



# CC-SG

## CommandCenter Secure Gateway

### Deployment Guide Release 3.2.1

Copyright © 2008 Raritan, Inc.  
DSD-0F-E  
January 2008  
255-80-5160-00

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

© Copyright 2008 Raritan, Inc., CommandCenter®, Dominion®, Paragon® 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 trademarks or registered trademarks are the property of their respective holders.

#### FCC Information

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

#### VCCI Information (Japan)

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

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



# Contents

Chapter 1	Introduction	5
	Prerequisites.....	5
	Intended Audience .....	6
	CC NOC Deployment and Paragon Integration .....	6
Chapter 2	Pre-Deployment Planning	7
	Prepare Infrastructure.....	8
	Basic Requirements for Dominion Products .....	9
	Prepare Network .....	9
	Allocate IP Addresses for Raritan Devices .....	9
	Open Ports for Firewall or IP Port Filters .....	9
	Prepare Target Servers.....	10
	Target Server Video Resolution .....	10
	Prepare User PC.....	11
	Install Java Runtime Environment.....	11
Chapter 3	Prepare Raritan Devices	12
	Local Console or Web Browser Access.....	12
	Default IP Address and Logins .....	13
	Direct Access is Restricted.....	13
	Fall Back to Stand-alone Mode .....	13
	Minimum Firmware Version .....	14
	Preparing Dominion Devices for CC-SG Management .....	14
	Dominion KX Devices .....	14
	Dominion KX II Devices.....	17
	Dominion KX II-101 .....	19
	Dominion SX Devices .....	32
	Dominion KSX Devices .....	34
	Dominion KSX II Devices.....	36
	Preparing IP-Reach Devices for CC-SG Management.....	43
	IP Reach TR or M Series .....	43

## Contents

Chapter 4	Install CC-SG	48
1.	Rack Mount the CC-SG Unit.....	48
2.	Physical Connections .....	48
3.	Set IP Address of CC-SG .....	50
Appendix A	Installation Template	51
	Blank Template .....	51
	Sample Template .....	53
Appendix B	Remote Power Management	57
	Device Configurations for Power Control in CC-SG.....	57
	Example: Remote Power Management Using SX, KX, and Powerstrip.....	58
	CC-SG Configuration.....	58
	Example: Remote Power Management for Multiple Power Connections .....	59
	CC-SG Configuration.....	59
Appendix C	CC-SG and Network Configuration	60
	Required Open Ports for CC-SG Networks: Executive Summary .....	60
	CC-SG Communication Channels.....	61
	CC-SG and Raritan Devices .....	62
	CC-SG Clustering .....	62
	Access to Infrastructure Services .....	62
	PC Clients to CC-SG .....	63
	PC Clients to Nodes.....	63
	CC-SG & Client for IPMI, iLO/RILOE, DRAC, RSA.....	64
	CC-SG & SNMP .....	64
	CC-SG & CC-NOC .....	65
	CC-SG Internal Ports .....	65
	CC-SG Access via NAT-enabled Firewall.....	66

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

---

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

---

## In This Chapter

Prerequisites .....	5
Intended Audience .....	6
CC NOC Deployment and Paragon Integration .....	6

---

## 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.

# Chapter 2    Pre-Deployment Planning

## In This Chapter

Prepare Infrastructure.....	8
Prepare Network.....	9
Prepare Target Servers.....	10
Prepare User PC.....	11

---

## 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 *Installation Template* (on page 51) 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. See *CC-SG and Network Configuration* (on page 60) for details.

---

### Prepare Target Servers

Target servers and systems that attach to KVM over IP Raritan devices, for example, Dominion KX, Dominion KX II, Dominion KX101, Dominion KX2-101, Dominion KSX, Dominion KSX II, 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	

---

## 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>  
<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 website.

# 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, such as KVM drawer or laptop.
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.

---

Note: The Dominion KX101 and KX2-101 are attached directly to one target and therefore, does not require a 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 *Installation Template* (on page 51) as a guide. You will need this information when you add the devices to CC-SG.

## In This Chapter

Local Console or Web Browser Access .....	12
Default IP Address and Logins.....	13
Direct Access is Restricted.....	13
Fall Back to Stand-alone Mode .....	13
Minimum Firmware Version .....	14
Preparing Dominion Devices for CC-SG Management.....	14
Preparing IP-Reach Devices for CC-SG Management.....	43

---

## 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 **admin** and password **raritan**.
- CC-SG's default login for versions 3.1 and higher is username **admin** and password **raritan**. CC-SG versions prior to 3.1 use the default username **ccroot** and password **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, which you can configure to allow local access even while under CC-SG control). 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.

➤ *To gain direct access to a device under CC-SG management:*

Use CC-SG's Pause Management feature to release a device from CC-SG management temporarily.

See 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. See 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 Quick Setup Guides for Dominion KX, Dominion KX II, Dominion KX101, Dominion KX2-101, Dominion SX, Dominion KSX, and Dominion KSX2 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 *Installation Template* (on page 51).

---

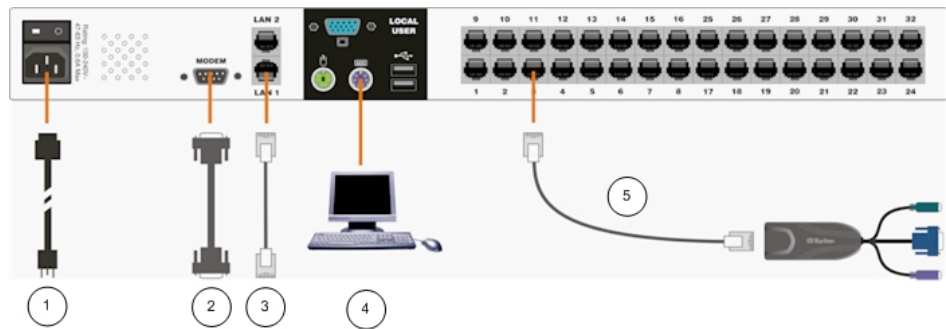


Diagram Key	
1	AC Power Cord
2	Modem Port (optional)

3	LAN 1 Network Port
4	Local Access Console Ports
5	Server Ports

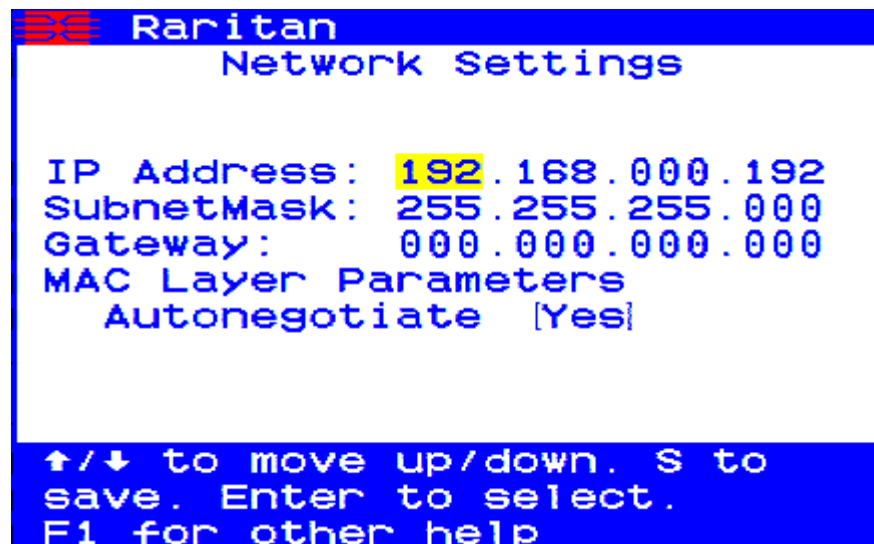
➤ *Attach Power Cord and Local Console*

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



## Preparing Dominion Devices for CC-SG Management

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

### ➤ *Connect to Network and Attach Servers*

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 KX II Devices

The following section provides you with the necessary background information and steps to install and configure Raritan Dominion KX II 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 *Installation Template* (on page 51).

---



➤ *Attach Power Cord and Local Console*

1. Attach the included AC power cord to the Dominion KX II 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 KX II IP Address*

1. Power ON the Dominion KX II using the power switch at the back of the unit. Please wait for the Dominion KX II unit to boot. (A beep signals that the boot is complete.)
2. Once the unit has booted, the KX II Local Console is visible on the monitor attached to the Dominion KX II local port. Type the default username (admin) and password (raritan) and click Login. The Change Password screen is displayed.

## Preparing Dominion Devices for CC-SG Management

3. Follow the prompts to change the default password. Please refer to Raritan's KX II 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 KX II 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 KX II 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 KX II unit.

### ➤ *Connect to Network and Attach Servers*

Dominion KX II 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 KX II, connect the appropriate Computer Interface Module (CIM). Please refer to Raritan's Dominion KX II 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 KX II unit.

---

### Dominion KX II-101

The following section provides you with the necessary background information and steps to install and configure Raritan Dominion KX II-101 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 *Installation Template* (on page 51).

---

## Preparing Dominion Devices for CC-SG Management

### Connecting the Dominion KX II-101

The Dominion KX II-101 has the physical connections described in the diagram below:



- 1 Attached Monitor and PS/2 Cable (See item 3.).
- 2 Mini-USB Port. Use to connect the device to the target server with the included USB cable if not using the attached PS/2 cable. A USB connection must be used in order to utilize the Absolute Mouse Sync or Virtual Media features.

- 3 Attached Monitor and PS/2 Cable. Use to connect the device to a monitor and to a target server if not using the USB cable.
- 4 LOCAL USER port. Use to connect a local keyboard, video, and mouse directly to the target server using an optional PS/2 cable.
- 5 Ethernet LAN/PoE Port. Provides LAN connectivity and power if using a PoE LAN connection.
- 6 Power Connector. Connects the power supply if you are not using a PoE (power over Ethernet) LAN connection.
- 7 Backlit LED power ON and boot-up indicator. Provides feedback on the operating status of the device.
- 8 Admin Port. Use to do one of the following:
  - Configure and manage the device with a terminal emulation program on your PC.
  - Configure and manage a power strip.
  - Connect an external modem to dial into the device.

### Connecting to the Target Server

The Dominion KX II-101 can use either the integrated PS/2 cables or the included USB cable to connect to the target server. Before connecting, configure your target server's video to a supported resolution and refresh rate as described in Setting Server Video Resolution in Raritan's *Dominion KX II-101 User Guide*.

#### *PS/2 Configuration*

➤ *To configure the Dominion KX II-101 for use with a PS/2 target server:*

1. Use the attached PS/2 keyboard, video, and mouse cabling to connect the Dominion KX II-101 to the target server.
2. Use the optional PS/2 cabling to attach the local keyboard, video, and mouse to the Local User port of the Dominion KX II-101.

---

Note: The Dominion KX II-101 must be powered for the Local User port to function.

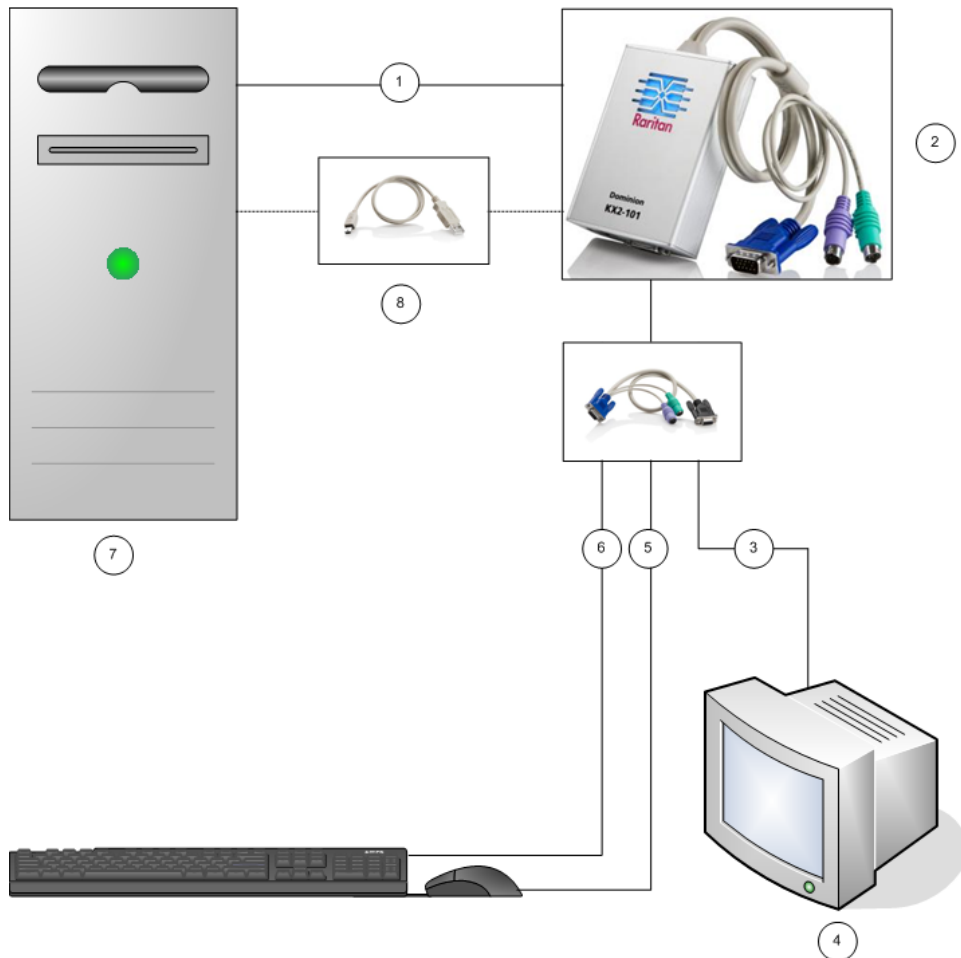
---

3. If you require Virtual Media (VM) connectivity, connect the mini-USB connector to the Dominion KX II-101 and the USB connector to any USB port on the target server.

## Preparing Dominion Devices for CC-SG Management

When you finish, you should have connections like those shown in the illustration below:

### PS/2 Configuration



- 1 Integrated PS/2 keyboard, video, and mouse connections from Dominion KX II-101 to target server.
- 2 Dominion KX II-101.
- 3 Video connection to local monitor (optional cable).
- 4 Local monitor.
- 5 PS/2 connection from Dominion KX II-101 to mouse (optional cable).
- 6 PS/2 connection from Dominion KX II-101 to keyboard (optional cable).
- 7 Target server.
- 8 Included mini-USB to USB connector from Dominion KX II-101 to target server for Virtual Media connectivity.

### USB Configuration

➤ *To configure the Dominion KX II-101 for use with a USB target server:*

1. Connect the mini-USB connector to the Dominion KX II-101 and the USB connector to a USB port on the target server.
2. Use the included PS/2 DKX2-101-LPKVMC cabling to attach only the local video to the Local User port of the Dominion KX II-101.

---

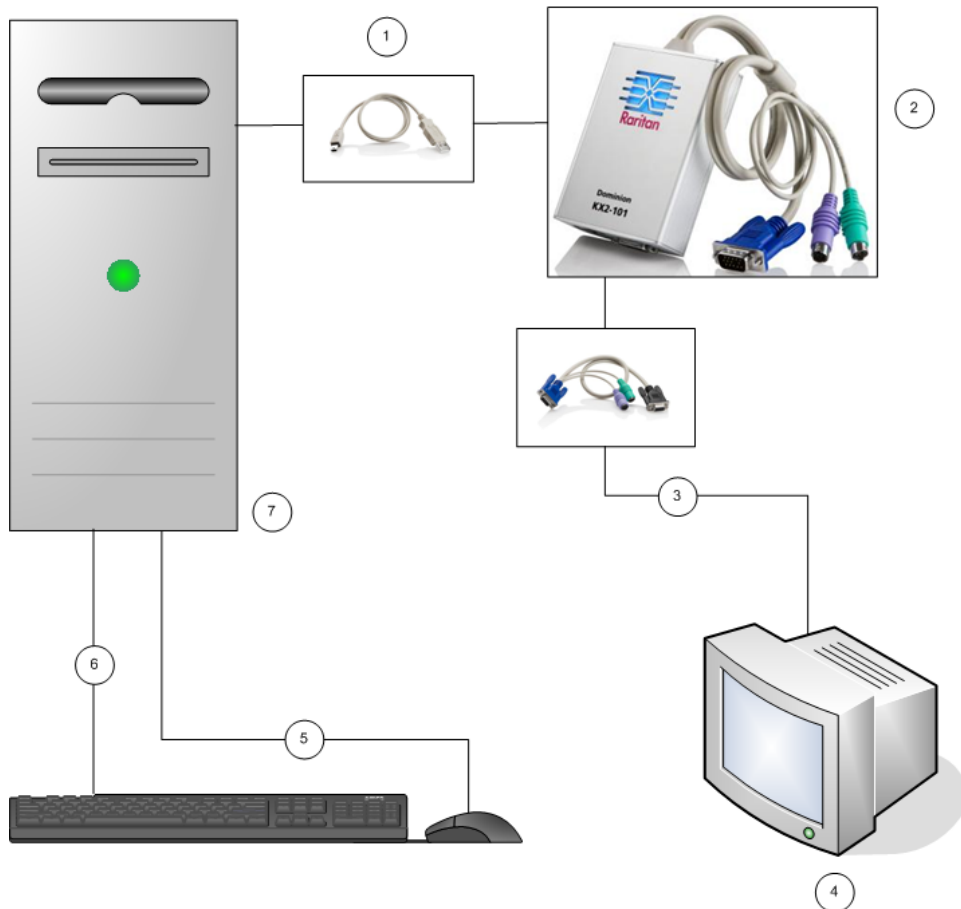
Note: The Dominion KX II-101 must be powered for the Local User port to function.

---

3. Use USB cables to connect the keyboard and mouse directly to the target server.

When you finish, you should have connections like those show in the following illustration:

### USB Configuration



## Preparing Dominion Devices for CC-SG Management

- 1 Included mini-USB to USB cable from Dominion KX II-101 to target server.
- 2 Dominion KX II-101.
- 3 Video connection to local monitor (optional cable).
- 4 Local monitor.
- 5 USB connection from target server to mouse.
- 6 USB connection from target server to keyboard.
- 7 Target server.

### Connecting to the Network

Connect a standard Ethernet cable from the network port labeled LAN to an Ethernet switch, hub, or router. The LAN LEDs that appear above the Ethernet connection indicate Ethernet activity. The yellow one blinks while the Dominion KX II-101 is in use, indicating IP traffic at 10Mbps. The green light indicates a 100Mbps connection speed.

### Powering the Dominion KX II-101

The Dominion KX II-101 can be powered with either the included standard AC power pack or by PoE (Power over Ethernet).

- For standard AC power, plug the included AC power adaptor kit into the Power Port and plug the other end into a nearby AC power outlet.
- For PoE, attach a 10/100Mbps cable to the LAN port, and plug the other end into a PoE-provisioned LAN.

After Dominion KX II-101 is powered ON, it goes through a boot-up sequence, during which the blue Raritan-logo LED will blink for about 45 seconds. Upon successful boot-up, the back-lit LED remains lit.



### Using the Admin Port

The Admin port enables you to perform configuration and setup for the Dominion KX II-101 using a terminal emulation program like HyperTerminal. Plug the min-DIN end of the included serial cable into the Admin port of the Dominion KX II-101 and plug the DB9 end into a serial port on your PC or laptop. The serial port communication settings should be configured to: to 115,200 Baud, 8 data bits, 1 stop bit, no parity, and no flow control.

For information about configuring the Dominion KX II-101 using the ADMIN port, see *Using a Terminal Emulation Program* in Raritan's *Dominion KX II-101 User Guide*.

### Configuring the Dominion KX II-101

The Dominion KX II-101 can be configured in two ways:

- Using the web-based Dominion KX II-101 Remote Console, which requires the unit to have a network connection to your workstation.
- Using a terminal emulation program like HyperTerminal, which requires a direct connection from the unit's ADMIN port to your workstation. The cable for this connection is included with the Dominion KX II-101.

This section describes both ways of configuring the Dominion KX II-101.

#### *Using the Remote Console*

The Dominion KX II-101 Remote Console is a web-based application that enables you to configure the unit prior to use. Before configuring the Dominion KX II-101 using the Remote Console, you must have both your workstation and the unit connected to a network.

To configure the Dominion KX II-101, you:

- Set a new password to replace the default
- Assign an IP address

#### **Setting a New Password**

When you first log into the Remote Console, you are prompted to set a new password to replace the default. Then you can configure the Dominion KX II-101.

1. Log on to a workstation with network connectivity to your Dominion KX II-101 unit.
2. Launch a supported Web browser such as Internet Explorer (IE) or Firefox.

## Preparing Dominion Devices for CC-SG Management

3. In the address field of the browser, enter the default IP address of the unit:

192.168.0.192

4. Press Enter. The login page opens.
5. Enter the user name `admin` and the password `raritan`.
6. Click Login.

The Change Password page is displayed.

7. Type `raritan` in the Old Password field.
8. 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 long and can consist of English alphanumeric and printable special characters.
9. Click Apply.

You will receive confirmation that the password was successfully changed.

10. Click OK. The Port Access page opens.

### Assigning an IP Address

1. In the Dominion KX II-101 Remote Console, choose Device Settings > Network Settings. The Network Basic Settings page opens.

Home > Device Settings > Network Settings

### Network Basic Settings

Device Name <sup>\*</sup>  
DominionKX2-101

IP auto configuration  
DHCP

Preferred host name (DHCP only)

IP address  
192.168.50.241

Subnet mask  
255.255.255.0

Gateway IP address  
192.168.50.126

Primary DNS server IP address  
192.168.50.114

Secondary DNS server IP address  
192.168.50.112

2. In the Device Name field, specify a meaningful name for your Dominion KX II-101 unit; up to 16 alphanumeric and special characters, no spaces.
3. Select the IP configuration from the IP auto configuration drop-down list:
  - None (Static IP). This is the default and recommended option because the Dominion KX II-101 is an infrastructure device and its IP Address should not change. This option requires that you manually specify the network parameters.
  - DHCP. With this option, network parameters are assigned by the DHCP server each time the Dominion KX II-101 is booted.

#### *Using a Terminal Emulation Program*

You can use the Admin serial console with a terminal emulation program like HyperTerminal to set the following configuration parameters for the Dominion KX II-101:

- IP address
- Subnet mask address
- Gateway address
- IP access control
- LAN speed
- LAN interface mode

To use a terminal emulation program with the Dominion KX II-101, you must first connect the included RS-232 serial cable from the Admin port on the Dominion KX II-101 to the COM1 port on your PC. See using the Using the Admin Port for information.

For demonstration purposes, the terminal emulation program described in this section is HyperTerminal. You can use any terminal emulation program.

#### *➤ To use a terminal emulation program to configure the Dominion KX II-101:*

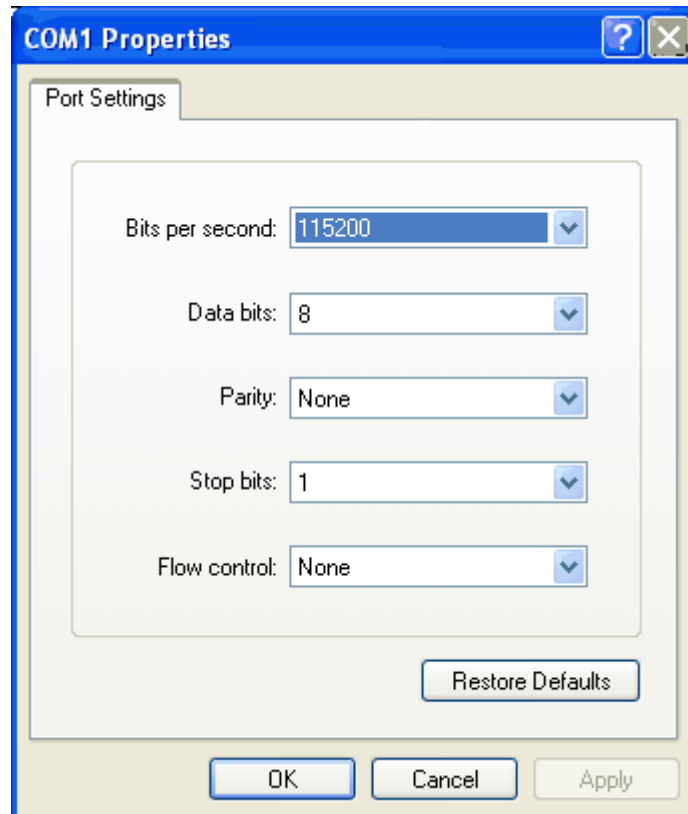
1. Connect the Dominion KX II-101 to a local PC using the included RS-232 serial cable.

Connect to the Admin port on the Dominion KX II-101 and the COM1 port on the PC.

2. Launch the terminal emulation program you want to use to configure the Dominion KX II-101.
3. Set the following port settings in the terminal emulation program:

## Preparing Dominion Devices for CC-SG Management

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None




4. Connect to the Dominion KX II-101.

The login screen appears.

A screenshot of a login screen with a double-line border. The text "Login:" is displayed in the top-left corner of the screen area.

5. Type the administrator user name and press Enter.

You are prompted to enter your password.

A screenshot of the login screen after the username has been entered. The text "Login: admin" and "Password: \_" is displayed in the top-left corner of the screen area.

6. Type your password and press Enter.

## Preparing Dominion Devices for CC-SG Management

The Admin Port prompt appears.

```
Login: admin
Password: MACADDR: 00:0d:5d:03:5d:23

-----
Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC          FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153         Idle Timeout: 30min
-----

Port Port      Port Port      Port
No.  Name      Type Status Availability
1 - Dominion_KXII-101_Port KVM up idle

Current Time: Fri Dec 28 19:44:16 2007
Admin Port >
```

7. At the Admin Port > prompt, type `config` and press Enter.
8. At the Config > prompt, type `network` and press Enter.
9. To view the current interface settings, at the Interface > prompt, type `interface` and press Enter.

The current interface settings appear:

```
Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC          FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153         Idle Timeout: 30min
-----

Port Port      Port Port      Port
No.  Name      Type Status Availability
1 - Dominion_KXII-101_Port KVM up idle

Current Time: Fri Dec 28 19:52:26 2007

Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface

IP auto configuration: dhcp
IP address: 192.168.50.153
Netmask: 255.255.255.0
Gateway: 192.168.50.126
Ethernet mode: Autodetect

Admin Port > Config > Network > _
```

10. To configure new network settings, at the Network prompt, type `interface` followed by one of the following commands and its appropriate argument (option), then press Enter.

Command	Argument	Options
ipauto	none dhcp	<p>none - Enables you to manually specify an IP address for the device. You must follow this option with the ip command and the IP address, as shown in the following example:</p> <pre>interface ipauto none ip 192.168.50.12</pre> <p>dhcp - Automatically assign an IP address to the device on startup.</p>
ip	IP address	The IP address to assign to the device. To manually set an IP address for the first time, this command must be used with the ipauto command and the none option. See ipauto for information. After you have manually assigned an IP address once, you can use the ip command alone to change the IP address.
mask	subnetmask	The subnet mask IP address.
gw	IP address	The gateway IP address
mode	mode	<p>The Ethernet mode. You have the following choices:</p> <p>auto - Automatically sets speed and interface mode based on the network.</p> <p>10hdx - 10 Mbs, half duplex.</p> <p>10fdx - 10 Mbs, full duplex</p> <p>100hdx - 100 Mbs, half duplex</p> <p>100fdx - 100 Mbs, full duplex</p>

When you have successfully changed a setting, you see a confirmation message like the following:

```
Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface ipauto none ip 192.168.50.126
Network interface configuration successful.
```

1. When you are finished configuring the Dominion KX II-101, type `logout` at the command prompt and press Enter.

You are logged out of the command line interface.

---

### 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 *Installation Template* (on page 51).

---

➤ *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*

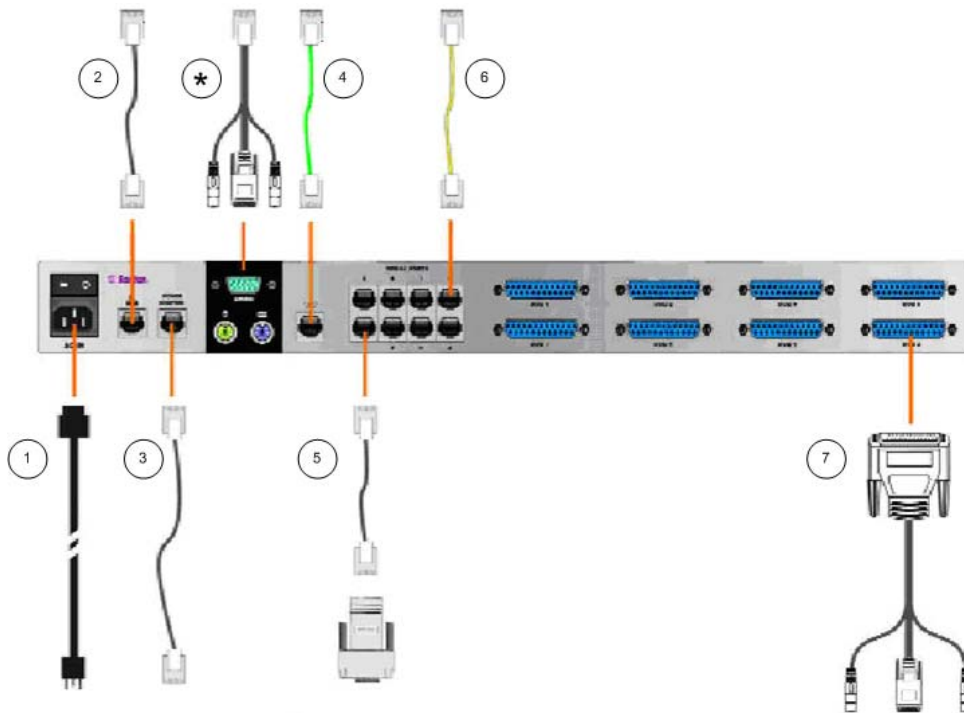
1. Power OFF the SX unit.
2. Disconnect from the installation computer, and move the Dominion SX to the location where it will be added to CC-SG.
3. Connect one end of a straight-through Cat5 cable to the SX.
4. Connect the other end of the Cat5 cable to the network.
5. To attach a device with a standard 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.

## Preparing Dominion Devices for CC-SG Management

### 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 *Installation Template* (on page 51).



#### Diagram Key

1	AC Power Cord
2	Network Port, Standard Cat5 Ethernet Cable, included
3	Power Port for Raritan Power Control Unit (p/n PCR8, PCS12, PCS20), Standard Cat5 Ethernet Cable
4	Analog Telephone Line, Telephone Cable, included
5	Serial Console Ports, Standard Cat5 Ethernet Cable with Nulling Serial Adapter (p/n ASCSDBxxx)

6	Serial Console Ports. Most Cisco RJ45 or Sun RJ45 Serial Ports require Rollover Cable (p/n CRLVR-15)
7	KVM Console Ports, KVM Console Cable (p/n CCPTxxx)
*	<p>Connection to Local or Admin Port, depending on unit type.</p> <p>The local port and the Admin Port locations depend on the Dominion KSX model you purchased. Dominion KSX units have a label on the underside of the chassis identifying the hardware version. The models that read either: Chassis RX440-F/S-0B or -0D or Chassis RX880-F/S-0B or -0D have the Local Admin ports on the rear panel and Local Access Console ports on the front panel (behind the bezel). For those models with labels that read Chassis RX440-F/S-0F or Chassis RX880-F/S-0F; these locations are reversed: the Local Admin ports are found on the front panel (behind the bezel) and Local Access Console ports are on the rear panel. Please consult the labeling on your Dominion KSX unit to determine where the Local and Admin ports are located.</p>

➤ *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.

## Preparing Dominion Devices for CC-SG Management

### ➤ *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.

---

### Dominion KSX II Devices

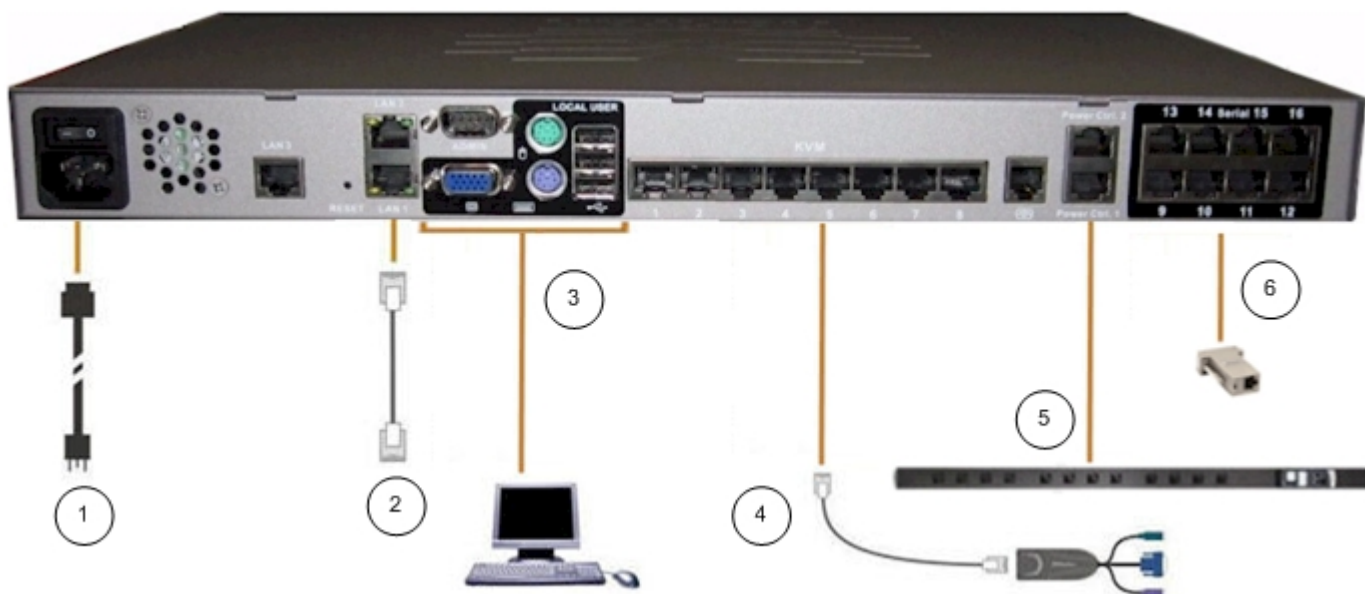
The following section provides you with the necessary background information and steps to install and configure Raritan Dominion KSX II units to conform to CC-SG's requirements.

---

Note: Be sure to document the device name, IP address, administrative username and password, and attached systems (port number, type, system name) in *Installation Template* (on page 51).

---

Connect the Dominion KSX II to the power supply, network, local PC, KVM target servers, and serial targets. The numbers in the diagram correspond to the sections describing the connection.



1. AC Power

➤ *To connect the power supply:*

1. Attach the included AC power cord to the Dominion KSX II and plug into an AC power outlet.

2. Network Ports

Dominion KSX II provides two Ethernet ports for failover purposes (not for load-balancing). By default, only LAN1 is active and the automatic failover is disabled. When enabled, if the Dominion KSX II internal network interface or the network switch to which it is connected becomes unavailable, LAN2 will be enabled using the same IP address.

➤ *To connect the network:*

1. Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router.
2. To make use of the optional Dominion KSX II Ethernet failover capabilities:
  - Connect a standard Ethernet cable from the network port labeled LAN2 to an Ethernet switch, hub, or router.
  - Enable Automatic Failover on the Network Configuration screen (refer to Network Settings, LAN Interface Settings in the Raritan Dominion KSX II User Guide for more information).

---

Use both network ports only if you want to use one as a failover port.

---

### 3. Local User Port (local PC) and Local Admin Port

For convenient access to KVM target servers and serial devices while at the rack, use the KSX II Local Access port. While the local port is required for installation and setup, it is optional for subsequent use. The local port provides the Dominion KSX II Local Console graphical user interface for administration and target server access.

➤ *To connect the Local User port:*

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).

You can use the Local Admin port to connect the Dominion KSX II directly to a workstation to manage your serial targets and configure the system with a terminal emulation program such as HyperTerminal. The Local Admin port requires the use of a standard null modem cable.

### 4. KVM Target Server Ports

The Dominion KSX II uses standard UTP cabling (Cat5/5e/6) to connect to each target server. Refer to Appendix A: Specifications in the Raritan Dominion KSX II User Guide for additional information.

➤ *To connect a KVM target server to the Dominion KSX II:*

1. Use the appropriate Computer Interface Module (CIM). Refer to Supported Operating Systems and CIMs in the Raritan Dominion KSX II User Guide for more information about the CIMs to use with each operating system.
2. Attach the HD15 video connector of your CIM to the video port of your KVM 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.
3. Attach the keyboard/mouse connector of your CIM to the corresponding ports on your target server. Using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an available server port on the back of your Dominion KSX II unit.

---

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

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

---

#### 5. Power Strip

➤ *To connect the Dominion PX to the KSX II:*

1. Plug one end of a Cat5 cable into the Serial port on the front of the Dominion PX.
2. Connect the other end of the Cat5 cable to either the Power Ctrl. 1 or Power Ctrl. 2 ports on the back of the KSX II.
3. Attach an AC power cord to the target server and an available power strip outlet.
4. Connect the power strip to an AC power source.
5. Power ON the KSX II unit.

---

**Important: When using CC-SG, the power ports should be inactive before attaching power strips that were swapped between the power ports. If not, there is a possibility that the number of power outlets will not be correctly detected, especially after swapping 8 and 20 outlet power strip models.**

---

#### 6. Serial Target Ports

To connect a serial target to the KSX II, use a Cat5 cable with an appropriate serial adapter.

The following table lists the necessary Dominion KSX II hardware (adapters and/or cables) for connecting the Dominion KSX II to common Vendor/Model combinations.

Vendor	Device	Console Connector	Serial Connection
Checkpoint	Firewall	DB9M	ASCSD9F adapter and a CAT 5 cable
Cisco	PIX Firewall		

## Preparing Dominion Devices for CC-SG Management

Vendor	Device	Console Connector	Serial Connection
Cisco	Catalyst	RJ-45	CRLVR-15 rollover cable; or CRLVR-1 adapter cable and a CAT5 cable  CRLVR-1 cable for connecting a terminal port (RJ-45 Connector type) of CommandCenter Secure Gateway-48 models that have this connector to another CommandCenter Secure Gateway.
Cisco	Router	DB25F	ASCSDDB25M adapter and a CAT 5 cable
Hewlett Packard	UNIX Server	DB9M	ASCSDDB9F adapter and a CAT 5 cable
Silicon Graphics	Origin		
Sun	SPARCStation	DB25F	ASCSDDB25M adapter and a CAT 5 cable
Sun	Netra T1	RJ-45	CRLVR-15 cable; or CRLVR-1 adapter and a CAT5 cable
Sun	Cobalt	DB9M	ASCSDDB9F adapter and a CAT 5 cable
Various	Windows NT		
Raritan	RPCU	RJ-45	CSCSPCS-10 cable or CSCSPCS-1 adapter cable

Go to the following link to obtain a list of commonly used cables and adapters <http://www.raritan.com/support>

### Dominion KSX II Initial Configuration

The first time you power up the Dominion KSX II unit, there is some initial configuration that you need to perform through the Dominion KSX II Local Console:

- Change the default password.
- Assign the IP Address.



### *Change the Default Password*

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

➤ *To change the default password:*

1. Power ON the CommandCenter Secure Gateway using the power switch(es) at the back of the unit. Wait for the CommandCenter Secure Gateway unit to boot. (A beep signals that the boot is complete.)
2. Once the unit has booted, the CommandCenter Secure Gateway Local Console is visible on the monitor attached to the CommandCenter Secure Gateway local port. Type the default username (admin) and password (raritan) and click Login. The Change Password screen is displayed.
3. Type your old password (raritan) in the Old Password field.
4. 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 the special characters identified in the table following these steps.
5. Click Apply.
6. You will receive confirmation that the password was successfully changed. Click OK. The Port Access page is displayed.

---

Note: The default password can also be changed from the Raritan Multi-Platform Client (MPC). For more information, refer to the Raritan Multi-Platform Client (MPC) User Guide.

---

## Preparing Dominion Devices for CC-SG Management

### Assign an IP Address

These procedures describe how to assign an IP Address using the Network Settings page. For complete information about all of the fields and the operation of this page, refer to Network Settings in the Raritan Dominion KSX II User Guide.

1. From the Dominion KSX II Local Console, select Device Settings > Network Settings. The Network Settings page opens.

Home > Device Settings > Network Settings

#### Network Basic Settings

Device Name <sup>\*</sup>  
PM\_KSX2

IP auto configuration  
None

Preferred host name (DHCP only)

IP address  
192.168.59.248

Subnet mask  
255.255.255.0

Gateway IP address  
192.168.59.126

Primary DNS server IP address

Secondary DNS server IP address

#### LAN Interface Settings

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

Current LAN interface parameters:  
autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed & Duplex  
Autodetect

☐ Enable Automatic Failover

Ping Interval (seconds) <sup>\*</sup>  
30

Timeout (seconds) <sup>\*</sup>  
60

Bandwidth Limit  
No Limit

[Set System ACL](#)

2. Specify a meaningful Device Name for your Dominion KSX II unit; up to 16 alphanumeric characters, special characters, and no spaces.
3. Select the IP auto configuration from the drop-down list:
  - None (Static IP). This option requires that you manually specify the network parameters. This is the recommended option because the Dominion KSX II is an infrastructure device and its IP Address should not change.
  - DHCP. With this option, network parameters are assigned by the DHCP server.
4. If you specify an IP configuration of None, type the TCP/IP parameters for your Dominion KSX II unit: IP address, Subnet mask, Gateway IP address, Primary DNS server IP address, and (optional) Secondary DNS server IP address.
5. When finished, click OK.

Your Dominion KSX II unit is now network accessible.

---

Note: In some environments, the LAN Interface Speed & Duplex setting default of Autodetect (auto-negotiation) does not properly set the network parameters, resulting in network issues. In these instances, setting the Dominion KSX II LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. Refer to the Network Settings page for more information.

---

---

## 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 *Installation Template* (on page 51).

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

---

---

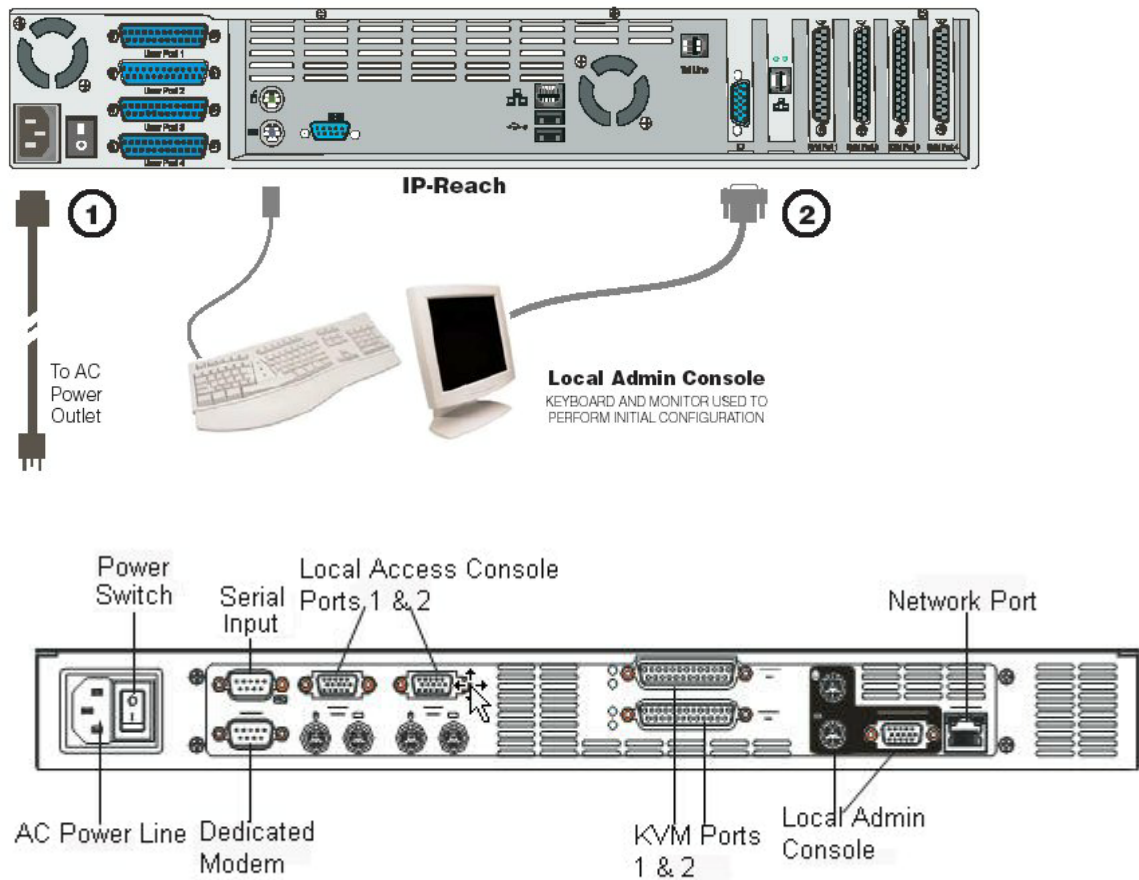
### IP Reach TR or M Series

➤ *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.

## Preparing IP-Reach Devices for CC-SG Management

### 3. Power ON the IP-Reach.



#### ➤ 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.

## Preparing IP-Reach Devices for CC-SG Management

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
```

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.

### In This Chapter

- |                                    |    |
|------------------------------------|----|
| 1. Rack Mount the CC-SG Unit ..... | 48 |
| 2. Physical Connections.....       | 48 |
| 3. Set IP Address of CC-SG.....    | 50 |

---

### 1. Rack Mount the CC-SG Unit

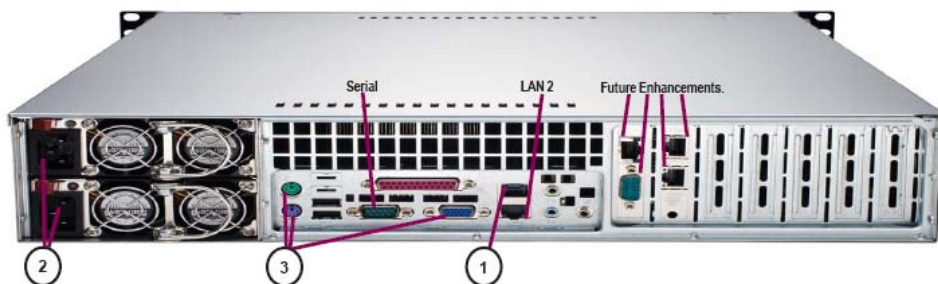
Follow the instructions on the Quick Setup Guide that came with your CC-SG unit.

---

### 2. Physical Connections

#### ➤ *Physical Connections for CC-SG E1 Units*

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



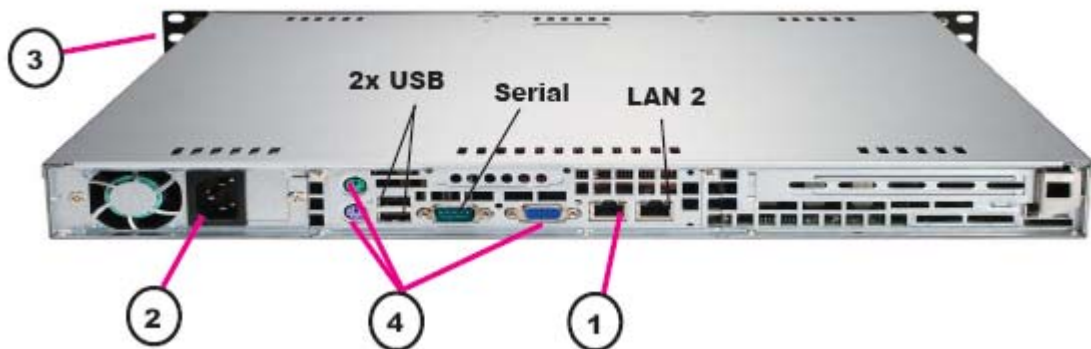
1. Connect the CAT 5 network LAN cable to the LAN 1 port on the rear panel of the CC-SG unit. Connect the other end of the cable to the network.



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*

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



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.

### 3. Set IP Address of CC-SG

---

**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*

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



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.

# Appendix A Installation Template

You can use the installation template to assist you in documenting your network configuration.

## In This Chapter

Blank Template .....	51
Sample Template .....	53

---

### Blank Template

<b>CommandCenter Secure Gateway</b>					
<b>IP address</b>	<b>netmask</b>	<b>default gateway</b>	<b>admin name</b>	<b>admin password</b>	
<b>Associations</b>					
<b>Category Name</b>	<b>string/integer</b>	<b>node/device/both</b>	<b>Element</b>	<b>Element</b>	<b>Element</b>
<b>Devices</b>					
<b>Name</b>	<b>Type</b>	<b>IP Address</b>	<b>Admin Name/ Password</b>	<b>Category/ Element1</b>	<b>Category/ Element2</b>
<b>Ports</b>					
<b>Name (system)</b>	<b>Device Name</b>	<b>Device Port #</b>			

Blank Template

<b>User Groups</b>					
<b>Name</b>	<b>Privileges</b>	<b>Policy name1</b>	<b>Policy name2</b>		
<b>Users</b>					
<b>Name</b>	<b>Password</b>	<b>User Group</b>			
<b>Device Groups</b>					
<b>Name</b>	<b>Member#1</b>	<b>Member#2</b>	<b>(Specify members by Category/Element)</b>		
<b>Node Groups</b>					
<b>Name</b>	<b>Member#1</b>	<b>Member#2</b>	<b>(Specify members by Category/Element)</b>		
<b>Policies</b>					
<b>Name</b>	<b>Day</b>	<b>Time</b>	<b>Control/ Deny</b>	<b>Device Group</b>	<b>Node Group</b>

---

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	Datacenter 1	Datacenter 2	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/ Datacenter 1	
Eng_KX1	KX		ccadmin/ rar123	location/ engineerin g	

## Sample Template

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				

## Sample Template

Policies					
Name	Day	Time	Control/ Deny	Device Group	Node Group
unixadmin_pol	all	all	control		unixport_group
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. Raritan powerstrips include Remote Power Control units PCR8, PCS12 and PCS20, and the Dominion PX.

## In This Chapter

Device Configurations for Power Control in CC-SG .....	57
Example: Remote Power Management Using SX, KX, and Powerstrip ...	58
Example: Remote Power Management for Multiple Power Connections	59

---

### 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, KX II or KSX device.

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

Some examples of acceptable configurations include:

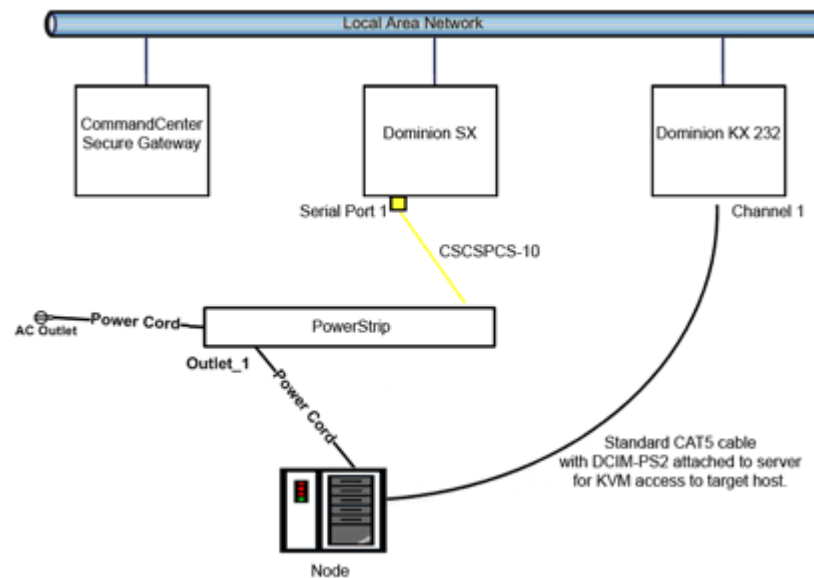
- Connect a powerstrip to Dominion SX to power nodes connected to the same Dominion SX.
- Connect a powerstrip to Dominion SX to power nodes connected to a Dominion KX.
- Connect a powerstrip to Dominion KX to power nodes connected to the same Dominion KX.
- Connect multiple powerstrips to a Dominion 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. Please refer to Chapter 3, or the Dominion KX User Guide for details.
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.



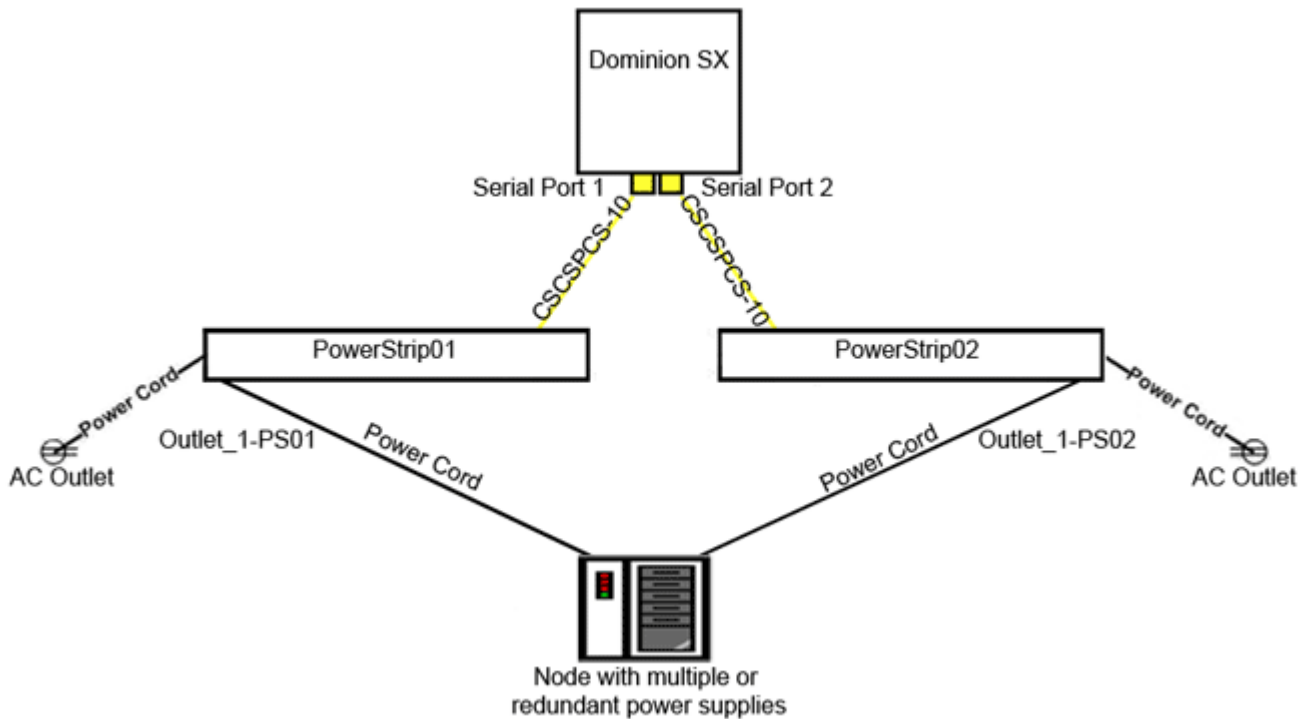
---

### CC-SG Configuration

Please refer to the CC-SG Administrators Guide 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..



### CC-SG Configuration

Please refer to the CC-SG Administrators Guide for details on adding the remote power management configuration to CC-SG.

# Appendix C CC-SG and Network Configuration

This appendix discloses network requirements (addresses, protocols and ports) of a typical CC-SG (CC-SG) deployment. It includes information about how to configure your network for both external access (if desired) and internal security and routing policy enforcement (if used). Details are provided for the benefit of a TCP/IP network administrator, whose role and responsibilities may extend beyond that of a CC-SG administrator and who may wish to incorporate CC-SG and its components into a site's security access and routing policies.

The tables that follow disclose the protocols and ports that are needed by CC-SG and its associated components.

## In This Chapter

Required Open Ports for CC-SG Networks: Executive Summary .....	60
CC-SG Communication Channels .....	61

---

## Required Open Ports for CC-SG Networks: Executive Summary

The following ports should be opened:

Port Number	Protocol	Purpose
80	TCP	HTTP Access to CC-SG
443	TCP	HTTPS (SSL) Access to CC-SG
8080	TCP	CC-SG <-> PC Client
2400	TCP	Node Access (Proxy Mode & In-Band Access)
5000	TCP	Node Access (Direct Mode)  These ports need to be opened per Raritan device that will be externally accessed. The other ports in the table need to be opened only for accessing CC-SG.
51000	TCP	SX Target Access (Direct Mode)

➤ *Possible exceptions:*

Port 80 can be closed if all access to the CC-SG is via HTTPS addresses.

Ports 5000 and 51000 can be closed if CC-SG Proxy mode is used for any connections from the firewall(s).

Thus, a minimum configuration only requires three (3) ports [443, 8080, and 2400] to be opened to allow external access to CC-SG.

---

## CC-SG Communication Channels

The communication channels are partitioned as follows:

- CC-SG to Raritan Devices
- CC-SG to CC-SG Clustering (optional)
- CC-SG to Infrastructure Services
- Clients to CC-SG
- Clients to Targets (Direct Mode)
- Clients to Targets (Proxy Mode)
- Clients to Targets (In-Band)
- CC-SG to CC-NOC

For each communication channel, the tables in the sections that follow:

- Represents the symbolic IP Addresses used by the communicating parties. These addresses have to be allowed over any communication path between the entities.
- Indicates the Direction in which the communication is initiated. This may be important for your particular site policies. For a given CC-SG role, the path between the corresponding communicating parties must be available and for any alternate re-route paths that might be used in the case of a network outage.
- Provides the Port Number and Protocol used by CC-SG.
- Indicates if the port is Configurable, which means the GUI or Diagnostic Console provides a field where you can change the port number to a different value from the default listed due to conflicts with other applications on the network or for security reasons.

## CC-SG Communication Channels

---

### CC-SG and Raritan Devices

A main role of CC-SG is to manage and control Raritan devices (for example, Dominion KX, KSX, etc.). Typically, CC-SG communicates with these devices over a TCP/IP network (local, WAN, or VPN) and both TCP and UDP protocols are used as follows:

Communication Direction	Port Number	Protocol	Configurable?
CC-SG to Local Broadcast	5000	UDP	yes
CC-SG to Remote LAN IP	5000	UDP	yes
CC-SG to Raritan Device	5000	TCP	yes
Raritan Device to CC-SG	5001	UDP	no

---

### CC-SG Clustering

When the optional CC-SG clustering feature is used, the following ports must be available for the inter-connecting sub-networks. If the optional clustering feature is not used, none of these ports need to be open.

Each CC-SG in the cluster may be on a separate LAN. However, the inter-connection between the units should be very reliable and not prone to periods of congestion.

Communication Direction	Port Number	Protocol	Configurable?
CC-SG to Local Broadcast	10000	UDP	no
CC-SG to Remote LAN IP	10000	UDP	no
CC-SG to CC-SG	5432	TCP	no
CC-SG to CC-SG	8732	TCP	no
CC-SG to CC-SG	3232	TCP	no

---

### Access to Infrastructure Services

The CC-SG can be configured to use several industry-standard services like DHCP, DNS, and NTP. In order for CC-SG to communicate with these optional servers, these ports and protocols are used.

## Appendix C: CC-SG and Network Configuration

Communication Direction	Port Number	Protocol	Configurable?
DHCP server to CC-SG	68	UDP	No
CC-SG to DHCP server	67	UDP	No
NTP server to CC-SG	123	UDP	No
CC-SG to DNS	53	UDP	No

---

### PC Clients to CC-SG

PC Clients connect to the CC-SG in one of these three modes:

- Admin or Access Client GUIs via a web browser
- Command Line Interface (CLI) via SSH
- Diagnostic Console

Communication Direction	Port Number	Protocol	Configurable?
PC Client to CC-SG GUI	443	TCP	no
PC Client to CC-SG GUI	80	TCP	no
PC Client to CC-SG GUI	8080	TCP	no
PC Client to CLI SSH	22	TCP	yes
PC Client to Diagnostic Console	23	TCP	yes

---

### PC Clients to Nodes

Another significant role of CC-SG is to connect PC clients to various nodes. These nodes can be serial or KVM console connections to Raritan devices (called Out-of-Band connections). Another mode is to use In-Band access (IBA) methods, for example, Virtual Network Computer (VNC), Windows Remote Desktop (RDP), or Secure Shell (SSH).

Another facet of PC client to node communication is whether:

- The PC client connects directly to the node (either via a Raritan device or In-Band access), which is called Direct Mode.
- Or, if the PC client connects to the node through CC-SG, which acts as an application firewall and is called Proxy Mode.

## CC-SG Communication Channels

Communication Direction	Port Number	Protocol	Configurable?
Client to CC-SG via Proxy to Node	2400 (on CC-SG)	TCP	no
Client to Raritan Device to Out-of-Band KVM Node (Direct Mode)	5000 (on Raritan Device)	TCP	yes
Client to Raritan Dominion SX Device to Out-of-Band Serial Node (Direct Mode)	51000 (on Raritan Device)	TCP	yes

---

### CC-SG & Client for IPMI, iLO/RILOE, DRAC, RSA

Another significant role of CC-SG is to manage third-party devices, such as iLO/RILOE, Hewlett Packard's Integrated Lights Out/Remote Insight Lights Out servers. Targets of an iLO/RILOE device are powered on/off and recycled directly. Intelligent Platform Management Interface (IPMI) servers can also be controlled by CC-SG. Dell DRAC and RSA targets can also be managed by CC-SG.

Communication Direction	Port Number	Protocol	Configurable?
CC-SG to IPMI	623	UDP	no
CC-SG to iLO/RILOE (uses HTTP ports)	80 or 443	UDP	no
CC-SG to DRAC	80 or 443	UDP	no
CC-SG to RSA	80 or 443	UDP	no

---

### CC-SG & SNMP

Simple Network Management Protocol (SNMP) allows CC-SG to push SNMP traps (event notifications) to an existing SNMP manager on the network. CC-SG also supports SNMP GET/SET operations with third-party Enterprise Management Solutions, such as HP OpenView.

Communication Direction	Port Number	Protocol	Configurable?
SNMP Manager to CC-SG	161	UDP	yes



## Appendix C: CC-SG and Network Configuration

Communication Direction	Port Number	Protocol	Configurable?
CC-SG to SNMP Manager	162	UDP	yes

---

### CC-SG & CC-NOC

CC-NOC is an optional appliance that can be deployed in conjunction with CC-SG. CC-NOC is a Raritan network-monitoring appliance that audits and monitors the status of servers, equipment, and Raritan devices that CC-SG manages.

Communication Direction	Port Number	Protocol	Configurable?
CC-SG to CC-NOC	9443	TCP	no

---

### CC-SG Internal Ports

CC-SG uses several ports for internal functions and its local firewall function blocks access to these ports. However, some external scanners may detect these as “blocked” or “filtered”. External access to these ports is not required and can be further blocked. The ports currently in use are:

- 1088
- 1098
- 2222
- 4444
- 4445
- 8009
- 8083
- 8093

In addition to these ports, CC-SG may use TCP and UDP ports in the 32xxx (or higher) range. External access to these ports is not required and can be blocked.

---

### CC-SG Access via NAT-enabled Firewall

If the firewall is using NAT (Network Address Translation) along with Port Address Translation (PAT), then Proxy mode should be used for all connections that use this firewall. The firewall must also be configured for external connections to ports 80 (non-SSL) or 443 (SSL), 8080 and 2400 to be forwarded to CC-SG (since the PC Client will initiate sessions on these ports).

---

**Note:** It is not recommended to run non-SSL traffic through a firewall.

---

All In-Band connections use CC-SG as the Proxy connection. No additional configuration is required. Out-of-Band connections using the firewall must be configured to use Proxy mode. Please refer to Connection Modes: Direct and Proxy for details. CC-SG will connect to the various targets (either IBA or OBA) on behalf of the PC Client requests. However, the CC-SG will terminate the PC Client to Target TCP/IP connection that comes through the firewall.



➤ *U.S./Canada/Latin America*

Monday - Friday  
8 a.m. - 8 p.m. ET  
Phone: 800-724-8090 or 732-764-8886  
For CommandCenter NOC: Press 6, then Press 1  
For CommandCenter Secure Gateway: Press 6, then Press 2  
Fax: 732-764-8887  
Email for CommandCenter NOC: tech-ccnoc@raritan.com  
Email for all other products: tech@raritan.com

➤ *China*

**Beijing**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +86-10-88091890

**Shanghai**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +86-21-5425-2499

**GuangZhou**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +86-20-8755-5561

➤ *India*

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +91-124-410-7881

➤ *Japan*

Monday - Friday  
9:30 a.m. - 5:30 p.m. local time  
Phone: +81-3-3523-5994  
Email: support.japan@raritan.com

➤ *Europe*

**Europe**

Monday - Friday  
8:30 a.m. - 5 p.m. GMT+1 CET  
Phone: +31-10-2844040  
Email: tech.europe@raritan.com

**United Kingdom**

Monday - Friday  
8:30 a.m. to 5 p.m. GMT+1 CET  
Phone +44-20-7614-77-00  
France  
Monday - Friday  
8:30 a.m. - 5 p.m. GMT+1 CET  
Phone: +33-1-47-56-20-39

**Germany**

Monday - Friday  
8:30 a.m. - 5 p.m. GMT+1 CET  
Phone: +49-20-17-47-98-0

➤ *Korea*

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +82-2-5578730

➤ *Melbourne, Australia*

Monday - Friday  
9:00 a.m. - 6 p.m. local time  
Phone: +61-3-9866-6887

➤ *Taiwan*

Monday - Friday  
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight  
Phone: +886-2-8919-1333  
Email: tech.rap@raritan.com