of the command line interface (CLI):

- `top` – Return to the top level of the CLI hierarchy, or the `username` prompt.
- `history` – Displays the last 200 commands the user entered into the LX II CLI.
- `logout` – Logs the user out of the current session.
- `quit` – Moves the user back one level in the CLI hierarchy.
- `help` - Displays an overview of the CLI syntax.

Supported Escape Key Characters

The default escape key is CTRL]

The following characters are supported for customized escape keys.

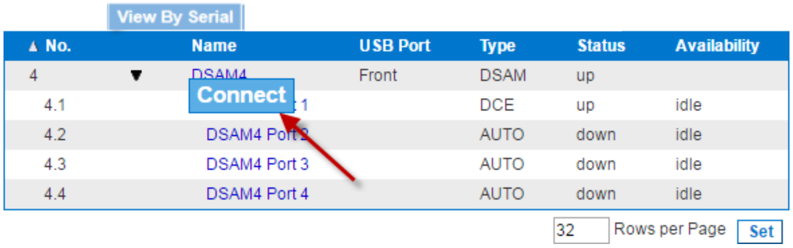
- A-Z
- a-z
- [ ]
- { }
- ^
- _
- \
- |

Connect to DSAM Serial Targets in Port Access Page

To connect to DSAM serial targets:

1. In the Port Access page, click the View By Serial tab to view the serial targets.

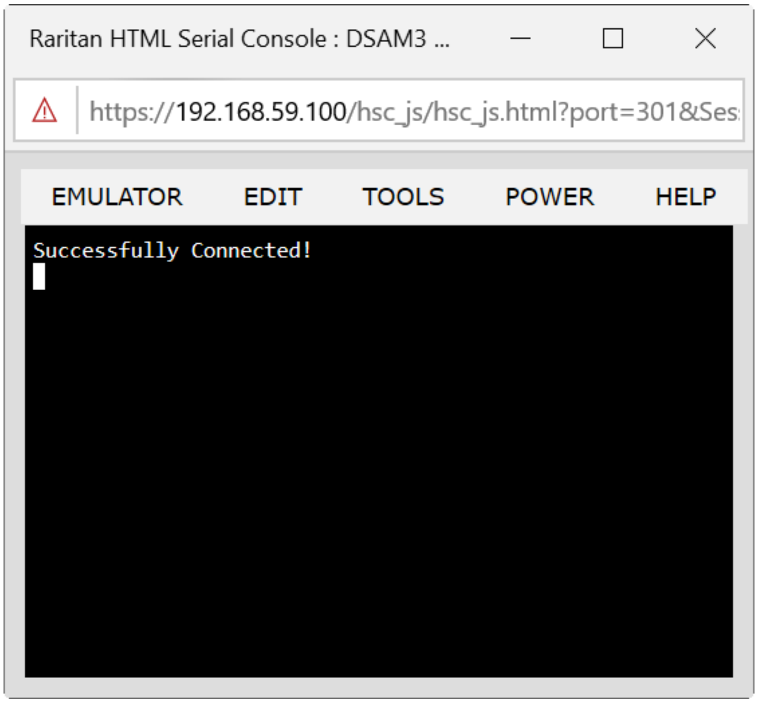
2. Click the port name you want to connect to. Click Connect.



▲ No.		Name	USB Port	Type	Status	Availability
4	▼	DSAM4	Front	DSAM	up	
4.1		1		DCE	up	idle
4.2		DSAM4 Port 2		AUTO	down	idle
4.3		DSAM4 Port 3		AUTO	down	idle
4.4		DSAM4 Port 4		AUTO	down	idle

32 Rows per Page Set

3. The HTML Serial Console (HSC) window opens. See ***HTML Serial Console (HSC) Help*** (on page 225)


Raritan HTML Serial Console : DSAM3 ...
https://192.168.59.100/hsc_js/hsc_js.html?port=301&Ses
EMULATOR
EDIT
TOOLS
POWER
HELP

```
Successfully Connected!
█
```

4. To exit the serial port, hit the hot-key. Default hot key is Scrolllock-Scrollock.

Connect to DSAM Serial Target with URL Direct Port Access

1. Choose Device Settings > Device Services, then select the Enable Direct Port Access via URL checkbox.
2. To connect with direct port access, type the URL:

   "https://IP Address>/dpa.asp?port=<serial port number>&username=<user name>&password=<password>"

   Example: https://192.168.51.101/dpa.asp?port=4.1&username=admin&password=raritan0

3. HTML Serial Client (HSC) launches and connects to the serial target.

Connect to DSAM Serial Target via SSH

1. Choose Device Settings > Device Services, then select the Enable SSH checkkbox.
2. Launch SSH client in client PC to connect to LX II.
3. After login, user will enter CLI interface.
4. Type command "connect <serial port number>", or type command "connect <name of serial port>".

Example-1: connect 4.1

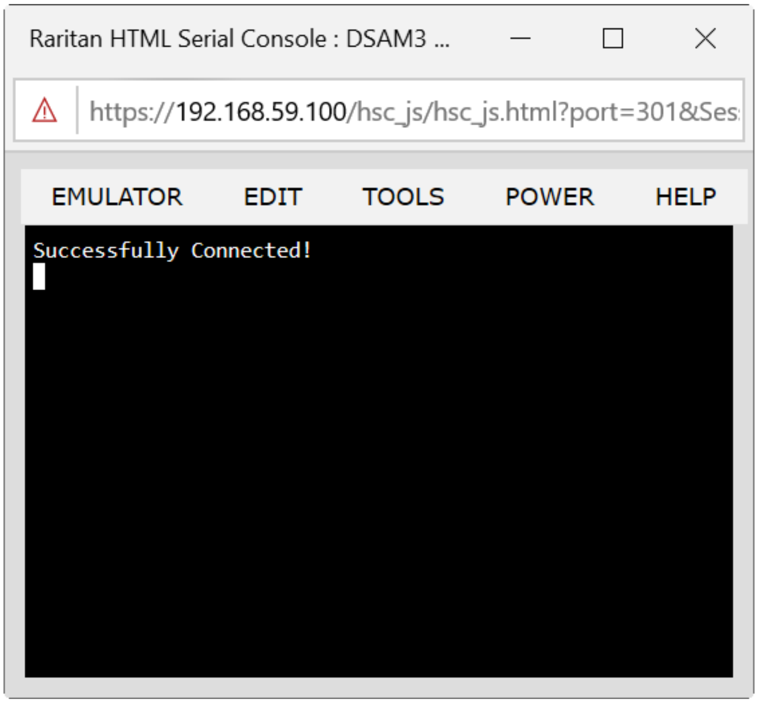
Example-2: connect "DSAM4 Port1"

5. If successful, serial target is accessed.
6. To exit serial target, type escape-key-sequence, default is Ctrl-], then enter port sub-menu CLI interface.
7. Type "quit", then enter main CLI interface.

HTML Serial Console (HSC) Help

Use HSC to connect to serial targets.

Note: You can also access targets via Direct Port Access, command line interface (CLI), local port GUI, and SSH.


Raritan HTML Serial Console : DSAM3 ...
https://192.168.59.100/hsc_js/hsc_js.html?port=301&Ses
EMULATOR
EDIT
TOOLS
POWER
HELP

```
Successfully Connected!
```

HSC Functions

Emulator

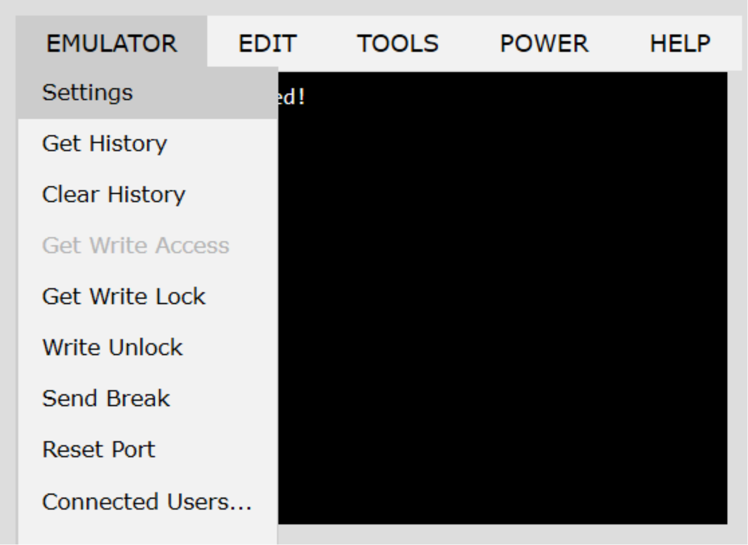
IMPORTANT: HSC sessions are affected by the LX II Idle Timeout.

If you have not changed the LX II Idle Timeout setting from the default, your session could be closed automatically if it exceeds the Idle Timeout period.

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

Access Emulator Options

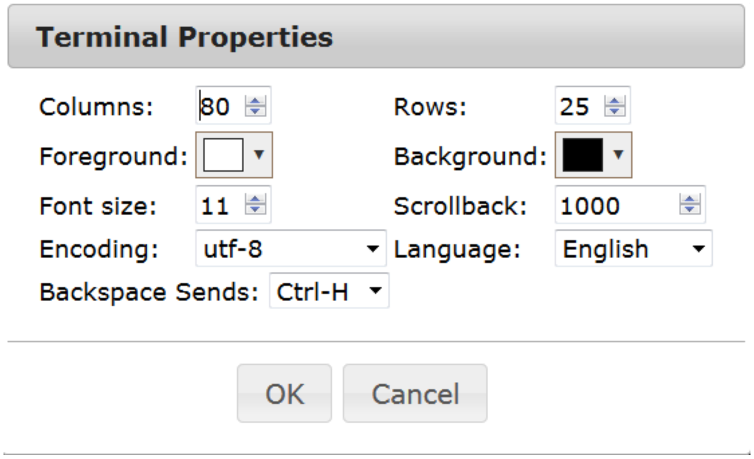
1. Select the Emulator drop-down menu to display a list of options.



Settings

Note: An Administrator can set Terminal emulation settings using Setup > Port Configuration.

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



Terminal Properties

Columns: 80 Rows: 25

Foreground: □ Background: ■

Font size: 11 Scrollback: 1000

Encoding: utf-8 Language: English

Backspace Sends: Ctrl-H

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

Get History

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

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

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

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

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

Clear History

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

Get Write Access

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

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

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

Get Write Lock

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

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

Write Unlock

To get Write Unlock, choose Emulator > Write Unlock.

Send Break

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

Only users with Write Access privileges can send a break.

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

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

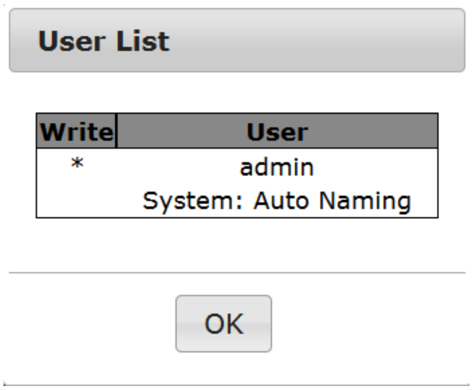
Reset Port

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

Connected Users

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

1. Choose Emulator > Connected Users.



Write	User
*	admin
	System: Auto Naming

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

Exit

1. Choose Emulator > Exit to close the HSC.

Copy and Paste and Copy All

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

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

If you need to paste a large amount of data, it is better to save the data in a file and use the Send a Text File function. Pasting a large amount of data in a browser windows can cause the browser to hang as it processes the data. See ***Send Text File*** (on page 230).

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

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

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

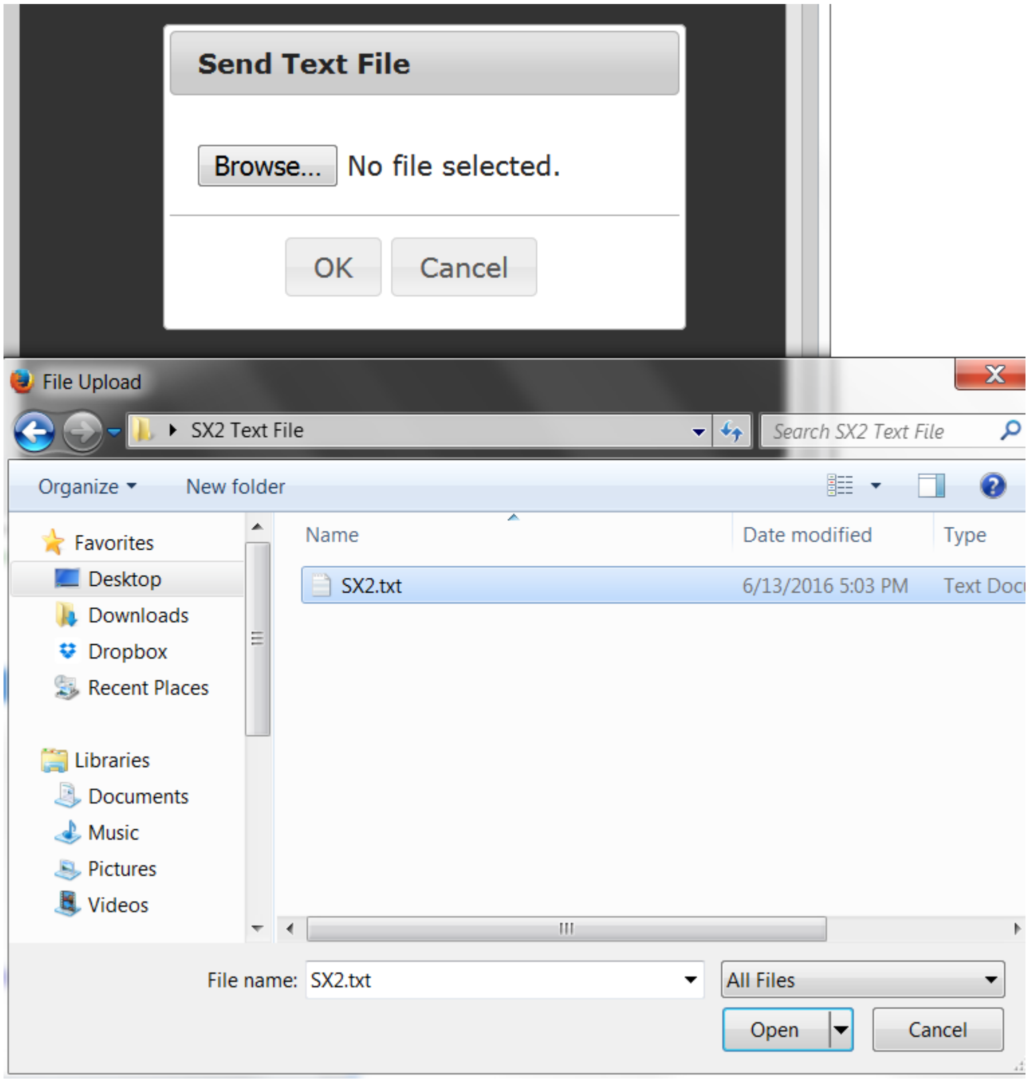
▶ Browser-specific behaviors

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

Send Text File

1. Select Edit> Send Text File.
2. In the Send Text File dialog, click Browse to find the text file.
3. Click OK.
   - When you click OK, the selected file sends directly to the port.

- If there is currently no target connected, nothing is visible on the screen.



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

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

Chapter 11 LX II Remote Console

In This Chapter

Overview

When you log in to the LX II using a network connection, you access the Remote Console. The first page accessed is the Port Access page.

See ***Logging In to LX II*** (on page 30) and Port Access Page (Remote Console Display)

Use the Remote Console to access and scan target servers, manage favorites, and change your password.

For more in the Remote Console interface elements, see LX II Remote Console Interface.

Scanning Ports - Remote Console

Use the port scanning feature to search for selected targets and display as part of a slide show.

This feature allows you to monitor up to 16 targets at one time since you can view each target server individually as it is displayed during the slide show.

Connect to targets or focus on a specific target as needed.

Scanning ports is not available in HKC.

Note: The scan port feature is available from the Remote Console and Local Console, but the feature varies slightly.

Scanning Ports Slide Show - Remote Console

When you start a scan, the Port Scan window opens.

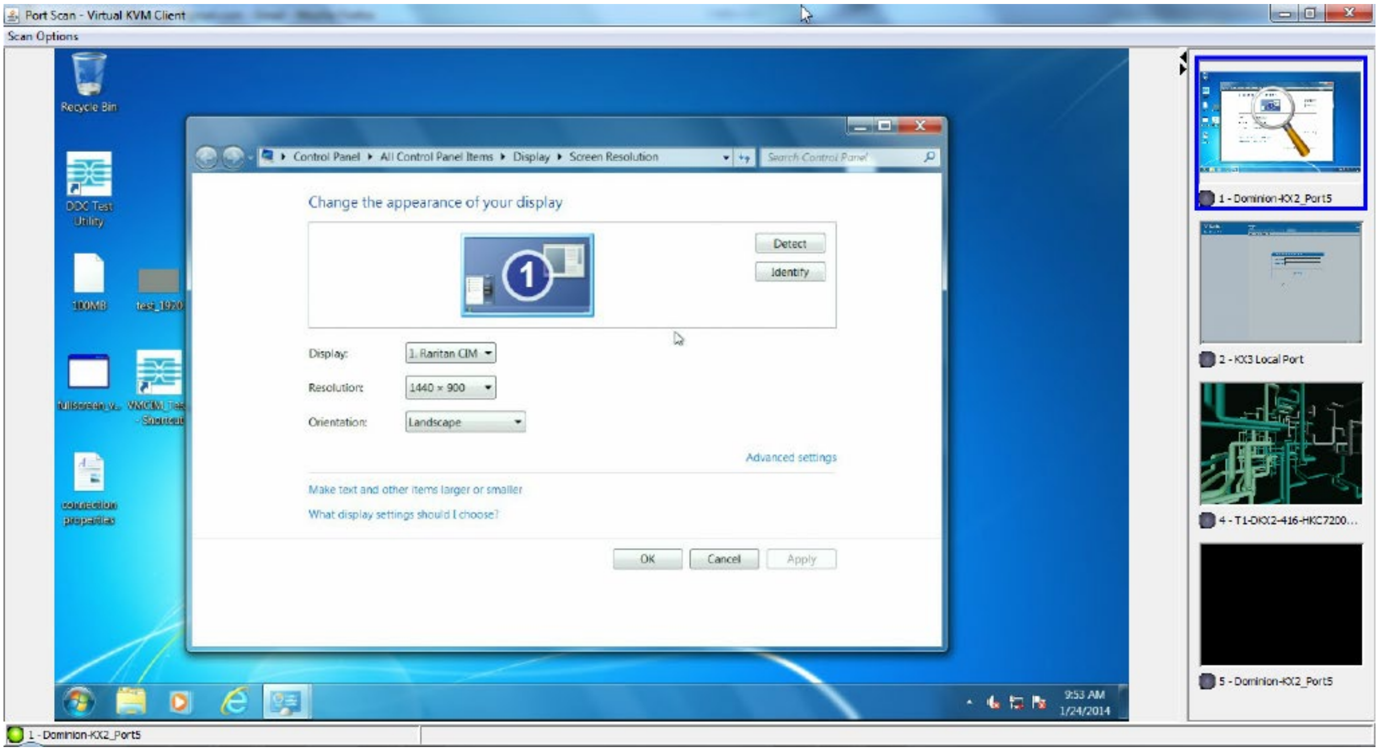
As each target is found, it is displayed as a thumbnail in a slide show.

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.

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.



Display: 1. Raritan CIM

Resolution: 1440 × 900

Orientation: Landscape

Configure scan settings for the Remote Console in the KVM client.

Note: Scan port settings for the Local Console are configured on the Local Port Settings page. See **Scanning Ports - Local Console** *(on page 243)*

Target Status Indicators During Port Scanning - Remote Console

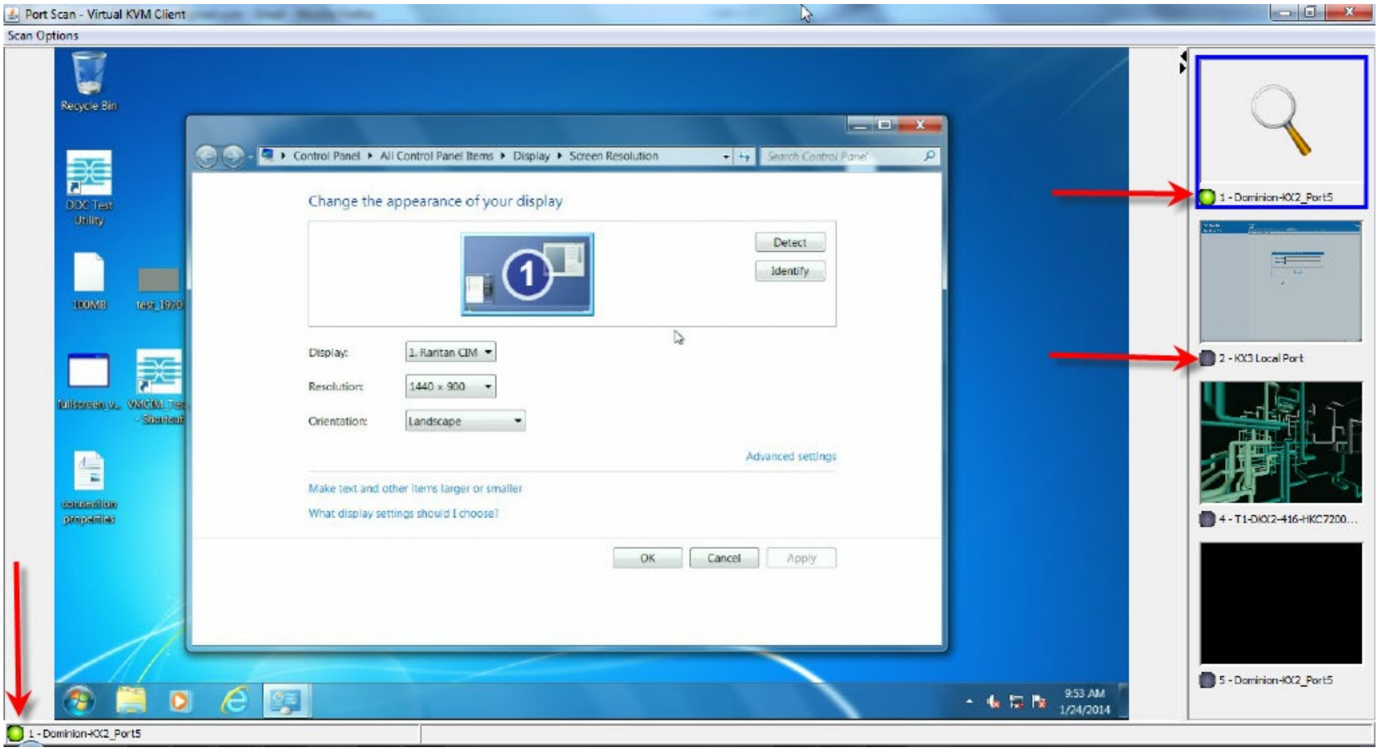
The status of each target is indicated by green, yellow and red lights that are displayed below the target thumbnail.

As the target is the focus of the rotation, the indicator is in the task bar also shows the status.

Lights for each target are gray until they are the focus of the slide show.

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



Change the appearance of your display

Display: 1. Raritan CIM

Resolution: 1440 x 900

Orientation: Landscape

Using Scan Port Options

Following are options available to you while scanning targets.

With the exception of the Expand/Collapse icon, all of these options are selected from the Options menu in the upper left of the Port Scan viewer.

The options will return to their defaults when you close the window.

Note: Configure scan settings such as the display interval from the KVM Client.

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

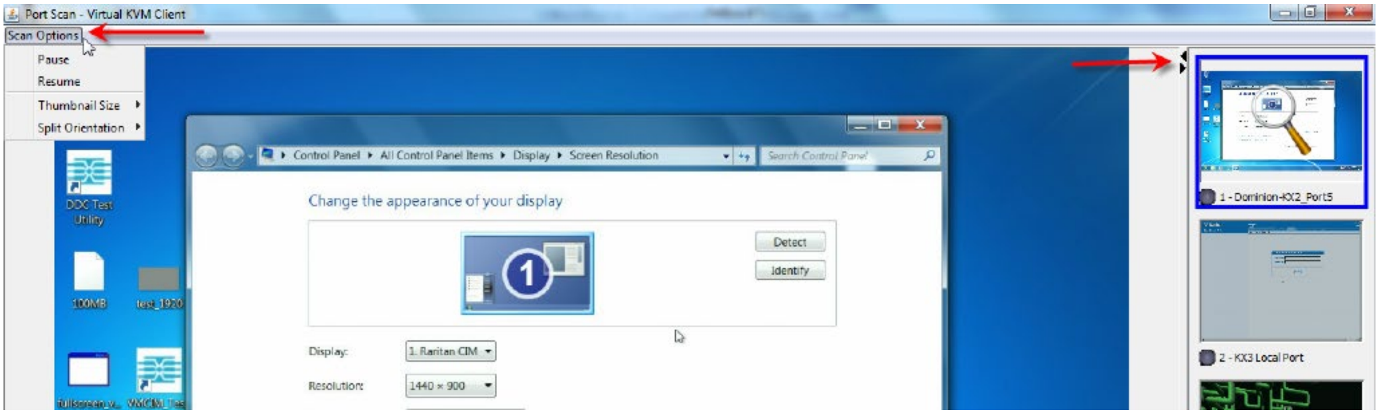
- Resume the thumbnail rotation by selecting Options > Resume.

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.

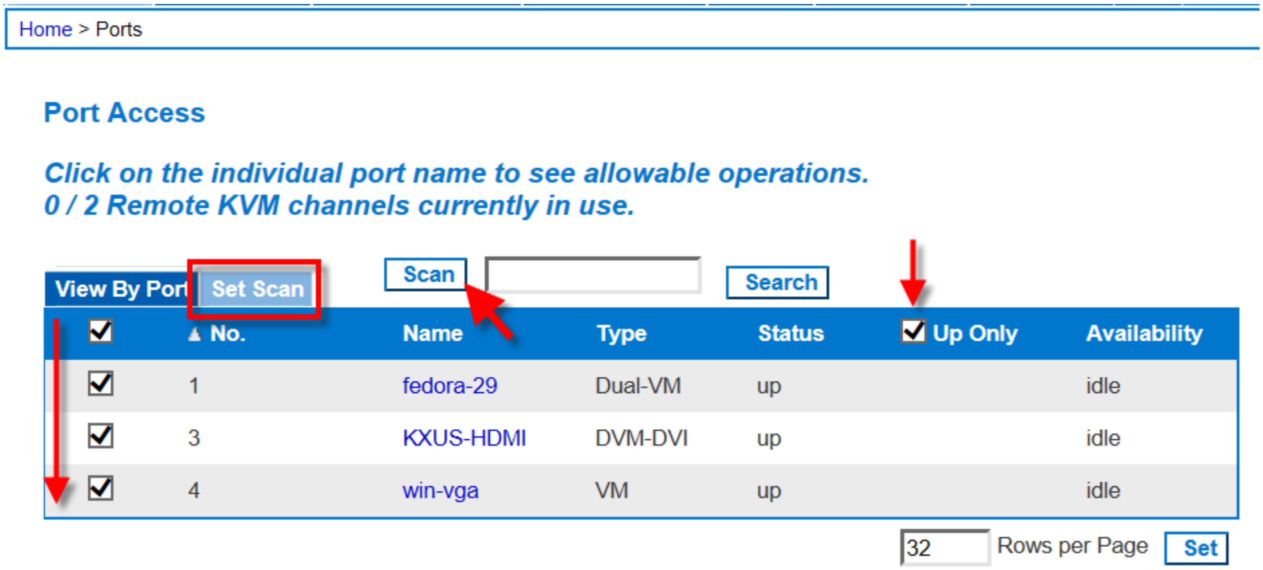


Scan for Targets

- **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.



Port Access

Click on the individual port name to see allowable operations.
0 / 2 Remote KVM channels currently in use.

☑	▲ No.	Name	Type	Status	☑ Up Only	Availability
☑	1	fedora-29	Dual-VM	up		idle
☑	3	KXUS-HDMI	DVM-DVI	up		idle
☑	4	win-vga	VM	up		idle

32 Rows per 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.

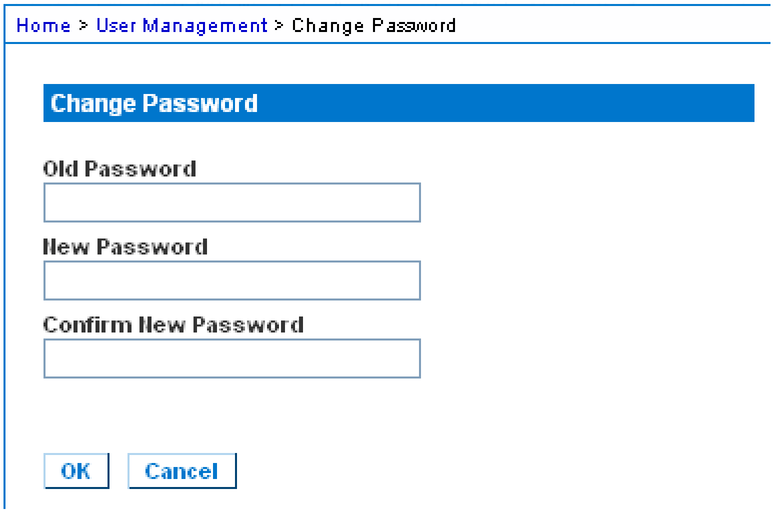
Changing a Password

- **To change your LX II 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 107).*



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 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 II devices on its subnet
- Retrieve discovered LX II devices from the connected Dominion device

Note: Due to browser limitations, HKC does not support Favorites.

Enable Favorites

- Click Enable in the Favorite Devices section of the left panel of the LX II interface, below Online Help.

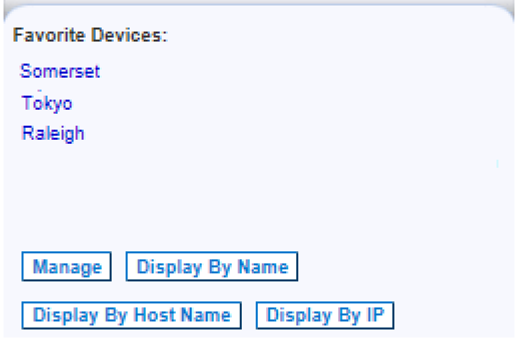
Access and Display Favorites

▶ To access a favorite LX II devices:

- Click on a LX II listed beneath Favorite Devices in the left of the Remote Console.

▶ To display favorites by Name, IP Address or Host Name:

- Click Display by Name, Display by IP, or Display by Host Name.



Discovering Devices on the Local Subnet

This option discovers LX II devices on your local subnet. This is the subnet where the LX II Remote Console is running.

These devices can be accessed directly from this page or you can add them to your list of favorites.

▶ 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 II Subnet

This feature is only available in the Java client , RSC.

This option discovers LX II devices on the device subnet. This is the subnet of the LX II device's IP address.

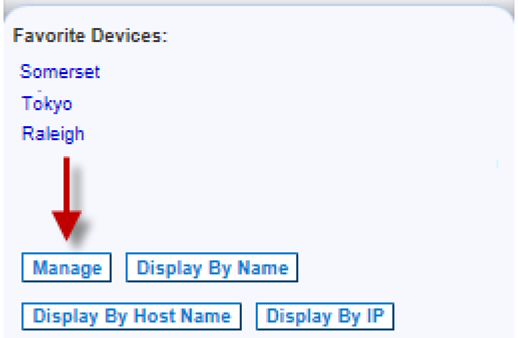
You can access these devices directly from the Subnet page or add them to your list of favorites.

This feature allows multiple LX II devices to interoperate and scale automatically.

The LX II Remote Console automatically discovers the LX II devices, and any other Raritan device, in the subnet of the LX II.

To discover devices on the device subnet:

1. Choose Manage > Discover Devices - LX II Subnet.



   The Discover Devices - LX II 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.

Chapter 12 LX II Local Console

The Local Console interface provides access to the LX II while at the rack.

This section contains help on tasks performed by end users at the Local Console.

In This Chapter

Integrated Switch/LED Drawers - Local Console

When you access the LX II at the rack using an integrated switch/LED drawer model, this is the local console.

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.

Local Console Video Resolution

LX II outputs video in the configured resolution.

▶ **Supported video resolutions:**

- 1024x768@60
- 1280x1024@60 (default)
- 1920x1080@60

Simultaneous Users

The LX II 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 II, you can still simultaneously access your servers from the rack via the Local Console.

Local Port Hot Keys and Connect Keys

Because the LX II Local Console interface is completely replaced by the interface for the target device 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 II Local Console user interface when a target device is currently being viewed.

See ***Select the Local Port Hotkey*** (on page 84) and ***Select the Local Port Connect Key*** (on page 85) for more information.

Return to the Local Console from a Target Device - Default Hot Key

- Press the Scroll Lock hot key twice rapidly

  The video display switches from the target device interface to the LX II Local Console interface.

Local Port Auto-Sense (Video Refresh) - Default Hot Key

▶ **To perform an auto-sense (video refresh) on the LX II local port via hot key:**

- Press and hold the Shift key, and quickly press the Scroll Lock key twice, and then release.

Connect Key Examples

Standard servers	
Connect key action	**Key sequence example**
Access a port from the local port	▪ Press Left ALT > Press and Release 5 > Release Left ALT
Switch between ports	▪ Press Left ALT > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and	▪ Double-click Scroll Lock

Standard servers	
Connect key action	**Key sequence example**
return to the local port	

Blade chassis	
Connect key action	**Key sequence example**
Access a port from the local port GUI	Access port 5, slot 2: ▪ Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 2 > Release Left ALT
Switch between ports	Switch from target port 5, slot 2 to port 5, slot 11: ▪ Press Left ALT > Press and Release 5 > Press and Release - > 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 5, slot 11 and return to the local port GUI (the page from which you connected to target): ▪ Double Click Scroll Lock

Special Sun Key Combinations

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

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

Sun key	Local port key combination
Mute	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	No key combination
Power	No key combination

Scanning Ports - Local Console

The scan port feature is available from the Remote Console and Local Console, but the feature varies slightly. See ***Scanning Ports - Remote Console*** (on page 232)

Click the thumbnail of any target server to exit scan mode and connect to the target, or use the Local Port ConnectKey sequence.

To exit scan mode, click the Stop Scan button in the thumbnail view, or use the Local Port Hotkey sequence hot key.

Scanning Port Slide Show - Local Console

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.

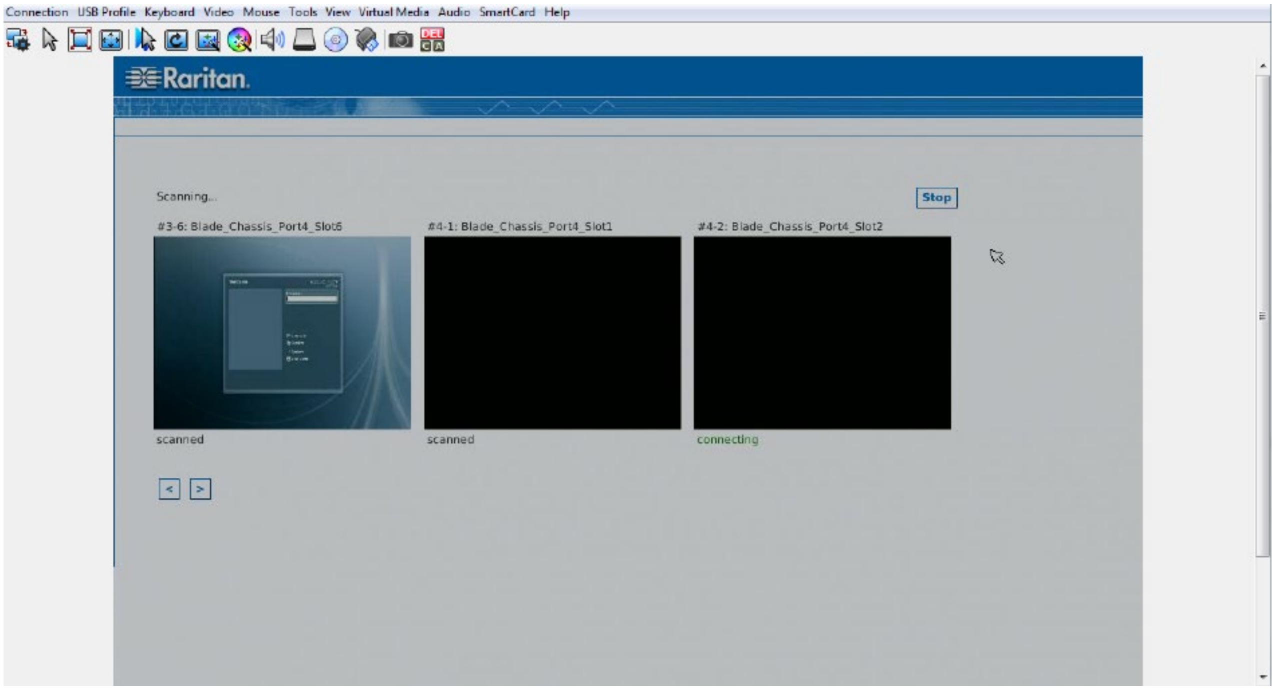
The name of the target is displayed below its thumbnail and in the task bar at the bottom of the window.

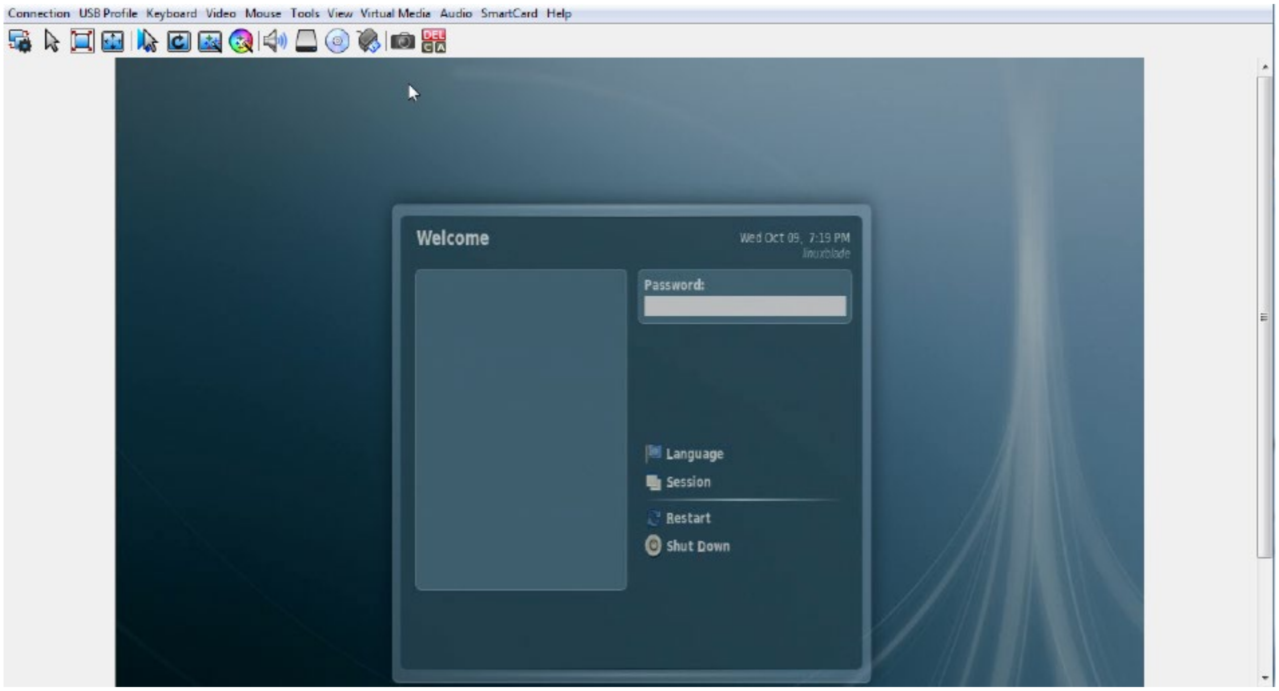
If a target is busy, a blank screen is displayed instead of the target server access page.

Configure the time between the slide show thumbnail rotation and the thumbnail focus interval on the Local Port Settings page.

See ***Configure Local Console Scan Settings*** (on page 246)

Note: Configure scan settings for the Remote Console from VKC, VKCS, or AKC. See **Configuring Port Scan Settings in VKC/VKCS and AKC** *(on page 205)*


Connection USB Profile Keyboard Video Mouse Tools View Virtual Media Audio SmartCard Help
Raritan.
Scanning...
Stop
#3-6: Blade_Chassis_Port4_Slot6
#4-1: Blade_Chassis_Port4_Slot1
#4-2: Blade_Chassis_Port4_Slot2
scanned
scanned
connecting
<
>


Connection USB Profile Keyboard Video Mouse Tools View Virtual Media Audio SmartCard Help
Welcome
Wed Oct 09, 7:19 PM
linuxblade
Password:
Language
Session
Restart
Shut Down

Scanning Port Slide Show - Local Console

When you start a scan, the Port Scan window opens. The slide show scrolls through the targets 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.

When scanning from the local console, there are no thumbnails. Only the name of the target is displayed.

If a target is busy, a blank screen is displayed instead of the target server access page.

Configure the time intervals for scanning in the Local Port Settings page.

See ***Configure Local Console Scan Settings*** (on page 246).

Target Status Indicators During Port Scanning - Local Console

When scanning on the Local Console, the status of each target is indicated below the thumbnail.

The scanning status of each target is displayed as:

- not scanned
- connecting
- scanned
- skipped

Configure Local Console Scan Settings

Do the following to configure Local Console scan port options.

To configure the Local Console scan port settings:

1. On the Local Console, select Device Settings.
2. In the Local Port Settings section, select Local Port Scan Mode.
3. Change the display interval as needed:
   - Display Interval - changes the scan display interval.
   - Interval Between Ports - change interval between switching different port during scan.

Scan for Targets - Local Console

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.

Local Console USB Profile Options

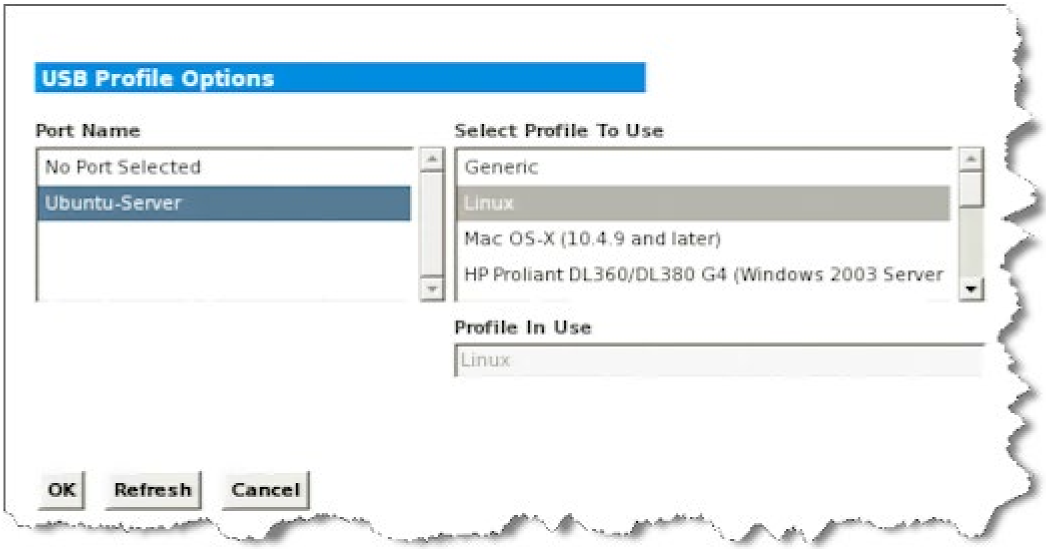
From the USB Profile Options section of the Tools page, you can choose from the available USB profiles.

The ports that can be assigned profiles are displayed in the Port Name field and the profiles that are available for a port appear in the Select Profile To Use field after the port is selected. The profiles selected for use with a port appear in the Profile In Use field.

To apply a USB profile to a local console port:

1. In the Port Name field, select the port you want to apply the USB profile to.
2. In the Select Profile To Use field, select the profile to use from among those available for the port.

3. Click OK. The USB profile will be applied to the local port and will appear in the Profile In Use field.



LX II Local Console Factory Reset

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 114).*

▶ 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 appliance completely to the factory defaults.

     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 appliance back to the default values (click Device Settings > Network Settings to access this information).
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 of full factory reset, the LX II device is automatically restarted.

Resetting the LX II Using the Reset Button

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

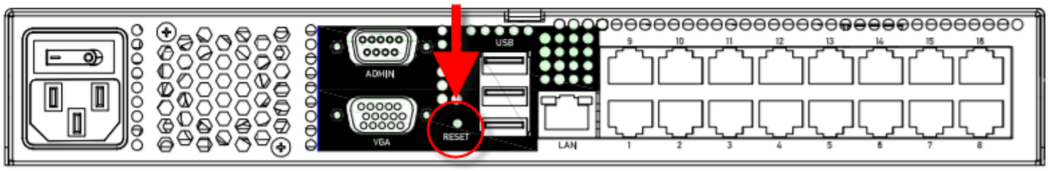
The actions that are performed when the Reset button is pressed are defined on the Encryption & Share page. See ***Encryption and Share*** (on page 109).

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 114).

To reset the device:

1. Power off the LX II.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the LX II device back on.
4. Continue holding the Reset button for 10 seconds.



Appendix A Feature Comparison: LX II and KX III

The following KX III features are not supported in LX II.

▶ Hardware:

- High density models (no 1x32, 2x32, 4x16, 4x32, 4x64, 8x8, 8x16, 8x32, 8x64)
- Dual power supplies and dual gigabit LAN
- Tiering Port
- Digital Local Port (DVI-D)

▶ Software:

- High performance video (no 30 frames-per-second)
- Integrated remote power control (with Raritan PX)
- Digital audio over IP
- 802.1X security
- FIPS 140-2 encryption module
- Dual monitor and KVM client launch options
- Blade server support
- Secure login banner
- Connect/Disconnect Scripts
- IP Access Control List
- SMTP email notifications

▶ External interfaces:

- CommandCenter management
- Dominion User Station Support
- Smart card/CAC support
- Dominion SDK/API

Appendix B Specifications

In This Chapter

Supported Target Server Video Resolutions

When using digital CIMs, you set the target's video resolution to match your monitor's native display resolution. The native display resolution is set when configuring ports for digital CIMs (see ***Configure the CIM Target Settings*** (on page 80)).

Following is a complete list of supported video resolutions when accessing a target from the Remote Console.

- 640x350@70Hz
- 640x350@85Hz
- 640x400@56Hz
- 640x400@84Hz
- 640x400@85Hz
- 640x480@60Hz
- 640x480@66.6Hz
- 640x480@72Hz
- 640x480@75Hz
- 640x480@85Hz
- 720x400@70Hz
- 720x400@84Hz
- 720x400@85Hz
- 800x600@56Hz
- 800x600@60Hz
- 800x600@70Hz
- 800x600@72Hz
- 800x600@75Hz
- 800x600@85Hz
- 800x600@90Hz
- 800x600@100Hz
- 832x624@75.1Hz
- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768@72Hz
- 1024x768@85Hz
- 1024x768@75Hz
- 1024x768@90Hz
- 1024x768@100Hz
- 1152x864@60Hz
- 1152x864@70Hz
- 1152x864@75Hz

- 1152x864@85Hz
- 1152x870@75.1Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x960@85Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1280x1024@85Hz
- 1360x768@60Hz
- 1366x768@60Hz
- 1368x768@60Hz
- 1400x1050@60Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x1200@60Hz (Requires Reduced Blanking Time)

  For 1920x1200@60Hz, you must use a digital CIM and set the CIM's preferred resolution to 1920x1200@60Hz.

Target Server Video Resolution - Supported Connection Distances and Refresh Rates

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.

The following table summarizes the maximum target server distance for various video resolutions and refresh rates:

Target server video resolution	Maximum distance
1024x768@60Hz (and below)	150' (45 m)
1280x1024@60Hz	100' (30 m)
1280×720@60Hz	75' (22 m)
1600x1200@60Hz	50' (15 m)
1920x1080@60Hz	50' (15 m)

See ***Supported Target Server Video Resolutions*** (on page 251) for the video resolutions supported by the LX II.

Note: Due to the multiplicity of server manufacturers and types, OS versions, video drivers, and so on, as well as the subjective nature of video quality, performance cannot be guaranteed across all distances in all environments.

Supported Computer Interface Module (CIMs) Specifications

Digital CIMs support Display Data Channels (DDC) and Enhanced Extended Display Identification Data (E-EDID).

Note: Both plugs must be plugged in for the HDMI and DVI CIMs.

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-DVUSB	Dual USB CIM for: ▪ OS virtual media ▪ Smartcard/CAC ▪ Audio ▪ Absolute Mouse Synchronization 	▪ 1.7" x 3.5" x 0.8" ▪ 43 x 90 x 19mm	▪ 0.25lb ▪ 0.11kg
D2CIM-VUSB	USB CIM for: ▪ OS virtual media ▪ Absolute Mouse Synchronization 	▪ 1.3" x 3.0" x 0.6" ▪ 33 x 76 x 15mm	▪ 0.20lb ▪ 0.09kg
D2CIM-VUSB-USBC	USB CIM for: ▪ USB-C ports on Macs and PCs ▪ USB keyboard, mouse, and virtual media ▪ DisplayPort video ▪ No Audio or Smartcard 	▪ 1.7" x 3.5" x 0.8" ▪ 43 x 90 x 19mm	▪ 0.25lb ▪ 0.11kg

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-DVUSB-DP	Digital CIM that provides digital-to-analog conversion and support for: ▪ OS virtual media ▪ Smartcard/CAC ▪ Audio ▪ Absolute and Relative Mouse Synchronization 	▪ 1.7" x 3.5" x 0.8" ▪ 43 x 90 x 19mm	▪ 0.25lb ▪ 0.11kg
D2CIM-DVUSB-HDMI	Digital CIM that provides digital-to-analog conversion and support for: ▪ OS virtual media ▪ Smartcard/CAC ▪ Audio ▪ Absolute and Relative Mouse Synchronization 	▪ 1.7" x 3.5" x 0.8" ▪ 43 x 90 x 19mm	▪ 0.25lb ▪ 0.11kg
D2CIM-DVUSB-DVI	Digital CIM that provides digital-to-analog conversion and support for: ▪ OS virtual media ▪ Smartcard/CAC ▪ Audio ▪ Absolute and Relative Mouse Synchronization	▪ 1.7" x 3.5" x 0.8" ▪ 43 x 90 x 19mm	▪ 0.25lb ▪ 0.11kg

CIM model	Description	Dimensions (WxDxH)	Weight
DCIM-PS2	CIM for PS2 	▪ 1.3" x 3.0" x 0.6" ▪ 33 x 76 x 15mm	▪ 0.20lb ▪ 0.09kg
DCIM-USBG2	CIM for USB and Sun USB 	▪ 1.3" x 3.0" x 0.6" ▪ 33 x 76 x 15mm	▪ 0.20lb ▪ 0.09kg

Supported Digital Video CIMs for Mac

Use a digital video CIM to connect to the following Mac® ports:

Mac port	CIM
USB-C	D2CIM-VUSB-USBC
DVI	D2CIM-DVUSB-DVI
HDMI	D2CIM-DVUSB-HDMI
DisplayPort or Thunderbolt	D2CIM-DVUSB-DP

If the Mac’s HDMI or DisplayPort video has a mini connector, a passive adapter cable may be required to connect to the full sized HDMI and DisplayPort plugs on the digital CIMs.

Alternatively, use the Mac VGA adapter with the D2CIM-VUSB or D2CIM-DVUSB. Note that this may be less reliable and the video quality may suffer.

For information on established modes supported by the LX II 2.5.0 (and later) for Mac, see ***Digital CIM Established and Standard Modes*** (on page 256).

Digital CIM Timing Modes

Following are the default timing modes that are used when the LX II communicates with a video source via a digital CIM.

The timing mode that is used is dependent on the native resolution of the video source.

- 960x1080@60Hz
- 1024x768@60Hz
- 1152x864@60Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz (default resolution applied to digital CIMs)
- 1360x768@60Hz
- 1400x1050@60Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x1200@60Hz

See ***Configuring CIM Ports*** (on page 79) for more information.

Digital CIM Established and Standard Modes

The following additional established and standard resolutions and timing modes are supported by the LX II 3.0.0 (and later).

Digital CIM Established Modes

- 720x400@70Hz IBM, VGA
- 640x480@60Hz IBM, VGA
- 640x480@67Hz Apple Mac® II
- 640x480@72Hz VESA
- 640x480@75Hz VESA
- 800x600@56Hz VESA
- 800x600@60Hz VESA
- 800x600@72Hz VESA
- 800x600@75Hz VESA
- 832x624@75Hz Apple Mac II
- 1024x768@60Hz VESA
- 1024x768@70Hz VESA
- 1024x768@75Hz VESA
- 1280x1024@75Hz VESA
- 1152x870@75Hz Apple Mac II

Digital CIM Standard Modes

- 1152x864@75Hz VESA
- 1280x960@60Hz VESA
- 1280x1024@60Hz VESA
- 1360x768@60Hz VESA
- 1400x1050@60Hz VESA
- 1440x900@60Hz VESA
- 1600x1200 @60Hz VESA
- 1680x1050@60Hz VESA
- 1920x1080@60Hz VESA

DVI Compatibility Mode

DVI Compatibility Mode may be required if you are using an HDMI CIM to connect to a Dell Optiplex target with an Intel video card, or a Mac® Mini with an HDMI video port.

Selecting this mode ensures a good video quality from the targets.

See ***Configuring CIM Ports*** (on page 79) in online help.

Supported Remote Connections

Remote connection	Details
Network	10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet
Protocols	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Network Speed Settings

LX II 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 II: 100/Full Switch: 100/Half	100/Half	LX II: 10/Full Switch: 10/Half	10/Half
	1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
	100/Full	LX II: 100/Half Switch: 100/Full	LX II: 100/Half Switch: 100/Full	100/Full	LX II: 100/Half Switch: 100/Full	No Communication	No Communication
	100/Half	100/Half	100/Half	LX II: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/Full	LX II: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	LX II: 10/Half Switch: 10/Full
	10/Half	10/Half	No Communication	No Communication	No Communication	LX II: 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 II behavior deviates from expected behavior

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

Certified Modems

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

LX II Supported Keyboard Languages

The LX II 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 II Local Console functions. For more information about non-US keyboards, see Informational Notes.

Note: It is strongly recommended 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	US Keyboard layout

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

Mac Mini BIOS Keystroke Commands

The following BIOS commands have been tested on Intel-based Mac® Mini target servers and Mac Lion® servers running Mac Snow Leopard®. The servers were attached to a LX II with D2CIM-DVUSB and D2CIM-VUSB CIMs. See below for the supported keys and any notes.

Keystroke	Description	Virtual Media CIM	Dual Virtual Media CIM	Mac Lion Server HDMI CIM
Press C during startup	Start up from a bootable CD or DVD, such as the Mac OS X Install disc	Yes	Yes	Yes
Press D during startup	Start up in Apple Hardware Test (AHT)	Yes May need BIOS Mac profile for the mouse to work	Yes May need BIOS Mac profile for mouse to work	Yes May need BIOS Mac profile for the mouse to work
Press Option-Command-P-R until you hear startup sound a second time.	Reset NVRAM		Yes	Yes
Press Option during startup	Start up in Startup Manager, where you can select a Mac OS X volume to start from	Yes	Yes	Yes
Press Eject, F12, or hold the mouse button	Ejects any removable media, such as an optical disc	Yes	Yes	
Press N during startup	Start up from a compatible network server (NetBoot)	Yes	Yes	Yes
Press T during startup	Start up in Target Disk mode			Yes
Press Shift during startup	Start up in Safe Boot mode and temporarily disable login items	Yes	Yes	Known issue with LION to boot to safe mode. "Safe Mode" in red does not appear for Lion
Press Command-V during startup	Start up in Verbose mode.admin	Yes	Yes	Yes
Press Command-S during startup	Start up in Single-User mode	Yes	Yes	Yes
Press Option-N during startup	Start from a NetBoot server using the default boot image	Yes	Yes	Yes
Press Command-R during startup	Start from Lion Recovery1	N/A	N/A	Yes

Using a Windows Keyboard to Access Mac Targets

A Windows® keyboard can be used to access a Mac® connected to a LX II. Windows keys are then used to emulate the special Mac keys. This is the same as connecting a Windows keyboard directly to the Mac.

TCP and UDP Ports Used

▶ **Listening TCP Ports:**

* 80: http access (configurable)

* 443: https access (configurable)

* 5000: CC-SG and KXUS access (configurable)

* 22: SSH access (if enabled, configurable)

▶ **Listening UDP Ports:**

* 162: SNMP access (if SNMP Agent is enabled)

* 5001: CC_SG event notification (if under CC-SG management)

▶ **TCP Ports Outgoing:**

* 389: LDAP authentication (if LDAP is enabled, configurable)

* 636: LDAPS/StartTLS (id LDAPS/StartTLS is enabled, configurable)

* 25: SMTP (email) (if enabled)

* 445: SMB (Windows File System) access (Remote ISO image access).

▶ **UDP Ports Outgoing:**

* 514: Syslog (if enabled, configurable)

* 5001: CC_SG event notification (if under CC-SG management, configurable)

* 1812: RADIUS authentication (if enabled, configurable)

* 1813: RADIUS authentication (if enabled, configurable)

Appendix C Updating the LDAP Schema

In This Chapter

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 II 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:

rciusergroup	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.

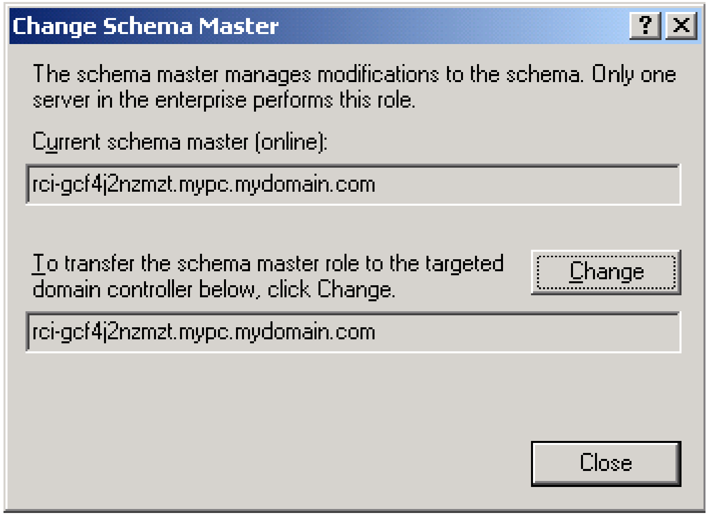
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

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.



Change Schema Master

The schema master manages modifications to the schema. Only one server in the enterprise performs this role.

Current schema master (online):

rci-gcf4j2nzmzt.mypc.mydomain.com

To transfer the schema master role to the targeted domain controller below, click Change.

rci-gcf4j2nzmzt.mypc.mydomain.com

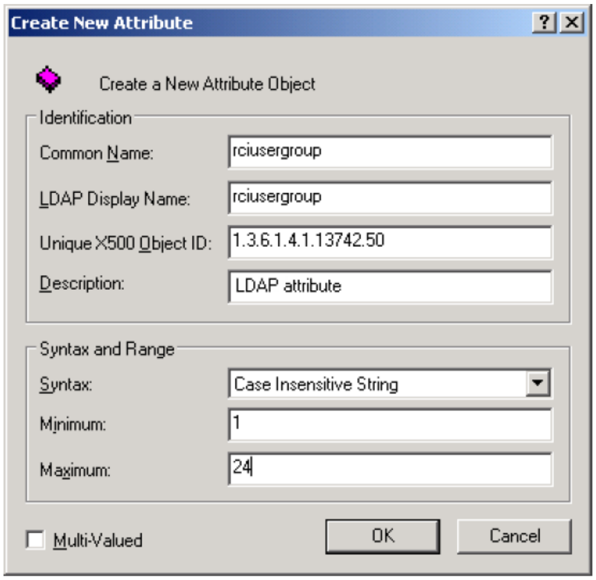
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

Creating a New Attribute

To create new attributes for the rciusergroup class:

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

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



Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: LDAP attribute

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

□ Multi-Valued

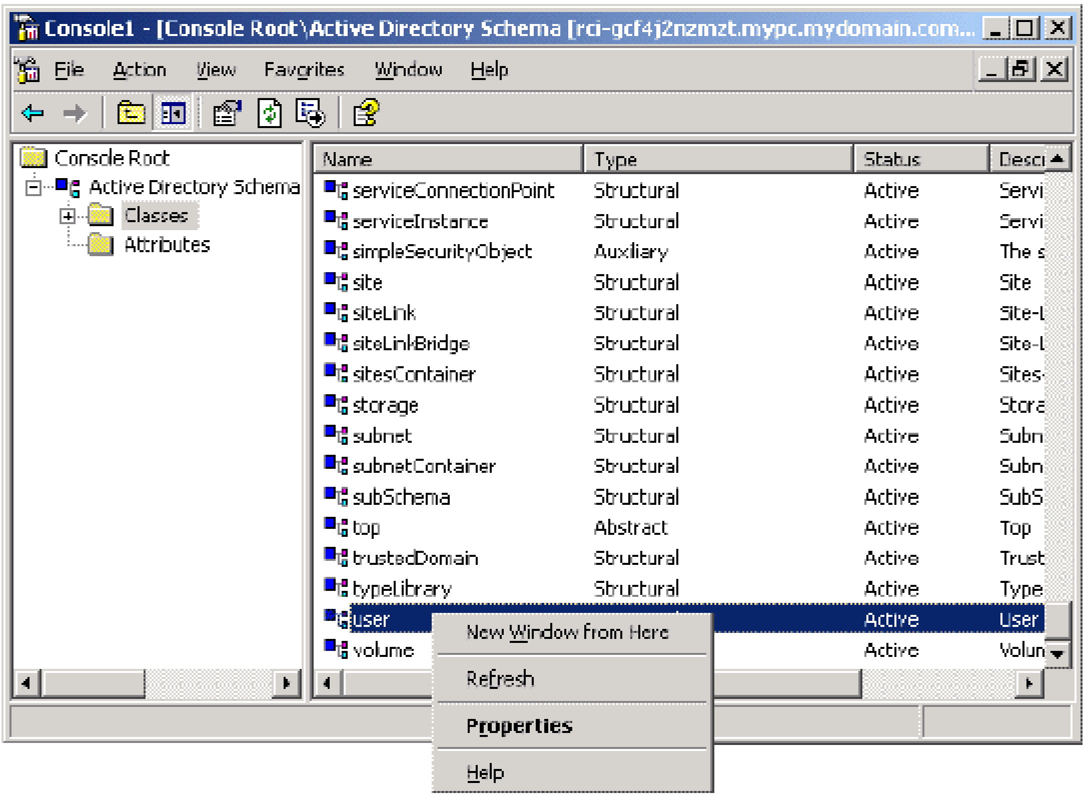
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String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

Adding Attributes to the Class

▶ **To add attributes to the class:**

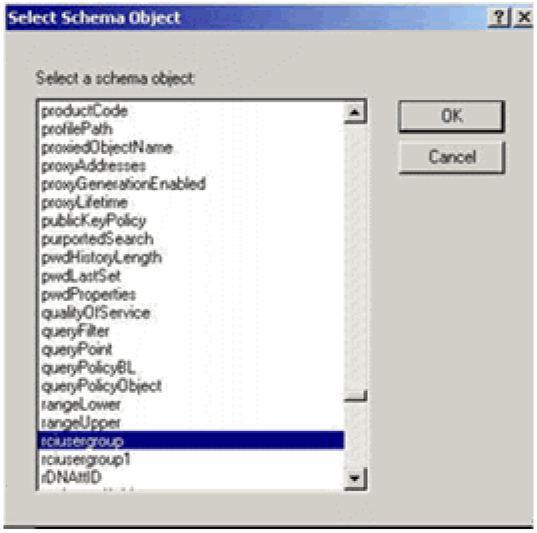
1. Click Classes in the left pane of the window.

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



Name	Type	Status	Desci
serviceConnectionPoint	Structural	Active	Servi
serviceInstance	Structural	Active	Servi
simpleSecurityObject	Auxiliary	Active	The s
site	Structural	Active	Site
siteLink	Structural	Active	Site-L
siteLinkBridge	Structural	Active	Site-L
sitesContainer	Structural	Active	Sites-
storage	Structural	Active	Stora
subnet	Structural	Active	Subn
subnetContainer	Structural	Active	Subn
subSchema	Structural	Active	SubS
top	Abstract	Active	Top
trustedDomain	Structural	Active	Trust
typeLibrary	Structural	Active	Type
user		Active	User
volume		Active	Volun

3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.
6. Choose rciusergroup from the Select Schema Object list.



Select a schema object:

productCode
profilePath
proxiedObjectName
proxyAddresses
proxyGenerationEnabled
proxyLifetime
publicKeyPolicy
purportedSearch
pwdHistoryLength
pwdLastSet
pwdProperties
qualityOfService
queryFilter
queryPoint
queryPolicyBL
queryPolicyObject
rangeLower
rangeUpper
rciusergroup
rciusergroup1
rDNAttID

7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

▶ **To update the schema cache:**

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

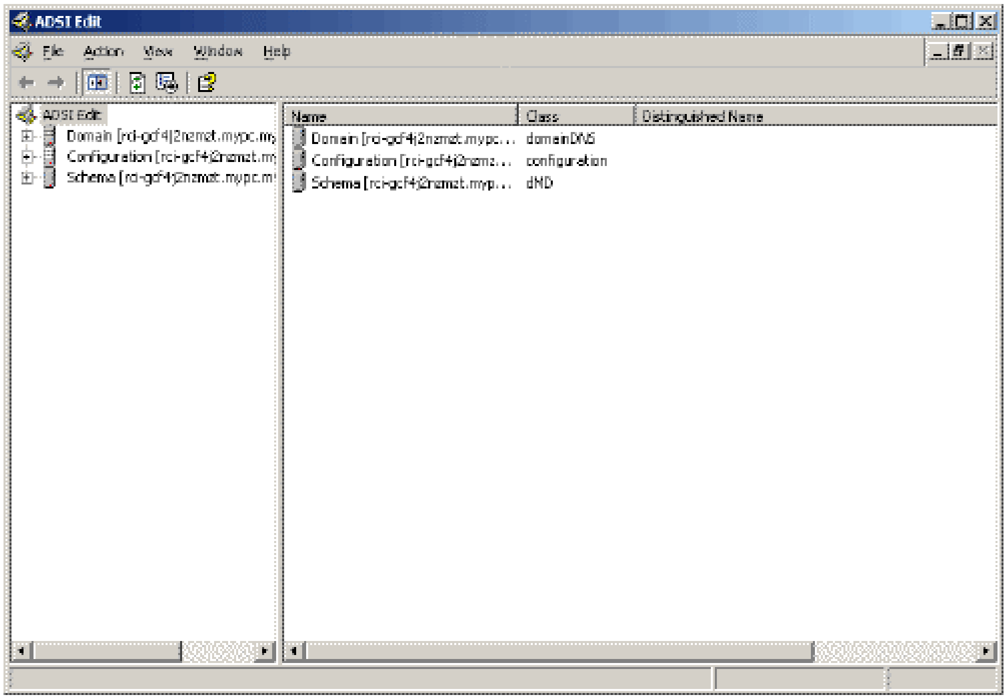
Editing rciusergroup Attributes for User Members

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 rciusergroup:**

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

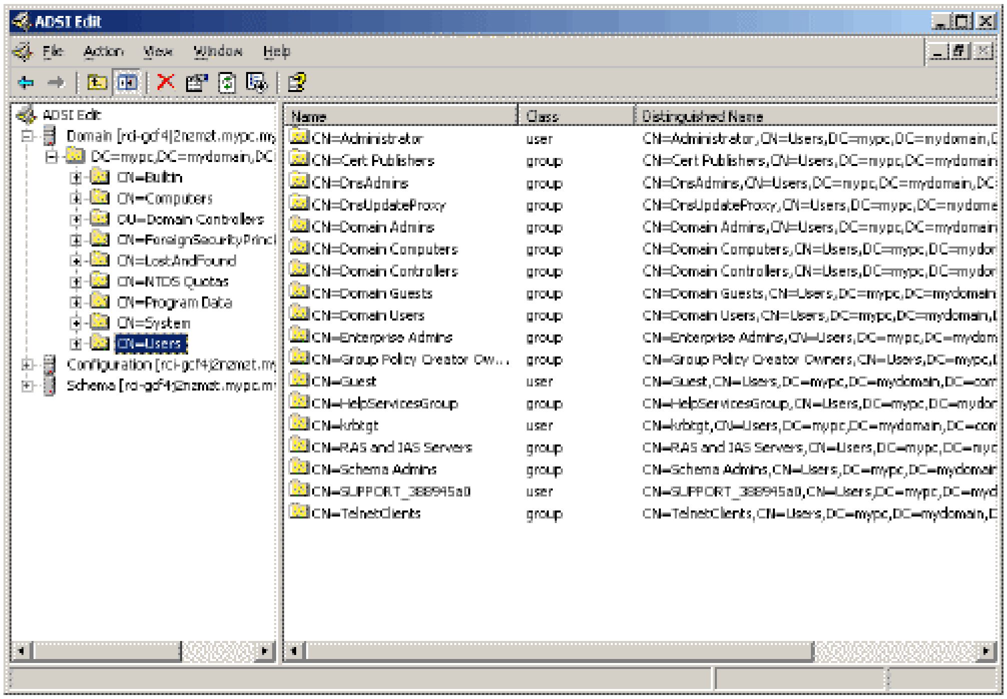
3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.


ADSI Edit
File Action View Window Help
ADSI Edit
Domain [rci-gcf4j2nzmzt.mypc.my
Configuration [rci-gcf4j2nzmzt.my
Schema [rci-gcf4j2nzmzt.mypc.m

Name	Class	Distinguished Name
Domain [rci-gcf4j2nzmzt.mypc...	domainDNS	
Configuration [rci-gcf4j2nzmz...	configuration	
Schema [rci-gcf4j2nzmzt.myp...	dMD	

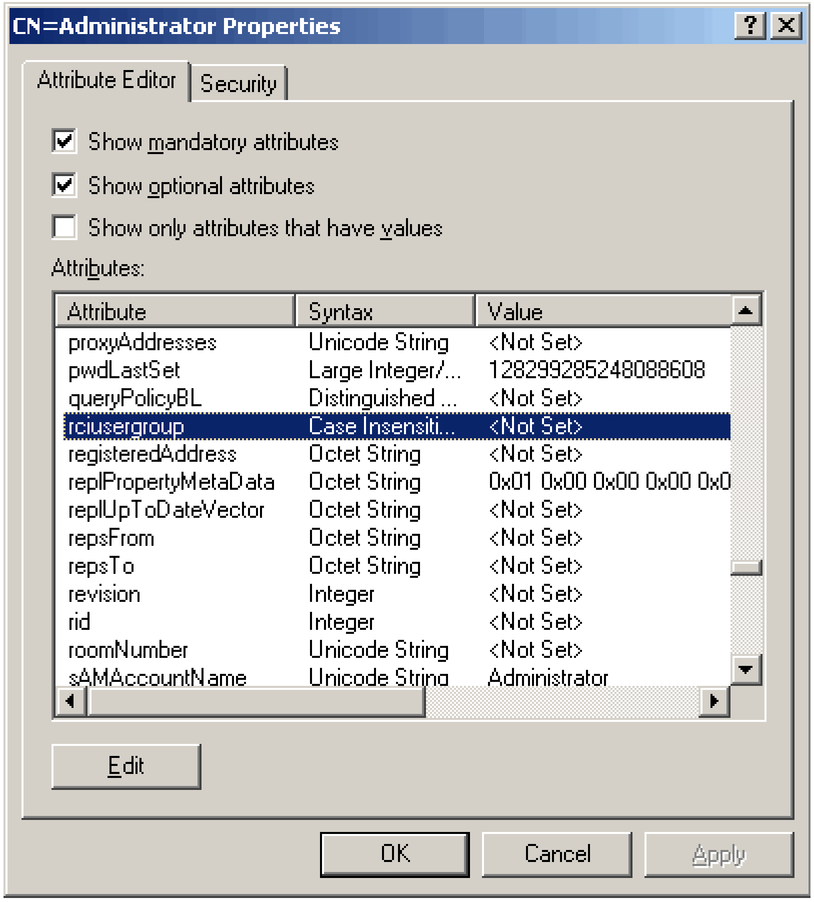
4. Open the Domain.

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



Name	Class	Distinguished Name
CN=Administrator	user	CN=Administrator,CN=Users,DC=mypc,DC=mydomain,D
CN=Cert Publishers	group	CN=Cert Publishers,CN=Users,DC=mypc,DC=mydomain
CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=mypc,DC=mydomain,DC
CN=DnsUpdateProxy	group	CN=DnsUpdateProxy,CN=Users,DC=mypc,DC=mydoma
CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=mypc,DC=mydomain
CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=mypc,DC=mydor
CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=mypc,DC=mydor
CN=Domain Guests	group	CN=Domain Guests,CN=Users,DC=mypc,DC=mydomain
CN=Domain Users	group	CN=Domain Users,CN=Users,DC=mypc,DC=mydomain,D
CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=mypc,DC=mydom
CN=Group Policy Creator Ow...	group	CN=Group Policy Creator Owners,CN=Users,DC=mypc,D
CN=Guest	user	CN=Guest,CN=Users,DC=mypc,DC=mydomain,DC=con
CN=HelpServicesGroup	group	CN=HelpServicesGroup,CN=Users,DC=mypc,DC=mydor
CN=krbtgt	user	CN=krbtgt,CN=Users,DC=mypc,DC=mydomain,DC=con
CN=RAS and IAS Servers	group	CN=RAS and IAS Servers,CN=Users,DC=mypc,DC=myc
CN=Schema Admins	group	CN=Schema Admins,CN=Users,DC=mypc,DC=mydomain
CN=SUPPORT_388945a0	user	CN=SUPPORT_388945a0,CN=Users,DC=mypc,DC=myd
CN=TelnetClients	group	CN=TelnetClients,CN=Users,DC=mypc,DC=mydomain,D

6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



☑ Show mandatory attributes

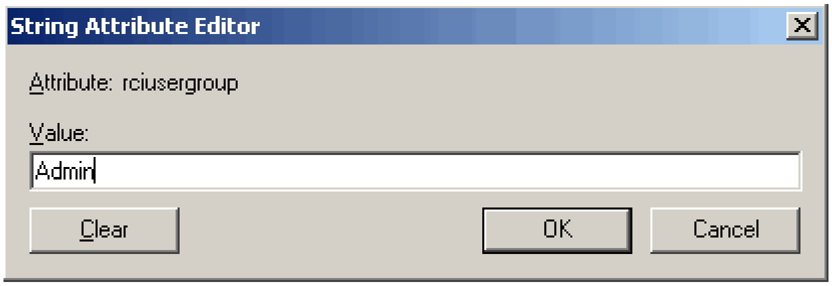
☑ Show optional attributes

□ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
proxyAddresses	Unicode String	<Not Set>
pwdLastSet	Large Integer/...	128299285248088608
queryPolicyBL	Distinguished ...	<Not Set>
rciusergroup	Case Insensiti...	<Not Set>
registeredAddress	Octet String	<Not Set>
replPropertyMetaData	Octet String	0x01 0x00 0x00 0x00 0x0
replUpToDateVector	Octet String	<Not Set>
repsFrom	Octet String	<Not Set>
repsTo	Octet String	<Not Set>
revision	Integer	<Not Set>
rid	Integer	<Not Set>
roomNumber	Unicode String	<Not Set>
sAMAccountName	Unicode String	Administrator

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



Attribute: rciusergroup

Value:

Admin

Index