



Raritan Digital Solution



CommandCenter Secure Gateway Deployment Guide

Copyright © 2007 Raritan, Inc.
DSD-0D-E
April 2007
255-80-5160-00

This page intentionally left blank.

Copyright and Trademark Information

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

© Copyright 2007 Raritan, CommandCenter, RaritanConsole, Dominion, and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. Java is a registered trademark of Sun Microsystems, Inc. Internet Explorer is a registered trademark of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communication Corporation. All other marks are the property of their respective owners.

FCC Information

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

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

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



For assistance in North or South America, please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail tech@raritan.com

Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.

For assistance around the world, please see the last page of this guide for regional Raritan office contact information.

Safety Guidelines

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor and appliance off the supply.

Rack Mount Safety Guidelines

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

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

Contents

Chapter 1: Introduction	1
Prerequisites	1
Intended Audience	1
CC NOC Deployment and Paragon Integration	1
Firmware and Software Requirements (Compatibility Matrix)	1
Chapter 2: Pre-Deployment Planning	3
Prepare Infrastructure	3
Basic Requirements for Dominion Products	3
Prepare Network	4
Allocate IP Addresses for Raritan Devices	4
Open Ports for Firewall or IP Port Filters	4
Prepare Target Servers	4
Target Server Video Resolution	5
Operating System Mouse and Video Settings	5
Prepare User PC	9
Install Java Runtime Environment	9
Chapter 3: Prepare Raritan Devices	11
Local Console or Web Browser Access	11
Default IP Address and Logins	11
Direct Access is Restricted	11
Fall Back to Stand-alone Mode	11
Minimum Firmware Version	12
Preparing Dominion Devices for CC-SG Management	12
Dominion KX Devices	12
Dominion KX2 Devices	14
Dominion SX Devices	15
Dominion KSX Devices	16
Preparing IP-Reach Devices for CC-SG Management	18
IP Reach TR or M Series	18
Chapter 4: Install CC-SG	21
1. Rack Mount the CC-SG Unit	21
2. Physical Connections	21
Physical Connections for CC-SG E1 Units	21
Physical Connections for CC-SG V1 Units	22
Physical Connections for CC-SG G1 Units	22
3. Set IP Address of CC-SG	23
Appendix A: Installation Template	25
Blank Template	25
Sample Template	27
Appendix B: Remote Power Management	29
Device Configurations for Power Control in CC-SG	29
Example: Remote Power Management Using SX, KX, and PowerStrip	30
CC-SG Configuration	30
Example: Remote Power Management for Redundant Power Supplies	31
CC-SG Configuration	31

Figures

Figure 1: Solaris Mouse Configuration Window 8

Figure 2 Dominion KX Physical Connections..... 12

Figure 3 Dominion KX Network Settings Screen..... 13

Figure 4 Dominion KX Connections 13

Figure 5 Dominion KX2 Connections 14

Figure 6 Dominion KSX Back panel Connections 16

Figure 7 IP-Reach TR Series 18

Figure 8 IP-Reach M Series..... 18

Figure 9 IP-Reach Initial Configuration Screen 19

Figure 10 IP-Reach Network Configuration Screen 19

Figure 11 Physical Connections for CCSG E1 Units..... 21

Figure 12 Physical Connections for CCSG V1 Units..... 22

Figure 13 Physical Connections for CCSG G1 Units 22

Figure 14 CC-SG and Remote Power Management..... 30

Figure 16 Redundant Power for Target Device..... 31

This page intentionally left blank.

Chapter 1: Introduction

CommandCenter Secure Gateway (CC-SG) provides a hardware-based management solution engineered to consolidate secure access and control of IT devices. It provides centralized management of serial, KVM and power control devices in multiple data centers, branch offices and remote locations via a single, secure browser-based access. Users can access target servers and systems (nodes) that are connected to Raritan devices, such as Dominion KX or IP-Reach.

In this guide, the term “Raritan devices” refers to the following equipment:

- Dominion KX
- Dominion KX2
- Dominion KX101
- Dominion KSX
- Dominion SX
- IP-Reach (all models)

Within CC-SG, target servers and systems are called nodes.

Prerequisites

This guide provides comprehensive instructions on deploying Raritan devices that are managed by CC-SG.

Additional installation information on Raritan devices and CC-SG is available on the User Manuals & Quick Setup Guides CD-ROM, or online in the Support section of the Raritan website.

Intended Audience

This guide is written for installation engineers and technicians installing Raritan devices and provides installation procedures and all relevant information that is needed to install CC-SG and its managed devices for a typical environment. Please read all pertinent information in this guide before starting installation of any products.

CC NOC Deployment and Paragon Integration

CommandCenter NOC (CC NOC) and integration with Paragon II systems (P2-SC) are NOT covered in this **Raritan Digital Solution Deployment Guide**. Please refer to the **Deployment Guide** that came with your CC NOC or P2-SC unit for additional information.

Firmware and Software Requirements (Compatibility Matrix)

Successful deployment of CC-SG depends on having the correct firmware versions of the Raritan devices, for example, Dominion KX, and applications, for example, Raritan Remote Client, to operate with your version of CC-SG. Please refer to the Compatibility Matrix for your particular version of CC-SG in the Support section of the Raritan website. You can use CC-SG to upgrade devices as needed once you add the devices to CC-SG.

This page intentionally left blank.

Chapter 2: Pre-Deployment Planning

Prepare Infrastructure

Planning for the installation of your CC-SG and Raritan devices is very much like the planning for any other new systems in your datacenter. HVAC, power, physical access and mounting, network, cabling, and remote access must be considered.

- **Heating and Cooling.** It is essential to have adequate heating and cooling so that the equipment can operate in the temperature and humidity ranges for which it has been designed. Please refer to the specific product User Guide for additional information.
- **Power Supplies.** Raritan products have auto-ranging power supplies so they can function in most datacenter environments. Some products have dual power supplies for power redundancy such as CC-SG.
- **Serial Device Connectivity.** Uses either a straight through Ethernet cable or a crossover cable. Sun and Cisco serial interfaces typically use a crossover cable that connects directly to an RJ45 port. Other serial targets typically use a standard Ethernet cable attached to a DB9 or DB25 serial connector.
- **Cabling Requirements.** Depends on the specific products deployed as well as datacenter distances and structured cabling design. Cables should be tested and within distance limitation guidelines for each device. IP-Reach, Dominion KSX, and Dominion KX101 devices should use Raritan-supplied KVM cabling.
- **LAN Ports.** All Raritan devices covered in this guide have an auto-sensing 10/100 Base-T network port for attachment to your LAN. Some devices, including CC-SG, have dual-LAN ports for redundancy. Some Raritan devices also have gigabit Ethernet.
- **Remote Access for Raritan Devices.** External remote access for some devices, in an emergency situation, can be accommodated via modem. Appropriate phone lines and modems should be obtained prior to installation.
- **Rack Mounts.** Most Raritan devices include rack mounts for installation into datacenter cabinets and racks. Some devices, such as the Dominion SX4 and SX8, have optional rack-mount kits available. Please refer to the specific product User Guide or Deployment Guide for additional information.

Basic Requirements for Dominion Products

All Dominion products include rack mounts for installation in standard 19 inch cabinets. Standard included power cables are for 110 VAC/15 amp receptacles. Power supplies are 110/220 auto switching.

- Dominion KX devices use standard CAT 5 or better cabling for connecting between the target and Dominion KX. The standard supported distance is 150 feet. Each target requires a CIM.
- Dominion SX serial devices use standard CAT 5 or better cabling for connecting to serial devices. Raritan DB9/DB25-RJ45 adapters need to be connected to the device serial port for connection to the CAT 5 cable. Serial devices that use a RJ45 rollover interface should be connected directly to the Dominion SX with a rollover cable. This applies to most Cisco and Sun products. Use a 1 foot Raritan rollover adapter cable to allow the use of standard CAT 5 or better cabling for these type devices.

Prepare Network

Network preparation is essential for Raritan devices and CC-SG to function properly over your LAN/WAN.

Allocate IP Addresses for Raritan Devices

IP addresses must be allocated and statically assigned for all Raritan devices. To eliminate any possible address conflicts, first test any allocated IP address to make sure it is not currently being used. Refer to **Appendix A: Installation Template** to document the IP addresses, default gateway, subnet mask, and administrative username and password for each device. This information is needed during setup and configuration.

Note: Dominion devices support 10/100 Ethernet. It is strongly recommended that all Dominion KX devices be hard coded on both the Dominion KX and Ethernet switch to eliminate auto negotiation problems.

Open Ports for Firewall or IP Port Filters

Raritan devices are accessed from a standard web browser. If a firewall or IP port filter is enabled between the user PC, CC-SG, and Raritan devices, ports must be opened to allow connectivity. These are documented in **Appendix B: CC-SG and Network Configuration** in the **CommandCenter Secure Gateway Administrator Guide**.

Prepare Target Servers

Target servers and systems that attach to KVM over IP Raritan devices, for example, Dominion KX, Dominion KX2, Dominion KX101, Dominion KSX, and IP-Reach, must have mouse and video settings adjusted for optimal performance and responsiveness over an IP network. This allows CC-SG to remotely control the target systems.

Adjust the mouse and video settings *before* connecting the target to the Raritan device.

Target Server Video Resolution

Ensure that each target server's video resolution and refresh rate is supported and that the signal is non-interlaced. Please refer to the specific Raritan product's User Guide for supported video resolutions. All Raritan devices support at least the following video resolutions:

640 x 480 @ 60Hz	800 x 600 @ 56Hz	1152 x 864 @ 60Hz
640 x 480 @ 72Hz	800 x 600 @ 60Hz	1152 x 864 @ 70Hz
640 x 480 @ 75Hz	800 x 600 @ 72Hz	1152 x 864 @ 75Hz
640 x 480 @ 85Hz	800 x 600 @ 75Hz	1152 x 900 @ 66Hz
	800 x 600 @ 85Hz	
720 x 400 @ 70Hz		1280 x 960 @ 60Hz
720 x 400 @ 85Hz	1024 x 768 @ 60Hz	1280 x 1024 @ 60Hz
	1024 x 768 @ 70Hz	
	1024 x 768 @ 75Hz	
	1024 x 768 @ 77Hz	
	1024 x 768 @ 85Hz	

Desktop Background

For optimal bandwidth efficiency and video performance, target servers running graphical user interfaces, such as Windows, Linux, X-Windows, Solaris, and KDE, should be configured with a predominately solid, plain, light-colored background. The desktop background need not be completely solid, but desktop backgrounds featuring photos or complex gradients might impact performance.

Operating System Mouse and Video Settings

This section provides video mode and mouse information specific to the Operating System in use on the target server.

Windows XP / Windows 2003 Settings

To configure target servers running Microsoft Windows XP/2003:

1. Configure the mouse settings:
 - a) Select Start > Control Panel > Mouse.
 - b) Open the **Pointer Options** tab. In the **Motion** group:
 - ✓ Set the mouse motion speed setting exactly to the middle speed.
 - ✓ Disable the **Enhanced pointer precision** option.
 - ✓ Click **OK**.
2. Disable transition effects:
 - a) Select the **Display** option from **Control Panel**.
 - b) Open the **Appearance** tab.
 - c) Click the **Effects** button.
 - d) Clear the **Use the following transition effect for menus and tooltips** option.
 - e) Click **OK**.
 - f) Close the **Control Panel**.

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

Windows XP and 2000 login screens revert to pre-set mouse parameters that differ from those suggested for optimal CC-SG performance. As a result, mouse synchronization may not be optimal for these screens. If you are comfortable adjusting the registry on Windows target servers, you can obtain better mouse synchronization at login screens by using the Windows registry editor to change the following settings (HKEY_CURRENT_USER\Control Panel\Mouse): *MouseSpeed = 0; MouseThreshold 1= 0; MouseThreshold 2 = 0.*

Windows 2000 Settings

To configure target servers running Microsoft Windows 2000:

1. Configure the mouse settings:
 - a) Select **Start > Control Panel > Mouse**.
 - b) Open the **Motion** tab.
 - ✓ Set the acceleration to **None**.
 - ✓ Set the mouse motion speed setting exactly to the middle speed.
 - ✓ Click **OK**.
2. Disable transition effects:
 - a) Select the **Display** option from **Control Panel**.
 - b) Open the **Effects** tab.
 - c) Clear the **Use the following transition effect for menus and tooltips** option.
 - d) Click **OK**.
 - e) Close the **Control Panel**.

Windows Vista

To configure target servers running Microsoft Windows Vista:

1. Configure the mouse settings:
 - a) Select **Start > Settings > Control Panel > Mouse**.
 - b) Open the **Pointer Options** tab. In the **Motion** group:
 - ✓ Set the mouse motion speed setting exactly to the middle speed.
 - ✓ Disable the **Enhanced pointer precision** option.
 - ✓ Click **OK**.
2. Disable animation and fade effects:
 - a) Select the **System** option from **Control Panel**.
 - b) Select **Advanced system settings**. The System Properties dialog box opens.
 - c) Open the **Advanced** tab.
 - d) Click the **Settings** button in the Performance group. The **Performance Options** dialog box opens.

- e) Under **Custom** options, clear the following checkboxes:

<i>Animation options:</i>	
<input type="checkbox"/>	Animate controls and elements inside windows
<input type="checkbox"/>	Animate windows when minimizing and maximizing
<i>Fade options:</i>	
<input type="checkbox"/>	Fade or slide menus into view
<input type="checkbox"/>	Fade or slide ToolTips into view
<input type="checkbox"/>	Fade out menu items after clicking

- f) Click **OK**.
- g) Close the **Control Panel**.

Linux Settings

To configure target servers running Linux (graphical user interface):

- Configure the mouse settings:
 - Select **System > Preferences > Mouse**. The Mouse Preferences dialog opens.
 - Open the **Motion** tab.
 - Set the **Speed Acceleration** to 1.
 - Set the **Drag & Drop Threshold** to 1.
- Configure the screen resolution:
 - Select **System > Preferences > Screen Resolution**. The Screen Resolution Preferences dialog opens.
 - Select a **Resolution** and **Refresh Rate** supported by Dominion KX2.

Note: In many Linux graphical environments, the command <CTRL> <ALT> <+> will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.

To configure target servers running Linux (command line):

- Set the mouse acceleration to exactly 1 and set the threshold to exactly 1. Enter this command: **xset mouse 1 1**. This should be set for execution upon login.
- Ensure that each target server running Linux is using a resolution supported by Dominion KX2 at a standard VESA resolution and refresh rate.
- Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values:
 - Go to the Xfree86 Configuration file XF86Config
 - Using a text editor, disable all non-Dominion KX2 supported resolutions
 - Disable the virtual desktop feature (not supported by Dominion KX2)
 - Check blanking times (+/- 40% of VESA standard)
 - Restart computer

Sun Solaris Settings

To configure target servers running Sun Solaris:

Set the mouse acceleration value to exactly 1 and the threshold to exactly 1. This can be performed:

- From the graphical user interface:

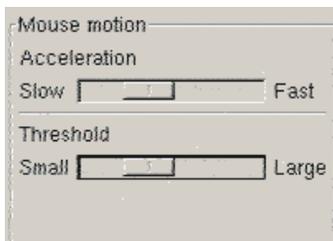


Figure 1: Solaris Mouse Configuration Window

- With the command line:

```
xset mouse a t
```

 (where “a” is the acceleration and “t” is the threshold.)

All target servers must be configured to one of the [display resolutions](#) supported by Dominion KX2. The most popular supported resolutions for Sun machines are:

1024 x 768 @ 60 Hz
1024 x 768 @ 70 Hz
1024 x 768 @ 75 Hz
1024 x 768 @ 85 Hz
1152 x 900 @ 66 Hz
1152 x 900 @ 76 Hz
1280 x 1024 @ 60 Hz

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

To change your Sun video card output from composite sync to the non-default VGA output:

1. Issue the **Stop+A** command to drop to bootprom mode.
2. Issue the following command to change the output resolution:

```
setenv output-device screen:r1024x768x70
```

3. Issue the “**boot**” command to reboot the server.

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

IF YOU HAVE:	USE THIS VIDEO OUTPUT ADAPTER:
Sun 13W3 with composite sync output	APSSUN II Guardian converter
Sun HD15 with composite sync output	1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync
Sun HD15 with separate sync output	APKMSUN Guardian converter

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

Apple Macintosh Settings

For target servers running an Apple Macintosh operating system, the preferred method is to use the D2CIM-VUSB and Absolute mouse mode.

IBM AIX Settings

To configure target servers running IBM AIX:

Go to the **Style Manager**, click on **Mouse Settings** and set **Mouse acceleration** to 1.0 and **Threshold** to 3.0.

Prepare User PC

Raritan devices and CC-SG are accessed via a web browser from a user's PC. The browser must have the correct version of Java Runtime Environment (JRE) installed to function correctly with Raritan devices. You must also disable all pop-up blockers and any firewall software that is enabled by default.

Install Java Runtime Environment

Install the currently approved version of Java on all PCs that are using CC-SG. You can download Java from <http://java.sun.com/j2se/index.jsp>. For the most current listing of compatible browsers, PC Platforms, and JRE versions, please refer to the **Compatibility Matrix** for your version of CC-SG in the Support section of the Raritan web site.

This page intentionally left blank.

Chapter 3: Prepare Raritan Devices

The Raritan devices must be configured and installed on the network prior to adding the devices to CC-SG.

Basic installation and configuration consists of the following steps:

1. Attach power cord and local access method.
2. Set device IP address.
3. Connect devices to network.
4. Attach CIMs to targets, and then attach targets to devices. Target servers should be powered on and connected to CIMs and CIMs should be connected to the Raritan device before configuring the ports in CC-SG. Otherwise, the blank CIM name overwrites the CC-SG port name. Servers may need to be rebooted after you connect the CIM, depending on the type of CIM.
5. Document the device IP address, device name, administrative username and password, device location, and attached servers and systems (port number, system name, system type). You can use the form provided in **Appendix A: Installation Template** as a guide. You will need this information when you add the devices to CC-SG.

Note: The Dominion KX101 is attached directly to one target and therefore, does not require a CIM.

Local Console or Web Browser Access

Most Raritan devices allow direct access via a local console to which you can attach a keyboard, video, and mouse, or via a web browser when operating in standalone mode (without CC-SG). You can use either of these mechanisms to access administrative functions for configuration of the Raritan device.

Default IP Address and Logins

- All Raritan IP-based products use the default IP address: 192.168.0.192.
- The default IP address to access CC-SG administrative functions is **192.168.0.192/admin**.
- Most Raritan products use the default username and password **admin/raritan**.
- CC-SG's default login for versions 3.1 and higher is **admin/raritan**. CC-SG versions prior to 3.1 use the default username and password **ccroot/raritan0**.

Direct Access is Restricted

Once a device is added to CC-SG, direct access to that device is prevented (except for Dominion SX devices). Restricting direct access helps keep your devices secure. Because of this security feature, it is very important to configure any options and settings appropriately before adding devices to CC-SG. From CC-SG, you can use **Pause Management** to release a device from CC-SG control temporarily. Please refer to Raritan's **CommandCenter Secure Gateway Administrator Guide** for additional information.

Fall Back to Stand-alone Mode

Should CC-SG become unreachable from a device for the amount of time configured as the heartbeat timeout (loss of connectivity by either a network or CC-SG failure), the device automatically falls back to stand-alone mode. This feature allows the device to continue functioning even during network outages. This feature also allows you to access the device from the console port or a browser to perform administrative functions if needed (disconnect the device from the network and use the console or a crossover network cable for browser access). Make sure all devices have a suitable configuration for stand-alone mode should you need to access them during a network outage.

Minimum Firmware Version

Raritan devices managed by CC-SG must have the current minimum firmware version to work correctly with CC-SG. Once you add Raritan devices to CC-SG, you can perform firmware upgrades from the CC-SG interface. Please refer to the Compatibility Matrix for CC-SG in the Support section of the Raritan website.

Preparing Dominion Devices for CC-SG Management

Prior to installation, please read the entire section for each device that will be managed by CC-SG.

***Note:** Consult the Raritan Quick Setup Guides for Dominion KX, Dominion KX2, Dominion KX101, Dominion SX, and Dominion KSX for additional information on configuration.*

Dominion KX Devices

The following section provides you with the necessary background information and steps to install and configure Raritan Dominion KX units to conform to CC-SG's requirements.

***Note:** Be sure to document the device name, IP address, administrative username and password, and attached systems (port number, type, system name) in **Appendix A: Installation Template**.*

Attach Power Cord and Local Console

1. Connect the included AC power cord to the Dominion KX unit and plug into an AC Power Outlet.



Figure 2 Dominion KX Physical Connections

2. Attach a multisync VGA monitor, mouse, and keyboard to the ports labeled **Local User** using either a PS/2 keyboard and mouse or a USB keyboard and mouse.
3. Power **ON** the Dominion KX unit. The device powers up and begins the boot process.

Set Dominion KX IP Address

After completing the boot process, you will see the Dominion KX's local access **On Screen Display (OSD)**.

1. Log in with the default username (**admin**) and password (**raritan**).
2. Press the **F5** key to activate the Administrative Menu.
3. Select option 3 **Network Settings**, and then press **ENTER** to display the screen.
4. Specify the IP address, subnet mask and default gateway for this Dominion KX unit.

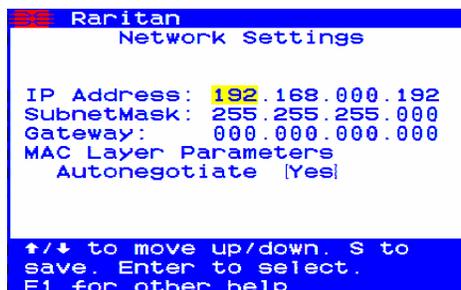


Figure 3 Dominion KX Network Settings Screen

4. Press the **S** key to save the settings. The Dominion KX unit will automatically reboot.

Connect to Network and Attach Servers

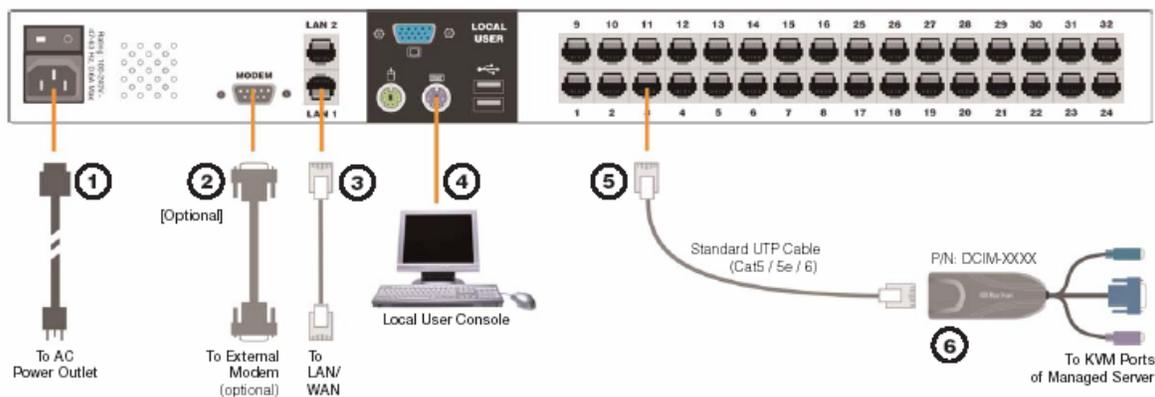


Figure 4 Dominion KX Connections

1. **[Optional]** Use a straight-through serial cable to connect an external modem.
2. Connect one end of a straight-through Ethernet cable (included) to the port labeled **LAN1** on the Dominion KX, and the other end to a network switch or router.
3. **[Optional]** For Ethernet redundancy, use a straight-through Ethernet cable to connect the **LAN2** port to another network switch or router. Should the Ethernet connectivity on LAN1 become unavailable, Dominion KX will failover to this port with the same TCP/IP settings — at all other times, this port will be disabled.
4. **[Optional]** Attach a keyboard and mouse (either PS/2 or USB), and a multi-sync monitor to the corresponding ports in the back of Dominion KX marked **Local User**. The Local User Console is used to access servers directly from the rack.
5. Connect one end of a standard, straight through UTP cable (Cat5 / 5e / 6) to an unoccupied server port; connect the other end to the RJ45 ports on a Dominion KX CIM.
6. Connect the remaining ports on the CIM to the corresponding KVM ports of a server that you want to manage using the Dominion KX.
7. Repeat these steps to connect all servers that you want to manage with this Dominion KX.

Dominion KX2 Devices

The following section provides you with the necessary background information and steps to install and configure Raritan Dominion KX2 units to conform to CC-SG's requirements.

Note: Be sure to document the device name, IP address, administrative username and password, and attached systems (port number, type, system name) in **Appendix A: Installation Template**.



Figure 5 Dominion KX2 Connections

Attach Power Cord and Local Console

1. Attach the included AC power cord to the Dominion KX2 and plug into an AC power outlet.
2. Attach a multi-sync VGA monitor, mouse, and keyboard to the respective Local User ports using either a PS/2 or USB keyboard and mouse.

Set Dominion KX2 IP Address

1. Power ON the Dominion KX2 using the power switch at the back of the unit. Please wait for the Dominion KX2 unit to boot. (A beep signals that the boot is complete.)
2. Once the unit has booted, the KX2 Local Console is visible on the monitor attached to the Dominion KX2 local port. Type the default username (**admin**) and password (**raritan**) and click **Login**. The Change Password screen is displayed.
3. Follow the prompts to change the default password. Please refer to Raritan's KX2 User Guide for details. Be sure to make a note of the new password.
4. You will receive confirmation that the password was successfully changed. Click **OK**. The Port Access page is displayed.
5. Select **Device Settings > Network Settings**.
6. Specify a meaningful **Device Name** for your Dominion KX2 unit; up to 16 alphanumeric characters, special characters, and no spaces.
7. Select None (Static IP) from the **IP auto configuration** drop-down list:
8. Type the TCP/IP parameters for your Dominion KX2 unit: **IP address**, **Subnet mask**, **Gateway IP address**, **Primary DNS server IP address**, and (optional) **Secondary DNS server IP address**.
9. Click **OK** to save the settings. Restart the Dominion KX2 unit.

Connect to Network and Attach Servers

Dominion KX2 uses standard UTP cabling (Cat5/5e/6) to connect to each target server.

1. Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router.
2. To connect a target server to Dominion KX2, connect the appropriate Computer Interface Module (CIM). Please refer to Raritan's Dominion KX2 User Guide for details.
3. Attach the HD15 video connector of your CIM to the video port of your target server. Ensure that your target server's video has already been configured to a supported resolution and refresh rate. For Sun servers, also ensure that your target server's video card has been set to output standard VGA (H-and-V sync) and not composite sync.
4. Attach the keyboard/mouse connector of your CIM to the corresponding ports on your target server. Using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an available server port on the back of your Dominion KX2 unit.

Dominion SX Devices

The following section provides you with the necessary background information and steps to install and configure Raritan Dominion SX units to conform to CC-SG's requirements.

Note: *Be sure to document the device name, IP address, administrative username and password, and attached systems (port number, type, system name) in **Appendix A: Installation Template**.*

Attach Power Cord and Installation Computer

1. Obtain a computer with a network card and a crossover network cable. This computer will be referred to as the **installation computer**.
2. Connect the crossover network cable to the primary LAN connection on the rear panel of the unit. On models with two Ethernet interfaces, the primary LAN is LAN 1.
3. Connect the other end of the crossover network cable to the network port on the installation computer.
4. Connect the included AC power cord to the Dominion SX unit and plug into an AC Power Outlet.
5. Power **ON** the Dominion SX unit.

Note: *The SX unit performs a hardware self-test, indicated by the green light on the back of the unit, and then starts the software boot sequence. The boot sequence is complete when the green light goes on and remains illuminated.*

Set Dominion SX IP Address

1. Access the SX unit through your installation computer's browser on the same subnet by typing the default URL **https://192.168.0.192** into the address field.
2. Log in with the default username (**admin**) and password (**raritan**).
3. Follow the prompts to change the default password. Be sure to make a note of the new password.
4. Click the **Setup** tab to display the Configuration and Logging topics.
5. Click the **Network** section of the Setup Configuration screen.
6. Type the data in the following fields: **IP Address:** Network address for this unit; **Subnet Mask:** Subnet mask for the network where this unit will reside; **Gateway IP Gateway:** Default gateway for this unit.
7. Accept all other default values or change as needed.
8. Click OK to save the settings. The SX unit reboots automatically once it has been configured.

Connect to Network and Attach Serial Devices

1. Power OFF the SX unit.
2. Disconnect from the installation computer, and move the Dominion SX to the location where it will be added to CC-SG.
3. Connect one end of a straight-through Cat5 cable to the SX.
4. Connect the other end of the Cat5 cable to the network.
5. To attach a device with a standard DB9 or DB25 serial console port, connect one end of a standard Cat5 Ethernet cable to a serial console port on the Dominion SX.
6. Connect the other end to a Raritan Nulling Serial Adapter (p/n ASCSDB9F, ASCSDB9M, ASCSDB25F, ASCSDB25M) as appropriate.
7. Connect the adapter to the console port of the device.

Dominion KSX Devices

The following section provides you with the necessary background information and steps to install and configure Raritan KSX units to conform to CC-SG's requirements.

Note: Be sure to document the device name, IP address, administrative username and password, and attached systems (port number, type, system name) in **Appendix A: Installation Template**.



Figure 6 Dominion KSX Back panel Connections

Attach Power Cord and Local Console

1. Connect the included AC power cord to the Dominion KSX unit and plug into an AC Power Outlet.
2. Attach a PS/2 keyboard and multi-sync monitor to the corresponding local Admin Console ports on the Dominion KSX. Depending on your KSX model, the local Admin Console ports may be on the front (remove the front bezel by pulling it towards you) or the rear panel of your KSX unit. The local Admin Console is used during initial setup, but may be removed after setup is complete.
3. Power ON the Dominion KSX.

Set Dominion KSX IP Address

1. After booting, the Dominion KSX displays the Setup Wizard on the Admin Console screen. Press **B** on the Admin Console keyboard to begin the initial configuration.
2. On the Network Configuration Screen, assign a unique name (for example, "Atlanta Office") and IP Address parameters for this Dominion KSX unit. Please refer to Raritan's Dominion KSX User Guide for additional information on administrative parameters.

3. Press **CTRL+S** to save the settings. The Main Menu appears.
4. Press **R** to restart.
5. Press **ENTER**.
6. Press **R** again to reboot the Dominion KSX.

Connect to Network and Attach Serial Devices

1. **[Optional]** Disconnect the PS/2 keyboard and multi-sync monitor from the Admin Console ports. Or leave them attached for future monitoring or configuration.
2. Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router.
3. To attach a device with a standard DB9 or DB25 serial console port to Dominion KSX, connect one end of a standard Cat5 Ethernet cable to a serial console port on the Dominion SX.
4. Connect the other end of the Cat5 Ethernet cable to a Raritan Nulling Serial Adapter (p/n ASCSDB9F, ASCSDB9M, ASCSDB25F, ASCSDB25M) as appropriate.

Preparing IP-Reach Devices for CC-SG Management

The following section provides you with the necessary background information and steps to install and configure Raritan IP-Reach units to conform to CC-SG's requirements.

Note: Be sure to document the device name, IP address, administrative username and password, and attached systems (port number, type, system name) in **Appendix A: Installation Template**.

Please refer to Raritan's *IP-Reach Quick Setup Guide* for additional information.

IP Reach TR or M Series

Attach Power Cord and Local Console

1. Connect the included AC power cord to the IP-Reach unit.
2. Attach a PS/2 keyboard and multi-sync monitor to the corresponding ports in the back of the IP-Reach marked **Admin Console**.
3. Power **ON** the IP-Reach.

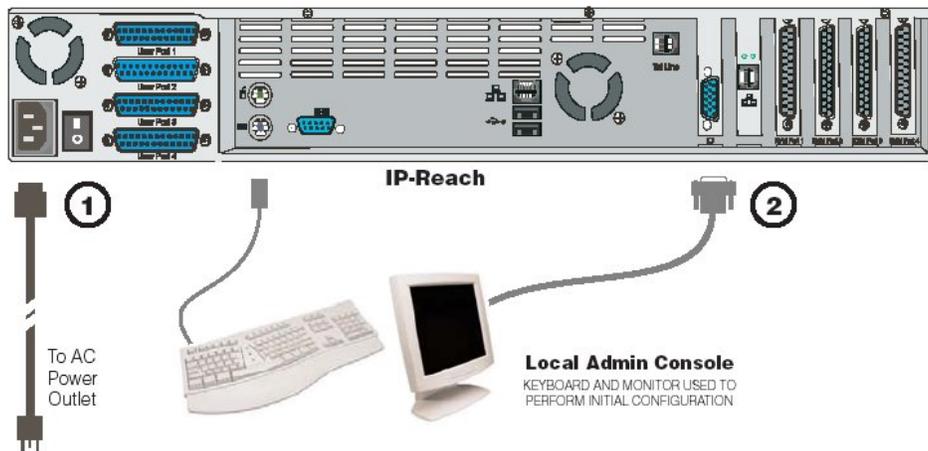


Figure 7 IP-Reach TR Series

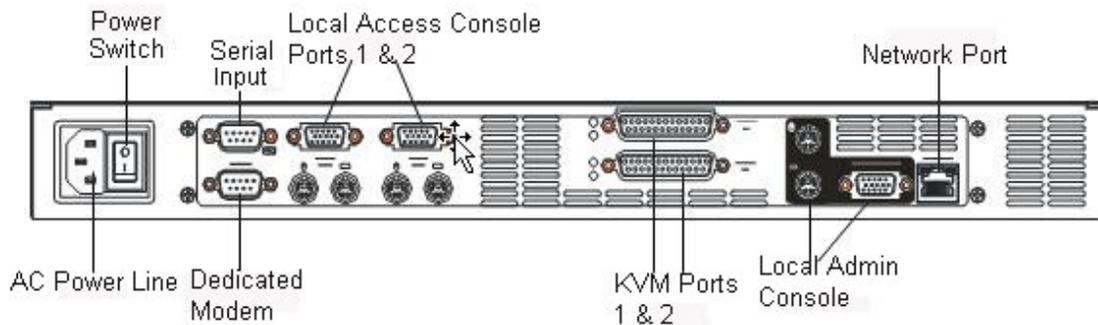


Figure 8 IP-Reach M Series

Set IP Reach IP Address

1. After the system boots, IP-Reach displays the Setup Wizard on the Admin Console screen.

Note: During initial configuration, the **IP-Reach Setup Wizard** helps you quickly set up IP-Reach for the first time. The IP-Reach Setup Wizard appears only when accessing the Administrative Menus on a non-configured IP-Reach.

```

Welcome to IP-Reach

IP-Reach has not been configured. Minimal configuration requirements
to make IP-Reach operational include entry of named-user software key
codes and assignment of an IP address or enabling the modem interface.

Following the IP-Reach Setup Wizard is the simplest way to perform
the configuration requirements needed to start working with IP-Reach.
Additional configuration options may be set at a later time through
the main menu - See Local Administrative Functions in your IP-Reach
User Manual.

Press B to begin the IPReach Setup Wizard.
Press X to bypass the Setup Wizard and proceed to the Main Menu.
  
```

Figure 9 IP-Reach Initial Configuration Screen

2. Press **B** on the Admin Console keyboard to begin configuring IP-Reach.

```

IP-Reach v3.20.59      Name [IPR-Joel      ]      IP Address [192.168. 51.150]
- Network Configuration -

Name                  [IPR-Joel      ]
Enable Ethernet Interface [YES]
Line Speed & Duplex    [Auto Detect  ]
Obtain IP address automatically (DHCP) [NO ]
IP Address             [192.168. 51.150]
Subnet Mask            [255.255.255. 0 ]
Default Gateway        [ 0 . 0 . 0 . 0 ]

Enable Modem Interface [NO ]
Enable Web Browser Interface [YES]
Use Default TCP Port 5000 [YES]

Enable IP Failover     [NO ]

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field
  
```

Figure 10 IP-Reach Network Configuration Screen

3. Based on your configuration, type the requested information.

Note: Do not obtain the IP-Address via DHCP. Obtain the IP-Address, the subnet mask, and default gateway from your network system administrator.

4. Press **CTRL+S** to save the settings.
5. On the Network Configuration Screen, assign a unique name (e.g. Server_Room) and IP Address parameters for IP-Reach.
6. The Main Menu appears. Browse through the Admin Console options to configure IP-Reach as appropriate to your environment. Please refer to Raritan's **IP-Reach User Guide** for additional information.

Connect to Network and Attach Servers or Switches

1. Connect a standard Ethernet cable from the network port to an Ethernet switch, hub, or router.
2. Connect the included CCP20 cable(s) from the **KVM In** port on the IP Reach unit to the KVM console of server or KVM switch to be accessed remotely.

Chapter 4: Install CC-SG

Basic installation of CC-SG comprises 3 steps:

1. Rack-mount the CC-SG unit.
2. Physically connect all cables. Each CC-SG model has a different setup. Follow the instructions for your CC-SG model number.
3. Set the CC-SG IP address.

Next Steps: When you have completed the installation, please refer to Raritan's CC-SG Administrators Guide for additional information on configuring your CC-SG. Use Guided Setup to easily set up your CC-SG environment.

1. Rack Mount the CC-SG Unit

Follow the instructions on the Quick Setup Guide that came with your CC-SG unit.

2. Physical Connections

Physical Connections for CC-SG E1 Units

Numbers on the diagram below correspond to the step numbers in this procedure.

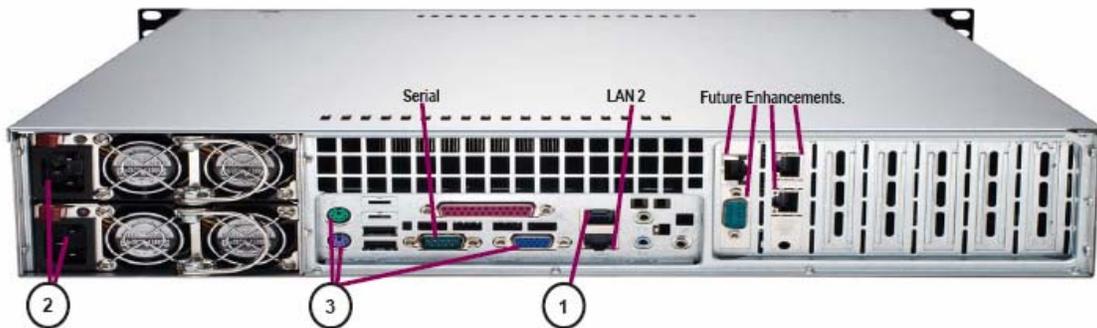


Figure 11 Physical Connections for CCSG E1 Units

1. Connect the CAT 5 network LAN cable to the LAN 1 port on the rear panel of the CC-SG unit. Connect the other end of the cable to the network.
2. Attach the 2 included AC power cords to the power ports on the rear panel of the CC-SG unit. Plug the other ends of the AC power cords into independent UPS protected outlets.
3. Connect a video monitor and keyboard using KVM cables to the corresponding ports on the rear panel of the CC-SG unit.

Physical Connections for CC-SG V1 Units

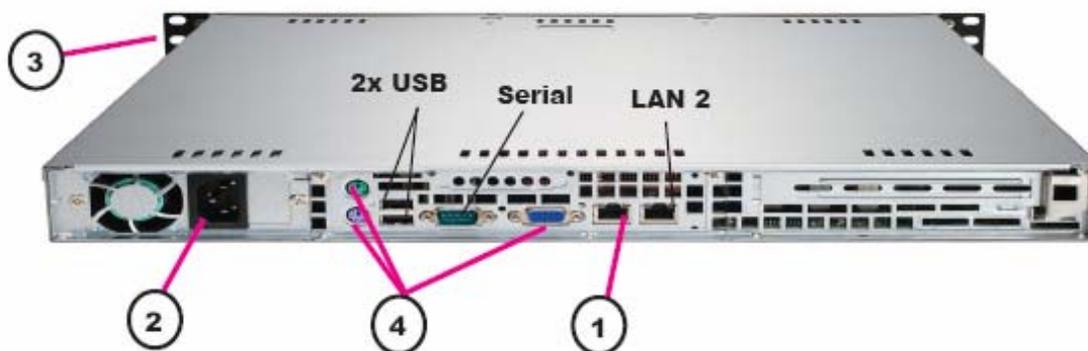


Figure 12 Physical Connections for CCSG V1 Units

1. Connect the network LAN cable to the LAN 1 port on the rear panel of the CC-SG unit. Connect other end of cable to the network.
2. Attach the included AC power cord to the port on rear panel of the CC-SG unit. Plug the other end of the cord into an AC power outlet.
3. Power ON CC-SG by popping off front bezel and pressing the POWER button.
4. Connect a video monitor and keyboard using KVM cables to the corresponding ports on the rear panel of the CC-SG unit.

*Note: The CC-SG V1 hardware ships with Gigabit Ethernet NIC adaptors. As long as the NIC interfaces are using the default **auto-negotiation** setting, practically any cable can successfully be used between the interfaces and an Ethernet port. Depending on the cable, full 1000Mbps connectivity may not be possible, but minimally you should get 100Mbps.*

Physical Connections for CC-SG G1 Units



Figure 13 Physical Connections for CCSG G1 Units

1. Connect the network LAN cable to the LAN 0 port on the rear panel of the CC-SG unit. Connect the other end of cable to the network.
2. Attach an included AC power cord to the power port 1 on the rear panel of the CC-SG unit. Plug the other end of the cord into an AC power outlet.
3. Connect a video monitor and keyboard using KVM cables to the corresponding ports on the rear panel of the CC-SG unit.

3. Set IP Address of CC-SG

1. When you see the CommandCenter login prompt on the video output, log in with the default username/password of **admin/raritan**. Usernames and passwords are case-sensitive. You will be prompted to change the local console password. You can still use admin/raritan the first time you access CC-SG via a browser or other client.
2. Press **CTRL+X**.
3. On the **Operation** menu, click **Network Interfaces** and then select **Network Interface Config**.
4. The Administrator Console appears. In the **Configuration** field, select **DHCP** or **Static**.
5. If you select **Static**, type a static IP address.
6. **[Optional]** Specify DNS servers, netmask, and gateway address.
7. Select **Save**. Please wait a few minutes as CC-SG restarts.

This page intentionally left blank.

Appendix A: Installation Template

Blank Template

Fill in the following template with information relevant to your installation. Once you have completed this step, you are ready to begin configuring CC-SG.

CommandCenter Secure Gateway

IP address	Net Mask	default gateway	admin name	admin password
			Default username is admin	Default password is raritan

Associations

Category Name	string/integer	node/device/both	Element	Element	Element

Raritan Devices

Name	Type	IP-Address	Admin Username-Password	Category/Element 1	Category/Element 2

Ports

Name	Device Name	Device Port Number

Nodes (In CC-SG, target servers are referred to as nodes.)

Name	Associated Port	Category/Element 1	Category/Element 2

User Groups

Name	Privileges	Policy Name 1	Policy Name 2

Users

Username	Password	User Group

Device Groups

Name	Member 1	Member 2	(Specify members by Category/Element)

Node Groups (In CC-SG, target servers are referred to as nodes.)

Name	Member 1	Member 2	(Specify members by Category/Element)

Policies

Name	Day	Time	Control/ Deny	Device Group	Port Group

Sample Template

CommandCenter Secure Gateway					
IP address	netmask	default gateway	admin name	admin password	
			admin	raritan	
Associations					
Category Name	string/integer	node/device/both	Element	Element	Element
location	string	both	Datacenter1	Datacenter2	engineering
node_type	string	node	Microsoft	Unix	Network
Devices					
Name	Type	IP Address	Admin Name/Password	Category/Element1	Category/Element2
DC1_SX1	SX		ccadmin/ rar123	location/ Datacenter1	
Eng_KX1	KX		ccadmin/ rar123	location/ engineering	
Ports					
Name (system)	Device Name	Device Port #			
MS_serv1	Eng_KX1	1			
Sun_Serv2	Eng_KX1	2			
Cisco_Rtr1	DC1_SX1	1			
DC2_Web1	DC1_SX1	2			
User Groups					
Name	Privileges	Policy name1	Policy name2		
Sysadmin	all (default)	full access (default)			
Unixadmins	Node access only	unixadmin_pol			
Msadmins	Node access only	msadmin_pol			
Netadmins	Node access only	netadmin_pol			

Users					
Name	Password	User Group			
Henryh	rar123	sysadmin			
Georgeh	rar123	sysadmin			
Ricka	rar123	msadmins			
Danf	rar123	unixadmins			

Device Groups					
Name	Member#1	Member#2	(Specify members by Category/Element)		

Node Groups					
Name	Member#1	Member#2	(Specify members by Category/Element)		
unixport_grp	node_type=unix				
msport_grp	node_type=microsoft				
netport_grp	node_type=network				

Policies					
Name	Day	Time	Control/Deny	Device Group	Node Group
unixadmin_pol	all	all	control		unixport_grp
msadmin_pol	all	all	control		msport_grp
netadmin_pol	all	all	control		netport_grp

Appendix B: Remote Power Management

In CC-SG, you can implement remote power management for nodes using Raritan powerstrips and Dominion series products.

Device Configurations for Power Control in CC-SG

When you connect a PowerStrip to a Dominion SX, you can use CC-SG to manage power to nodes connected to the same SX or any other SX, KX, KX2 or KSX device.

When you connect a PowerStrip to a Dominion KX or KX2 device, you can use CC-SG to manage power only to nodes that are connected to the same KX or KX2 device to which the PowerStrip is connected.

Some examples of acceptable configurations include:

- Connect a PowerStrip to Dominion SX to power nodes connected to the same Dominion SX.
- Connect a PowerStrip to Dominion SX to power nodes connected to a Dominion KX.
- Connect a PowerStrip to Dominion KX to power nodes connected to the same Dominion KX.
- Connect multiple PowerStrips to a Dominion KX to provide power failover to nodes with redundant power supplies connected to the same KX.
- Connect one PowerStrip to a Dominion SX, connect a second PowerStrip to another Dominion SX to provide power failover to nodes with redundant power supplies connected to any other device.

Example: Remote Power Management Using SX, KX, and PowerStrip

The following diagram illustrates the physical connections for managing remote power control.

1. Connect the red RJ45 connector end of the CSCSPCS-10 cable to the RJ45 port on the PowerStrip.
2. Connect the other end of the CSCSPCS-10 power control cable to any serial port on the Dominion SX.
3. Connect the node to a Dominion KX with standard CAT5 cable with a DCIM-PS2 attached.
4. Plug the power cord of the node into an outlet port of the PowerStrip.
5. Plug the power cord of the PowerStrip into an AC outlet. Please refer to the powerstrip's documentation for details.

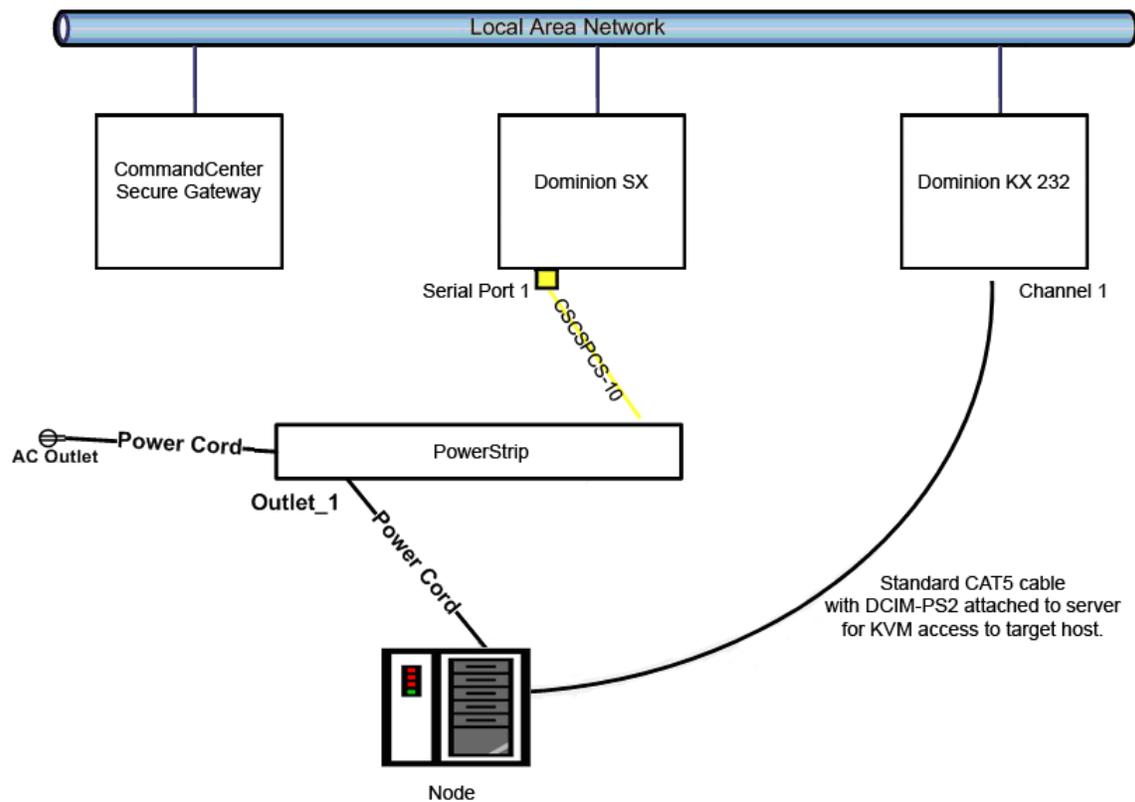


Figure 14 CC-SG and Remote Power Management

CC-SG Configuration

Please refer to the CC-SG Administrators Guide, Chapter 6: Configuring Power Control for details on adding the remote power management configuration to CC-SG.

Example: Remote Power Management for Multiple Power Connections

Many data center devices, network routers, switches, and servers are equipped with redundant power or multiple power supplies requiring several AC electrical connections. In the following scenario two separate power strips are provided for the node. A fully redundant configuration would include an additional Dominion SX with PowerStrip02 connected, thereby providing a separate and redundant control of the power strips. This example is limited to the simpler configuration of a single Dominion SX managing two power strips..

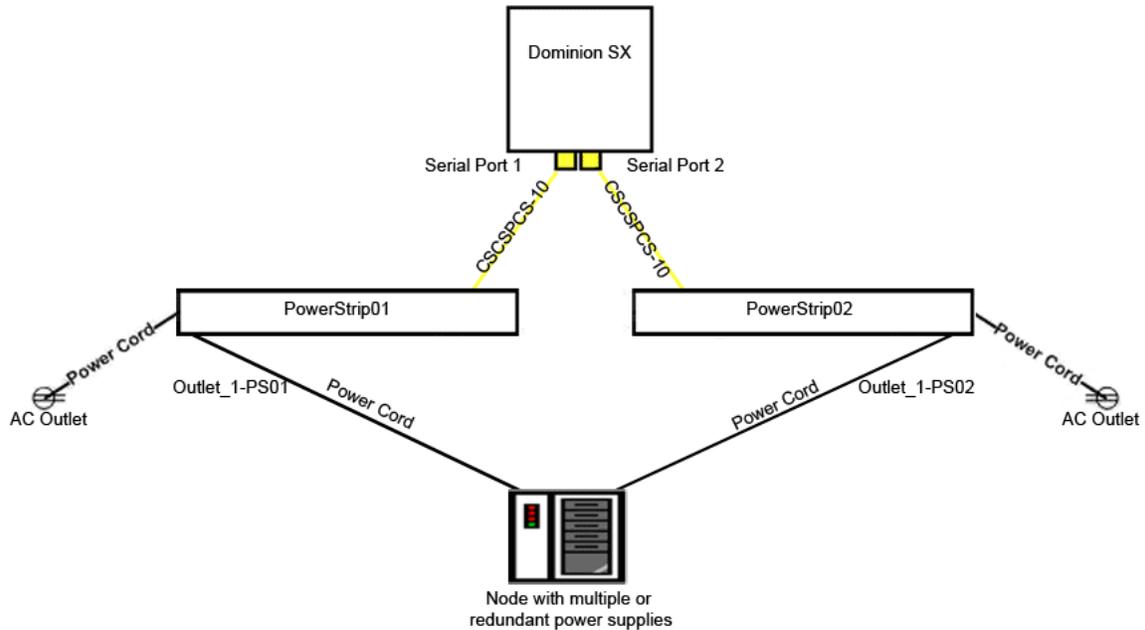


Figure 15 Redundant Power for Target Device

CC-SG Configuration

Please refer to the CC-SG Administrators Guide, Chapter 6: Configuring Power Control for details on adding the remote power management configuration to CC-SG.

World Headquarters

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. (732) 764-8886
Fax. (732) 764-8887
Email: sales@raritan.com
Web: raritan.com

Raritan America

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. (732) 764-8886
Fax. (732) 764-8887
Email: sales@raritan.com
Web: raritan.com

Asia Pacific Headquarters

Raritan Asia Pacific, Inc.
5F, 121, Lane 235, Pao-Chiao Road,
Hsin Tien 231,
Taipei, Taiwan, ROC
Tel. (886) 2 8919-1333
Fax. (886) 2 8919-1338
Email: sales.asia@raritan.com
Web: raritan-ap.com

Raritan China Offices

Raritan Beijing
No. 35 Financial St, Xicheng District
Room 1035, Block C,
Corporate Square
Beijing 100032, China
Tel: (86) 10-8809-1890
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Shanghai
Rm 17E Cross Region Plaza
899 Lingling Rd., Shanghai, China
(200030)
Tel. (86) 21 5425-2499
Fax. (86) 21 5425-3992
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Guangzhou
1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou (510075), China Raritan
Tel. (86) 20 8755-5581
Fax. (86) 20 8755-5571
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Korea

#3602, Trade Tower, World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
Tel. (82) 2 557-8730
Fax. (82) 2 557-8733
Email: sales.korea@raritan.com
Web: raritan.co.kr

Raritan Japan

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku, Tokyo 104-
0033
Tel. (81) 03-3523-5991
Fax. (81) 03-3523-5992
Email: sales@raritan.co.jp
Web: raritan.co.jp

Raritan Osaka
3rd Floor,
Osaka Kagaku Sen'I Kaikan Bldg.
4-6-8 Kawara-machi, Chuo-ku,
Osaka 541-0048
Tel. (81) 03-3523-5953
Fax. (81) 03-3523-5992
Web: raritan.co.jp

Raritan Australia Offices

Raritan Melbourne
Level 2, 448 St Kilda Rd.,
Melbourne, VIC3004
Australia
Tel. (61) 3-9866-6887
Fax. (61) 3-9866-7706
Email: sales.au@raritan.com
Web: raritan.com.au

Raritan Sydney
Suite 1, Level 9,
75 Miller Street North Sydney
PO Box 591,
North Sydney, NSW 2059,
Australia
Tel: (61) 2-9029-2558
Fax: (61) 2-8012-1103
Email: sales.au@raritan.com
Web: raritan.com.au

Raritan India

210 2nd Floor Orchid Square
Sushant Lok 1, Block B, Mehrauli
Gurgaon Rd, Gurgaon 122 002
Haryana, India
Tel. (91) 124 410-7881
Fax. (91) 124 410-7880
Email: enquiry.india@raritan.com
Web: raritan.co.in

Raritan Taiwan

5F, 121, Lane 235, Pao-Chiao Road
Hsin-Tien City
Taipei Hsien, Taiwan, ROC
Tel. (886) 2 8919-1333
Fax. (886) 2 8919-1338
Email: sales.taiwan@raritan.com
Web: raritan.com.tw

Raritan Singapore

350 Orchard Road
#11-08, Suite 21, Shaw House
Singapore 238868
Tel: (65) 6725 9871
Fax : (65) 6725 9872
Email: sales.ap@raritan.com
Web: raritan-ap.com

European Headquarters

Raritan Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. (31) 10-284-4040
Fax. (31) 10-284-4049
Email: sales.europe@raritan.com
Web: www.raritan.fr
www.raritan.de

Raritan France

120 Rue Jean Jaures
92300 Levallois-Perret, France
Tel. (33) 14-756-2039
Fax. (33) 14-756-2061
Email: sales.france@raritan.com
Web: www.raritan.fr

Raritan Deutschland GmbH

Lichtstraße 2
D-45127 Essen, Germany
Tel. (49) 201-747-98-0
Fax. (49) 201-747-98-50
Email: sales.germany@raritan.com
Web: www.raritan.de

Raritan Italia

Via dei Piatti 4
20123 Milan
Italy
Tel. (39) 02-454-76813
Fax. (39) 02-861-749
Email: sales.italy@raritan.com
Web: raritan.it
www.raritan.info

Raritan Canada

Raritan Inc.
4 Robert Speck Pkwy., Suite 1500
Mississauga, ON L4Z 1S1
Canada
Tel. 1-905-949-3650
Email: sales.canada@raritan.com
Web: raritan.ca

Raritan U.K.

9th Floor, 12-20 Camomile St
London EC3A 7EX, United Kingdom
Tel. (44) (0)20-7614-7700
Email: sales.uk@raritan.com
Web: raritan.co.uk