CC-SG

CommandCenter Secure Gateway

Administrators Guide

Release 3.2

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 7   Managed Powerstrips   51

Chapter 8   Nodes, Node Groups, and Interfaces   58

Chapter 9   Users and User Groups 78

Chapter 10   Policies for Access Control   91

Chapter 11   Custom Views for Devices and Nodes   99

Chapter 12   Remote Authentication   107

Chapter 14   System Maintenance   140

Appendix B CC-SG and Network Configuration   239

Contents

How-To: CC-SG Essentials

This chapter includes some of the most common use cases to help familiarize users quickly with practical use of CC-SG. Please note that this section provides common examples, which could vary according to your actual configuration and operations.

In This Chapter

How to configure and enforce strong passwords

1. Choose **Administration** > **Security**.

2. Open the **Login Settings** tab.

3. Check the **Strong Passwords Required for All Users** checkbox.

4. Select a **Maximum Password Length**. Passwords must contain fewer than the maximum number of characters.

5. Select a **Password History Depth**. The number specifies how many previous passwords are kept in the history and cannot be reused. For example, if **Password History Depth** is set to 5, users cannot reuse any of their previous 5 passwords.

6. Select a **Password Expiration Frequency**. All passwords expire after a set number of days. After a password expires, users will be asked to choose a new password the next time they log in.

7. Select **Strong Password Requirements**:

   ▪ Passwords must contain at least one lower case letter.

   ▪ Passwords must contain at least one upper case letter.

- Passwords must contain at least one number.

- Passwords must contain at least one special character (for example, an exclamation point or ampersand).

8. Click **Update** to save your changes.

Please refer to *Login Settings* (on page 175) for more details on login security.

Upgrade CC-SG to a new firmware version

You can upgrade CC-SG's firmware when a newer version is released. You can find firmware files in the Support section of the Raritan website.

Download the firmware file to your client PC before proceeding with the upgrade.

You should back up CC-SG before upgrading. If you are operating a CC-SG cluster, you must remove the cluster first and upgrade each node separately.

Note: If you are upgrading from 3.0.2 to 3.1, and you use Active Directory, please refer to the Readme for the 3.1 release for special instructions.

Important!

If you need to upgrade both CC-SG and a device or group of devices, perform the CC-SG upgrade first, and then perform the device upgrade.

CC-SG will reboot as part of the upgrade process from 3.1.1 to 3.2. DO NOT stop the process, reboot the unit manually, power off or power cycle the unit during the upgrade

➢ *To upgrade CC-SG:*

1. Download the firmware file to your client PC.

2. *Enter Maintenance Mode* (on page 141)

3. Once CC-SG is in maintenance mode, choose **System Maintenance > Upgrade**.

4. Click **Browse**. Navigate to and select the CC-SG firmware file, and then click **Open**.

5. Click **OK** to upload the firmware file to CC-SG.

After the firmware file is uploaded to CC-SG, a success message appears to indicate that CC-SG has has begun the upgrade process. All users will be disconnected from CC-SG at this time.

6. Click **OK** to exit CC-SG and allow it to restart. You must wait approximately 8 minutes while CC-SG restarts.

7. Close your browser window, and then clear your browser cache.

8. After 8 minutes, open a new browser window and launch CC-SG.

9. Choose **Help** > **About Raritan Secure Gateway**. Check the version number to verify that the upgrade was successful.

   ▪ If the version has not upgraded, repeat the previous steps.

   ▪ If upgrade was successful, proceed to the next step.

Exit Maintenance Mode (on page 141)

Control power to a node group and monitor the power control operation

Node Group Power Control

You can power on, power off, cycle power, and perform graceful shutdown for all nodes that have associated power interfaces in a node group.

This is useful if you need to power down all nodes in a node group so that you can rewire the rack that they are mounted on, or if you need to perform other types of maintenance on a node group.

Please refer to Tips on Controlling Power to Nodes with Multiple Interfaces (in the CC-SG User Guide) for more details on setting up power control operations for nodes with more than one power control interface.

1. Click the **Nodes** tab.

2. On the **Nodes** menu, click **Group Power Control**. The **Group Power Control** screen appears.

3. Click the **Node Group** drop-down arrow and select the node group whose power you want to control from the list.

4. In the **Available** list, select the specific interface that you want to perform power control on, and then click **Add** to move the interface to the **Selected** list. Repeat this step until you have added all necessary interfaces to the **Selected** list. If you must remove an interface, select the interface in the **Selected** list, and then click **Remove**.

5. You must put the interfaces in the **Selected** list into the order in which you would like CC-SG to perform the power operation. Select an interface in the **Selected** list, and then click the up and down arrows to move the interfaces into the desired sequence.

6. Click the **Operation** drop-down arrow, and select **Power On**, **Power Off**, **Power Cycle** or **Graceful Shutdown** from the list.

7. If you selected **Power On**, **Power Off** or **Graceful Shutdown** in the **Operation** field, type the number of seconds, from 0-120, that should elapse between interfaces in the **Sequence Interval (seconds)** field.

8. Click **OK** to send the power operation request through the selected interfaces. A confirmation message appears in the screen.

9. A Power Status Messages window opens to show you the status of the power control operation. Messages populate the window as new information is received about the power control operation. Keep this window open until all power control operations are complete, so you can monitor progress.

   Please refer to *Power Status Messages* (on page 18) for details about how CC-SG alerts you to successful and failed power control operations.

Power Status Messages

The Power Status Messages window appears when you begin a power control operation. You should keep this window open until all power control operations are completed.

You can resize, minimize, or maximize the Power Status Messages window. You can select and then copy and paste the text in the window.

The messages in the Power Status Messages window are updated as new information is received about the status of the power control operation.

A new message appears in the Power Status Messages window when:

- Power control operation request is sent.

- Power control operation fails.

- Power control operation completes successfully.

- All power control operations requested complete successfully.

> ### How to get status updates if you close the Power Status Messages window:

If you close the status window before the power control operation has completed:

- When a power control operation fails, an alert message pops up with information about the failed operation.

- The status bar at the bottom of your browser window displays an alert message when the entire operation completes successfully.

- Alert messages pop up only for failed operations. Alert messages do not pop up for successful operations.

Upgrade multiple devices within a limited time period

You can schedule a task to upgrade multiple devices of the same type, such as KX or SX, within a device group. Once the task begins, an Upgrade Device Firmware report is available in the Reports > Scheduled Reports menu to view the upgrade status in real time. This report is also emailed if you specify the option in the Notification tab.

Please refer to the Raritan User Guide for each device for estimated upgrade times.

> ### To schedule a Device Firmware Upgrade:

1. Choose Administration > Tasks.

2. Click New.

3. In the Main tab, type a name and description for the task. The Name you choose will be used to identify the task and the report associated with the task.

4. Open the Task Data tab.

5. Specify the device upgrade details:

   a. Task Operation: Select Upgrade Device Firmware.

   b. Device Group: Select the device group that contains the devices you want to upgrade.

   c. Device Type: Select the type of device you want to upgrade. If you need to upgrade more than one device type, you must schedule a task for each type.

d. Concurrent Upgrades: Specify the number of devices that should begin the file transfer portion of the upgrade simultaneously. Maximum is 10. As each file transfer completes, a new file transfer will begin, ensuring that only the maximum number of concurrent transfers occurs at once.

e. Upgrade File: Select the firmware version you want to upgrade to. Only available upgrade files that are appropriate for the device type selected will display as options.

6. Specify the time period for the upgrade:

a. Start Date/Time: Select the date and time at which the task begins. The start date/time must be later than the current date/time.

b. Restrict Upgrade Window and Latest Upgrade Start Date/Time: If you must finish all upgrades within a specific window of time, use these fields to specify the date and time after which no new upgrades can begin. Select Restrict Upgrade Window to enable the Latest Upgrade Start Date/Time field.

7. Specify which devices will be upgraded, and in what order. Place higher priority devices at the top of the list.:

a. In the Available list, select each device you want to upgrade, and click Add to move it to the Selected list.

b. In the Selected list, select a device and use the arrow buttons to move the devices into the order in which you want upgrades to proceed.

8. Open the Retry tab. Specify whether failed upgrades should be retried.

a. Retry Count: Type the number of times CC-SG should retry a failed upgrade.

b. Retry Interval: Enter the time that should elapse between retries. Default times are 30, 60, and 90 minutes. These are the optimal retry intervals.

9. Open the Notification tab. Specify email addresses that should receive notifications of success and failure. By default, the email address of the user currently logged in is available. User email addresses are configured in the User Profile.

a. Click Add, type the email address in the window that appears, and then click OK.

b. Select On Failure if you want an email sent if an upgrade fails.

    c.   Select On Success if you want an email sent when all upgrades complete successfully

10. Click OK to save your changes.

When the task starts running, you can open the Upgrade Device Firmware report any time during the scheduled time period to view the status of the upgrades. Please refer to *Upgrade Device Firmware Report* (on page 139) for details.

Assign a Default Custom View of Nodes for All Users

If you have the CC Setup and Control privilege, you can assign a default custom view for all users.

1. Click the Nodes tab.

2. Choose Nodes > Change View > Create Custom View.

3. Click the **Name** drop-down arrow, and select the custom view you want assign as a system-wide default view.

4. Check the **System Wide** checkbox, and then click **Save.**

All users who log in to CC-SG will see the Nodes tab sorted according to the selected custom view. Users can still change the custom view.

Please refer to *Custom Views* (see "Custom Views for Devices and Nodes" on page 99) for details on types of custom views and instructions for creating them.

Chapter 1 Introduction

The CommandCenter Secure Gateway (CC-SG) Administrators Guide offers instructions for administering and maintaining your CC-SG.

This guide is intended for administrators who typically have all available privileges.

Users who are not administrators should refer to Raritan's **CommandCenter Secure Gateway User Guide** for details.

In This Chapter

Prerequisites

Before configuring a CC-SG according to the procedures in this document, refer to Raritan's **Digital Solution Deployment Guide** for more comprehensive instructions on deploying Raritan devices that are managed by CC-SG.

Terminology/Acronyms

Terms and acronyms found in this document include:

Access Client - An HTML based client intended for use by normal access users who need to access a node managed by CC-SG. The Access Client does not allow the use of administration functions.

Admin Client-A Java-based client for CC-SG useable by both normal access users and administrators. It is the only client that permits administration.

Associations-are the relationship between categories, elements of a category, and ports or devices or both. For example, if you want to associate the "Location" category with a device, create associations first before adding devices and ports in CC-SG.

Category-is a variable that contains a set values or elements. An example of a Category is Location, which may have elements such as "New York City, "Philadelphia", or "Data Center 1". When you add devices and ports to CC-SG, you will associate this information with them. It is easier if you set up associations correctly first, before adding devices and ports to them. Another example of a Category is "OS Type", which may have elements such as "Windows " or "Unix " or "Linux ".

CIM (Computer Interface Module)-is the hardware used to connect a target server and a Raritan device. Each target requires a CIM, except for the Dominion KX101 which is attached directly to one target and therefore, does not require a CIM. Target servers should be powered on and connected to CIMs, and CIMs should be connected to the Raritan device BEFORE adding the device and configuring ports in CC-SG. Otherwise, a blank CIM name will overwrite the CC-SG port name. Servers need to be rebooted after connecting to a CIM.

CommandCenter NOC (CC NOC)-is a network monitoring appliance that audits and monitors the status of servers, equipment, and Raritan devices that CC-SG manages.

Device Group-a defined group of devices that are accessible to a user. Device groups are used when creating a policy to control access to the devices in the group.

Devices-are Raritan products such as Dominion KX, Dominion KX II, Dominion SX, Dominion KSX, IP-Reach, Paragon II System Controller, Paragon II UMT832 with USTIP, that are managed by CC-SG. These devices control the target servers and systems, or "nodes" that are connected to them. Please check the CC-SG Compatibility Matrix on the Raritan Support web site for a list of supported devices.

Elements-are the values of a category. For example, the "New York City" element belongs to the "Location" category. Or, the "Windows" element belongs to the "OS Type" category.

Ghosted Ports-When managing Paragon devices, a ghosted port can occur when a CIM or target server is removed from the system or powered off (manually or accidentally). Refer to Raritan's Paragon II User Manual for details.

Hostname-A hostname can be used if DNS server support is enabled. Please refer to About Network   in *Advanced Administration* (on page 150) for details. The hostname and its Fully-Qualified Domain Name (FQDN = Hostname + Suffix) cannot exceed 257 characters. It can consist of any number of components, as long as they are separated by   "."   . Each component has a maximum size of 63 characters and the first character must be alphabetic. The remaining characters can be alphabetic, numeric, or
 "- " (hyphen or minus). The last character of a component may not be
 "-"   . While the system preserves the case of the characters entered into the system, the FQDN is case-insensitive when used.

iLO/RILOE-Hewlett Packard's Integrated Lights Out/Remote Insight Lights Out servers that can be managed by CC-SG. Targets of an iLO/RILOE device are powered on/off and recycled directly. iLO/RILOE devices cannot be discovered by CC-SG; they have to be manually added as nodes.

In-band Access-going through the TCP/IP network to correct or troubleshoot a target in your network. KVM and Serial devices can be accessed via these in-band applications: RemoteDesktop Viewer, SSH Client, RSA Client, VNC Viewer.

IPMI Servers (Intelligent Platform Management Interface)-servers that can be controlled by CC-SG. IPMI are discovered automatically but can be added manually as well.

Out-of-Band Access-using applications such as Raritan Remote Console (RRC), Raritan Console (RC), or Multi-Platform Client (MPC) to correct or troubleshoot a KVM or serial managed node in your network.

Policies-define the permissions, type of access, and to which nodes and devices a user group can access. Policies are applied to a user group and have several control parameters to determine the level of control, such as date and time of access.

Nodes-are the target systems, such as servers, desktop PCs, and other networked equipment, that CC-SG users can access.

Interfaces-Interfaces are ways a Node can be accessed, whether through an out-of-band solution such as a Dominion KX101 connection, or through an in-band solution such as a VNC server.

Node Groups-a defined group of nodes that are accessible to a user. Node groups are used when creating a policy to control access to the nodes in the group.

Ports-are connection points between a Raritan Device and a Node. Ports only exist on Raritan devices and identify a pathway from that device to a node.

SASL (Simple Authentication and Security Layer) -A method for adding authentication support to connection-based protocols.

SSH-Clients, such as PuTTY or OpenSSH, that provide a command line interface to CC-SG. Only a subset of CC-SG commands is provided via SSH to administer devices and CC-SG itself.

User Groups-sets of users that share the same level of access and privileges.

Chapter 2   Accessing CC-SG

You can access CC-SG in several ways:

- **Browser**: CC-SG supports numerous web browsers. (For a complete list of supported browsers, please refer to the Compatibility Matrix on the Raritan Support website.

- **Thick Client**: You can install a Java Web Start thick client on your client computer. The thick client functions exactly like the browser-based client.

- **SSH**: Remote devices connected via the serial port can be accessed using SSH. Please refer to *Advanced Administration* (on page 150)for details.

- **Diagnostic Console**: Provides emergency repair and diagnostics only and is not a replacement for the browser-based GUI to configure and operate CC-SG. Please refer to *Advanced Administration* (on page 150) for details.

Note: Users can be connected simultaneously, using the browser, thick client, and SSH while accessing CC-SG.

In This Chapter

Browser-Based Access

1. Using a supported Internet browser, type this URL: https://<IP_address>/admin where <IP_address> is the IP address of the CC-SG. For example, **https://10.20.3.30/admin**.

2. When the security alert window appears, click **Yes** to continue.

3. You will be warned if you are using an unsupported Java Runtime Environment version on your machine. From the window that pops up, select whether you will download the correct JRE version from the CC-SG server (if available), download it from the Sun Microsystems website, or continue with the incorrect version, and then click **OK**. The Login window appears.

4. If the Restricted Service Agreement is enabled, read the agreement text, and then check the **I Understand and Accept the Restricted Service Agreement** checkbox.

5. Type your **Username** and **Password**, and then click **Log In**.

Thick Client Access

The CC-SG thick client allows you to connect to CC-SG by launching a Java Web Start application instead of running an applet through a web browser. The advantage of using the thick client instead of a browser is that the client can outperform the browser in terms of speed and efficiency.

Install the Thick Client

➢ *To download the thick client from CC-SG:*

1. Launch a web browser and type this URL: **http(s)://<IP_address>/install** where <IP_address> is the IP address of the CC-SG.

   ▪ If a security warning message appears, click **Start** to continue the download.

   ▪ If your client computer is running Java version 1.4, a **Desktop Integration** window appears. If you want Java to add a shortcut icon for the thick client to your desktop, click **Yes**.

2. When the download is complete, a new window in which you can specify the CC-SG IP address appears.

3. Type the IP address of the CC-SG unit you want to access in the **IP to Connect** field. Once you have connected, this address will be available from the **IP to Connect** drop-down list. The IP addresses are stored in a properties file that is saved to your desktop.

4. If the CC-SG is configured for secure browser connections, you must check the **Secure Socket Layer (SSL)** checkbox. If the CC-SG is not configured for secure browser connections, you must clear the **Secure Socket Layer (SSL)** checkbox. This setting must be correct or the thick client will not be able to connect to CC-SG.

5. **To check the setting in CC-SG:** Choose **Administration** > **Security**. In the **Encryption** tab, look at the **Browser Connection Protocol** option. If the **HTTPS/SSL** option is selected, then you must check the **Secure Socket Layer SSL** checkbox in the thick client's IP address specification window. If the HTTP option is selected, then you must clear the **Secure Socket Layer SSL** checkbox in the thick client's IP address specification window.

6. Click **Start**.

- A warning message appears if you are using an unsupported Java Runtime Environment version on your machine. Follow the prompts to either download a supported Java version, or continue with the currently installed version.

7. The login screen appears.

8. If the Restricted Service Agreement is enabled, read the agreement text, and then select the **I Understand and Accept the Restricted Service Agreement** checkbox.

9. Type your **Username** and **Password** in the corresponding fields, and then click **Login** to continue.

Use the Thick Client

Once the thick client is installed, there are 2 different ways to access it on your client computer. These are determined by the Java version you are using.

➢ *Java 1.4.x*

If your client computer is running **Java version 1.4.x** and you clicked **Yes** in the **Desktop Integration** window when you installed the thick client, you can double-click the shortcut icon on your desktop to launch the thick client and access CC-SG. If you do not have a shortcut icon, you can create one at any time: search your client computer for **AMcc.jnlp**, and create a shortcut to that file.

➢ *Java 1.5*

If your client computer is running **Java version 1.5**, you can:

- Launch the thick client from the Java Control Panel's Java Application Cache Viewer.

- Use the Java Control Panel's Java Application Cache Viewer to install a shortcut icon on your desktop for the thick client.

CC-SG Admin Client

Upon valid login, the CC-SG Admin Client appears.
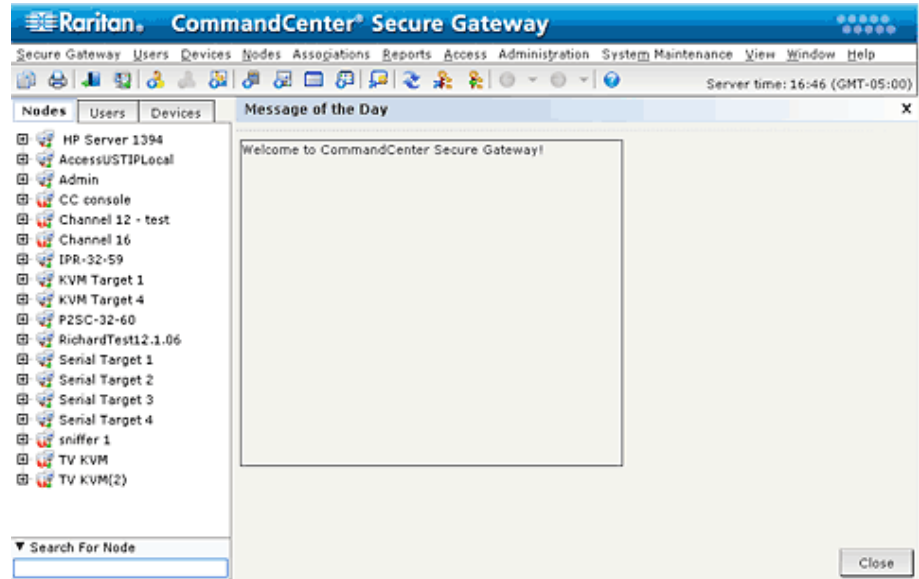
- **Nodes tab**: Click the **Nodes** tab to display all known target nodes in a tree view. Click a node to view the Node Profile. Interfaces are grouped under their parent nodes. Click the + and - signs to expand or collapse the tree. Right-click an interface and select **Connect** to connect to that interface. You can sort the nodes by Node Name (alphabetical) or Node Status (Available, Busy, Unavailable). Right-click the tree view, select **Node Sorting Options**, and then select **By Node Name** or **By Node Status**.

- **Users tab**: Click the **Users** tab to display all registered Users and Groups in a tree view. Click the + and - signs to expand or collapse the tree.

- **Devices tab**: Click the **Devices** tab to display all known Raritan devices in a tree view. Different device types have different icons. Ports are grouped under their parent devices. Click the + and - signs to expand or collapse the tree. Click a port to view the Port Profile. Right-click a port and select **Connect** to connect to that port. You can sort the ports by Port Name (alphabetical) or Port Status (Available, Busy, Unavailable). Right-click the tree view, select **Port Sorting Options**, and then select **By Node Name** or **By Node Status**.

- **Quick Commands toolbar**: This toolbar offers some shortcut buttons for executing common commands.

- **Operation and Configuration menu bar**: These menus contain commands to operate and configure CC-SG. You can also access some of these commands by right-clicking on the icons in the **Nodes**, **Users**, and **Devices** Selection tabs. The menus and menu items you see are determined by your user access privileges.

- **Server time:** The current time and time zone as configured on CC-SG in Configuration Manager. This time is used when scheduling tasks in Task Manager. Please refer to *Task Manager* (on page 186) for details. This time may be different than the time your client PC uses.

Chapter 3   Getting Started

Upon the first login to CC-SG, you should confirm the IP address, set the CC-SG server time, and check the firmware and application versions installed. You may need to upgrade the firmware and applications.

Once you have completed your initial configurations, you can proceed to *Configuring CC-SG with Guided Setup* (on page 13).

In This Chapter

Confirm IP Address

1. Choose **Administration** > **Configuration**.

2. Click the **Network Setup** tab.

3. (Optional) Check that the network setting are correct, and make changes if needed. Please refer to *About Network Setup* (on page 155) for details.

4. Click **Update Configuration** to submit your changes.

5. Click **Restart Now** to confirm your settings and restart CC-SG.

Set the CC-SG Server Time

CC-SG's time and date must be accurately maintained to provide credibility for its device-management capabilities.

> **Important! The Time/Date configuration is used when scheduling tasks in Task Manager. Please refer to *Task Manager* (on page 186) for details. The time set on your client PC may be different than the time set on CC-SG.**

Only the CC Super-User and users with similar privileges can configure Time and Date.

Changing the time zone is disabled in a cluster configuration.

➢ **To configure the CC-SG server time and date:**

1. Choose Administration > Configuration.

2. Click the **Time/Date** tab.

   a. **To set the date and time manually: Date**-click the drop-down arrow to select the **Month**, use the up and down arrows to select the **Year**, and then click the **Day** in the calendar area. **Time**-use the up and down arrows to set the **Hour, Minutes,** and **Seconds**, and then click the **Time zone** drop-down arrow to select the time zone in which you are operating CC-SG.

   b. **To set the date and time via NTP:** Check the **Enable Network Time Protocol** checkbox at the bottom of the window, and then type the IP addresses for the **Primary NTP server** and the **Secondary NTP server** in the corresponding fields**.**

   Note: Network Time Protocol (NTP) is the protocol used to synchronize the attached computer's date and time data with a referenced NTP server. When CC-SG is configured with NTP, it can synchronize its clock time with the publicly available NTP reference server and maintain correct and consistent time.

3. Click **Update Configuration** to apply the time and date changes to CC-SG.

4. Click **Refresh** to reload the new server time in the **Current Time** field.

Choose **System Maintenance** > **Restart** to restart CC-SG.

Check the Compatibility Matrix

The Compatibility Matrix lists the firmware versions of Raritan devices and software versions of applications that are compatible with the current version of CC-SG. CC-SG checks against this data when you add a device, upgrade device firmware, or select an application for use. If the firmware or software version is incompatible, CC-SG displays a message to warn you before you continue. Each version of CC-SG will only support the current and previous firmware versions for Raritan devices at the time of release. You can also view the compatibility matrix on the Raritan Support web site.

➢ *To check the Compatibility Matrix:*

- On the **Administration** menu, click **Compatibility Matrix**.

Check and Upgrade Application Versions

Check and upgrade the CC-SG applications, such as Raritan Console (RC) and Raritan Remote Client (RRC).

➢ *To check an application version:*

1. Choose **Administration** > **Applications**.

2. Select an **Application name** from the list. Note the number in the **Version** field. Some applications do not automatically show a version number.

➢ *To upgrade an application:*

If the application version is not current, you must upgrade the application. You can download the application upgrade file from the Raritan website. For a complete list of supported application versions, please refer to the **Compatibility Matrix** on the Raritan Support website.

1. Save the application file to your client PC.

2. Click the **Application name** drop-down arrow and select the application that must be upgraded from the list. If you do not see the application, you must add it first. *Add an Application* (on page 152)

3. Click **Browse**, locate and select the application upgrade file from the dialog that displays, and then click **Open**.

4. The application name appears in the **New Application File** field in the **Application Manager** screen.

5. Click **Upload**. A progress window indicates that the new application is being uploaded. When complete, a new window will indicate that the application has been added to the CC-SG database and is available to use.

6. If the **Version** field does not automatically update, type the new version number in the **Version** field. The **Version** field will automatically update for some applications.

7. Click **Update**.

Chapter 4 Configuring CC-SG with Guided Setup

Guided Setup offers a simple way to complete initial CC-SG configuration tasks, once the network configuration is complete. The Guided Setup interface leads you through the process of defining Associations, discovering and adding devices to CC-SG, creating device groups and node groups, creating user groups, assigning policies and privileges to user groups, and adding users. Once you have completed Guided Setup, you can always edit your configurations individually.

Guided Setup is divided into 4 tasks:

- *Associations* (see "Associations in Guided Setup" on page 14)-Define the categories and elements that you use to organize your equipment.
- *Device Setup* (on page 14)-Discover devices in your network and add them to CC-SG. Configure device ports.
- *Create Groups* (on page 16)-Categorize the devices and nodes that CC-SG manages into groups and create full access policies for each group.
- *User Management* (on page 19)-Add users and user groups to CC-SG, and select the policies and privileges that govern user access within CC-SG and to devices and nodes.

Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

In This Chapter

Before you Use Guided Setup

Before proceeding with CC-SG configuration, you must complete system configuration.

- Configure and install Dominion series and IP-Reach appliances (both serial and KVM devices), including assigning an IP address.

Associations in Guided Setup

Create Categories and Elements

1. In the Guided Setup window, click **Associations**, and then click **Create Categories** in the left panel to open the **Create Categories** panel.

2. In the **Category Name** field, type the name of a category you want to organize your equipment into, such as "Location."

3. In the **Applicable for** field, you can indicate whether you want to category to be available for devices, nodes, or both. Click the **Applicable for** drop-down menu, and then select a value from the list.

4. In the **Elements** table, type the name of an element within the category, such as "Raritan US."

   - Click the Add New Row icon to add more rows to the **Elements** table as needed.

   - To delete an element, select its row, and then click the Delete Row icon to delete the selected element from the **Elements** table.

5. Repeat these steps until you have added all the elements within the category to the **Elements** table.

6. (Optional) If you want to create another category, click **Apply** to save this category, and then repeat the steps in this section to add additional categories.

7. When you have finished creating categories and elements, click **OK**. The Association Summary panel displays a list of the categories and elements that you created.

8. Click **Continue** to start the next task, **Device Setup**. Follow the steps in the next section.

Device Setup

The second task of Guided Setup is **Device Setup**. Device Setup allows you to search for and discover devices in your network, and add those devices to CC-SG. When adding devices you may select one element per category to be associated with the device.

Important: Ensure that no other users are logged into the device during

CC-SG configuration.

Discover and Add Devices

The **Discover Devices** panel opens when you click **Continue** at the end of the Associations task. You can also click **Device Setup**, and then click **Discover Devices** in the **Guided Tasks** tree view in the left panel to open the **Discover Devices** panel.

1. Type the IP address range in which you want to search for devices in the **From address** and **To address** fields.

2. Type the subnet mask in which you want to search for devices in the **Mask** field.

3. In the **Device types** list, select the type of device you want to search for in the range specified. Press and hold down the **CONTROL** key while you click device types to select multiple device types.

4. Check **Broadcast discovery** if searching for devices on the same subnet on which CC-SG resides. Uncheck **Broadcast discovery** to discover devices across all subnets.

5. Click **Discover**.

6. When the discovery is complete, a confirmation message pops up. Click **OK** in the confirmation message.

7. If CC-SG has discovered devices of the specified type and in the specified address range, the devices display in a table in the bottom section of the **Discover Devices** panel. You can click the black arrow at the top of the panel to hide the top section, expanding your view of the discovery results in the bottom section of the panel.

8. In the table of discovered devices, select the device you want to add to CC-SG, and then click **Add**. The **Add Device** panel opens. The **Add Device** panel is slightly different depending on the type of device you are adding.

9. You can change the **Device name** and **Description** by typing new information in the corresponding fields.

10. Confirm that the IP address you assigned when you prepared the device to be added to CC-SG displays in the **Device IP or Hostname** field, or type the correct address in the field if necessary.

11. The **TCP Port Number** field will be populated automatically based on the device type.

12. Type the **Username** and **Password** you created when you prepared the device to be added to CC-SG in the corresponding fields.

13. In the **Heartbeat timeout** field, type the number of seconds that should elapse before timeout between the device and CC-SG.

14. If you are adding a Dominion SX device, check the **Local access: Allowed** checkbox if you want to allow local access to the device. Clear the **Local access: Allowed** checkbox if you do not want to allow local access to the device.

15. If you are manually adding a PowerStrip device, click the **Number of ports** drop-down arrow and select the number of outlets the PowerStrip contains.

16. If you are adding an IPMI Server, type an **Interval** that is used to check for availability, and an **Authentication Method**, which needs to match what has been configured on the IPMI Server, in the corresponding fields.

17. If you want to configure all available ports on the device, check the **Configure all ports** checkbox. CC-SG will add all ports on the device to CC-SG and create a node for each port.

18. In the **Device Associations** section at the bottom of the panel, click the drop-down arrow in the Element column that corresponds to each Category you want to assign to the device, and then select the element you want to associate with the device from the list.

19. If you want the Element to apply to the device and to the nodes connected to the device, check the **Apply to Nodes** checkbox.

20. (Optional) If you want to add another device, click **Apply** to save this device, and then repeat the steps in this section to add additional devices.

21. When you have finished adding devices, click **OK**. The **Device Summary** panel displays a list of the devices that you added.

22. Click **Continue** to start the next task, **Create Groups**. Follow the steps in the next section.

Create Groups

The third task of Guided Setup is **Create Groups**. Create Groups allows you to define groups of devices and groups of nodes and specify the set of devices or nodes included in each group. Administrators can save time by managing groups of similar devices and nodes, rather than managing each device or node individually.

Add Device Groups and Node Groups

1. The **Devices Groups Manager** panel opens when you click **Continue** at the end of the Device Setup task. You can also click **Create Groups**, and then click **Add Devices Groups** in the **Guided Tasks** tree view in the left panel to open the **Devices Groups Manager** panel.

2. In the **Group name** field, type a name for a device group you want to create.

3. There are two ways to add devices to a group, **Select Devices** and **Describe Devices**. The Select Devices tab allows you to select which devices you want to assign to the group by selecting them from the list of available devices. The Describe Devices tab allows you to specify rules that describe devices, and the devices whose parameters follow those rules will be added to the group.

Select Devices

   a. Click the Select Devices tab in the Add Devices Groups panel.

   b. In the **Available** list, select the device you want to add to the group, and then click **Add** to move the device into the **Selected** list. Devices in the **Selected** list will be added to the group.

   ▪ To remove a device from the group, select the device name in the **Selected** list, and then click **Remove**.

   ▪ You can search for a device in either the **Available** or **Selected** list. Type the search terms in the field below the list, and then click **Go**.

Describe Devices

   a. Click the **Describe Devices** tab in the **Add Devices Groups** panel. In the Describe Devices tab, you create a table of rules that describe the devices you want to assign to the group.

   b. Click the Add New Row icon ⊞ to add a row to the table.

   c. Double-click the cell created for each column to activate a drop-down menu. Select the rule components you want to use from each list.

1. Check the **Create Full Access Policy for Group** checkbox if you want to create a policy for this device group that allows access to all nodes and devices in the group at all times with control permission.

2. (Optional) If you want to add another device group, click **Apply** to save this group, and then repeat the steps in this section to add additional device groups.

3. When you have finished adding device groups, click **OK**. The **Nodes Group Manager** panel opens. You can also click **Create Groups**, and then click **Add Node Groups** in the **Guided Tasks** tree view in the left panel to open the **Node Groups Manager** panel.

4. In the **Group name** field, type a name for a node group you want to create.

5. There are two ways to add nodes to a group, **Select Nodes** and **Describe Nodes**. The Select Nodes section allows you to select which nodes you want to assign to the group by selecting them from the list of available nodes. The Describe Nodes section allows you to specify rules that describe nodes, and the nodes whose parameters follow those rules will be added to the group.

Select Nodes

   a. Click the **Select Nodes** tab in the **Add Nodes Groups** panel.

   b. In the **Available** list, select the node you want to add to the group, and then click **Add** to move the node into the **Selected** list. Nodes in the **Selected** list will be added to the group.

   c. If you want to remove a node from the group, select the node name in the **Selected** list, and then click **Remove**.

   d. You can search for a node in either the **Available** or **Selected** list. Type the search terms in the field below the list, and then click **Go**.

Describe Nodes

   a. Click the **Describe Nodes** tab in the **Add Nodes Groups** panel. In the Describe Nodes tab, you create a table of rules that describe the nodes you want to assign to the group.

   b. Click the Add New Row icon to add a row to the table.

   c. Double-click the cell created for each column to activate a drop-down menu. Select the rule components you want to use from each list. *Policies for Access Control* (on page 91).

   d. Check the **Create Full Access Policy for Group** checkbox if you want to create a policy for this node group that allows access to all nodes in the group at all times with control permission.

e. (Optional) If you want to add another node group, click **Apply** to save this group, and then repeat the steps in this section to add additional node groups.

1. When you have finished adding node groups, click **OK**. The **Group Summary** panel displays a list of the groups that you added.

2. Click **Continue** to start the next task, **User Management**. Follow the steps in the next section.

User Management

The fourth task of Guided Setup is **User Management**. User Management allows you to select the **Privileges** and **Policies** that govern the access and activities of groups of users. Privileges specify which activities the members of the user group can perform in CC-SG. Policies specify which devices and nodes the members of the user group can view and modify. Policies are based on Categories and Elements. When you have created the user groups, you can define individual users and add them to the user groups.

Add User Groups and Users

The **Add User Group** panel opens when you click **Continue** at the end of the Create Groups task. You can also click **User Management**, and then click **Add User Group** in the **Guided Tasks** tree view in the left panel to open the **Add User Group** panel.

1. In the **User group name** field, type a name for the user group you want to create. User group names can contain up to 32 characters.

2. In the **Description** field, type a description of the user group.

3. Click the **Privileges** tab, and then check the checkboxes that correspond to the **Privileges**, or types of CC-SG activities, that you want to assign to the user group.

4. In the **Node Access** section, you can specify whether you want the user group to have access to **In band** and **Out of band** nodes, and to **Power Management** functions. Check the checkboxes that correspond to the types of access you want to assign to the group.

5. Click the **Policies** tab.

6. In the **All Policies** list, select the **Policy** that you want to assign to the user group then click **Add** to move the **Policy** to the **Selected Policies** list. Policies in the **Selected Policies** list will be assigned to the user group. Repeat this step to add additional policies to the user group.

7. If you want to remove a policy from the user group, select the policy name in the **Selected Policies** list, and then click **Remove**.

8. If you want to associate remotely authenticated users with Active Directory modules, click the **Active Directory Associations** tab. Check the checkbox that corresponds with each Active Directory module you want to associate with the user group.

9. (Optional) If you want to add another user group, click **Apply** to save this group, and then repeat the steps in this section to add additional user groups.

10. When you have finished adding user groups, click **OK**. The **Add User** panel opens. You can also click **User Management**, and then click **Add User** in the **Guided Tasks** tree view in the left panel to open the **Add User** panel.

11. In the **Username** field, type the name that the user you want to add will use to log in to CC-SG.

12. Check the **Login Enabled** checkbox if you want the user to be able to log in to CC-SG.

13. Check the **Remote Authentication** checkbox only if you want the user to be authenticated by an outside server, such as TACACS+, RADIUS, LDAP, or AD. If you are using remote authentication, a password is not required. The **New Password** and **Retype New Password** fields will be disabled when **Remote Authentication** is checked.

14. In the **New Password** and **Retype New Password** fields, type the password that the user will use to log in to CC-SG.

15. Check the **Force Password Change on Next Login** if you want the user to be forced to change the assigned password the next time the user logs in.

16. Check the **Force Password Change Periodically** checkbox if you want to specify how often the user will be forced to change the password.

17. In the **Expiration Period (Days)** field, type the number of days that the user will be able to use the same password before being forced to change it.

18. In the **Email address** field, type the user's email address.

19. Click the **User Group** drop-down arrow and select the user group to which you want to assign the user from the list.

20. (Optional) If you want to add another user, click **Apply** to save this user, and then repeat the steps in this section to add additional users.

21. When you have finished adding users, click **OK**. The **User Summary** panel displays a list of the user groups and users that you added.

Chapter 5 Associations, Categories, and Elements

In This Chapter

About Associations

You can set up Associations to help organize the equipment that CC-SG manages. Each Association includes a Category, which is the top-level organizational group, and its related Elements, which are subsets of a Category. For example, you may have Raritan devices that manage target servers in data centers in America, Asia Pacific, and Europe. You could set up an Association that organizes this equipment by location. Then, you can customize the CC-SG to display your Raritan devices and nodes according to your chosen Category-Location, and its associated Elements- America, Asia Pacific, and Europe, in the CC-SG interface. You can customize the CC-SG to organize and display your servers however you like.

Association Terminology

- **Associations**-are the relationships between categories, elements of a category, and nodes and devices.

- **Category**-is a variable that contains a set of values called elements. An example of a category is Location, which may have elements such as "America," and "Asia Pacific." Another example of a category is "OS Type", which may have elements such as "Windows" or "Unix" or "Linux".

- **Elements**-are the values of a category. For example, the "America" element belongs to the "Location" category.

Associations--Defining Categories and Elements

Raritan devices and nodes are organized by categories and elements. Each category/element pair is assigned to a device, a node, or both. Therefore, you need to define your categories and elements before you add a Raritan device to CC-SG.

A category is a group of similar elements. For example, to group your Raritan devices by location, you would define a category, Location, which would contain a set of elements, such as New York, Philadelphia, and New Orleans.

Policies also use categories and elements to control user access to servers. For example, the category/element pair Location/New York can be used to create a Policy to control user access to servers in New York.

Other examples of typical Association configurations of Category and Elements are as follows:

Category	Elements
Location	New York City, Philadelphia, New Orleans
OS Type	Unix, Windows, Linux
Department	Sales, IT, Engineering

Association configurations should be kept simple to accomplish server/node organizational objectives and user access objectives. A node can only be assigned to a single element of a category. For example, a target server cannot be assigned to both the Windows and Unix elements of the OS Type category.

A useful approach to organizing your systems when servers are similar and need to be randomly organized is the following:

Category	Element
usergroup1	usergroup1node
usergroup2	usergroup2node
usergroup3	usergroup3node

As you add devices and nodes to CC-SG, you link them to your predefined categories and elements. When you create node and device groups and assign policies to them, you will use your categories and elements to define which nodes and devices belong in each group.

How to Create Associations

There are two ways to create associations, Guided Setup and Association Manager.

- **Guided Setup** combines many configuration tasks into an automated interface. Guided Setup is recommended for your initial CC-SG configuration. Once you have completed Guided Setup, you can always edit your configurations individually. *Configuring CC-SG with Guided Setup* (on page 13)

- **Association Manager** only allows you to work with associations, and does not automate any configuration tasks. You can also use Association Manager to edit your Associations after using Guided Setup. *Association Manager* (on page 24)

Association Manager

Association Manager allows you to add, edit, or delete Categories and Elements.

Add a Category

1. Choose **Associations** > **Association**.

2. Click **Add**. The **Add Category** window appears.

3. Type a category name in the **Category Name** field. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

4. Select the Data Type for Elements.

   - Select **String** if the value is read as text.

   - Select **Integer** if the value is a number.

5. In the Applicable For field, select whether this category applies to: **Devices, Nodes**, or **Device and Nodes**.

6. Click **OK** to create the new category. The new category name appears in the **Category Name** field.

Edit a Category

Please note that a string value cannot be changed to an integer value, and vice versa. If you must make this type of change, please delete the category, and add a new one.

1. Choose **Associations** > **Association**.

2. Click the **Category Name** drop-down arrow and select the category you want to edit.

3. Click **Edit** in the **Category** panel of the screen to edit the category. The **Edit Category** window appears.

4. Type the new category name in **Category Name** field.

5. Click the **Applicable For** drop-down arrow to change whether this category applies to **Device, Node,** or **Both**.

6. Click **OK** to save your changes. The updated category name appears in the **Category Name** field.

Delete a Category

Deleting a category deletes all of the elements created within that category. The deleted category will no longer appear in the Nodes or Devices trees once the screen refreshes or the user logs out and then logs back into CC-SG.

1. Choose **Associations** > **Association**.

2. Click the **Category Name** drop-down arrow and select the category you want to delete.

3. Click **Delete** in the **Category** panel of the screen to delete the category. The **Delete Category** window appears.

4. Click **Yes** to delete the category.

Add an Element

1. Choose **Associations** > **Association.**

2. Click the **Category Name** drop-down arrow and select the category to which you want to add a new element.

3. Click the Add a new row icon.

4. Type the new element name in the blank row. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths. Element names are case-sensitive.

5. Click **OK** to save your changes.

Edit an Element

1. On the **Associations** menu, click **Association Manager.**

2. Click the **Category Name** drop-down arrow and select the category whose element you want to edit.

3. Select the element to be edited from the **Element For Category** list, and then click **Edit** in the **Elements For Category** panel. The **Edit Element** window appears.

4. Type the new name of the element in the **Enter New Value for Element** field. Element names are case-sensitive.

5. Click **OK** to update the element or **Cancel** to close the window. The new element name is displayed in the **Element For Category** list.

Delete an Element

Deleting an element removes that element from all associations, leaving association fields blank.

1. Choose **Associations** > **Association.**

2. Click the **Category Name** drop-down arrow and select the category whose element you want to delete.

3. Select the element to be deleted from the **Elements** list, and then click the Remove Row icon.

4. Click OK to save your changes.

Chapter 6   Devices and Ports

If you want to add Raritan PowerStrip Devices that are connected to other Raritan devices to CC-SG, please refer to *Configuring Power Control* (see "Managed Powerstrips" on page 51)for details.

*Note: To configure iLO/RILOE devices, IPMI devices, Dell DRAC devices, IBM RSA devices or other non-Raritan devices, use the **Add Node** menu and add these items as an interface. Please refer to **Nodes, Node Groups, and Interfaces** (on page 58) for details.*

In This Chapter

Viewing Devices

The Devices Tab

Click the **Devices** tab to display all devices under CC-SG management.
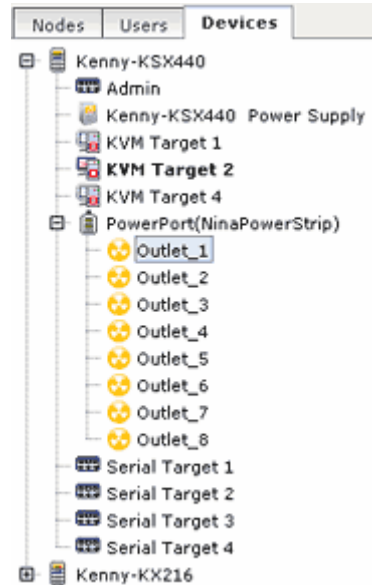
Each device's configured ports are nested under the devices they belong to. Devices with configured ports appear in the list with a + symbol. Click the + symbol to show or hide the list of ports.

Device Profile Screen

When you click a device from the Devices tab, the **Device Profile** screen appears, displaying information about the selected device.
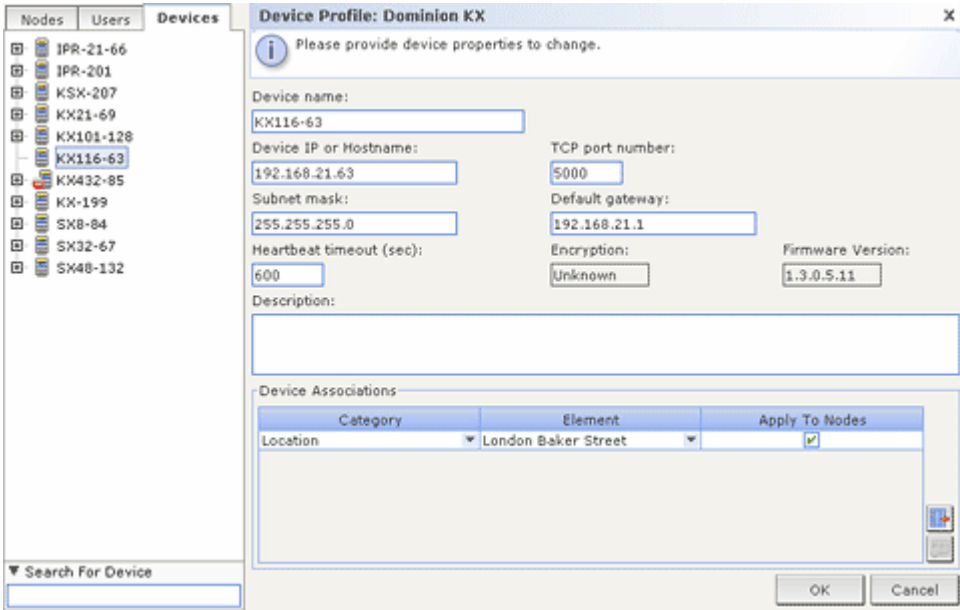
Device and Port Icons

For easier identification, KVM, Serial, and Power devices and ports have different icons in the Devices tree. Hold the mouse pointer over an icon in the Devices tree to view a tool tip containing information about the device or port.

Icon	Meaning
	Device available
	KVM port available or connected
	KVM port inactive
	Serial port available
	Serial port unavailable
	Ghosted port (See Raritan's Paragon II User Guide for details on Ghosting Mode.)
	Device paused

	Device unavailable
	Power strip
	Outlet port

Port Sorting Options

Configured ports are nested under their parent devices in the Devices tab. You can change the way ports are sorted. Ports arranged by status are sorted alphabetically within their connection status grouping. Devices will also be sorted accordingly.

1. Choose **Devices** > **Port Sorting Options**.

2. Select **By Port Name** or **By Port Status** to arrange the ports within their devices alphabetically by name or by availability status.

Right Click Options in the Devices Tab

You can right-click a device or port in the Devices tab to display a menu of commands available for the selected device or port.

Search for Devices

The Devices tab provides the ability to search for devices within the tree. Searching will only return devices as results and will not include port names. The method of searching can be configured in **My Profile** (see "Change your default search preference" on page 88).

➢ *To search for a device:*

- At the bottom of the Devices Tab, type a search string in **Search For Device** field, then press **ENTER**.

- *Wildcards* (see "Wildcards for Search" on page 30) are supported in the search string.

Wildcards for Search

Wildcard	Description
?	Indicates any character.
[-]	Indicates a character in range.
*	Indicates zero or more characters.

Wildcard Examples

Example	Description
KX?	Locates **KX1**, and **KXZ**, but not **KX1Z**.
KX*	Locates **KX1**, **KX**, **KX1**, and **KX1Z**.
KX[0-9][0-9]T	Locates **KX95T**, **KX66T**, but not **KXZ** and **KX5PT**.

Discover Devices

Discover Devices initiates a search for all Raritan devices on your network. After discovering the devices, you may add them to CC-SG if they are not already managed.

➢ *To discover devices:*

1. Choose **Devices** > **Discover Devices**.

2. Type the range of IP addresses where you expect to find the devices in the **From Address** and **To Address** fields. The **To Address** should be larger than the **From Address**. Specify a mask to apply to the range. If a mask is not specified, then a broadcast address of **255.255.255.255** is sent, which broadcasts to all local networks. To discover devices across subnets, you must specify a mask.

3. Check **Broadcast discovery** if searching for devices on the same subnet on which CC-SG resides. Uncheck **Broadcast discovery** to discover devices across different subnets.

4. To search for a particular type of device, select it in the list of **Device types**. By default, all device types are selected. Use **CTRL+click** to select more than one device type.

5. Check **Include IPMI Agents** if you want to find targets that provide IPMI power control.

6. Click **Discover** to start the search. At any time during the discovery, you can click **Stop** to discontinue the discovery process. Discovered devices appear in a list.

7. To add one or more discovered devices to CC-SG, select the devices from the list, and then click **Add**. The Add Device screen appears with some of the data already populated.

If you selected more than one device to add, you can click **Previous** and **Skip** at the bottom of the screen to navigate through the Add Device screens for the devices you want to add.

8. Type the user name and password in the **Username** and **Password** fields to allow CC-SG to authenticate the device when communicating with it in the future.

9. Select the **Categories** and **Elements** you want to apply to the device.

10. If you want a Category and Element to apply to the nodes connected to the device, check the corresponding **Apply to Nodes** checkbox.

11. (Optional) Edit the **Device Name**, **Heartbeat Timeout**, **Local Access** (if available for the device type), **Description, Configure all ports,** and **Device Association** fields.

12. When you are done configuring this device, click **Apply** to add this device and open the Add Device screen for the next discovered device. Or, click **OK** to add this device without continuing to the other discovered devices.

   If the firmware version of a device is not compatible with CC-SG, a message appears. Click **Yes** to add the device to CC-SG, or **No** to cancel the operation. You can upgrade the device firmware after adding the device to CC-SG. Please refer to **Upgrade Devices** for details.

Add a Device

Devices must be added to CC-SG before you can configure ports or add interfaces that provide access to the nodes connected to ports. **Add Device** is used to add devices whose properties you know and can provide to CC-SG.

If you want to add Raritan PowerStrip Devices that are connected to other Raritan devices to CC-SG, please refer to *Configuring Power Control* (see "Managed Powerstrips" on page 51) for details.

➢ *To add a device to CC-SG:*

1. Choose **Devices** > **Device Manager** > **Add Device**.

2. Click the **Device Type** drop-down arrow and then select the type of device you are adding from the list. If you select **PowerStrip**, you will see a slightly different Add Device screen.

Add a KVM or Serial Device

1. Type a name for the device in the **Device name** field. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

2. Type the IP Address or Hostname of the device in the **Device IP or Hostname** field. For hostname rules, please refer to *Terminology/Acronyms* (on page 2).

3. Type number of the TCP communication port used to communicate with the device in the **TCP Port Number** field. Maximum is 5 numeric characters. The default port number for most Raritan devices is 5000.

4. Type the name used to log onto this device in the **Username** field. The user must have administrative access.

5. Type the password needed to access this device in the **Password** field. The user must have administrative access.

6. Type the time (in seconds) that should elapse before timeout between the new device and CC-SG in the **Heartbeat timeout (sec)** field.

7. When adding a Dominion SX device, the Allow Local Port Access checkbox enables you to allow or deny local port access to the device. Select the checkbox if you want to allow users to have direct access to this device while it is managed by CC-SG.

8. (Optional) Type a short description of this device in the **Description** field.

9. Check **Configure all ports** if you want to automatically add all ports on this device to the Devices tab, and create a Node for each port on this device in the Nodes tab.

    -   Corresponding nodes and ports will be configured with matching names.

    -   A new node will be created for each port, and an out-of-band interface will be created for that node.

10. A list of **Categories** and **Elements** can be configured to better describe and organize this device and the nodes connected to it. Please refer to *Associations* (see "Associations, Categories, and Elements" on page 22) for details.

a. For each **Category** listed, click the **Element** drop-down menu, and then select the element you want to apply to the device from the list. Select the blank item in the **Element** field for each Category you do not want to use.

If you want to assign the Element to the related nodes as well as the device, check the **Apply to Nodes** checkbox.

If you do not see the **Category** or **Element** values you want to use, you can add more through the **Associations** menu. Please refer to *Associations* (see "Associations, Categories, and Elements" on page 22) for details.

11. When you are done configuring this device, click **Apply** to add this device and open a new blank Add Device screen that allows you to continue adding devices. Or, click **OK** to add this device without continuing to a new Add Device screen.

12. If the firmware version of the device is not compatible with CC-SG, a message appears. Click **Yes** to add the device to CC-SG. You can upgrade the device firmware after adding it to CC-SG. Please refer to *Upgrade a Device* **(on page 38)** for details..

Add a PowerStrip Device

The process of adding a PowerStrip Device to CC-SG varies depending on which Raritan device the powerstrip is connected to physically. Please refer to *Managed PowerStrips* (on page 51) for details.

Edit a Device

You can edit a device to rename it and modify its properties.

> *To edit a device:*

1. Click the **Devices** tab and select the device you want to edit.

2. In the Device Profile screen, change the parameters as needed.

3. Click **OK** to save your changes.

Edit a PowerStrip Device

You can edit a Managed PowerStrip device to rename it, modify its properties, and view outlet configuration status.

1. Click the **Devices** tab and select the PowerStrip device you want to edit.

2. Type the new device properties in the appropriate fields on this screen. If necessary, edit the Categories and Elements associated with this device.

3. Click the **Outlet** tab to view all outlets of this PowerStrip.

4. If an outlet is associated with a node, you can click the **Node** hyperlink to open the Node Profile.

5. If an outlet is associated with a node, you can select the outlet, and then click **Power Control** to open the Power Control screen for the associated node.

6. Click **OK** to save your changes. A message appears when the device has been modified.

Delete a Device

You can delete a device to remove it from CC-SG management.

Important: Deleting a device will remove all ports configured for that device. All interfaces associated with those ports will be removed from the nodes. If no other interface exists for these nodes, the nodes will also be removed from CC-SG.

*Note: You must first pause KSX devices before they can be successfully deleted from CC-SG. To pause a KSX device, right-click the device in the Devices tab, and then click **Pause Management**. Click **Yes** in the message that appears to confirm. The KSX device will restart. Once the device has been paused, you can delete it from CC-SG.*

1. Click the **Devices** tab and select the device you want to delete.

2. Choose **Devices** > **Device Manager** > **Delete Device**.

3. Click **OK** to delete the device. A message appears when the device has been deleted.

Configure Ports

If the ports of a device were not all automatically added by checking **Configure all ports** when you added the device in the **Add Device** screen, you can use the Configure Ports screen to add individual ports or a set of ports on the device to CC-SG. You must configure ports before any Out-of-Band interfaces can be added to nodes.

Configure a Serial Port

1. Click the **Devices** tab and select a serial device.

2. Choose **Devices** > **Port Manager** > **Configure Ports**.

3. Click a column header to sort the ports by that attribute in ascending order. Click the header again to sort the ports in descending order.

4. Click the **Configure** button that corresponds to the serial port you want to configure.

5. Type a port name in **Port Name** field. For ease of use, name the port after the target that is connected to the port. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

6. Type a node name in the **Node Name** field to create a new node with an Out-of-Band interface from this port. For ease of use, name the node after the target that is connected to the port. This means that you will type the same name in the **Port name** and **Node Name** fields.

7. Click the **Access Application** drop-down menu and select the application you want to use when you connect to this port from the list. To allow CC-SG to automatically select the correct application based on your browser, select **Auto-Detect**.

8. Click **OK** to add the port.

Configure a KVM Port

1. Click the **Devices** tab and select a KVM device.

2. Choose **Devices** > **Port Manager** > **Configure Ports**.

   ▪ Click a column header to sort the ports by that attribute in ascending order. Click the header again to sort the ports in descending order.

3. Click the **Configure** button that corresponds to the KVM port you want to configure.

4. Type a port name in the **Port Name** field. For ease of use, name the port after the target that is connected to the port. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

5. Type a node name in the **Node Name** field to create a new node with an Out-of-Band interface from this port. For ease of use, name the node after the target that is connected to the port. This means that you will type the same name in the **Port name** and **Node Name** fields.

6. Click the **Access Application** drop-down menu and select the application you want to use when you connect to this port from the list. To allow CC-SG to automatically select the correct application based on your browser, select **Auto-Detect**.

7. Click **OK** to add the port.

Edit a Port

You can edit ports to change the name or access application.

1. Click the **Devices** tab and select a port you want to edit.

2. Type a new name for the port in the **Port Name** field, if necessary.

3. Click the **Access Application** drop-down menu and select the application you want to use when you connect to this port from the list. To allow CC-SG to automatically select the correct application based on your browser, select **Auto-Detect**.

4. Click **OK** to save your changes.

Delete a Port

Delete a port to remove the port entry from a Device.

Important: If you delete a port that is associated with a node, the associated out-of-band KVM or Serial interface provided by the port will be removed from the node. If the node has no other interfaces, the node will also be removed from CC-SG.

1. Click the **Devices** tab and select a device whose ports you want to delete.

2. Choose **Devices** > **Port Manager** > **Delete Ports**.

3. Check the ports you wish to delete from the device.

4. Click **OK** to delete the selected port. A message appears when the port has been deleted.

Bulk Copy for Device Categories and Elements

The Bulk Copy command allows you to copy the assigned categories and elements from one device to multiple other devices. Please note that categories and elements are the only properties copied in this process.

1. Click the **Devices** tab and select a device from Devices tree.

2. Choose **Devices** > **Device Manager** > **Bulk Copy**.

3. In the **All Devices** list, select the devices to which you are copying the categories and elements of the device in the **Device Name** field.

4. Click **>** to add a device to the **Selected Devices** list.

5. To remove a device from the **Selected Devices** list, select the device, and then click **<**.

6. Click **OK** to bulk copy. A message appears when the device categories and elements have been copied.

Upgrade a Device

You can upgrade a device when a new versions of device firmware is available.

Important! Please check the Compatibility Matrix to make sure the new device firmware version is compatible with your CC-SG firmware version. If you need to upgrade both CC-SG and a device or group of devices, perform the CC-SG upgrade first, and then perform the device upgrade.

1. Click the **Devices** tab and select a device from the Devices tree.

2. Choose **Devices** > **Device Manager** > **Upgrade Device**.

3. **Firmware Name:** Select the appropriate firmware from the list. Raritan or your reseller will provide this information.

4. Click **OK** to upgrade the device.

   ▪ Upgrading SX and KX devices takes about 20 minutes.

   ▪ If the firmware version of the device is not compatible with CC-SG, a message appears. Click **Yes** to upgrade the device. Click **No** to cancel the upgrade.

5. A message appears. Click **Yes** to restart the device. A message appears when the device has been upgraded.

6. To ensure that your browser loads all upgraded files, close your browser window, and then login to CC-SG in a new browser window.

Backup Device Configuration

You can back up all user configuration and system configuration files for a selected device. If anything happens to the device, you can restore the previous configurations from CC-SG using the backup file created. Each device may back up different components of the configuration. Please refer to the User Guide for the device you want to back up for details.

1. Click the **Devices** tab and select the device you want to back up**.**

2. Choose **Devices** > **Device Manager** > **Configuration** > **Backup**.

3. Type a name in the **Backup name** field to identify this backup.

4. (Optional) Type a short description of the backup in the **Description** field.

5. Click **OK** to back up the device configuration. A message appears when the device configuration has been backed up.

Note: When you backup an SX 3.0.1 device, attached PowerStrip configurations are not backed up. If you restore the SX 3.0.1 device from the backup, you must reconfigure the PowerStrips.

Restore Device Configurations

About Restoring Device Configurations

The following device types allow you to restore a full backup of the device configuration.

- KX
- KSX
- KX101
- SX
- IP-Reach

KX2 devices allow you to choose which components of a backup you want to restore to the device.

- **Protected**: The entire content of the selected backup file, except the network settings (personality package), will be restored to the device.
- **Full**: The entire content of the selected backup file will be restored to the device.
- **Custom**: Allows you to restore Device Setting, User and User Group Settings, or both.

Restore a Device Configuration (KX, KSX, KX101, SX, IP-Reach)

You can restore a full backup configuration to KX, KSX, KX101, SX, and IP-Reach devices.

1. Click the **Devices** tab and select the device you want to restore to a backup configuration.
2. Choose **Devices** > **Device Manager** > **Configuration** > **Restore**.
3. In the **Available Backups** table, select the backup configuration you want to restore to the device.
4. Click **OK**.
5. Click **Yes** to restart the device. A message appears when all data has been restored.

Restore All Configuration Data Except Network Settings to a KX2 Device

The Protected restore option allows you to restore all configuration data in a backup file, except network settings, to a KX2 device.

1. Click the **Devices** tab and select the device you want to restore to a backup configuration.
2. Choose **Devices** > **Device Manager** > **Configuration** > **Restore**.
3. In the **Available Backups** table, select the backup configuration you want to restore to the device.
4. **Restore Type**: select **Protected**.
5. Click **OK**.
6. Click **Yes** to restart the device. A message appears when all user and system configuration data has been restored.

Restore Only Device Settings or User and User Group Data to a KX2 Device

The Custom restore option allows you restore Device Settings, User and User Group Data, or both.

1. Click the **Devices** tab and select the device you want to restore to a backup configuration.
2. Choose **Devices** > **Device Manager** > **Configuration** > **Restore**.
3. In the **Available Backups** table, select the backup configuration you want to restore to the device.
4. **Restore Type**: select **Custom**.
5. **Restore Options**: select the components you want to restore to the device: Device Settings, User and User Group Data.
6. Click **OK**.
7. Click **Yes** to restart the device. A message appears when data has been restored.

Restore All Configuration Data to a KX2 Device

The Full restore option allows you to restore all configuration data in a backup file to a KX2 device.

1. Click the **Devices** tab and select the device you want to restore to a backup configuration.

2. Choose **Devices** > **Device Manager** > **Configuration** > **Restore**.

3. In the **Available Backups** table, select the backup configuration you want to restore to the device.

4. **Restore Type**: select **Full**.

5. Click **OK**.

6. Click **Yes** to restart the device. A message appears when all user and system configuration data has been restored.

Copy Device Configuration

You can copy configurations from one device to another or multiple devices.

Note: Configuration can only be copied between Dominion SX units that have the same number of ports.

1. Click the Devices tab and select the device whose configuration you wish to copy to other devices from the Devices tree.

2. Choose Devices > Device Manager > Configuration > Copy Configuration.

3. If you have used the Backup Device option on this device, you can copy that configuration instead by selecting From Saved Configuration and then selecting the configuration from the saved configuration drop-down menu.

4. Highlight the devices you want to copy this configuration to in the Available Devices column, and then click the right arrow to move them to the Copy Configuration To column. The left arrow moves selected devices out of the Copy Configuration To column.

5. Click OK to copy the configuration to the devices in the Copy Configuration To column.

6. When the Restart message appears, click Yes to restart the device. A message appears when the device configuration has been copied.

Restart Device

Use the Restart Device function to restart a device.

1. Click the **Devices** tab and select the device you want to restart.

2. Choose **Devices** > **Device Manager** > **Restart Device**.

3. Click **OK** to restart the device.

4. Click Yes to confirm that all users accessing the device will be logged off.

Ping Device

You can ping a device to determine if the device is available in your network.

1. Click the **Devices** tab and select the device you want to ping.

2. Choose **Devices** > **Device Manager** > **Ping Device**. The **Ping Device** screen appears, showing the result of the ping.

Pause Management

You can pause a device to temporarily suspend CC-SG control of it without losing any of the configuration data stored within CC-SG.

1. Click the **Devices** tab and select the device for which you want to pause CC-SG management.

2. Choose **Devices** > **Device Manager** > **Pause Management**. The device's icon in the Device Tree will indicate the device's paused state.

Resume Management

You can resume CC-SG management of a paused device to bring it back under CC-SG control.

1. Click the **Devices** tab and select the paused device from the Devices tree.

2. Choose **Devices** > **Device Manager** > **Resume Management**. The device icon in the Device Tree will indicate the devices active state.

Device Power Manager

Device Power Manager is used to view the status of a PowerStrip device (including voltage, current, and temperature) as well as manage all power outlets on a PowerStrip device. Device Power Manager provides a PowerStrip-centric view of its outlets.

Before using the Device Power Manager, a physical connection needs to be made between a PowerStrip and a Dominion SX or Dominion KSX unit. When you add the PowerStrip device, you must define which Raritan device is providing the connection. This will associate it with the Dominion SX serial port or with Dominion KSX dedicated power port that is providing management of the PowerStrip.

1. In the **Devices** tab, select a PowerStrip device.

2. Choose **Devices** > **Device Power Manager**.

3. The outlets are listed in the **Outlets Status** panel. You may have to scroll to view all outlets.

   ▪ Click the **On** or **Off** radio buttons for each outlet to power ON or power OFF the outlet.

   ▪ Click **Recycle** to restart the device connected to the outlet.

Launch Admin

If available for the device selected, the **Launch Admin** command will provide you access to the device's administrator interface.

1. Click the **Devices** tab and select the device whose administrator interface you want to launch.

2. Choose **Devices** > **Device Manager** > **Launch Admin**. The administrator interface for the selected device appears.

Topological View

Topological View displays the structural setup of all the connected appliances in your configuration.

Until you Close the Topological View, this view replaces the Device Profile screen that normally appears when a device is selected.

1. Click the **Devices** tab and select the device whose topological view you want to see.

2. Choose **Devices** > **Device Manager** > **Topological View.** The **Topological View** for the selected device appears.

- Click + or - to expand or collapse the view.

Disconnect Users

Administrators can terminate any user's session with a device. This includes users who are performing any kind of operation on a device, such as connecting to ports, backing up the configuration of a device, restoring a device's configuration, or upgrading the firmware of a device.

Firmware upgrades and device configuration backups and restores are allowed to complete before the user's session with the device is terminated. All other operations will be terminated immediately.

For Dominion SX devices only, you can disconnect users who are directly logged onto the device as well as those who are connected to the device via CC-SG.

1. Click the **Devices** tab and select the device you want to disconnect one or more users from.

2. Choose Devices > Device Manager > Disconnect Users.

3. Select the users whose session you want to disconnect in the **Disconnect users** table.

4. Click **Disconnect** to disconnect them from the device.

Special Access to Paragon II System Devices

Paragon II System Controller (P2-SC)

Paragon II System Integration users can add their P2-SC devices to the CC-SG Devices tree and configure them via the P2-SC Admin application from within CC-SG. Please refer to Raritan's **Paragon II System Controller User Guide** for details on using P2-SC Admin.

After adding the Paragon System device (the Paragon System includes the P2-SC device, connected UMT units, and connected IP-Reach units) to CC-SG, it appears in the Devices tree.

➢ *To access Paragon II System Controller:*

1. Click the **Device** tab, and then select the Paragon II System Controller.

2. Right-click the Paragon II System Controller, and then click **Launch Admin** to launch the Paragon II System Controller application in a new browser window. You can then configure the PII UMT units.

IP-Reach and UST-IP Administration

You can also perform administrative diagnostics on IP-Reach and UST-IP devices connected to your Paragon System setup directly from the CC-SG interface.

After adding the Paragon System device to CC-SG, it appears in the Devices tree.

➢ *To access Remote User Station Administration:*

1. Click the **Devices** tab, and then select the **Paragon II System Controller**.

2. Right-click the **Paragon II System Controller**, and select **Remote User Station Admin.** The Remote User Station Admin screen appears, listing all connected IP-Reach and UST-IP units.

3. Click **Launch Admin** in the row of the device you want to work with to activate Raritan Remote Console and launch the blue device configuration screen in a new window.

Device Group Manager

Use the Device Groups Manager to add device groups, edit device groups, and remove device groups. When you add a new device group, you can create a full access policy for the group. Please refer to *Policies for Access Control* (on page 91) for details.

Add a Device Group

1. Choose **Associations** > **Device Groups**. The Device Groups Manager window opens. Existing device groups display in the left panel.

2. Click the New Group icon in the toolbar. The **Device Group: New** panel displays.

3. In the **Group name** field, type a name for a device group you want to create. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

4. There are two ways to add devices to a group, **Select Devices** and **Describe Devices**. The Select Devices tab allows you to select which devices you want to assign to the group by selecting them from the list of available devices. The Describe Devices tab allows you to specify rules that describe devices, and the devices whose parameters follow those rules will be added to the group.

➢ *Select Devices*

   a. Click the Select Devices tab.

   b. In the **Available** list, select the device you want to add to the group, then click **Add** to move the device into the **Selected** list. Devices in the **Selected** list will be added to the group.

   ▪ To remove a device from the group, select the device name in the **Selected** list, and then click **Remove**.

   ▪ You can search for a device in either the **Available** or **Selected** list. Type the search terms in the field below the list, and then click **Go**.

➢ *Describe Devices*

   a. Click the **Describe Devices** tab in the **Device Group: New** panel. In the Describe Devices tab, you create a table of rules that describe the devices you want to assign to the group.

   b. Click the Add New Row icon to add a row to the table.

   c. Double-click the cell created for each column to activate a drop-down menu. Select the rule components you want to use from each list.

1. **Prefix** - Leave this blank or select **NOT**. If **NOT** is selected, this rule will filter for values opposite of the rest of the expression.

2. **Category** - Select an attribute that will be evaluated in the rule. All categories you created in the **Association Manager** will be available here.

3. **Operator** - Select a comparison operation to be performed between the Category and Element items. Three operators are available: **=** (is equal to), **LIKE** (used for find the Element in a name) and **<>** (is not equal to)**.**

4. **Element** - Select a value for the Category attribute to be compared against. Only elements associated with the selected category will display here (for example: if evaluating a "Department" category, "Location" elements will not appear here).

5. **Rule Name**- This is a name assigned to the rule in this row. It is not editable, it is used for writing descriptions in the **Short Expression** field.

6. If you want to add another rule, click **Add New Row**, and then make the necessary configurations. Configuring multiple rules will allow more precise descriptions by providing multiple criteria for evaluating devices.

7. The table of rules only makes available criteria for evaluating nodes. To write a description for the device group, add the rules by **Rule Name** to the **Short Expression** field. If the description only requires a single rule, then simply type that rule's name in the field. If multiple rules are being evaluated, type the rules into the field using a set of logical operators to describe the rules in relation to each other:

& - the AND operator. A node must satisfy rules on both sides of this operator for the description (or that section of a description) to be evaluated as true.

| - the OR operator. A device only needs to satisfy one rule on either side of this operator for the description (or that section of a description) to be evaluated as true.

(and **)** - grouping operators. This breaks the description into a subsection contained within the parentheses. The section within the parentheses is evaluated first before the rest of the description is compared to the node. Parenthetical groups can be nested inside another parenthetical group.

Example1: If you want to describe devices that belong to the engineering department, create a rule that says Department = Engineering. This will become Rule0. Then type Rule0 in the **Short Expression** field.

Example 2: If you want to describe a group of devices that belong to the engineering department, or are located in Philadelphia, and specify that all of the machines must have 1 GB of memory you need to start by creating three rules. Department = Engineering (Rule0) Location = Philadelphia (Rule1) Memory = 1GB (Rule2).These rules need to be arranged in relation to each other. Since the device can either belong to the engineering department or be located in Philadelphia, use the OR operator, **|,** to join the two: Rule0|Rule1. We will make this comparison first by enclosing it parentheses: (Rule0|Rule1). Finally, since the devices must both satisfy this comparison AND contain 1GB of memory, we use the AND connector, **&,** to join this section with Rule2: (Rule0|Rule1)&Rule2. Type this final expression in the **Short Expression** field.

- If you want to remove a row from the table, select the row, and then click the Remove Selected Row icon [icon].

- If you want to see the list of devices whose parameters follow the rules you have defined, click **View Devices**.

  a. Click **Validate** when a description has been written in the **Short Expression** field. If the description is formed incorrectly, you will receive a warning. If the description is formed correctly, a normalized form of the expression appears in the **Normalized Expression** field.

  b. Click **View Devices** to see what nodes satisfy this expression. A **Devices in Device Group Results** window appears displaying the devices that will be grouped by the current expression. This can be used to check if the description was correctly written. If not, you can return to the rules table or the **Short Expression** field to make adjustments.

  c. Check the **Create Full Access Policy for Group** checkbox if you want to create a policy for this device group that allows access to all devices in the group at all times with control permission.

  d. (Optional) If you want to add another device group, click **Apply** to save this group, then repeat the steps in this section to add additional device groups. If you have finished adding device groups, click **OK** to save your changes.

Edit a Device Group

1. Choose **Associations** > **Device Groups**. The Device Groups Manager window opens.

2. Existing device groups display in the left panel. Select the Device Group whose name you want to edit. The Device Group Details panel appears.

3. (Optional) Type a new name for the device group in the **Group Name** field.

4. Edit the device group's included devices using the Select Device or Describe Devices tabs. Please refer to **Add a Device Group** (on page 46) for details.

5. Click **OK** to save your changes.

Delete a Device Group

1. Choose **Associations** > **Device Groups**. The Device Groups Manager window opens.

2. Existing device groups display in the left panel. Select the device group you want to delete. The Device Group Details panel appears.

3. Choose **Groups** > **Delete**.

4. The Delete Device Group panel appears. Click **Delete**.

5. Click **Yes** in the confirmation message that displays.

Chapter 7 Managed Powerstrips

In CC-SG, PowerStrips must be connected to one of the following devices:

- Dominion KX
- Dominion KX2
- Dominion SX 3.0
- Dominion SX 3.1
- Dominion KSX
- Paragon II System Controller (P2SC)

To configure PowerStrips in CC-SG , you must know which Raritan device the powerstrip is connected to physically.

In This Chapter

Process for Configuring Power Control in CC-SG

1. Complete all physical connections between the device, the powerstrip, and the nodes that are powered by the powerstrip. Please refer to the RPC Quick Setup Guide, Dominion PX Quick Setup Guide, and CC-SG Deployment Guide for details on physical connections between PowerStrips, devices, and nodes.

2. Add the managing device to CC-SG. The procedure varies for different Raritan devices. Please refer to the section that corresponds to the device to which the PowerStrip is connected:

   - *Configuring PowerStrips Connected to KX, KX2, and P2SC* (on page 52)

   - *Configuring PowerStrips Connected to SX 3.0 and KSX* (on page 53)

   - *Configuring PowerStrips Connected to SX 3.1* (on page 55).

3. *Configure outlets* (see "Configure Outlets on a PowerStrip" on page 56).

4. Associate each outlet with the node that it powers: *Add a Managed PowerStrip interface to the node* (see "Interfaces for Managed Power Strip connections" on page 65)

Configuring PowerStrips Connected to KX, KX2, and P2SC

CC-SG automatically detects PowerStrips connected to KX and KX2 devices. You can perform the following tasks in CC-SG to configure and manage PowerStrips connected to KX and KX2 devices.

- Add a PowerStrip Device Connected to a KX or KX2 Device
- Move a KX or KX2's PowerStrip to a Different Port
- Delete a PowerStrip Connected to a KX or KX2 Device

Add a PowerStrip Device Connected to a KX, KX2, or P2SC Device

When you add a KX or KX2 device that is connected to a PowerStrip to CC-SG, the PowerStrip is added automatically. The PowerStrip will display in the Devices tab, beneath the KX or KX2 device that it is connected to.

Next Steps:

1. *Configure outlets* (see "Configure Outlets on a PowerStrip" on page 56).

2. Associate each outlet with the node that it powers: *Add a Managed PowerStrip interface to the node* (see "Interfaces for Managed Power Strip connections" on page 65)

Move a KX, KX2, or P2SC's PowerStrip to a Different Port

When you physically move a PowerStrip from one KX, KX2, or P2SC device or port to another KX, KX2, or P2SC device or port, CC-SG automatically detects the PowerStrip and updates its association to the correct device. You do not have to add the PowerStrip to CC-SG separately.

Note: When you physically remove a PowerStrip from a P2SC port, but you do not connect it to another port, CC-SG does not remove the PowerStrip from the old port. You must perform a partial or full database reset of the UMT to which the PowerStrip is connected to remove the PowerStrip from the Devices tab. Please refer to the Raritan

Delete a PowerStrip Connected to a KX, KX2, or P2SC Device

You cannot delete a PowerStrip connected to a KX or KX2 device from CC-SG. You must physically disconnect the PowerStrip from the KX or KX2 device to delete the PowerStrip from CC-SG. When you physically disconnect the PowerStrip from a KX or KX2 device, the PowerStrip and all configured outlets disappear from the Devices tab.

Configuring PowerStrips Connected to SX 3.0 and KSX

You can perform the following tasks in CC-SG to configure and manage PowerStrips connected to SX 3.0 or KSX devices.

Note: PowerStrips must be physically connected to the Power Port of a KSX device.

- Add a PowerStrip Connected to an SX 3.0 or KSX Device
- Delete a PowerStrip Connected to an SX 3.0 or KSX Device
- Change a PowerStrip's Device or Port Association (SX 3.0, KSX)

Add a PowerStrip Connected to an SX 3.0 or KSX device

1. *Add the SX 3.0 or KSX device to CC-SG* (see "Add a KVM or Serial Device" on page 33).

2. Choose **Devices** > **Device Manager** > **Add Device**.

3. Select **PowerStrip** from the **Device type** drop-down menu.

4. Type a name for the PowerStrip in the **Power Strip Name** field. Hold your cursor over the field to see the number of characters allowed in the name. Spaces are not permitted.

5. Click the **Number of Outlets** drop-down menu and select the number of outlets this PowerStrip contains.

6. Click the **Managing Device** drop-down menu, and then select the SX 3.0 or KSX device that is connected to this power strip.

7. Click the **Managing Port** drop-down menu, and then select the port on the SX 3.0 or KSX device to which this power strip is connected.

8. (Optional) Type a short description of this PowerStrip in the **Description** field

9. (Optional) Check **Configure All Outlets** if you want to automatically add each outlet on this PowerStrip device to the **Devices** tab. If you don't configure all outlets now, you can *configure them later* (see "Configure Outlets on a PowerStrip" on page 56).

10. (Optional) For each **Category** listed, click the **Element** drop-down menu, and then select the element you want to apply to the device from the list. Select the blank item in the **Element** field for each Category you do not want to use. Please refer to *Associations* (see "Associations, Categories, and Elements" on page 22) for details.

11. When you are done configuring this PowerStrip, click **Apply** to add this device and open a new blank Add Device screen that allows you to continue adding devices. Or, click **OK** to add this Power Strip without continuing to a new Add Device screen.

Next Steps:

1. *Configure outlets* (see "Configure Outlets on a PowerStrip" on page 56).

2. Associate each outlet with the node that it powers: *Add a Managed PowerStrip interface to the node* (see "Interfaces for Managed Power Strip connections" on page 65)

Delete a PowerStrip Connected to an SX 3.0 or KSX Device

You can delete a powerstrip connected to an SX 3.0, KSX or P2SC device, even if the powerstrip is still physically connected. If you disconnect the powerstrip from the SX 3.0, KSX or P2SC device it is associated with, it will still appear in the devices tab beneath that device. If you want to remove it from display, you must delete the powerstrip.

1. In the Devices tab, select the PowerStrip you want to delete.

2. Choose Devices > Device Manager > Delete Device.

3. Click OK to delete the PowerStrip. A message appears when the PowerStrip has been deleted. The PowerStrip icon is removed from the Devices tab.

Change a PowerStrip's Device or Port Association (SX 3.0, KSX)

If a PowerStrip is physically moved from one SX 3.0 or KSX device or port to another SX 3.0 or KSX device or port, you must change the association in the PowerStrip Profile in CC-SG.

1. In the Devices tab, select the PowerStrip that has been moved from one SX 3.0 or KSX device or port to another.

2. Click the **Managing Device** drop-down menu, and then select the SX 3.0 or KSX device that is connected to this powerstrip.

3. Click the **Managing Port** drop-down menu, and then select the port on the SX 3.0 or KSX device to which this powerstrip is connected.

4. Click **OK**.

Configuring PowerStrips Connected to SX 3.1

You can perform the following tasks in CC-SG to configure and manage PowerStrips connected to SX 3.1 devices.

- Add a PowerStrip Device Connected to a SX 3.1 Device
- Move an SX 3.1's PowerStrip to a Different Port
- Delete a PowerStrip Connected to an SX 3.1 Device

Add a PowerStrip Device Connected to an SX 3.1 Device

The procedure for adding a powerstrip connected to an SX 3.1 device varies depending on whether the SX 3.1 device has been added to CC-SG.

If the PowerStrip is connected to the SX 3.1 device, and the device has not been added to CC-SG yet:

1. *Add the SX 3.1 device to CC-SG* (see "Add a KVM or Serial Device" on page 33).

2. CCSG detects the PowerStrip and adds it automatically. The PowerStrip will display in the Devices tab, beneath the SX 3.1 device that it is connected to.

If the SX 3.1 device has already been added to CC-SG, and the PowerStrip is connected to the device later:

1. *Add the SX 3.1 device to CC-SG* (see "Add a KVM or Serial Device" on page 33).

2. *Configure the ports of the SX 3.1 device.* (see "Configure Ports" on page 35)

3. In the **Devices** tab, select the SX 3.1 device to which the PowerStrip is connected.

4. Click the + next to the device icon to expand the list of ports.

5. Right-click the SX 3.1 port that the PowerStrip is connected to, and select Add Powerstrip from the pop-up menu.

6. Enter the number of outlets that the PowerStrip contains, and then click **OK**.

Next Steps:

1. *Configure outlets* (see "Configure Outlets on a PowerStrip" on page 56).

2. Associate each outlet with the node that it powers: *Add a Managed PowerStrip interface to the node* (see "Interfaces for Managed Power Strip connections" on page 65)

Move an SX 3.1's PowerStrip to a Different Port

When you physically move a PowerStrip from one SX 3.1 device or port to another SX 3.1 device or port, you must *delete the PowerStrip from the old SX 3.1 port* (see "Delete a PowerStrip Connected to a SX 3.1 Device" on page 56), and *add it to the new SX 3.1 port* (see "Add a PowerStrip Device Connected to an SX 3.1 Device" on page 55).

Delete a PowerStrip Connected to a SX 3.1 Device

You can delete a powerstrip connected to an SX 3.1 device, even if the powerstrip is still physically connected. If you disconnect the powerstrip from the SX 3.1 device it is associated with, it will still appear in the devices tab beneath that device. If you want to remove it from display, you must delete the powerstrip.

1. In the **Devices** tab, select the PowerStrip you want to delete.

2. Choose **Devices** > **Device Manager**, **Delete Device**.

3. Click **OK** to delete the PowerStrip. A message appears when the PowerStrip has been deleted. The PowerStrip icon is removed from the Devices tab.

Configure Outlets on a PowerStrip

You must configure the outlets on a PowerStrip before you can associate each outlet with a node by *adding the Managed Powerstrip interface to the node.*

 (see "Interfaces for Managed Power Strip connections" on page 65)To configure outlets from the PowerStrip profile:

1. In the **Devices** tab, click the + next to the device that is connected to the PowerStrip to expand all ports.

2. Select the PowerStrip whose outlets you want to configure.

3. In the Device Profile: PowerStrip screen, select the **Outlets** tab.

4. Select the checkbox for each outlet you want to configure, and then click **OK**.

The outlets will display beneath the PowerStrip icon in the **Devices** tab.

➤ *To configure outlets from the Configure Ports screen:*

1. In the **Devices** tab, click the + next to the device that is connected to the PowerStrip to expand all ports.

2. Select the PowerStrip whose outlets you want to configure.

3. Choose **Devices** > **Port Manager** > **Configure Ports**.

   ▪ To configure multiple outlets with the default names shown in the screen, select the checkbox for each outlet you want to configure, and then click **OK** to configure each outlet with the default name.

   ▪ To configure each outlet individually, click the **Configure** button next to the outlet, and then type a name for the outlet in the **Port name** field. Click **OK** to configure the port.

➤ *To delete an outlet:*

1. In the **Devices** tab, click the + next to the device that is connected to the PowerStrip to expand all ports.

2. Click the + next to the PowerStrip to expand all outlets.

3. Choose **Devices** > **Port Manager**, **Delete Ports**.

4. Select the checkbox for each outlet you want to delete, and then click **OK** to delete the outlet.

Chapter 8 Nodes, Node Groups, and Interfaces

This section covers how to view, configure, and edit nodes and their associated interfaces, and how to create node groups. Connecting to nodes is covered briefly. Please refer to Raritan's **CommandCenter Secure Gateway User Guide** for details on connecting to nodes.

In This Chapter

Viewing Nodes

In CC-SG, you can view all nodes in the Nodes tab, and select a node to view its Node Profile.

Nodes Tab

When you click the Nodes tab, all nodes you can access display in a tree structure.

Nodes are displayed alphabetically by name, or grouped by their availability status. Nodes grouped by availability status are sorted alphabetically within their availability grouping. To switch between sorting methods, right-click the tree, click **Node Sorting Options**, then click **By Node Name** or **By Node Status**.

Please refer to *Custom Views* (see "Custom Views for Devices and Nodes" on page 99) for more information on viewing the Nodes tab in different ways.

Node Profile

Click a Node in the Nodes tab to open the **Node Profile** screen, which includes information about the node, its interfaces, the default interface, and the categories and elements assigned to the node. Nodes that support virtual media include an additional column that shows whether virtual media is enabled or disabled.
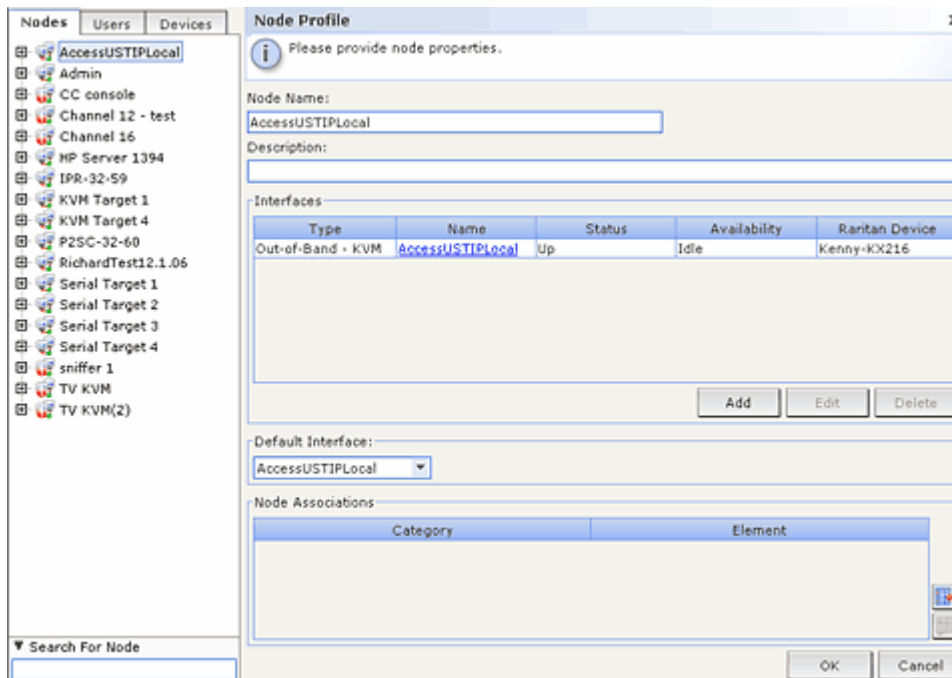
Node and Interface Icons

For easier identification, nodes have different icons in the Nodes tree. Hold the mouse pointer over an icon in the Nodes tree to view a tool tip containing information about the node.

Icon	Meaning
	Node available - the node has at least one interface that is **up**.
	Node unavailable - the node has does not have an interface that is **up**.

Nodes and Interfaces Overview

About Nodes

Each node represents a target that is accessible through CC-SG, either via In-Band (direct IP) or Out-of Band (connected to a Raritan device) methods. For example, a node can be a server in a rack connected to a Raritan KVM over IP device, a server with an HP iLO card, a PC on the network running VNC, or a piece of networking infrastructure with a remote serial management connection.

You can manually add nodes to CC-SG after you have added the devices to which they are connected. However, nodes can also be created automatically, by checking the **Configure all ports** checkbox on the Add Device screen when you are adding a device. This option allows CC-SG to automatically add all device ports, and add a node and an out-of-band KVM or serial interface for each port. You can always edit these nodes, ports, and interfaces later.

Node Names

Node names must be unique. CC-SG will prompt you with options if you attempt to manually add a node with an existing node name. When CC-SG automatically adds nodes, a numbering system ensures that node names are unique.

About Interfaces

In CC-SG, nodes are accessed through interfaces. You must add at least one interface to each new node. You can add different types of interfaces to a node to provide different kinds of access, such as Out-of-Band KVM, serial, or power control, or In-Band SSH/RDP/VNC, DRAC/RSA/ILO, depending on the node type.

A node can have multiple interfaces. A node can only have one out-of-band serial or KVM interface. For example, a Windows Server may have an out-of-band KVM interface for the keyboard, mouse, and monitor ports, and a power interface to manage the outlet to which the server is connected.

Add a Node

➢ *To add a node to CC-SG:*

1. Click the **Nodes** tab.

2. Choose Nodes > **Add Node**.

3. Type a name for the node in the **Node Name** field. All node names in CC-SG must be unique. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

4. (Optional) Type a short description for this node in the **Description** field.

5. You must configure at least one interface. Click **Add** in the **Interfaces** area of the Add Node screen to add an interface. Please refer to *Add an Interface* (on page 62) for details.

6. (Optional) A list of **Categories** and **Elements** can be configured to better describe and organize this node. Please refer to *Associations* (see "Associations, Categories, and Elements" on page 22) for details.

   ▪ For each **Category** listed, click the **Element** drop-down menu, and then select the element you want to apply to the node from the list.

   ▪ Select the blank item in the **Element** field for each Category you do not want to use.

   ▪ If you do not see the **Category** or **Element** values you want to use, you can add more through the **Associations** menu. Please refer to *Associations* (see "Associations, Categories, and Elements" on page 22) for details.

7. Click **OK** to save your changes. The node will be added to the node list.

Nodes Created by Configuring Ports

When you configure the ports of a device, a node is created automatically for each port. An interface is also created for each node.

When a node is automatically created, it is given the same name as the port to which it is associated. If this node name already exists, an extension is added to the node name. For example, Channel1(1). The extension is the number in parentheses. This extension is not included as part of the character count for the node name. If you edit the node name, the new name will be restricted to the maximum number of characters. Please refer to *Naming Conventions* (on page 271) for details.

Add an Interface

1. For an existing node: click the **Nodes** tab, and then select the node to which you want to add an interface. In the **Node Profile** screen that appears, click **Add** in the **Interfaces** section.

   If you are adding a new node: click **Add** in the **Interfaces** section of the **Add Node** screen.

   The **Add Interface Window** appears.

2. Click the **Interface Type** drop-down menu and select the type of connection being made to the node:

   In-Band Connections (see "Interfaces for In-Band connections" on page 64)

   ▪ **In-Band - DRAC KVM**: Select this item to create a KVM connection to a Dell DRAC server through the DRAC interface. You will be required to configure a DRAC Power interface as well.

   ▪ **In-Band - iLO Processor KVM**: Select this item to create a KVM connection to an HP server through an iLO or RILOE interface.

   ▪ **In-Band - RDP**: Select this item to create a KVM connection to a node using Remote Desktop Protocol (for example, the Remote Desktop Connection on a Windows server).

   ▪ **In-Band - RSA KVM**: Select this item to create a KVM connection to an IBM RSA server through its RSA interface. You will be required to configure an RSA Power interface as well.

- **In-Band - SSH**: Select this item to create an SSH connection to a node.

- **In-Band - VNC**: Select this item to create a KVM connection to a node through VNC server software.

Out-of-Band Connections (see "Interfaces for Out-of-Band KVM, Out-of-Band Serial connections" on page 64)

- **Out-of-Band - KVM**: Select this item to create a KVM connection to a node through a Raritan KVM device (KX, KX101, KSX, IP-Reach, Paragon II).

- **Out-of-Band - Serial**: Select this item to create a serial connection to a node through a Raritan serial device (SX, KSX).

Power Control Connections (see "Interfaces for DRAC, RSA and ILO Processor power control connections" on page 64)

- **Power Control - DRAC**: Select this item to create a power control connection to a Dell DRAC server.

- **Power Control - iLO Processor**: Select this item to create a power control connection to an HP iLO/RILOE server.

- **Power Control - IPMI** (see "Interfaces for IPMI Power Control connections" on page 65): Select this item to create a power control connection to a node with an IPMI connection.

- **Power Control - RSA**: Select this item to create a power control connection to an RSA server.

Managed PowerStrip Connections **(see** "Interfaces for Managed Power Strip connections" **on page 65)**

- **Managed PowerStrip**: Select this item to create a power control connection to a node powered through a Raritan PowerStrip, such as Dominion PX.

Web Browser Connections (see "Web Browser Interface" on page 66)

- **Web Browser**: Select this item to create a connection to a device with an embedded Web server.

3. A default name appears in the **Name** field depending on the type of interface you select. You can change the name. This name appears next to the interface in the Nodes list. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

Interfaces for In-Band connections

1. Type the IP Address or Hostname for this interface in the **IP Address/Hostname** field.

2. (Optional) Type a TCP Port for this connection in the **TCP Port** field.

3. Type a username for this connection in the **Username** field.

4. (Optional) Type a password for this connection in the **Password** field.

5. (Optional) Type a description of this interface in the **Description** field.

6. Click **OK** to save your changes.

Interfaces for Out-of-Band KVM, Out-of-Band Serial connections

1. **Application name**: select the application you want to use to connect to the node with the interface from the list. To allow CC-SG to automatically select the application based on your browser, select **Auto-Detect**.

2. **Raritan Device Name**: select the Raritan device providing access to this node. Note, a device must be added to CC-SG first before appearing in this list.

3. **Raritan Port Name**: select the port on the Raritan device providing access to this node. The port must be configured in CC-SG before it appears in this list. On serial connections the **Baud Rate**, **Parity** and **Flow Control** values will populate based on the port's configuration.

4. (Optional) Type a description of this interface in the **Description** field.

5. Click **OK** to save your changes.

Interfaces for DRAC, RSA and ILO Processor power control connections

1. Type the IP Address or Hostname for this interface in the **IP Address/Hostname** field.

2. (Optional) Type a TCP Port for this connection in the **TCP Port** field.

3. Type a username for this connection in the **Username** field.

4. (Optional) Type a password for this connection in the **Password** field.

5. (Optional) Type a description of this interface in the **Description** field.

6. Click **OK** to save your changes.

Interfaces for Managed Power Strip connections

When you create a Managed Power Strip interface that specifies a KX as the managing device, the outlet you specify will be renamed with the associated node's name.

1. **Managing Device:** select the Raritan device that the Power Strip is connected to. The device must be added to CC-SG.

2. **Managing Port:** select the port on the Raritan device that the Power Strip is connected to.

3. **Power Strip Name**: select the Power Strip that provides power to the node. The power strip must be configured in CC-SG before it appears in this list.

4. **Outlet Name**: select the name of the outlet the node is plugged into.

5. (Optional) Type a description of this interface in the **Description** field.

6. Click **OK** to save your changes.

Interfaces for IPMI Power Control connections

1. Type the IP Address or Hostname for this interface in the **IP Address/Hostname** field.

2. Type a UDP Port number for this interface in the **UDP Port** field.

3. **Authentication:** select an authentication scheme for connecting to this interface.

4. Type a check interval for this interface in the **Check Interval (seconds)** field.

5. Type a username for this interface in the **Username** field.

6. (Optional) Type a password for this interface in the **Password** field.

7. (Optional) Type a description of this interface in the **Description** field.

8. Click **OK** to save your changes.

Web Browser Interface

You can add a Web Browser Interface to create a connection to a device with an embedded web server, such as a Dominion PX. *Example: Adding a Web Browser Interface to a PX Node* (on page 67) A Web Browser interface can also be used to connect to any web application, such as the web application associated with an RSA, DRAC or ILO Processor card.

A Web Browser Interface may not allow automatic login if the web application requires information other than username and password, such as a session ID.

Users must have the *Node In-Band Access privilege* (see "Add a User Group" on page 81) to access a Web Browser Interface.

You must have DNS configured or URLs will not resolve. You do not need to have DNS configured for IP addresses.

1. The default name for a Web Browser Interface is Web Browser. You can change the name in the Name field. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

2. Type the URL or domain name for the web application in the URL field. Note that you must enter the URL at which the web application expects to read the username and password. Maximum is 120 characters. Follow these examples for correct formats:

    ▪ http(s)://192.168.1.1/login.asp

    ▪ http(s)://www.example.com/cgi/login

    ▪ http(s)://example.com/home.html

3. (Optional) Type the username and password that will allow access to this interface.

    Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications, or the connection will fail.

4. Type the field names for the username and password fields used in the login screen for the web application in the Username Field and Password Field. You must view the HTML source of the login screen to find the field names, not the field labels. *Tips for Adding a Web Browser Interface* (on page 67)

5. (Optional) Type a description of this interface in the **Description** field.

6. Click **OK** to save your changes.

Tips for Adding a Web Browser Interface

To configure the Web Browser Interface, you must gather some information from the HTML source to help identify the actual field names of the Username and Password fields. All vendors implement these authentication fields differently, and the names of these fields vary from device to device, as well as among firmware versions for a particular device. For this reason, there isn't a single method for finding the field names. Please refer to the procedure below for one possible method.

You may want the help of a software engineer or system administrator to locate and identify the proper field names.

➢ *Tip for locating field names:*

1. In the HTML source code for the login page of the web application, search for the field's label, such as Username and Password.

2. When you find the field label, look in the adjacent code for a tag that looks like this: `name="user"`

   The word in quotes is the field name.

Example: Adding a Web Browser Interface to a PX Node

A Dominion PX managed powerstrip can be added to CC-SG as a node. You can then add a Web Browser Interface to the node that will enable users to access the Dominion PX's Web-based administration application.

➢ *Use the following values to add a Web Browser Interface for a Dominion PX node:*

URL: `<DOMINION PX IP ADDRESS>/auth.asp`

Username: The Dominion PX administrator's username

Password: The Dominion PX administrator's password

Username Field = `login`

Password Field = `password`

Results of Adding an Interface

When you add an interface to a node, it appears in the **Interfaces** table and the **Default Interface** drop-down menu of the **Add Node** or **Node Profile** screen. You can click the drop-down menu to select the default interface to use when making a connection to the node.

After changes to the **Add Node** or **Node Profile** screen are saved, the name of the interface(s) will also appear on the Nodes list, nested under the node it provides access to.

When you add a Managed Power Strip interface that specifies a KX as the managing device, the outlet you specify will be renamed with the associated node's name.

Edit an Interface

> **To edit an interface:**

1. Click the **Nodes** tab.

2. Click the node with the interface you want to edit.

3. In the **Interfaces** table, select the row of the interface you want to edit.

4. Click **Edit**.

5. Edit the fields as needed. See *Add an Interface* (on page 62) for field details.

6. Click **OK** to save your changes.

Delete an Interface

> **To delete an interface from a node:**

1. Click the **Nodes** tab.

2. Click the node with the interface you want to delete.

3. In the **Interfaces** table, click the row of interface you want to delete.

4. Click **Delete**. A confirmation message appears.

5. Click **Yes** to delete the interface.

Bookmark an Interface

If you frequently access a node via a particular interface, you can bookmark it so it is readily available from your browser.

➢ **To bookmark an interface in any browser:**

1. In the Nodes tab, select the interface you want to bookmark. You must expand the node to view the interfaces.

2. Choose Nodes > Bookmark Node Interface.

3. Select Copy URL to Clipboard.

4. Click OK. The URL is copied to your clipboard.

5. Open a new browser window, and paste the URL into the address field.

6. Press ENTER to connect to the URL.

7. Add the URL as a bookmark (also known as a Favorite) to your browser.

➢ **To bookmark an interface in Internet Explorer (add an interface to your Favorites):**

1. In the Nodes tab, select the interface you want to bookmark. You must expand the node to view the interfaces.

2. Choose Nodes > Bookmark Node Interface.

3. Select Add Bookmark (IE Only).

4. A default name for the bookmark displays in the Bookmark Name field. You can change the name. This name will display in your Favorites list in Internet Explorer.

5. Click OK. The Add Favorite window appears.

6. Click OK to add the bookmark to your Favorites list.

➢ **To access a bookmarked interface:**

1. Open a browser window.

2. Choose the bookmarked interface from the list of bookmarks in the browser.

3. When the CC-SG Access Client appears, log in as a user who has access to the interface. The connection to the interface opens.

Edit a Node

You can edit a node to change it's name, description, interfaces, default interface, or associations.

> ➢ *To edit a node:*

1. Click the **Nodes** tab, and then select the node you want to edit. The Node Profile appears.

2. Edit the fields as needed

   - **Node Name**: The node name that displays in the Node Profile screen and in the Nodes tab All node names in CC-SG must be unique.

   - **Description**: A description of the node to help users identify it.

   - **Interfaces**: Add an interface, edit an interface or delete an interface.

   - **Default Interface**: The interface used to connect to a node by default.

   - **Node Associations**: A list of **Categories** and **Elements** configured to better describe and organize this node.

3. Click **OK** to save your changes.

Delete a Node

Deleting a node will remove it from the Nodes tab. The node will no longer be available for users to access. When you delete a node, all interfaces, associations, and associated ports are deleted.

> ➢ *To delete a node:*

1. In the **Nodes** tab, select the node you want to delete.

2. Choose **Nodes** > **Delete Node**. The **Delete Node** screen appears.

3. Click **OK** to delete the node.

4. Click **Yes** to confirm that deleting the node also deletes all interfaces and associated ports. A list of all deleted items appears when the deletion is complete.

Bulk Copy for Node Categories and Elements

The Bulk Copy command allows you to copy the assigned categories and elements from one node to multiple other nodes. Categories and elements are the only properties copied in this process.

1. Click the **Nodes** tab and select a node.

2. Chooses **Nodes** > **Bulk Copy**.

3. In the **All Nodes** list, select the nodes to which you are copying the categories and elements of the node in the **Node Name** field.

   ▪ Click the right arrow button to add a node to the **Selected Nodes** list.

   ▪ To remove a node from the **Selected Nodes** list, select the node, and then click the left arrow button.

4. Click **OK** to bulk copy. A message appears when the node categories and elements have been copied.

Connect to a Node

Once a node has an interface, you can connect to that node through the interface in a number of ways. Please refer to Raritan's **CommandCenter Secure Gateway User Guide** for details.

➢ *To connect to a node:*

1. Click the **Nodes** tab.

2. Select the node you want to connect to, and:

   ▪ In the **Interfaces** table, click the name of the interface you want to connect with.

   ▪ In the **Nodes** tab, expand the list of interfaces underneath the node you want to connect to. Double-click the name of the interface you want to connect with.

Ping a Node

You can ping a node from CC-SG to make sure that the connection is active.

➢ *To ping a node:*

1. Click the **Nodes** tab, and then select the node you want to ping.

2. Choose **Nodes** > **Ping Node**. The ping results appear in the screen.

Chat

Chat provides a way for users connected to the same node to communicate with each other. You must be connected to a node to start a chat session for that node. Only users on the same node can chat with each other.

➢ *To start a chat session:*

1. Choose **Nodes** > **Chat** > **Start Chat Session**.

2. Type a message in the lower left field and click **Send**. The message appears in the upper left field for all users to see.

➢ *To join a chat session already in progress:*

- Choose **Nodes** > **Chat** > **Show Chat Session**.

➢ *To end a chat session:*

1. Click **Close** in the chat session. A confirmation message appears.

   - Click **Yes** to close the chat session for all participants.

   - Click **No** to exit the chat session but leave it running for other participants.

About Node Groups

Node groups are used to organize nodes into a set. The node group will become the basis for a policy either allowing or denying access to this particular set of nodes. Please refer to *Add a Policy* (on page 92) for details. Nodes can be grouped manually or by creating a Boolean expression that describes a set of common attributes.

If you used Guided Setup to create categories and elements for nodes, some means to organize nodes along common attributes have already been created. CC-SG automatically creates default access policies based on these elements. Please refer to *Associations* (see "Associations, Categories, and Elements" on page 22) for more details on creating categories and elements.

➢ *To view node groups:*

- Choose **Associations** > **Node Groups**. The **Node Groups Manager** window displays. A list of existing node groups is displayed on the left, while details about the selected node group displays in the main panel.

  ▪ A list of existing node groups is displayed on the left. Click a node group to view the details of the group in the node group manager.

  ▪ If the group was formed arbitrarily, the **Select Nodes** tab will be displayed showing a list of nodes in the group and a nodes not in the group.

  ▪ If the group was formed based on common attributes, the **Describe Nodes** tab will be displayed showing the rules that govern selection of the nodes for the group.

  ▪ To search for a node in the node group list, type a string in the **Search** field at the bottom of the list, and then click **Search**. The method of searching is configured through the **My Profile** screen. Please refer to *Configuring Users and User Groups* (see "Users and User Groups" on page 78) for details.

  ▪ If viewing a group based on attributes, click **View Nodes** to display a list of nodes currently in the Node Group. A **Nodes In Node Group** window appears displaying the nodes and all their attributes.

Add a Node Group

> ➢ *To add a node group:*

1. Choose **Associations** > **Node Group**. The **Node Groups Manager** window displays.

2. Choose **Groups** > **Add**. A template for a node group appears.

3. In the **Group name** field, type a name for a node group you want to create. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

4. There are two ways to add nodes to a group, **Select Nodes** and **Describe Nodes**. The Select Nodes method allows you to arbitrarily assign nodes to the group by selecting them from the list of available nodes. The Describe Nodes method allows you to specify rules that describe nodes; nodes that match the description will be included in the group.

Select Nodes

1. Click the **Select Nodes** tab.

2. Click the **Device Name** drop-down menu and select a device if you want to filter the **Available** list to only display nodes with interfaces from that device.

3. In the **Available** list, select the nodes you want to add to the group, and then click **Add** to move the node into the **Selected** list. Nodes in the **Selected** list will be added to the group.

4. If you want to remove a node from the group, select the node name in the **Selected** list, and then click **Remove**.

5. You can search for a node in either the **Available** or **Selected** list. Type the search terms in the field below the list, and then click **Go**

6. If you want to create a policy that allows access to the nodes in this group at any time, check **Create Full Access Policy For This Group**.

7. When you are done adding nodes to the group, click **Add** to create the node group. The group will be added to the list of Node Groups on the left.

Describe Nodes

1. Click the **Select Nodes** tab.

2. Click **Add New Row** to add a row in the table for a new rule. Rules take the form of an expression which can be compared against nodes.

3. Double-click each column in the row to turn the appropriate cell into a drop-down menu, then select the appropriate value for each component:

   ▪ **Prefix** - Leave this blank or select **NOT**. If **NOT** is selected, this rule will filter for values opposite of the rest of the expression.

   ▪ **Category** - Select an attribute that will be evaluated in the rule. All categories you created in the **Association Manager** will be available here. Also included are **Node Name** and **Interface**.

   ▪ **Operator** - Select a comparison operation to be performed between the Category and Element items. Three operators are available: **=** (is equal to), **LIKE** (used for find the Element in a name) and **<>** (is not equal to)**.**

   ▪ **Element** - Select a value for the Category attribute to be compared against. Only elements associated with the selected category will display here (for example: if evaluating a "Department" category, "Location" elements will not appear here).

   Rule Name- This is a name assigned to the rule in this row. You cannot edit these values. Use these values for writing descriptions in the **Short Expression** field.

   An example rule might be Department = Engineering, meaning it describes all nodes that the **category** "Department" set to "Engineering." This is exactly what happens when you configure the associations during an **Add Node** operation.

4. If you want to add another rule, click **Add New Row** again, and make the necessary configurations. Configuring multiple rules will allow more precise descriptions by providing multiple criteria for evaluating nodes.

   ▪ If you want to remove a rule, highlight the rule in the table, and then click **Remove Row**.

5. The table of rules makes available criteria for evaluating nodes. To write a description for the node group, add the rules by **Rule Name** to the **Short Expression** field. If the description only requires a single rule, then type that rule's name in the field. If multiple rules are being evaluated, type the rules into the field using a set of logical operators to describe the rules in relation to each other:

- **&** - the AND operator. A node must satisfy rules on both sides of this operator for the description (or that section of a description) to be evaluated as true.

- **|** - the OR operator. A node only needs to satisfy one rule on either side of this operator for the description (or that section of a description) to be evaluated as true.

- **(** and **)** - grouping operators. This breaks the description into a subsection contained within the parentheses. The section within the parentheses is evaluated first before the rest of the description is compared to the node. Parenthetical groups can be nested inside another parenthetical group.

  Example 1: If you want to describe nodes that belong to the engineering department, create a rule that says Department = Engineering. This will become Rule0. Then, type Rule0 in the **Short Expression** field.

  Example 2: If you want to describe a group of nodes that belong to the engineering department, OR are located in Philadelphia, and specify that all of the machines must have 1 GB of memory you need to start by creating three rules.

  - Department = Engineering (Rule0)

  - Location = Philadelphia (Rule1)

  - Memory = 1GB (Rule2)

  These rules need to be arranged in relation to each other. Since the node can either belong to the engineering department or be located in Philadelphia, use the OR operator, **|**, to join the two: Rule0|Rule1. Make this comparison first by enclosing it in parentheses: (Rule0|Rule1). Finally, since the nodes must both satisfy this comparison and contain 1GB of memory, use the AND connector, **&**, to join this section with Rule2: (Rule0|Rule1)&Rule2. Type this final expression in the **Short Expression** field.

6. Click **Validate** when a description has been written in the **Short Expression** field. If the description is formed incorrectly, a warning appears. If the description is formed correctly, a normalized form of the expression appears in the **Normalized Expression** field.

7. Click **View Nodes** to see what nodes satisfy this expression. A **Nodes in Node Group** window appears displaying the nodes that will be grouped by the current expression. This can be used to check if the description was correctly written. If not, you can return to the rules table or the **Short Expression** field to make adjustments.

8. If you know you want to create a policy that allows access to the nodes in this group at all times, check **Create Full Access Policy For This Group**.

9. When you are done describing the nodes that belong in this group, click **Add** to create the node group. The group will be added to the list of Node Groups on the left.

Edit a Node Group

Edit a node group to change the membership or description of the group.

> *To edit a node group:*

1. Choose **Associations** > **Node Group**. The **Node Groups Manager** window opens.

2. Click the node you want to edit in the Node Group List. The details of that node appear in the **Node Groups** window.

3. Refer to the instructions in the **Select Nodes** or **Describe Nodes** sections for details on how to configure the node group.

4. Click **OK** to save your changes.

Delete a Node Group

1. Choose **Associations** > **Node Group**. The **Node Groups Manager** window displays.

2. Select the node you want to delete in the Node Group List to the left.

3. Choose **Groups** > **Delete**.

Chapter 9   Users and User Groups

User accounts are created so that users can be assigned a username and password to access CC-SG.

A **User Group** defines a set of privileges for its members. You cannot assign privileges to users themselves, only to user groups. All users must belong to at least one user group.

CC-SG maintains a centralized user list and user group list for authentication and authorization.

Configuring CC-SG to use external authentication is covered in *Remote Authentication* (on page 107).

Creating policies for access that you can assign to user groups is covered in *Policies for Access Control* (on page 91).

In This Chapter

The Users Tab

Click the **Users** tab to display all user groups and users in CC-SG.

Users are nested underneath the user groups they belong to. User groups with users assigned to them appear in the list with a + symbol next to them. Click the + symbol to expand or hide the list of users in a group. Active users, those currently logged into CC-SG, appear in bold.

The Users tab provides the ability to search for users within the tree.

Default User Groups

CC-SG is configured with three user groups by default: **CC-Super User**, **System Administrators**, and **CC Users**.

CC Super-User Group

The **CC Super-User** group has full administrative and access privileges. Only one user can be a member of this group. The default username is **admin**. You can change the default username. You cannot delete the CC-Super User group. You cannot change the privileges assigned to the CC-Super User group, add members to it, or delete the only user from the group. Strong passwords are always enforced for the member of the CC-Super User group. Strong password requirements are:

- Passwords must contain at least one lower case letter.

- Passwords must contain at least one upper case letter.

- Passwords must contain at least one number.

- Passwords must contain at least one special character (for example, an exclamation point or ampersand).

System Administrators Group

The **System Administrators** group has full administrative and access privileges. Unlike the CC-Super User group, you can change the privileges and add or delete members.

CC Users Group

The **CC Users** group has in-band and out-of-band nodes access. You can change the privileges and add or delete members.

Important! Many menu items cannot be selected unless the appropriate User Group or User is first selected.

Add a User Group

Creating user groups first will help you organize users when they are added. When a user group is created, a set of privileges is assigned to the user group. Users assigned to the group will inherit those privileges. For example, if you create a group and assign it the **User Management** privilege, all users assigned to the group will be able to see and execute the commands on the **User Manager** menu. Please refer to *Appendix C: User Group Privileges* (see "User Group Privileges" on page 246) for details on each privilege.

Configuring user groups involves four basic steps:

- Name the group and give it a description.
- Select the privileges the user group will have.
- Select the interface types the user group can use to access nodes.
- Select policies that specify which nodes the user group can access.

➢ *To add a user group:*

1. Choose **Users** > **User Group Manager** > **Add User Group**. The **Add User Group** screen appears

2. Type a name for the user group in the **User Group Name** field. User Group names must be unique. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

3. (Optional) Type a short description for the group in the **Description** field.

4. Click the **Privileges** tab.

5. Check the checkbox that corresponds to each privilege you want to assign to the user group.

6. Below the privileges table is the **Node Access** area with privileges for three kinds of node access: **Node Out-of-Band Access**, **Node In-Band Access**, and **Node Power Control**. Check the checkbox that corresponds to each type of node access you want to assign to the user group.

7. Click the **Device/Node Policies** tab. A table of policies appears.

   The **All Policies** table lists all the policies available on CC-SG. Each policy represents a rule allowing or denying access to a group of nodes. Please refer to *Configuring Policies and Node Groups* (see "Policies for Access Control" on page 91) for more information on policies and how they are created.

8. In the **All Policies** list, select a policy that you want to assign to the user group, and then click **Add** to move the policy to the **Selected Policies** list. Policies in the **Selected Policies** list allow or deny access to the nodes or devices controlled by the policy.

   Repeat this step to add additional policies to the user group.

   ▪ If you want to allow this group to access all available nodes, select the **Full Access Policy** in the **Add Policies** list, and then click **Add**.

   ▪ If you want to remove a policy from the user group, select the policy name in the **Selected Policies** list, and then click **Remove**.

9. (Optional) When you are done configuring policies for this group, click **Apply** to save this group and create another. Repeat the steps in this section to add user groups.

10. Click **OK** to save your changes.

Edit a User Group

Edit a User Group to change the existing privileges and policies for that group.

*Note: You cannot edit the Privileges or Policies of the **CC-Super User** group.*

➢ **To edit a group:**

1. Click the **Users** tab to the left.

2. Click the user group in the **Users** tab. The **User Group Profile** appears.

3. (Optional) Type a new name for the user group in the **User Group Name** field.

4. (Optional) Type a new description for the user group in the **Description** field.

5. Click the **Privileges** tab.

6. Check the checkbox that corresponds to each privilege you want to assign to the user group. Uncheck a privilege to remove it from the group.

7. In the **Node Access** area, click the drop-down menu for each kind of interface you want this group to have access through and select **Control**.

8. Click the drop-down menu for each kind of interface you do not want this group to have access through and select **Deny**.

9. Click the **Policies** tab. Two tables of policies appear.

10. For each policy you want to add to the group, select policy in the **All Policies**, then click **Add** to move the policy to the **Selected Policies** list. Policies in the **Selected Policies** list will allow or deny users access to the node (or devices) controlled by this policy.

11. For each policy you want to remove from the user group, select the policy name in the **Selected Policies** list, and then click **Remove**.

12. Click **OK** to save your changes.

Delete a User Group

You can delete a user group if it is does not have any members.

> ### To delete a User Group:

1. Click the **Users** tab to the left.

2. Click the user group you want to delete in the **Users** tab.

3. Choose **Users** > **User Group Manager** > **Delete User Group**.

4. Click **OK** to delete the User Group.

Add a User

When you add a user to CC-SG, you must specify a user group to give the user the access privileges assigned to the user group.

> ### To add a user:

1. In the **Users** tab, select the group to which you want to add a user.

2. Choose **Users** > **User Manager** > **Add User**.

3. In the **Username** field, type the user name of the user you want to add. This name is used to log in to CC-SG. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

4. Check **Login Enabled** if you want the user to be able to log in to CC-SG.

5. Check **Remote Authentication** only if you want the user to be authenticated by an external server, such as TACACS+, RADIUS, LDAP, or AD. If you are using remote authentication, a password is not required and the **New Password** and **Retype New Password** fields will be disabled.

6. In the **New Password** and **Retype New Password** fields, type the password that the user will use to log in to CC-SG.

> Note: Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for password lengths.
>
> If strong passwords are enabled, the password entered must conform to the established rules. The information bar at the top of the screen will display messages to assist with the password requirements. Please refer to *Advanced Administration* (on page 150) for details on strong passwords.

7. Check **Force Password Change on Next Login** if you want to force the user to change the assigned password the next time they log in.

8. Check **Force Password Change Periodically** if you want to specify how often the user will be forced to change their password.

9. If checked, in the **Expiration Period (Days)** field, type the number of days that the user will be able to use the same password before being forced to change it.

10. In the **Email address** field, type the user's email address. This will be used to send the user notifications.

11. Click the **User Groups** drop-down menu and select the group to which the user will be added.

12. When you are done configuring this user, click **Apply** to add this user and create another one, or click **OK** to add the user without creating more. The users you create appear in the **Users** tab, nested underneath the user groups to which they belong.

Edit a User

You cannot edit a user to change what group they belong to. Please refer to *Assign a User to a Group* (on page 86) for details.

> ➢ *To edit a user:*

1. In the **Users** tab, click the + symbol to expand the user group that contains a user you want to edit, and then select the user. The **User Profile** appears.

2. Clear **Login enabled** if you want to prevent this user from logging in to CC-SG. Check **Login enabled** if you want to allow this user to log into CC-SG.

3. Check **Remote Authentication** only if you want the user to be authenticated by an external server, such as TACACS+, RADIUS, LDAP, or AD. If you are using remote authentication, a password is not required and the **New Password** and **Retype New Password** fields will be disabled.

4. In the **New Password** and **Retype New Password** fields, type a new password to change this user's password.

   Note: If Strong Passwords are enabled the password entered must conform to the established rules. The information bar at the top of the screen will assist with the password requirements. Please refer to *Advanced Administration* (on page 150) for more information on Strong Passwords.

5. Check **Force Password Change on Next Login** if you want to force the user to change the assigned password the next time they log in.

6. In the **Email address** field, type a new email address to add or change the user's configured email address. This will be used to send the user notifications.

7. Click **OK** to save your changes.

Delete a User

Deleting a user completely removes the user from CC-SG. This is useful for removing user accounts that are no longer needed.

This procedure deletes all instances of a user, even if the user exists in multiple user groups. Please refer to *Delete a User From a Group* (on page 87) if you want to remove the user from a group without deleting the user from CC-SG.

➢ *To delete a user:*

1. In the **Users** tab, click the + symbol to expand the user group that contains a user you want to delete, and then select the user. The **User Profile** appears.

2. Choose **Users** > **User Manager**, **Delete User**.

3. Click **OK** to permanently delete the user from CC-SG.

Assign a User to a Group

Use this command to assign an existing users to a group they currently do not belong to. Users assigned in this way will be added to their new group while still existing in any group they were previously assigned to. To move a user, use this command in conjunction with **Delete User From Group**.

➢ *To assign a user to a group:*

1. In the **Users** tab, select the user group you want to assign users to.

2. Choose **Users** > **User Group Manager** > **Assign Users To Group**.

3. The user group you selected appears in the **User group name** field.

4. Users who are not assigned to the target group appear in the **Users not in group** list.

    ▪ Select the users you want to add from this list, and then click **>** to move them to the **Users in group** list.

    ▪ Click the **>>** button to move all users not in the group to the **Users in group** list.

    ▪ To remove people from the target group, select the users you want to remove in the **Users in group** list, and then click the **<** button.

    ▪ Click the **<<** button to remove all users from the **Users in group** list.

5. When all the users have been moved to the appropriate column, click **OK**. The users in the **Users in group** list will be added to the selected User Group.

Delete a User From a Group

When you delete a user from a group the user is removed only from the specified group. The user remains in all other assigned groups. Deleting a user from a group does not delete the user from CC-SG.

If a user only belongs to one group, you cannot delete the user from the group. You can only delete the user from CC-SG.

➢ *To delete a user from a group:*

1. In the **Users** tab, click the + symbol to expand the user group that contains a user you want to delete from the group, and then select the user. The **User Profile** appears.

2. Choose **Users** > **User Manager** > **Delete User From Group**. The **Delete User** screen appears.

3. Click **OK** to delete the user from the group.

Your User Profile

About My Profile

My Profile allows all users to view details about their account, change some details and customize usability settings. It is the only way for the **admin** account to change the account name.

➢ *To view your profile:*

- Choose **Secure Gateway** > **My Profile**. The **Change My Profile** screen appears, displaying details about your account.

Change your password

1. Choose **Secure Gateway** > **My Profile**.

2. Check **Change Password**.

3. Type your current password in the **Old Password** field.

4. Type your new password in the **New Password** field. A notice appears if Strong Passwords are required.

5. Type your new password again in the **Retype New Password** field.

6. Click **OK** to save your changes.

Change your default search preference

1. Choose **Secure Gateway** > **My Profile**.

2. In the **Search Preference** area, select a preferred method to search nodes, users and devices.

   - **Filter by Search Results** - Allows the use of wildcards and will limit the display of nodes, users or devices to all names that contain the search criteria.

   - **Find Matching String** - Does not support the use of wildcards and will highlight the closest match in the nodes, users or devices as you type. The list will be limited to those items that contain the search criteria after clicking **Search**.

3. Click **OK** to save your changes.

Change the CC-SG default font size

1. Choose **Secure Gateway** > **My Profile**.

2. Click the **Font Size** drop-down menu to adjust the font size the standard CC-SG client uses.

3. Click **OK** to save your changes.

Change your email address

1. Choose **Secure Gateway** > **My Profile**.

2. Type a new address in the **Email address** field to add or change the address CC-SG will use to send you notifications.

3. Click **OK** to save your changes.

Change the CC-SG Super User's Username

You must be logged into CC-SG using the CC Super User account to change the CC Super User's username. The default CC Super User username is **admin**.

1. Choose **Secure Gateway** > **My Profile**.

2. Type a new name in the **Username** field.

3. Click **OK** to save your changes.

Logout Users

You can log active users out of CC-SG, either individually or by user group.

> ➢ *To log out users:*

1. In the **Users** tab, click the + symbol to expand the user group that contains a user you want to logout from CCSG, and then select the user.

   ▪ To select multiple users, hold the **Shift** key as you click additional users.

2. Choose **Users** > **User Manager** > **Logout Users**. The **Logout Users** screen appears with the list of selected users.

3. Click **OK** to log the users out of CC-SG.

> ➢ *To log out all users of a User Group:*

1. In the **Users** tab, select the user group you want to logout of CC-SG.

   ▪ To log out multiple user groups, hold the **Shift** key as you click additional user groups.

2. Choose **Users** > **User Group Manager** > **Logout Users**. The **Logout Users** screen appears with a list of active users from the selected groups.

3. Click **OK** to log the users out of CC-SG.

Bulk Copy for Users

You can use Bulk Copy for users to copy one user's user group affiliations to another user, or list of users. If the users you are copying to have existing group affiliations, the affiliations will be removed.

> ➢ *To perform a Bulk Copy for users:*

1. In the **Users** tab, click the + symbol to expand the user group that contains a user whose policies and privileges you want to copy, and then select the user.

2. Choose **Users** > **User Manager** > **Bulk Copy**. The **Username** field displays the user whose policies and privileges you are copying.

3. In the **All Users** list, select the users that will be adopting the policies and privileges of the user in the **Username** field.

▪ Click **>** to move a user name to the **Selected Users** list.

▪ Click **>>** to move all users into the **Selected Users** list.

▪ To remove a user from the **Selected Users** list, select the user, and then click **<**.

▪ Click **<<** to remove all users from the **Users in group** list.

4. Click **OK** to copy.

Chapter 10 Policies for Access Control

In This Chapter

Controlling Access Using Policies

Policies are rules that define which nodes and devices users can access, when they can access them, and whether virtual-media permissions are enabled, where applicable. The easiest way to create policies is to categorize your nodes and devices into node groups and device groups, and then create policies that allow and deny access to the nodes and devices in each group. After you create a policy, you assign it to a user group (Please refer to *Assigning Policies To User Groups* (on page 98)).

CC-SG also includes a **Full Access Policy**. If you want to give all users access to all nodes and devices at all times, assign the **Full Access Policy** to all user groups.

If you completed **Guided Setup,** a number of basic policies may already have been created. Please refer to *Configuring CC-SG with Guided Setup* (on page 13) for details.

- Create Node Groups to organize the nodes you want to create access rules for.

- Create Device Groups to organize the devices you want to create access rules for.

- Create a policy for a node or device group specifying when access to that node or device group can occur.

- Apply the policy to a user group.

Add a Policy

If you create a policy that denies access (**Deny**) to a node group or device group, you also must create a policy that allows access (**Control**) for the selected node group or device group. Users will not automatically receive **Control** rights when the **Deny** policy is not in effect.

Note: When CC-SG is in Proxy or Both mode, you cannot give users access to Virtual Media. **Connection Modes: Direct and Proxy** *(on page 167)*

➢ *To add a policy:*

1. Choose **Associations** > **Policies**. The **Policy Manager** window displays.

2. Click **Add**. A dialog window appears requesting a name for the policy.

3. Type a name for the new policy in the **Enter policy name** field. Please refer to *Naming Conventions* (on page 271) for details on CC-SG's rules for name lengths.

4. Click **OK**. The new policy will be added to the **Policy Name** list in the Policy Manager screen.

5. Click the **Device Group** drop-down arrow, and select the Device Group this policy governs access to.

6. Click the **Node Group** drop-down arrow and select the Node Group this policy governs access to.

7. If the policy will cover only one type of group, only select a value for that group.

8. Click the **Days** drop-down arrow, and then select which days of the week this policy covers: **All** days, **Weekday** (Monday through Friday only) and **Weekend** (Saturday and Sunday only), or **Custom** (select specific days).

9. Select **Custom** to select your own set of days. The individual day checkboxes will become enabled.

10. Check the checkbox that corresponds to each day you want this policy to cover.

11. In the **Start Time** field, type the time of day this policy goes into effect. The time must be in 24-Hour format.

12. In the **End Time** field, type the time of day this policy ends. The time must be in 24-Hour format.

13. In the **Device/Node Access Permission** field, select **Control** to define this policy to allow access to the selected node or device group for the designated times and days. Select **Deny** to define this policy to deny access to the selected node or device group for the designated times and days.

14. If you selected **Control** in the **Device/Node Access Permission** field, the Virtual Media Permission section will become enabled. In the **Virtual Media Permission** field, select an option to allow or deny access to virtual media available in the selected node or device groups for the designated times and days:

    ▪ **Read-Write** allows both read and write permission to virtual media

    ▪ **Read-only** allows only read permission to virtual media

    ▪ **Deny** denies all access to virtual media

15. Click **Update** to add the new policy to CC-SG, and then click **Yes** in the confirmation message that appears.

Edit a Policy

When you edit a policy, the changes do not affect users who are currently logged in to CC-SG. The changes will go into effect at the next login.

If you need to ensure that your changes go into effect sooner, first enter Maintenance Mode, and then edit policies. When you enter Maintenance Mode, all current users are logged off of CC-SG until you exit Maintenance Mode, when users can login again. Please refer to *About Maintenance Mode* (see "Maintenance Mode" on page 140) for details.

➢ **To edit a policy:**

1. On the **Associations** menu, click **Policies**. The **Policy Manager** window displays.

2. Click the **Policy Name** drop-down arrow, and then select the policy you want to edit from the list.

3. (Optional) To edit the name of the policy, click **Edit**. An **Edit Policy** window appears. Type a new name for the policy in the field, and then click **OK** to change the name of the policy.

4. Click the **Device Group** drop-down arrow, and select the Device Group this policy governs access to.

5. Click the **Node Group** drop-down arrow and select the Node Group this policy governs access to.

6. If the policy will cover only one type of group, only select a value for that type.

7. Click the **Days** drop-down arrow, and then select which days of the week this policy covers: **All** (everyday), **Weekday** (Monday through Friday only) and **Weekend** (Saturday and Sunday only), or **Custom** (select specific days).

8. Select **Custom** to select your own set of days. The individual day checkboxes will become enabled.

9. Check the checkbox that corresponds to each day you want this policy to cover.

10. In the **Start Time** field, type the time of day this policy goes into effect. The time must be in 24-Hour format.

11. In the **End Time** field, type the time of day this policy ends. The time must be in 24-Hour format.

    ▪ In the **Device/Node Access Permission** field:

    ▪ Select **Control** to define this policy to allow access to the selected node or device group for the designated times and days.

    ▪ Select **Deny** to define this policy to deny access to the selected node or device group for the designated times and days.

12. If you selected **Control** in the **Device/Node Access Permission** field, the Virtual Media Permission section will become enabled. In the **Virtual Media Permission** field, select an option to allow or deny access to virtual media available in the selected node or device groups for the designated times and days:

    ▪ **Read-Write** allows both read and write permission to virtual media

    ▪ **Read-only** allows only read permission to virtual media

    ▪ **Deny** denies all access to virtual media

13. Click **Update** to save your changes.

14. Click **Yes** in the confirmation message that appears.

Delete a Policy

> ➢ **To delete a policy:**

1. Choose **Associations** > **Policies**. The **Policy Manager** window displays.

2. Click the **Policy Name** drop-down arrow, and then select the policy you want to delete from the list.

3. Click **Delete**.

4. Click **Yes** in the confirmation message that appears.

Support for Virtual Media

CC-SG provides remote virtual media support for nodes connected to virtual media-enabled KX II devices. For detailed instructions on accessing virtual media, please refer to the Dominion KX II User Guide. Please refer to *Add a Policy* (on page 92) for details on creating policies to assign virtual media permission to user groups in CC-SG.

What is Virtual Media?

Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from the client PC and network file servers. With this feature, media mounted on the client PC and network file servers is essentially mounted virtually by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself. Virtual media can include internal and USB-mounted CD and DVD drives, USB mass storage devices, PC hard drives, and ISO images (disk images).

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

- transferring files
- running diagnostics
- installing or patching applications
- complete installation of the operating system

This expanded KVM control eliminates most trips to the data center, saving time and money, thereby making virtual media very powerful.
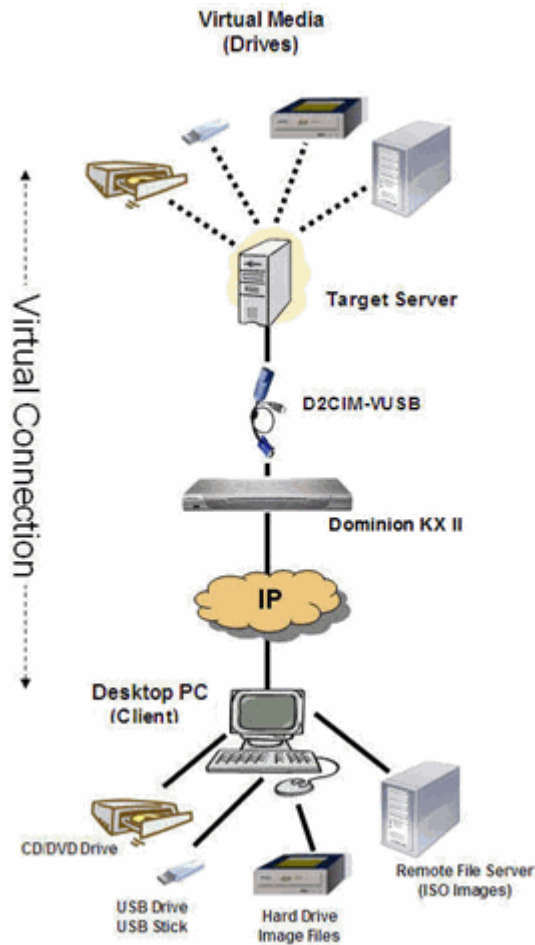
All Dominion KX2 models support virtual media. The benefits of virtual media - mounting of remote drives/media on the target server to support software installation, and diagnostics - are now available in all of the Dominion KX2 models.

Each Dominion KX2 comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, internal and remote drives and images. Unlike other solutions, the Dominion KX2 supports virtual media access of hard drives and remotely mounted images for added flexibility and productivity.

Virtual media sessions are secured using 128-bit AES or RC4 encryption.

The new D2CIM-VUSB CIM (computer interface module) supports virtual media sessions to KVM target servers supporting the USB 2.0 interface. This new CIM also supports Absolute Mouse Synchronization as well as remote firmware update.

Assigning Policies To User Groups

Policies must be assigned to a User Group before they take effect. Once a policy is assigned to a User Group, the members of the group will have their access governed by that policy. Please refer to *Configuring Users and User Groups* (see "Users and User Groups" on page 78) for details on assigning policies to a user group.

Chapter 11   Custom Views for Devices and Nodes

Custom Views enable you to specify different ways to display the nodes and devices in the left panel, using Categories, Node Groups, and Device Groups.

In This Chapter

Types of Custom Views

There are three types of custom views: View by Category, Filter by Node Group, and Filter by Device Group.

View by Category

All nodes and devices described by the categories you specify will display in the nodes or devices lists when a View by Category custom view is applied. Nodes or devices that do not have a category assigned will also display as "unassociated."

Filter by Node Group

Only the node groups you specify will display in the nodes list when a Filter by Node Group custom view is applied. The first level of organization is the node group name. A node may appear several times in the list if the node belongs to more than one node group defined in the custom view. Nodes that do not belong to a node group specified by the custom view will not appear in the list.

Filter by Device Group

Only the device groups you specify will display in the devices list when a Filter by Device Group custom view is applied. The first level of organization is the device group name. A device may appear several times in the list if the device belongs to more than one device group defined in the custom view. Devices that do not belong to a device group specified by the custom view will not appear in the list.

Using Custom Views in the Admin Client

Custom Views for Nodes

Add a Custom View for Nodes

➢ *Add a Custom View for Nodes*

1. Click the **Nodes** tab.

2. On the **Nodes** menu, click **Change View,** and then click **Create Custom View**. The **Custom View** screen appears.

3. In the **Custom View** panel, click **Add**. The **Add Custom View** window appears.

4. Type a name for the new custom view in the **Custom View Name** field.

5. In the Custom View Type section:

   ▪ Select **Filter by Node Group** to create a custom view that displays only the node groups you specify.

   ▪ Select **View by Category** to create a custom view that displays nodes according to the categories you specify.

6. Click **OK.**

7. In the **Custom View Details** section:

   a. Select an item you want to include in the custom view from the Available list, and then click **Add** to add to move the item to the Selected list. Repeat this step to add as many items as you want.

   b. Put the items in the **Selected** list into the order in which you would like each grouping to display in the Nodes tab. Select an item, and then click the arrow buttons to move the items into the desired sequence.

c. If you must remove an item from the list, select it, and then click **Remove.**

8. Click **Save** to save the custom view. A message confirms that the custom view has been added.

9. If you want to apply the new custom view, click **Set Current**.

Apply a Custom View for Nodes

➢ *Apply a Custom View to the Nodes list*

1. On the **Nodes** menu, click **Change View** and then click **Custom View**. The **Custom View** screen appears.

2. Click the **Name** drop-down arrow, and select a custom view from the list.

3. Click **Apply View** to apply the custom view.

OR

• Choose Nodes > Change View. All defined custom views are options in the pop-up menu. Choose the custom view you want to apply.

Change a Custom View for Nodes

1. Click the **Nodes** tab.

2. On the **Nodes** menu, click **Change View,** and then click **Create Custom View**. The **Custom View** screen appears.

3. Click the **Name** drop-down arrow, and select a custom view from the list. Details of the items included and their order appear in the **Custom View Details** panel

➢ *To change a custom view's name:*

1. In the **Custom View** panel, click **Edit**. The **Edit Custom View** window appears.

2. Type a new name for the custom view in the **Enter new name for custom view** field, and then click **OK**. The new view name appears in the **Name** field in the Custom View screen.

➢ *To change the custom view's contents:*

1. In the **Custom View Details** section:

a. Select an item you want to include in the custom view from the Available list, and then click **Add** to add to move the item to the Selected list. Repeat this step to add as many items as you want.

b. Put the items in the **Selected** list into the order in which you would like each grouping to display in the Nodes tab. Select an item, and then click the arrow buttons to move the items into the desired sequence.

c. If you must remove an item from the list, select it, and then click **Remove.**

2. Click **Save** to save the custom view. A message confirms that the custom view has been added.

3. If you want to apply the new custom view, click **Set Current**.

Delete a Custom View for Nodes

1. Click the **Nodes** tab.

2. On the **Nodes** menu click **Change View,** and then click **Create Custom View**. The **Custom View** screen appears.

3. Click the **Name** drop-down arrow, and select a custom view from the list. Details of the items included and their order appear in the **Custom View Details** panel

4. In the **Custom View** panel, click **Delete**. The **Delete Custom View** confirmation message appears.

5. Click **Yes** in the confirmation message.

Assign a Default Custom View for Nodes

1. Click the **Nodes** tab.

2. On the **Nodes** menu, click **Change View,** and then click **Create Custom View**. The **Custom View** screen appears.

3. Click the **Name** drop-down arrow, and select a custom view from the list.

4. In the **Custom View** panel, click **Set as Default**. The next time you login the selected custom view will be used by default.

Assign a Default Custom View of Nodes for All Users

If you have the CC Setup and Control privilege, you can assign a default custom view for all users.

1. Click the Nodes tab.

2. Choose Nodes > Change View > Create Custom View.

3. Click the **Name** drop-down arrow, and select the custom view you want assign as a system-wide default view.

4. Check the **System Wide** checkbox, and then click **Save.**

All users who log in to CC-SG will see the Nodes tab sorted according to the selected custom view. Users can still change the custom view.

Custom Views for Devices

Add a Custom View for Devices

➢ *Add a Custom View for Devices*

1. Click the Devices tab.

2. On the Devices menu, click **Change View,** and then click **Create Custom View**. The **Custom View** screen appears.

3. In the **Custom View** panel, click **Add**. The **Add Custom View** window appears.

4. Type a name for the new custom view in the **Custom View Name** field.

5. In the Custom View Type section:

   ▪ Select **Filter by Device Group** to create a custom view that displays only the device groups you specify.

   ▪ Select **View by Category** to create a custom view that displays devices according to the categories you specify.

6. Click **OK.**

7. In the **Custom View Details** section:

   a. Select an item you want to include in the custom view from the Available list, and then click **Add** to add to move the item to the Selected list. Repeat this step to add as many items as you want.

   b. Put the items in the **Selected** list into the order in which you would like each grouping to display in the Nodes tab. Select an item, and then click the arrow buttons to move the items into the desired sequence.

   c. If you must remove an item from the list, select it, and then click **Remove.**

8. Click **Save** to save the custom view. A message confirms that the custom view has been added.

9. If you want to apply the new custom view, click **Set Current**.

Apply a Custom View for Devices

➤ *Apply a Custom View to the Devices list*

1. On the Devices menu, click **Change View** and then click **Custom View**. The **Custom View** screen appears.

2. Click the **Name** drop-down arrow, and select a custom view from the list.

3. Click **Set Current** to apply the custom view.

OR

Choose Devices > Change View. All defined custom views are options in the pop-up menu. Choose the custom view you want to apply.

Change a Custom View for Devices

1. Click the **Devices** tab.

2. On the Devices menu, click **Change View,** and then click **Create Custom View**. The **Custom View** screen appears.

3. Click the **Name** drop-down arrow, and select a custom view from the list. Details of the items included and their order appear in the **Custom View Details** panel

➤ *To change a custom view's name:*

1. In the **Custom View** panel, click **Edit**. The **Edit Custom View** window appears.

2. Type a new name for the custom view in the **Enter new name for custom view** field, and then click **OK**. The new view name appears in the **Name** field in the Custom View screen.

➤ *To change the custom view's contents:*

1. In the **Custom View Details** section:

   a. Select an item you want to include in the custom view from the Available list, and then click **Add** to add to move the item to the Selected list. Repeat this step to add as many items as you want.

   b. Put the items in the **Selected** list into the order in which you would like each grouping to display in the Nodes tab. Select an item, and then click the arrow buttons to move the items into the desired sequence.

c.   If you must remove an item from the list, select it, and then click **Remove.**

2.   Click **Save** to save the custom view. A message confirms that the custom view has been added.

3.   If you want to apply the new custom view, click **Set Current**.

Delete a Custom View for Devices

1.   Click the Devices tab.

2.   Choose Devices > **Change View** > **Create Custom View**. The **Custom View** screen appears.

3.   Click the **Name** drop-down arrow, and select a custom view from the list. Details of the items included and their order appear in the **Custom View Details** panel

4.   In the **Custom View** panel, click **Delete**. The **Delete Custom View** confirmation message appears.

5.   Click **Yes** in the confirmation message.

Assign a Default Custom View for Devices

1.   Click the Devices tab.

2.   Choose Devices > **Change View** > **Create Custom View**. The **Custom View** screen appears.

3.   Click the **Name** drop-down arrow, and select a custom view from the list.

4.   In the **Custom View** panel, click **Set as Default**. The next time you login the selected custom view will be used by default.

Assign a Default Custom View of Devices for All Users

If you have the Device, Port and Node Management privilege, you can assign a default custom view for all users.

1.   Click the Devices tab.

2.   Choose Devices> Change View > Create Custom View.

3.   Click the **Name** drop-down arrow, and select the custom view you want assign as a system-wide default view.

4.   Check the **System Wide** checkbox, and then click **Save.**

All users who log in to CC-SG will see the Devices tab sorted according to the selected custom view. Users can still change the custom view.

Chapter 12 Remote Authentication

In This Chapter

About Authentication and Authorization (AA)

Users of CC-SG can be locally authenticated and authorized on the CC-SG or remotely authenticated using the following supported directory servers:

- Microsoft Active Directory (AD)

- Netscape's Lightweight Directory Access Protocol (LDAP)

- TACACS+

- RADIUS

Any number of remote servers can be used for external authentication. For example, you could configure three AD servers, two iPlanet (LDAP) servers, and three RADIUS servers.

Only AD can be used for remote authorization of users.

Flow for Authentication

When remote authentication is enabled, authentication and authorization follow these steps:

1. The user logs into CC-SG with the appropriate user name and password.

2. CC-SG connects to the external server and sends the user name and password.

3. User name and password are either accepted or rejected and sent back. If authentication is rejected, this results in a failed login attempt.

4. If authentication is successful, authorization is performed. CC-SG checks if the user name entered matches a group that has been created in CC-SG or imported from AD, and grants privileges per the assigned policy.

When remote authentication is disabled, both authentication and authorization are performed locally on CC-SG.

User Accounts

User Accounts must be added to the authentication server for remote authentication. Except when using AD for both authentication and authorization, all remote authentication servers require that users be created on CC-SG. The user's username on both the authentication server and on CC-SG must be the same, although the passwords may be different. The local CC-SG password is used only when remote authentication is disabled. Please refer to *Configuring Users and User Groups* (see "Users and User Groups" on page 78) for details on adding users who will be remotely authenticated.

Note: *If remote authentication is used, users have to contact their Administrators to change their passwords on the remote server. Passwords cannot be changed on CC-SG for remotely authenticated users.*

Distinguished Names for LDAP and AD

Configuration of remotely authenticated users on LDAP or AD servers requires entering user names and searches in Distinguished Name format. The full Distinguished Name format is described in **RFC2253** (http://www.rfc-editor.org/rfc/rfc2253.txt).

To configure CC-SG, you must know how to enter Distinguished Names and the order in which each component of the name should be listed.

Specifying a Distinguished Name for AD

Distinguished Names for AD should follow this structure. You do not have to specify both **common name** and **organization unit**:

- common name (cn), organizational unit (ou), domain component (dc)

Specifying a Distinguished Name for LDAP

Distinguished Names for Netscape LDAP and eDirectory LDAP should follow this structure:

- user id (uid), organizational unit (ou), organization (o)

Specifying a Username for AD

When authenticating CC-SG users on an AD server by specifying **cn=administrator,cn=users,dc=xyz,dc=com** in **username**, if a CC-SG user is associated with an imported AD group, the user will be granted access with these credentials. Note that you can specify more than one common name, organizational unit, and domain component.

Specifying a Base DN

You also enter a Distinguished Name to specify where the search for users begins. Enter a Distinguished Name in the **Base DN** field to specify an AD container in which the users can be found. For example, entering: **ou=DCAdmins,ou=IT,dc=xyz,dc=com** will search all users in the **DCAdmins** and **IT** organizational units under the **xyz.com** domain.

Specify Modules for Authentication and Authorization

Once you have added all the external servers as modules in CC-SG, you specify whether you want CC-SG to use each of them for either authentication, authorization, or both.

➢ **To specify modules for authentication and authorization:**

1. Choose Administration > Security.

2. Choose the Authentication tab. All configured external Authorization and Authentication Servers display in a table.

3. For each server listed:

a. Select the **Authentication** checkbox if you want CC-SG to use the server for authentication of users.

b. Select the **Authorization** checkbox if you want CC-SG to use the server for authorization of users. Only AD servers can be used for authorization.

4. Click **Update** to save your changes.

Establish Order of External AA Servers

CC-SG will query the configured external authorization and authentication servers in the order that you specify. If the first checked option is unavailable, CC-SG will try the second, then the third, and so on, until it is successful.

➢ *To establish the order in which CC-SG uses external authentication and authorization servers:*

1. Choose Administration > Security.

2. Choose the Authentication tab. All configured external Authorization and Authentication Servers display in a table.

3. Select a server from the list, and then click the up and down arrows to prioritize the order of engagement.

4. Click **Update** to save your changes.

About AD and CC-SG

CC-SG supports authentication and authorization of users imported from an AD domain controller, without requiring that users be defined locally in CC-SG. This allows users to be maintained exclusively on the AD server. Once your AD server is configured as a module in CC-SG, CC-SG can query all domain controllers for a given domain. You can synchronize your AD modules in CC-SG with your AD servers to ensure that CCSG has the most current authorization information on your AD user groups.

Add an AD Module to CC-SG

Important: Create appropriate AD user groups and assign AD users to them before starting this process. Also, make sure that you have configured the CC-SG DNS and Domain Suffix in Configuration Manager. Please refer to *Configuring the CC-SG Network* **(on page 154).**

➢ *To add an AD module to CC-SG:*

1. Choose Administration > Security.

2. Choose the Authentication tab.

3. Click **Add** to open the Add Module window.

4. Click the **Module Type** drop-down menu and select **AD** from the list.

5. Type a name for the AD server in the **Module name** field.

   ▪ The maximum number of characters is 31.

   ▪ All printable characters may be used.

   ▪ The module name is optional and is specified only to distinguish this AD server module from any others that you configure in CC-SG. The name is not connected to the actual AD server name.

6. Click **Next** to proceed. The **General** tab opens.

AD General Settings

In the **General** tab, you add the information that allows CC-SG to query the AD server.

1. Type the AD domain you want to query in the **Domain** field. For example, if the AD domain is installed in the xyz.com domain, type **xyz.com** in the **Domain** field. CC-SG and the AD server you want to query must be configured either on the same domain or on different domains that trust each other.

   Note: CC-SG will query all known domain controllers for the domain specified.

2. Type the IP address of the DNS server in the **DNS Server IP Address** field. Or, check **Use default CC-SG DNS** checkbox to use the DNS configured in the Configuration Manager section of CC-SG. Please refer to *Advanced Administration* (on page 150) for details.

3. Check **Anonymous Bind** if you want to connect to the AD server without specifying a username and password. If you use this option, ensure that the AD server allows anonymous queries.

   Note: By default, Windows 2003 does NOT allow anonymous queries. Windows 2000 servers do allow certain anonymous operation whose query results are based on the permissions of each object.

4. If you are not using anonymous binding, type the username of the user account you want to use to query the AD server in the **User name** field. The format required will depend on your AD version and configuration. Use one of the following formats.

   A user named User Name with a login name UserN in the raritan.com domain could be entered as:

   ▪ cn=UserName,cn=users,dc=Raritan,dc=com

   ▪ **UserName@raritan.com**

   ▪ Raritan/UserName

   Note: The user specified must have permission to execute search queries in the AD domain. For example, the user may belong to a group within AD that has **Group scope** set to **Global**, and **Group type** set to **Security**.

5. Type the password for the user account you want to use to query the AD server in the **Password** and **Confirm Password** fields.

6. Click **Test Connection** to test the connection to the AD server using the given parameters. You should receive a confirmation of a successful connection. If you do not see a confirmation, review the settings carefully for errors and try again.

7. Click **Next** to proceed. The **Advanced** tab opens.

AD Advanced Settings

➢ *To configure advanced AD settings:*

1. Click the Advanced tab.

2. Type the port number on which the AD server is listening. The default port is **389**. If you are using secure connections for LDAP, you may need to change this port. The standard port for secure LDAP connections is **636**.

3. Check **Secure Connection for LDAP** if you want to use a secure channel for the connection. If checked, CC-SG uses LDAP over SSL to connect to AD. This option may not be supported by your AD configuration.

4. Specify a **Base DN** (directory level/entry) under which the authentication search query will be executed. CC-SG can do a recursive search downward from this Base DN.

Example	Description
dc=raritan,dc=com	The search query for the user entry will be made over the whole directory structure.
cn=Administrators,cn=Users,dc=raritan,dc=com	The search query for the user entry will be performed only in the Administrators sub-directory (entry).

5. Type a user's attributes in **Filter** so the search query will be restricted to only those entries that meet this criterion. The default filter is **objectclass=user**, which means that only entries of the type **user** are searched.

6. Specify the way in which the search query will be performed for the user entry.

   ▪ Check **Use Bind** if the user logging in from the applet has permissions to perform search queries in the AD server. If a username pattern is specified in **Bind username pattern**, the pattern will be merged with the username supplied in the applet and the merged username will be used to connect to the AD server.

     Example: If you specify **cn={0},cn=Users,dc=raritan,dc=com** and **TestUser** has been supplied in the applet, then CC-SG uses **cn=TestUser,cn-Users,dc=raritan,dc=com** to connect to the AD server.

   ▪ Check **Use Bind After Search** to use the username and password you specified in the **General** tab to connect to the AD server. The entry is searched in the specified Base DN and is found if it meets the specified filtering criterion and if the attribute "samAccountName" is equal to the username entered in the applet. Then, a second connection is attempted using the username and password supplied in the applet. This second bind assures that the user provided the correct password.

7. Click **Next** to proceed. The **Groups** tab opens.

AD Group Settings

In the Groups tab, you can specify the exact location from which you want to import AD user groups.

Important: You must specify Group settings before you can import groups from AD.

1. Click the **Groups** tab.

2. Specify a **Base DN** (directory level/entry) under which the groups, containing the user to be authorized, will be searched.

Example	Description
dc=raritan,dc=com	The search query for the user in the group will be made over the whole directory structure.
cn=Administrators,cn=Users,dc=raritan,dc=com	The search query for the user in the group will be performed only in the Administrators sub-directory (entry).

3. Type a user's attributes in **Filter** so the search query for the user in the group will be restricted to only those entries that meet this criterion.

   For example, if you specify **cn=Groups,dc=raritan,dc=com** as the Base DN and (**objectclass=group**) as the Filter, then all entries that are in the **Groups** entry and are of type **group** will be returned.

4. Click **Next** to proceed. The **Trusts** tab opens.

AD Trust Settings

In the Trusts tab, you can set up trust relationships between this new AD domain and any existing domains. A trust relationship allows resources to be accessible by authenticated users across domains. Trust relationships can be incoming, outgoing, bidirectional, or disabled. You should set up trust relationships if you want AD modules that represent different forests in AD to be able to access information from each other. The trusts you configure in CC-SG should match the trusts configured in AD.

1. Click the **Trusts** tab. If you have configured more than one AD domain, all other domains are listed in the **Trusts** tab.

2. For each domain in the **Trust Partner** column, click the **Trust Direction** drop-down menu, and then select the direction of trust you want to establish between the domains. Trust directions are updated in all AD modules when you make changes to one AD module.

   ▪ **Incoming**: information will be trusted coming in from the domain. In the figure above, AD Module 2 would trust information coming in from AD Module 1

   ▪ **Outgoing**: information will be trusted going to the selected domain. In the figure above, AD Module 1 would trust information coming in from AD Module2.

   ▪ **Bidirectional**: information will be trusted in both directions from each domain.

   ▪ **Disabled**: information will not be exchanged between the domains.

3. Click **Apply** to save your changes, and then click **OK** to save the AD module and exit the window.

   The new AD module appears in the Security Manager screen, under External AA Servers.

4. Check the **Authentication** checkbox if you want CC-SG to use the AD module for authentication of users. Check the **Authorization** checkbox if you want CC-SG to use the AD module for authorization of users.

5. Click **Update** to save your changes.

Edit an AD Module

Once you have configured AD modules, you can edit them at any time.

➢ *To edit an AD module:*

1. Choose Administration > Security.

2. Choose the Authentication tab. All configured external Authorization and Authentication Servers display in a table.

3. Select the AD module you want edit, and then click **Edit**.

4. Click each tab in the Edit Module window to view the configured settings. Make changes as needed. Please refer *AD General Settings* (on page 111), *AD Advanced Settings* (on page 112), *AD Group Settings* (on page 114), and *AD Trust Settings* (on page 114) for details.

5. If you change the connection information, click **Test Connection** to test the connection to the AD server using the given parameters. You should receive a confirmation of a successful connection. If you do not see a confirmation, review the settings carefully for errors and try again.

6. Click **OK** to save your changes.

7. You must synchronize the AD user groups you changed, or you can synchronize all AD modules to synchronize all groups and users in all modules. Please refer to *Synchronize AD User Groups* (see "Synchronize All User Groups with AD" on page 118) and *Synchronize All AD Modules* (on page 119) for details.

Import AD User Groups

You must specify Group settings in the AD module before you can import groups from the AD server. Please refer to *AD Group Settings* (on page 114).

After making a change to imported groups or users, you must synchronize the AD user groups you changed so that the imported groups are mapped to the appropriate groups on AD, and synchronize all AD modules to synchronize all groups and users in all modules. Please refer to *Synchronize AD User Groups* (see "Synchronize All User Groups with AD" on page 118) and *Synchronize All AD Modules* (on page 119) for details.

You can import nested groups from AD.

Note: Make sure that you have configured the CC-SG DNS and Domain Suffix in Configuration Manager before attempting to import AD user groups. **Advanced Administration** *(on page 150)*

➢ **To import AD user groups:**

1. Choose Administration > Security.

2. Choose the Authentication tab. All configured Authorization and Authentication Servers display in a table.

3. Select the AD server whose AD user groups you want to import.

4. Click **Import AD User Groups** to retrieve a list of user group values stored on the AD server. If any of the user groups are not already on the CC-SG, you can import them here and assign them an access policy.

5. Select the groups you want to import to CC-SG.

- Imported user group names can include up to 64 characters.

- To search for user groups, type a search string in the **Search for User Group** field, and then click **Go**.

- Click a column header to sort the list of user groups by the information in that column.

- Click **Select all** to select all user groups for import.

- Click **Deselect all** to deselect all selected user groups.

6. In the **Policies** column, select a CC-SG access policy from the list to assign the policy to the selected group.

7. Click **Import** to import the selected user groups.

*Tip: To check that the group imported properly and to view the privileges of the group just imported, click the **Users** tab, then select the imported group to open the User Group Profile screen. Verify the information in the **Privileges** and **Device/Node Policies** tab. Click the **Active Directory Associations** tab to view information on the AD module associated with the user group.*

Synchronize AD with CC-SG

There are several methods for synchronizing the information CC-SG has with your AD server.

- Daily synchronization of all modules: You can enable scheduled synchronization to allow CC-SG to synchronize all AD modules daily at the time you choose. Please refer to *Synchronize All AD Modules* (on page 119). This synchronization is only necessary when you are using AD for authorization.

- On Demand Synchronization: You can perform 2 types of synchronization whenever you choose.

  1. *All Active Directory Modules* (see "Synchronize All AD Modules" on page 119): This option performs the same operation as daily synchronization of all modules, but you can use it to synchronize at any time on demand. This synchronization is only necessary when you are using AD for authorization.

2. *All User Groups* (see "Synchronize All User Groups with AD" on page 118): Use this option when you have changed a user group. Synchronizing all user groups allows you to map imported and local user groups to user groups identified as part of an AD module. Synchronizing user groups does not update access information in CC-SG. You must synchronize all AD modules, either by waiting for daily synchronization to run, or running the on-demand synchronization of all modules, to update access information.

Synchronize All User Groups with AD

You should synchronize all user groups if you have made a change to a user group. For example, if you know that a user group was moved from one AD module to another. (You can also change the AD association of a user group manually, in the User Group Profile, Active Directory Associations tab.)

If you have made changes to users or domain controllers, you should *synchronize all AD modules* (on page 119).

When you synchronize AD user groups, CC-SG retrieves the groups for the selected AD module, compares their names with the user groups that have already been imported from AD, and identifies the matches. CC-SG will present the matches and allow you to select which groups in AD you want to associate with CC-SG. This does not update user access information in CC-SG. Synchronizing AD User Groups only maps the group names from AD to CC-SG.

➢ **To synchronize all user groups with AD:**

1. *Enter Maintenance Mode.* (see "Enter Maintenance Mode" on page 141)

2. Choose Administration > Security

3. Choose the Authentication tab. All configured Authorization and Authentication Servers display in a table.

4. Select the AD server whose user groups you want to synchronize with the user groups in CC-SG.

5. In the On Demand Synchronization list, select All User Groups, then click the arrow button.

6. A list of all user groups found in the AD module whose names match user groups in CC-SG appears. Select the user groups you want to synchronize, and then click OK.

7. A confirmation message appears when all imported user groups in the selected module have been successfully synchronized.

8. *Exit Maintenance Mode.* (see "Exit Maintenance Mode" on page 141)

Synchronize All AD Modules

You should synchronize all AD Modules whenever you change or delete a user in AD, change user permissions in AD, or make changes to a domain controller.

When you synchronize all AD modules, CC-SG retrieves the user groups for all configured AD modules, compares their names with the user groups that have been imported into CC-SG or associated with the AD module within CC-SG, and refreshes the CC-SG local cache. The CC-SG local cache contains all domain controllers for each domain, all user groups that are associated with modules in CC-SG, and the user information for the known AD users. If user groups have been deleted from the AD modules, CC-SG removes all associations to the deleted group from its local cache as well. This ensures that CC-SG has the most current AD user group information.

➢ *To synchronize all AD modules:*

1. *Enter Maintenance Mode.* (see "Enter Maintenance Mode" on page 141)

2. Choose **Administration** > **Security**.

3. Choose the Authentication tab. All configured Authorization and Authentication Servers display in a table.

4. In the On Demand Synchronization list, select All Active Directory Modules, then click the arrow button. A confirmation message appears when all AD modules have been successfully synchronized.

5. *Exit Maintenance Mode.* (see "Exit Maintenance Mode" on page 141)

Enable or Disable Daily Synchronization of All AD Modules

➢ *To enable daily synchronization of all AD modules:*

1. Choose **Administration** > **Security**.

2. Choose the Authentication tab. All configured Authorization and Authentication Servers display in a table.

3. Select the Daily synchronization of All Modules checkbox.

4. In the **Synchronization Time** field, click the up and down arrows to select the time at which you want CC-SG to perform the daily synchronization of all AD modules.

5. Click **Update** to save your changes.

➢ *To disable daily synchronization of all AD modules:*

1. Choose **Administration** > **Security**.

2. Choose the Authentication tab. All configured Authorization and Authentication Servers display in a table.

3. Clear the Daily synchronization of All Modules checkbox.

4. Click **Update** to save your changes.

Change the Daily AD Synchronization Time

When daily synchronization is enabled, you can specify the time at which automatic synchronization occurs. By default, daily synchronization occurs at 23:30.

➢ *To change the daily AD synchronization time:*

1. Choose **Administration** > **Security**.

2. Choose the Authentication tab. Ensure that Daily synchronization of All Modules is checked.

3. In the **Synchronization Time** field at the bottom of the screen, click the up and down arrows to select the time at which you want CC-SG to perform the daily synchronization of all AD modules.

4. Click **Update** to save your changes.

About LDAP and CC-SG

Once CC-SG starts and a username and password are entered, a query is forwarded either through CC-SG or directly to the LDAP server. If the username and password match those in the LDAP directory, the user is authenticated. The user will then be authorized against the local user groups on the LDAP server.

Add an LDAP (Netscape) Module to CC-SG

➢ *To add an LDAP (Netscape) module to CC-SG:*

1. Choose **Administration** > **Security**.

2. Click the Authentication tab.

3. Click **Add…** to open the Add Module window.

4. Click the **Module Type** drop-down menu and select LDAP from the list.

5. Type a name for the LDAP server in the **Module name** field.

6. Click **Next** to proceed. The **General** tab opens.

LDAP General Settings

1. Click the **General** tab.

2. Type the IP address or hostname of the LDAP server in the **IP Address/Hostname** field. For hostname rules, please refer to *Terminology/Acronyms* (on page 2).

3. Type the port value in the **Port** field. The default port is 389.

4. Select **Secure Connection for LDAP** if using a secure LDAP server.

5. Select **Anonymous Bind** if your LDAP server allows anonymous queries. You do not need to enter a user name and password with anonymous binding.

   Note: By default, Windows 2003 does NOT allow anonymous queries. Windows 2000 servers do allow certain anonymous operations, whose query results are based on the permissions of each object.

6. If you are not using anonymous binding, type a username in the **User name** field. Type a Distinguished Name (DN) to specify the credentials used to query the LDAP server. For DN, enter the common name, organizational unit, and domain. For example, type **uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**. Separate the values with commas but do not use spaces before or after the comma. The values can include spaces, such as **Command Center**.

7. Type the password in the **Password** and **Confirm Password** fields.

8. To specify where the search for users begins, enter a Distinguished Name in **Base DN**. For example, **ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**, searches all organizational units under the domain.

9. To narrow searching to only particular types of objects, type a value in the **Filter** field. For example, **(objectclass=person)** will narrow searching to only person objects.

10. Click **Test Connection** to test the LDAP server using the given parameters. You should receive a confirmation of a successful connection. If not, review the settings carefully for errors and try again.

11. Click **Next** to proceed to the **Advanced** tab to set advanced configuration options for the LDAP server.

LDAP Advanced Settings

1. Click the **Advanced** tab.

2. Select **Base 64** if you want the password to be sent to the LDAP server with encryption. Select **Plain Text** if you want the password to be sent to the LDAP server as plain text.

3. **Default Digest**: select the default encryption of user passwords.

4. Type the user attribute and group membership attribute parameters in the **User Attribute** and **Group Membership Attribute** fields. These values should be obtained from your LDAP directory schema.

5. Type the bind pattern in the **Bind Username Pattern** field.

   ▪ Check **Use bind** if you want CC-SG to send the username and password entered at login to the LDAP server for authentication. If **Use Bind** is not checked, CC-SG will search the LDAP server for the user name, and if found, will retrieve the LDAP object and locally compare the associated password with the one entered.

   ▪ On some LDAP servers, the password cannot be retrieved as part of the LDAP object. Check **Use bind after search** to instruct CC-SG to bind the password to the LDAP object again and send it back to the server for authentication.

6. Click **OK** to save your changes. The new LDAP module appears in the Security Manager screen, under External AA Servers.

7. Select the **Authentication** checkbox if you want CC-SG to use the LDAP module for authentication of users.

8. Click **Update** to save your changes.

Sun One LDAP (iPlanet) Configuration Settings

If using a Sun One LDAP server for remote authentication, use this example for parameter settings:

Parameter Name	SUN One LDAP Parameters
IP Address/Hostname	<Directory Server IP Address>
User Name	CN=<Valid user id>
Password	<Password>
BaseDN	O=<Organization>
Filter	(objectclass=person)
Passwords (Advanced Screen)	Plain Text
Password Default Digest (Advanced)	SHA
Use Bind	unchecked
Use Bind After Search	Checked

OpenLDAP (eDirectory) Configuration Settings

If using an OpenLDAP server for remote authentication, use this example:

Parameter Name	Open LDAP Parameters
IP Address/Hostname	<Directory Server IP Address>
User Name	CN=<Valid user id>, O=<Organization>
Password	<Password>
User Base	O=accounts, O=<Organization>
User Filter	(objectclass=person)
Passwords (Advanced screen)	Base64
Password Default Digest (Advanced)	Crypt
Use Bind	Unchecked
Use Bind After Search	Checked

About TACACS+ and CC-SG

CC-SG users who are remotely authenticated by a TACACS+ server need to be created on the TACACS+ server and on CC-SG. The user name on the TACACS+ server and on CC-SG must be the same, although the passwords may be different. Please refer to *Users and User Groups* (on page 78) for details.

Add a TACACS+ Module

1. Choose **Administration** > **Security**.

2. Click the Authentication tab.

3. Click **Add** to open the Add Module window.

4. Choose **Module Type** > TACACS+.

5. Type a name for the TACACS+ server in the **Module name** field.

6. Click **Next**. The **General** tab opens.

TACACS+ General Settings

1. Type the IP address or hostname of the TACACS+ server in the **IP Address/Hostname Name** field. For hostname rules, please refer to *Terminology/Acronyms* (on page 2).

2. Type the port number on which the TACACS+ server is listening in the **Port Number** field. The default port number is **49.**

3. Type the authentication port in the **Authentication Port** field.

4. Type the shared key in the **Shared Key** and **Shared key confirm** fields.

5. Click **OK** to save your changes. The new TACACS+ module appears in the Security Manager screen, under External AA Servers.

6. Check the **Authentication** checkbox if you want CC-SG to use the TACACS+ module for authentication of users.

7. Click **Update** to save your changes.

About RADIUS and CC-SG

CC-SG users who are remotely authenticated by a RADIUS server need to be created on the RADIUS server and on CC-SG. The user name on the RADIUS server and on CC-SG must be the same, although the passwords may be different. Please refer to *Users and User Groups* (on page 78) for details on adding users who will be remotely authenticated.

Add a RADIUS Module

1. Choose **Administration** > **Security**.
2. Click the Authentication tab.
3. Click **Add** to open the Add Module window.
4. Click the **Module Type** drop-down menu and select RADIUS from the list.
5. Type a name for the RADIUS server in the **Module name** field.
6. Click **Next** to proceed. The **General** tab opens.

RADIUS General Settings

1. Click the **General** tab.
2. Type the IP address or hostname of the RADIUS server in the **IP Address/Hostname** field. For hostname rules, please refer to *Terminology/Acronyms* (on page 2).
3. Type the port number in the **Port Number** field. The default port number is 1812.
4. Type the authentication port in the **Authentication Port** field.
5. Type the shared key in the **Shared Key** and **Shared key confirm** fields.
6. Click **OK** to save your changes.
7. The new RADIUS module appears in the Security Manager screen, under External AA Servers. Check the **Authentication** checkbox if you want CC-SG to use the RADIUS   module for authentication of users.
8. Click **Update** to save your changes.

Two-Factor Authentication Using RADIUS

By using an RSA RADIUS Server that supports two-factor authentication in conjunction with an RSA Authentication Manager, CC-SG can make use of two-factor authentication schemes with dynamic tokens.

In such an environment, the user logs into CC-SG by first typing their username in the **Username** field. Then the user types their fixed password, followed by the dynamic token value in the **Password** field.

Configuration of CC-SG is identical to standard RADIUS remote authentication described above. Please refer to *Two-Factor Authentication* **(on page 261)** for details.

Chapter 13 Reports

In This Chapter

Using Reports

Sort report data

- Click a column header to sort report data by the values in that column. The data will refresh in ascending order alphabetically, numerically, or chronologically.

- Click the column header again to sort in descending order.

Resize report column width

The column widths you choose become the default report view the next time you log in and run reports.

1. Hold your mouse pointer on the column divider in the header row until the pointer becomes a double-headed arrow.

2. Click and drag the arrow to the left or right to adjust column width.

View report details

- Double-click a row to view details of the report.

- When a row is highlighted, press ENTER to view details.

Navigate multiple page reports

- Click the arrow icons at the bottom of the report to navigate through multiple page reports.

Print a report display

You can print the report as it displays in your screen. To print all report details, first *save the report to a file* (see "Save a report to a file" on page 128), and then print the file.

1. Generate the report you want to print.

2. Choose Secure Gateway > Print.

Save a report to a file

You can save a report to a .CSV file, which can be opened in Excel. When you save a report to a file, all the report's details are saved, not just the details you can view in the report screen.

1. Generate the report you want to save to a file.

2. Click Save to File. (Or, click Manage Report Data, and then click Save.)

3. Type a name for the file and choose the location where you want to save it

4. Click Save.

Purge a report's data from CC-SG

You can purge the records reported in the Audit Trail and Error Log reports. Purging these reports deletes all data currently present in the Audit Trail log or Error log from CC-SG permanently.

1. Generate the report whose data you want to delete from CC-SG.

2. Click Purge.

3. Click Yes to confirm.

Show or hide report filters

Some reports offer a set of filtering criteria at the top of the report screen. You can hide the filtering section, which will allow the report area to expand.

➢ *To show or hide the report filters:*

- Click the Filter toolbar at the top of the screen to hide the filtering section.

- Click the Filter toolbar again to show the filtering section.

Audit Trail Report

The **Audit Trail** report displays audit logs and access in CC-SG. It captures actions such as adding, editing, or deleting devices or ports, and other modifications.

CC-SG maintains an Audit Trail of the following events:

- When CC-SG is launched

- When CC-SG is stopped

- When a user logs on CC-SG

- When a user logs off CC-SG

- When a user starts a node connection

➢ *To generate the Audit Trail report:*

1. Choose Reports > Audit Trail.

2. Set the date range for the report in the **Start Date** and **End Date** fields. Click each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number.

3. You can limit the data that the report will contain by entering additional parameters in the **Message**, **Username**, and **User IP address** fields. Wildcards are accepted in these fields.

   - To limit the report by the message text associated with an activity, type the text in the **Message** field.

   - To limit the report to a particular user's activities, type the user's username in the **Username** field.

   - To limit the report to a particular IP address's activities, type the user's IP address in the **User IP address** field.

4. Click Apply to generate the report.

- Click **Purge (see** "Purge a report's data from CC-SG" **on page 128)** to delete the Audit Trail.

Error Log Report

CC-SG stores error messages in a series of Error Log files, which can be accessed and used to help troubleshoot problems. The Error Log includes a subset of the Audit Trail entries that are associated with an error condition.

➢ *To generate the Error Log report:*

1. Choose Reports > Error Log.

2. Set the date range for the report in the **Start Date** and **End Date** fields. Click each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number.

3. You can limit the data that the report will contain by entering additional parameters in the **Message**, **Username**, and **User IP address** fields. Wildcards are accepted in these fields.

- To limit the report by the message text associated with an activity, type the text in the **Message** field.

- To limit the report to a particular user's activities, type the user's username in the **Username** field.

- To limit the report to a particular IP address's activities, type the user's IP address in the **User IP address** field.

4. Click Apply to generate the report.

- Click *Purge* (see "Purge a report's data from CC-SG" on page 128) to delete the Error Log.

Access Report

Generate the Access report to view information about accessed devices and nodes, when they were accessed, and the user who accessed them.

➢ *To generate the Access Report:*

1. Choose Reports > Access Report.

2. Select Node or Devices.

3. Set the date range for the report in the **Start Date** and **End Date** fields. Click each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number.

4. You can limit the data that the report will contain by entering additional parameters in the **Device name**, **Node name**, **Username**, and **User IP address** fields.

   ▪ To limit the report to a particular device, type the device name in the **Device name** field.

   ▪ To limit the report to a particular node, type the port name in the **Node name** field.

   ▪ To limit the report to a particular user's activities, type the user's username in the **Username** field.

   ▪ To limit the report to a particular IP address's activities, type the user's IP address in the **User IP address** field.

5. In the Entries to Display field, select the number of entries to display in the report screen.

6. Click Apply to generate the report.

Availability Report

The Availability Report displays the status of all connections to devices or nodes. This report gives you full availability information for all devices or nodes in your CC-SG-managed network. Report information includes:

➢ *To generate the Availability Report:*

1. Choose Reports > Availability Report.

2. Select the Nodes or Devices option.

3. Click Apply.

Active Users Report

The Active Users report displays current users and user sessions. You can select active users from the report and disconnect them from CC-SG.

➢ **To generate the Active Users report:**

- Choose Reports > Users > Active Users.

➢ **To disconnect a user from an active session in CC-SG:**

1. In the Active Users report, select the user name you want to disconnect.

2. Click **Logout**.

Locked Out Users Report

The Locked Out Users report displays users who are currently locked out of CC-SG because they made too many unsuccessful login attempts. You can unlock users from this report. *Lockout Settings* (on page 177)

➢ **To generate the Locked Out Users report:**

- Choose Reports > Users > Locked Out Users.

➢ **To unlock a user who has been locked out of CC-SG:**

- Select the user name you want to unlock, and then click **Unlock User**.

User Data Report

The User Data report displays certain data on all users in the CC-SG database.

➢ **To generate the User Data report:**

- Choose Reports > Users > User Data.
  - The **User Name** field displays the user names of all CC-SG users.
  - The **Phone** field displays the user's dial back telephone number, which is only applicable for users of CC-SG G1 systems that include a modem.

- The **Enabled** field displays **true** if the user is able to log in to CC-SG, or **false** if the user is not able to log in to CC-SG, based on whether the **Login Enabled** checkbox is checked in the User Profile. Please refer to *Add a User* (on page 83) for details.

- The **Password Expiration** field displays the number of days that the user can use the same password before being forced to change it. Please refer to *Add a User* (on page 83) for details.

- The **Groups** field displays the user groups that the user belongs to.

- The **Privileges** field displays the CC-SG privileges assigned to the user. Please refer to *Appendix C: User Group Privileges* (see "User Group Privileges" on page 246) for details.

- The **Email** field displays the email address for the user, as specified in the User Profile.

- The **User Type** field displays **local** or **remote**, depending on the user's access method.

Users in Groups Report

The Users In Group report displays data on users and the groups with which they are associated.

➢ *To generate the Users in Groups report:*

- Choose Reports > Users > Users In Groups.
- Double-click the User Group to view the assigned Policies.

Group Data Report

The Group Data report displays user group, node group, and device group information. View user groups by name and description, view node groups by name, and view device groups by name, all in one screen.

➢ *To generate the Group Data report:*

- Choose Reports > Users > Group Data.
   - Click the … button next to a row to display either the policies associated with the user group, the list of nodes that satisfy the node group rule, or the list of devices that satisfy the device group rule.

AD User Group Report

The AD Users Group report displays all users in groups that were imported into CC-SG from Active Directory servers that have been configured for both authentication and authorization. The report does not include users who were added locally, via CC-SG, to the AD user groups.

➢ **To generate the AD Users Group report:**

1. Choose Reports > Active Directory > AD Users Group Report.

2. The **AD Server** list includes all AD servers that have been configured on CC-SG for both authentication and authorization. Check the checkbox that corresponds to each AD server you want CC-SG to include in the report.

3. In the **AD User Groups** section, the **Available** list includes all user groups that were imported into CC-SG from the AD servers you checked in the **AD Server** list. Select the user groups you want to include in the report, and then click **Add** to move the user groups to the **Selected** list.

4. Click **Apply** to generate the report.

Asset Management Report

The **Asset Management** report displays data on devices currently managed by CC-SG.

➢ **To generate the Asset Management report:**

1. Choose Reports > Devices > Asset Management Report. The **Asset Management** report is generated for all devices.

   ▪ To filter the report data by device type, click the **Device** type drop-down arrow, select a device type from the list, and then click **Apply**. The report is generated again with the selected filter applied.

   ▪ Devices whose versions do not comply with the Compatibility Matrix will display in red text in the **Device Name** field.

   ▪ Click **Refresh** to generate a new report. The report may take several minutes to generate, based on the size of your system configuration.

Node Asset Report

The Node Asset report displays node name, interface name and type, device name and type, and node group for all nodes under CC-SG management. You can also filter the report to include only data about nodes that correspond to a specified node group, interface type, device type, or device.

➢ *To generate the Node Asset report:*

1. Choose Reports > Nodes > Node Asset Report.

2. Select the filtering criteria you want to apply to the report, All Nodes, Node Group, Device Group, or Devices.

   ▪ If you select Node Group, Interface Type or Device Group, click the corresponding drop-down arrow, and then select a parameter from the list.

   ▪ If you select Devices, select the devices in the Available list whose node assets you want to include in the report, and then click Add to move them to the Selected list.

3. Click Apply to generate the report. The Node Asset Report generates.

Active Nodes Report

The Active Nodes report includes the name and type of each active interface, the current user, a timestamp, and the user IP address for each node with an active connection. You can view the active nodes list and disconnect nodes from this report.

➢ *To generate the Active Nodes report:*

1. Choose Reports > Nodes > Active Nodes. The Active Nodes report generates if there are currently active nodes.

   ▪ To disconnect a node from a current session, select the node you want to disconnect, and then click **Disconnect**.

Node Creation Report

The Node Creation report lists all node creation attempts, both successful and unsuccessful, within a specified timeframe. You can specify whether you want to see all node creation attempts, or only those that are potential duplicate nodes.

➢ *To generate the Node Creation report:*

1. Choose Reports > Nodes > Node Creation.

2. Set the date range for the report in the Start Date and End Date fields. Click each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number.

3. Select All Nodes or Potential Duplicates to specify whether you want to limit the report to only those nodes that have been flagged as potential duplicates.

4. Click Apply. The Node Creation report is generated.

   ▪ The Result field displays Success, Failed, or Potential Duplicate to describe the outcome of the node creation attempt

Query Port Report

The Query Port Report displays all ports according to port status.

➢ *To generate the Query Port report:*

1. Choose Reports > Ports > Query Port.

2. In the **Port Status/Availability** section, select the port states you want to include in the report. Selecting more than one checkbox will include ports with all selected states. You must select at least one Availability option when a Status option is specified.

State Type	Port State	Definition
	All	All ports.
Status:		
	Up	
	Down	Connection to port is not possible since the device is down and unavailable.

State Type	Port State	Definition
Availability:		
	Idle	Port has been configured and connection to port is possible.
	Connected	
	Busy	A user is connected to this port.
	Power on	
	Power off	
Unconfigured:		
	New	Port has a target server attached, but the port has not been configured.
	Unused	Port does not have a target server connected, and the port has not been configured.

3. (Optional) Select **Ghosted Ports** to include ports that are ghosted. A ghosted port can occur when a CIM or target server is removed from a Paragon system or powered off (manually or accidentally). Refer to Raritan's **Paragon II User Manual** for details.

4. (Optional) Select Paused Ports or Locked Ports to include ports that are paused or locked. Paused ports occur when a device is paused. Locked ports occur when a device is being upgraded.

5. Select the number of rows of data to display in the report screen in the Entries to Display field.

Note: This preference doesn't apply when generating the report as a task.

6. Click **Apply** to generate the report.

Active Ports Report

The Active Ports report displays out-of-band ports that are currently in use. You can view the active ports list and disconnect ports from this report.

➢ **To generate the Active Ports report:**

• Choose Reports > Ports > Active Ports.

➢ **To disconnect a port from a current session:**

• In the Active Ports report, select the port you want to disconnect, and then click **Disconnect**.

Scheduled Reports

Scheduled Reports displays reports that were scheduled in the Task Manager. You can find the Upgrade Device Firmware reports and Restart Device reports in the Scheduled Reports screen. All Scheduled Reports can be viewed in HTML format. Please refer to *Task Manager* (on page 186) for details.

➢ **To access Scheduled Reports:**

1. Choose Reports > Scheduled Reports.

2. Click **Get Reports** to view the entire list of all scheduled reports that were created by all owners. By default, all reports that were scheduled from one hour ago until the current time are displayed.

   ▪ To view a report, select the report in the list, and then click **Show Report**.

   ▪ (Optional) Filter the reports displayed:

   a. Enter parameters.

      ▪ Select a **Report Type**

      ▪ Select a **Report Owner**

      ▪ Change the start and end dates in the **Reports generated between** fields.

      ▪ Enter a **Report Name** to filter on the name. You can enter the full name or part of the name. Matches are not case sensitive. Wildcards are not allowed.

   b. Click **Get Reports** to view the filtered list.

Upgrade Device Firmware Report

The Upgrade Device Firmware report can be found in the Scheduled Reports list. This report is generated when an Upgrade Device Firmware task is running. View the report to get real-time status information about the task. Once the task has completed, the report information is static.

Please refer to *Scheduled Reports* (on page 138) for details on viewing the reports.

CC-NOC Synchronization Report

The CC-NOC Synchronization report lists all targets, along with their IP addresses, that the CC-SG subscribes to and that are monitored by a CC-NOC given a particular discovery date. Any new targets that are discovered in the configured range are displayed here as well. Please refer to *Add a CC-NOC* **(on page 193)** for details. You can also purge targets from the CC-SG database from this report.

➢ **To generate the CC-NOC Synchronization report:**

1. Choose Reports > CC-NOC Synchronization.

2. Select a **Last Discovered Date**, and then click **Get Targets.** The targets that were discovered on or earlier than the **Last Discovered Date** are displayed under **Targets Discovered**.

   ▪ If you want to purge a target from the CC-SG database, select the target you want to purge, and then click **Purge**.

   ▪ If you want to purge the entire list of targets from the CC-SG database, click **Purge All.**

Chapter 14 System Maintenance

In This Chapter

Maintenance Mode

Maintenance mode restricts access to CC-SG so that an administrator can perform various operations without disruption, such as upgrading CC-SG.

Current users, except the administrator who is initiating Maintenance Mode, are alerted and logged out after the configurable time period expires. While in Maintenance Mode, other administrators are allowed to log into CC-SG, but non-administrators are prevented from logging in. An SNMP trap is generated each time CC-SG enters or exits Maintenance Mode.

Note: Maintenance Mode is only available on standalone CC-SG units and not in a cluster configuration. Upgrade CC-SG is disabled until you enter Maintenance Mode.

Scheduled Tasks and Maintenance Mode

Scheduled tasks cannot execute while CC-SG is in Maintenance Mode. Please refer to *Task Manager* (on page 186) for details on scheduled tasks. When CC-SG exits Maintenance Mode, scheduled tasks will be executed as soon as possible.

Enter Maintenance Mode

1. Enter maintenance mode:

   a. Choose System Maintenance > Maintenance Mode > Enter Maintenance Mode.

   b. Password: Type your password. Only users with the CC Setup and Control privilege can enter maintenance mode.

   c. Broadcast message: Type the message that will display to users who will be logged off CC-SG.

   d. Enter maintenance mode after (min): Enter the number of minutes, from 0-30, that should elapse before CC-SG enters maintenance mode. Entering zero minutes causes Maintenance Mode to begin immediately.

   e. Click OK.

   f. Click OK in the confirmation dialog box.

Exit Maintenance Mode

1. Exit Maintenance Mode:

   a. Choose System Maintenance > Maintenance Mode > Exit Maintenance Mode.

   b. Click **OK** to exit Maintenance Mode.

   A message appears when CC-SG has exited Maintenance Mode. All users will now be able to access CC-SG normally.

Backup CC-SG

The best practice is to enter Maintenance Mode before backing up CC-SG. Entering Maintenance Mode ensures that no changes are made to the database while it is being backed up.

1. Choose **System Maintenance** > **Backup**.

2. Type a name for this backup in the **Backup Name** field.

3. (Optional) Type a short description for the backup in the **Description** field.

4. Select a **Backup Type**.

- **Custom** - Allows you to specify which components to add to the backup by checking them in the **Backup Options** area below. Check each of the following to include them in the backup.

- **Data** - CC-SG configuration, Device and Node configuration and User Data. (Standard)

- **Logs** - Error logs and event reports stored on CC-SG

- **CC-SG firmware files** - Stored firmware files used for updating the CC-SG server itself.

- **Device firmware files** - Stored firmware files used for updating Raritan devices managed by CC-SG.

- **Application files** - Stored applications used by CC-SG to connect users to nodes.

- **Full** - Creates a backup of all **Data**, **Logs**, firmware and **Application Files** stored on CC-SG. This produces the largest sized backup files.

- **Standard** - Only creates a back up of critical **Data** on CC-SG. This backup includes CC-SG configuration information, Device and Node configurations and User configurations. This produces the smallest sized backup file.

5. (Optional) If you want to save a copy of this backup file to an external server, check **Backup to Remote Location**.

6. Select a **Protocol** used to connect to the remote server, either **FTP** or **SFTP**

7. Type the IP address or hostname of the server in the **Hostname** field.

8. If you are not using the default port for the selected protocol (FTP: 21, SFTP: 22) type the communications port used in the **Port Number** field.

9. Type a username for the remote server in the **Username** field.

10. Type a password for the remote server in the **Password** field.

11. In the **Directory** field, specify the directory used to store the backup on the remote server. You must specify the absolute path to the directory.

12. Click **OK**.

A confirmation message appears when the backup completes. The backup file is saved in the CC-SG file system, and if specified in the **Backup to Remote Location** field, to a remote server as well. This backup can be restored at a later time.

Saving and Deleting Backup Files

You can save and delete backups stored on the CC-SG system from the **Restore CommandCenter** screen. Saving backups allows you to maintain a copy of the backup file on another PC. You can create an archive of backup files. Backup files saved to another location can be uploaded to other CC-SG units, and then restored to copy a configuration from one CC-SG to another.

Deleting backups you don't need saves space on the CC-SG.

Save a backup file

1. Choose **System Maintenance** > **Restore Command Center**.

2. From the **Available Backups** table, select the backup you want to save to your PC.

3. Click **Save to File**. A Save dialog appears.

4. Type a name for the file and choose the location where you want to save it.

5. Click Save.

   The backup file is copied to the specified location.

Delete a backup file

1. From the **Available Backups** table, select the backup you want to delete.

2. Click **Delete**. A confirmation dialog appears.

3. Click **OK** to delete the backup from the CC-SG system.

Restore CC-SG

➢ *To restore CC-SG:*

1. Choose **System Maintenance** > **Restore.** The **Restore CommandCenter** screen appears with a table of back up sessions available to CC-SG. The table lists the type of backup, the date of the backup, the description, what CC-SG version it was made from and the size of the backup file.

2. (Optional) If you want to restore from a backup stored off of the CC-SG system, you must first upload the backup file to CC-SG.

   a. Click **Upload**. An open dialog screen appears.

b. Browse for the backup file, and select it in the dialog window. You can retrieve the file from anywhere on your client's network.

c. Click **Open** to upload this file to CC-SG. When complete, the back-up file appears in the **Available Backups** table.

3. Select the backup you want to restore in the **Available Backups** table.

4. If applicable, select what kind of restore you want to perform from this backup:

    ▪ **Standard** - Only restores critical **Data** to CC-SG. This includes CC-SG configuration information, Device and Node configurations and User configurations.

    ▪ **Full** - Restores all **Data**, **Logs**, firmware and **Application Files** stored in the backup file. This requires that a full backup was made for the file.

    ▪ **Custom** - Allows you to specify which components of the backup to restore to CC-SG by checking them in the **Restore Options** area. Check each of the following to include them in the restore:

    ▪ **Data** - CC-SG configuration, Device and Node configuration and User Data.

    ▪ **Logs** - Error logs and event reports stored on CC-SG

    ▪ **CC firmware files** - Stored firmware files used for updating the CC-SG server itself.

    ▪ **Device firmware files** - Stored firmware files used for updating Raritan devices managed by CC-SG.

    ▪ **Application files** - Stored applications used by CC-SG to connect users to nodes.

5. Type the number of minutes, from 0-60, that CC-SG will wait before performing the restore operation in the **Restore after** field. This allows users time to complete their work and log off.

6. In the **Broadcast Message** field, type a message to notify other CC-SG users that a restore will occur.

7. Click **Restore**. CC-SG waits for the time specified in the **Restore after** field before restoring its configuration from the selected backup. When the restore occurs, all other users are logged off.

Reset CC-SG

You can reset CC-SG to purge the database. When the database is purged, all devices, nodes and users are removed. All remote authentication and authorization servers are removed.

Resetting does not reset system configuration data, such as the IP address of CC-SG. The following actions occur when you reset CC-SG:

- reset CC-SG database
- reset SNMP configuration
- reset to default firmware
- load default firmware into CC-SG database
- reset the Diagnostic Console to default values

You should perform a backup and save the backup file to another location before resetting CC-SG.

➢ *To reset CC-SG:*

1. Choose **System Maintenance** > **Reset.**

2. Type your CC-SG **password**.

3. Broadcast message: Type the message that will display to users who will be logged off CC-SG.

4. Enter the number of minutes, from 0-30, that should elapse before CC-SG performs the reset operation.

5. Click **OK** to reset CC-SG. A message appears to confirm the reset.

Restart CC-SG

The restart command is used to restart the CC-SG software. Restarting CC-SG will log all active users out of CC-SG.

Restarting will not cycle power to the CC-SG. To perform a full reboot you must access Diagnostic Console or the power switch on the CC-SG unit.

1. Choose **System Maintenance** > **Restart**.

2. Type your password in the **Password** field.

3. Broadcast message: Type the message that will display to users who will be logged off CC-SG.

4. Restart after (min): Enter the number of minutes, from 0-30, that should elapse before CC-SG restarts.

5. Click **OK** to restart CC-SG.

Upgrade CC-SG

You can upgrade CC-SG's firmware when a newer version is released. You can find firmware files in the Support section of the Raritan website.

Download the firmware file to your client PC before proceeding with the upgrade.

You should back up CC-SG before upgrading. If you are operating a CC-SG cluster, you must remove the cluster first and upgrade each node separately.

Note: If you are upgrading from 3.0.2 to 3.1, and you use Active Directory, please refer to the Readme for the 3.1 release for special instructions.

Important!

If you need to upgrade both CC-SG and a device or group of devices, perform the CC-SG upgrade first, and then perform the device upgrade.

CC-SG will reboot as part of the upgrade process from 3.1.1 to 3.2. DO NOT stop the process, reboot the unit manually, power off or power cycle the unit during the upgrade

➢ *To upgrade CC-SG:*

1. Download the firmware file to your client PC.

2. *Enter Maintenance Mode* (on page 141)

3. Once CC-SG is in maintenance mode, choose **System Maintenance** > **Upgrade**.

4. Click **Browse**. Navigate to and select the CC-SG firmware file, and then click **Open**.

5. Click **OK** to upload the firmware file to CC-SG.

    After the firmware file is uploaded to CC-SG, a success message appears to indicate that CC-SG has has begun the upgrade process. All users will be disconnected from CC-SG at this time.

6. Click **OK** to exit CC-SG and allow it to restart. You must wait approximately 8 minutes while CC-SG restarts.

7. Close your browser window, and then clear your browser cache.

8. After 8 minutes, open a new browser window and launch CC-SG.

9. Choose **Help** > **About Raritan Secure Gateway**. Check the version number to verify that the upgrade was successful.

   ▪ If the version has not upgraded, repeat the previous steps.

   ▪ If upgrade was successful, proceed to the next step.

10. *Exit Maintenance Mode* (on page 141)

Shutdown CC-SG

Shutting down CC-SG shuts down the CC-SG software, but it does not power off the CC-SG unit.

After CC-SG shuts down, all users are logged out. Users cannot log back in until you restart CC-SG, either via the Diagnostic Console, or by recycling the CC-SG power.

➢ *To shutdown CC-SG:*

1. Choose **System Maintenance** > **Shutdown CommandCenter**.

2. Type your password in the **Password** field.

3. Accept the default message or type a message to display to any users currently online in the **Broadcast message** field (for example, you might give users a brief time period to finish their tasks in CC-SG and tell them when they can expect the system to be functional again). All users will be disconnected when you shutdown CC-SG.

4. Type the number of minutes, from 0-60, that should pass before CC-SG shuts down in the **Shutdown after (min)** field.

5. Click **OK** to shut down CC-SG.

Restarting CC-SG after Shutdown

After shutting down CC-SG, use one of these two methods to restart the unit:

• Use the Diagnostic Console. Please refer to *Diagnostic Console* (on page 204) for details.

• Recycle the power to your CC-SG unit.

Power Down CC-SG

If CC-SG loses AC power while it is up and running, it will remember the last power state. Once AC power is restored, CC-SG automatically reboots. However, if CC-SG loses AC power when it is powered off, it will remain powered off when AC power is restored.

> **Important: Do not hold the POWER button to forcibly power down CC-SG. The recommended way to power down CC-SG is to use the following procedure.**

➢ *To power down the CC-SG:*

1. Remove the bezel and firmly tap the **POWER** button. On G1 units, the **POWER** button is on the back of the unit.

2. Wait approximately one minute while CC-SG gracefully powers down.

> **Note:** Users logged into CC-SG via Diagnostic Console will receive a short broadcast message when the CC-SG unit is powered down. Users logged into CC-SG via a web browser or SSH will not receive a message when the CC-SG unit is powered down.

3. If you must remove the AC power cord, let the power down process finish completely before removing the power cord. This is required for CC-SG to complete all transactions, close the databases, and place the disk drives into a safe state for power removal.

End CC-SG Session

There are two ways to end a CC-SG Session.

Log Out (see "Log Out of CC-SG" on page 148) to end your session while keeping the client window open.

Exit (see "Exit CC-SG" on page 149) to end your session and close the client window.

Log Out of CC-SG

1. Choose **Secure Gateway** > **Logout**. The **Logout** window appears.

2. Click **Yes** to log out of CC-SG. Once you log out, the CC-SG login window appears.

Exit CC-SG

1. Choose **Secure Gateway** > **Exit**.

2. Click **Yes** to exit CC-SG.

Chapter 15 Advanced Administration

In This Chapter

Configuring a Message of the Day

The Message of the Day allows you to provide a message for all users to view upon login. You must have the **CC Setup and Control** privilege to configure the message of the day.

➢ **To configure the Message of the Day:**

1. Choose **Administration** > **Message of the Day Setup**.

2. (Optional) Select **Display Message of the Day for All Users** if you want the message to be displayed to all users after they log in.

3. Select **Message of the Day Content** if you want to type a message in CC-SG, or select **Message of the Day File** if you want to load the message from an existing file.

   ▪ If you select **Message of the Day Content**:

   a. Type a message in the dialog box provided.

   b. Click the **Font Name** drop-down menu and select a font to display the message in.

c.   Click the **Font Size** drop-down menu and select a font size to display the message in.

▪   If you select **Message of the Day File**:

a.   Click **Browse** to browse for the message file.

b.   Select the file in the dialog window that opens, and then click **Open**.

c.   Click **Preview** to review the contents of the file.

4.   Click **OK** to save your changes.

Configuring Applications for Accessing Nodes

About Applications for Accessing Nodes

CC-SG provides various applications that you can use to access nodes. You can use the Application Manager to view applications, add new applications, delete applications, and set the default application for each device type.

➢   *To view applications available in CC-SG:*

1.   Choose **Administration** > **Applications**.

2.   Click the Application name drop-down menu to view the list of applications available in CC-SG.

Check and Upgrade Application Versions

Check and upgrade the CC-SG applications, such as Raritan Console (RC) and Raritan Remote Client (RRC).

➢   *To check an application version:*

1.   Choose **Administration** > **Applications**.

2.   Select an **Application name** from the list. Note the number in the **Version** field. Some applications do not automatically show a version number.

> ## To upgrade an application:

If the application version is not current, you must upgrade the application. You can download the application upgrade file from the Raritan website. For a complete list of supported application versions, please refer to the **Compatibility Matrix** on the Raritan Support website.

1. Save the application file to your client PC.

2. Click the **Application name** drop-down arrow and select the application that must be upgraded from the list. If you do not see the application, you must add it first. *Add an Application* (on page 152)

3. Click **Browse**, locate and select the application upgrade file from the dialog that displays, and then click **Open**.

4. The application name appears in the **New Application File** field in the **Application Manager** screen.

5. Click **Upload**. A progress window indicates that the new application is being uploaded. When complete, a new window will indicate that the application has been added to the CC-SG database and is available to use.

6. If the **Version** field does not automatically update, type the new version number in the **Version** field. The **Version** field will automatically update for some applications.

7. Click **Update**.

Add an Application

When you add an application to CC-SG, you must specify which device types the application will function with. If a device provides both KVM and serial access, the device is listed twice, once for each method.

1. Choose **Administration** > **Applications**.

2. Click **Add**. The **Add Applications** dialog window appears.

3. Type a name for the application in the **Application name** field.

4. Select the Raritan devices the application will function with from the **Available** list, and then click **Add** to add them to the **Selected** list.

   - To remove devices from use with the application, select the device in the **Selected** list, and then click **Remove**.

5. Click **OK**. An Open dialog window appears.

6. Navigate to and select the application file (usually a .jar or .cab file), and then click **Open**.

The selected application loads on to CC-SG.

Delete an Application

1. Choose **Administration** > **Applications**.

2. Select an application from the **Application Name** drop-down menu.

3. Click **Delete**. A confirmation dialog appears.

4. Click **Yes** to delete the application.

Configuring Default Applications

About Default Applications

You can specify which application you want CC-SG to use by default for each device type.

View the Default Application Assignments

1. Choose **Administration** > **Applications**.

2. Click the **Default Applications** tab to view and edit the current default applications for various Interfaces and Port Types. Applications listed here will become the default choice when configuring a node to allow access through a selected interface.

Set the Default Application for an Interface or Port Type

1. Choose **Administration** > **Applications**.

2. Click the **Default Applications** tab.

3. Select the Interface or Port Type whose default application you want to set.

4. Double-click the **Application** arrow listed on that row. The value becomes a drop-down menu. Grayed-out values cannot be changed.

5. Select the default application to use when connecting to the selected Interface or Port Type.

    -   **Auto-Detect**: CC-SG will automatically select an appropriate application based on the client browser.

6. Click **Update** to save your changes.

Managing Device Firmware

CC-SG stores firmware for Raritan devices that you can use to upgrade the devices under its control. The firmware manager is used to upload and delete device firmware files to and from CC-SG. Once a firmware file has been uploaded, you can access it to perform a device upgrade. *Upgrade a Device* (on page 38)

Upload Firmware

You can upload different versions of device firmware to CC-SG. When new firmware versions become available, they are posted on the Raritan website.

1. Choose **Administration** > **Firmware**.

2. Click **Add** to add a new firmware file. A search window appears.

3. Navigate to and select the firmware file you want to upload to CC-SG, and then click **Open**. When the upload completes, the new firmware appears in the **Firmware Name** field.

Delete Firmware

1. Choose **Administration** > **Firmware**.

2. Click the **Firmware Name** drop-down arrow and select the firmware you want to delete.

3. Click **Delete**. A confirmation message appears.

4. Click **Yes** to delete the firmware.

Configuring the CC-SG Network

You can configure the network settings for your CC-SG-managed network in the Configuration Manager.

About Network Setup

CC-SG offers two modes for network setup:

- *Primary/Backup mode* (see "What is Primary/Backup mode?" on page 156)
- Active/Active mode

CC-SG also allows either Static or DHCP-assigned IP addresses. Please refer to *Recommended DHCP Configurations for CC-SG* (on page 161) for best practices on using DHCP with your CC-SG.

About CC-SG LAN Ports

A CC-SG provides two main LAN ports: Primary LAN and Secondary LAN. Primary/Backup and Active/Active modes require you to connect the CC-SG LAN ports in different ways.

Please refer to the tables below to check the locations of the Primary and Secondary LAN ports on your CC-SG model.

G1 LAN Ports

Model	Primary LAN Name	Primary LAN Location	Secondary LAN Name	Secondary LAN Location
G1	LAN0	Right LAN port	LAN1	Left LAN port

V1 LAN Ports

Model	Primary LAN Name	Primary LAN Location	Secondary LAN Name	Secondary LAN Location
V1	LAN1	Left LAN port	LAN2	Right LAN port

E1 LAN Ports

Model	Primary LAN Name	Primary LAN Location	Secondary LAN Name	Secondary LAN Location
E1	Not labeled.	Top LAN port in set of 2 ports in center of unit back panel	Not labeled.	Bottom LAN port in set of 2 ports in center of unit back panel

What is Primary/Backup mode?

Primary/Backup mode enables you to use two CC-SG LAN ports to implement network failover and redundancy. In this mode, only one LAN port is active at a time.

Please refer to *About CC-SG LAN Ports* (on page 155) for the locations of the Primary LAN and Secondary LAN ports on each CC-SG model.
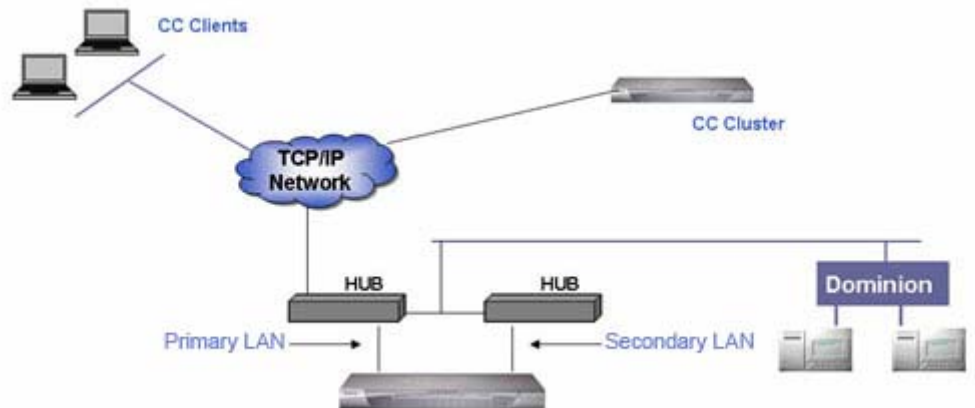
If the Primary LAN is connected and receiving a Link Integrity signal, CC-SG uses this LAN port for all communications. If the Primary LAN loses Link Integrity, and Secondary LAN is connected, CC-SG will failover its assigned IP address to the Secondary LAN. The Secondary LAN will be used until the Primary LAN returns to service. When the Primary LAN is back in service, CC-SG automatically reverts to using the Primary LAN.

As long as one LAN connection is viable, a client should not notice any disruption in service during a failure.

➢ *Setup for Primary/Backup mode*

When implementing Primary/Backup mode for your CC-SG network:

- Both CC-SG LAN ports must be attached to the same LAN sub-network.
- (Optional) You can attach each LAN port to a different switch or hub on the same subnetwork for reliability.

➢ *To configure Primary/Backup mode in CC-SG*

1. Choose **Administration** > **Configuration**.
2. Click the **Network Setup** tab.
3. Select **Primary/Backup mode**.
4. Type the CC-SG hostname in the Host name field. Please refer to *Terminology/Acronyms* (on page 2) for hostname rules. When you click **Update Configuration** to save the configuration, the **Host name** field will be updated to reflect the Fully-Qualified Domain Name (FQDN) if a DNS and domain suffix have been configured.
5. Click the **Configuration** drop-down arrow and select either **DHCP** or **Static**.

   DHCP:

   - If you choose DHCP, the Primary DNS, Secondary DNS, Domain Suffix, IP address, Subnet mask, and Default gateway fields will be automatically populated (if your DHCP server is configured to provide this information) once you save this network setup and restart CC-SG.
   - With the information the DHCP server provides, CC-SG registers itself dynamically with the DNS server if it accepts dynamic updates.
   - Please refer to *Recommended DHCP Configurations for CC-SG* (on page 161) for details.

Static:

- If you choose **Static**, type Primary DNS, Secondary DNS, Domain Suffix, IP address, Subnet mask, and Default gateway in the appropriate fields.

6. Click the **Adapter Speed** drop-down arrow and select a line speed from the list. Make sure your selection agrees with your switch's adapter port setting.

7. If you selected **Auto** in the **Adapter Speed** field, the **Adapter Mode** field is disabled, with **Full Duplex** selected automatically. If you specified an Adapter Speed other than Auto, click the **Adapter Mode** drop-down arrow and select a duplex mode from the list.

8. Click **Update Configuration** to save your changes. Your changes will not take effect until CC-SG restarts.

   - Click **Restart Now** if you want to automatically restart CC-SG now.

   - Click **Restart Later** if you would like to manually *restart CC-SG* (on page 145) later.

       - Click **Cancel** to return to the Network Setup panel without saving your changes. You must click **Update Configuration**, then click **Restart Now** or **Restart Later** to save your changes.

Note: If CC-SG is configured with DHCP, you can access CC-SG via the hostname after a successful registration with the DNS server.

What is Active/Active mode?

Active/Active mode allows you to use CC-SG to manage devices and nodes that are on two separate networks. In this mode, CC-SG manages traffic between the two separate IP domains. Active/Active mode does not offer failover. If either LAN connection fails, users won't have access.

Please refer to *About CC-SG LAN Ports* (on page 155) for the locations of the Primary LAN and Secondary LAN ports on each CC-SG model.

Note: Clustering cannot be configured when using Active/Active mode.
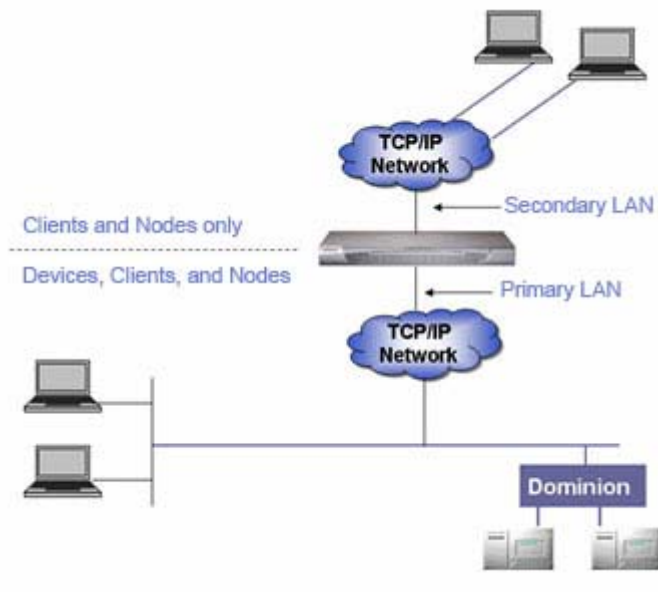
➢ *Setup for Active/Active mode*

When implementing Active/Active mode for your CC-SG network:

- Each CC-SG LAN port must be connected to a different sub-network.
- Raritan devices must be connected to the Primary LAN only.
- Clients and nodes may be connected to either the Primary LAN or the Secondary LAN.
- Specify at most one Default Gateway in the Network Setup panel in CC-SG. Use Diagnostic Console to *add more static routes* (see "Editing Static Routes (Network Interfaces)" on page 214) if needed.

➢ *To configure Active/Active mode in CC-SG*

1. Choose Administration > Configuration.

2. Click the Network Setup tab.

3. Select Active/Active mode.

4. Type the CC-SG hostname in the Host name field. Please refer to *Terminology/Acronyms* (on page 2) for hostname rules. When you click Update Configuration to save the configuration, the Host name field will be updated to reflect the Fully-Qualified Domain Name (FQDN) if a DNS and domain suffix have been configured.

5. Configure the Primary LAN in the left column, and the Secondary LAN in the right column:

6. Click the Configuration drop-down arrow and select either DHCP or Static.

   DHCP:

   ▪ If you choose DHCP, the Primary DNS, Secondary DNS, Domain Suffix, IP address, Subnet mask, and Default gateway fields will be automatically populated (if your DHCP server is configured to provide this information) once you save this network setup and restart CC-SG.

   ▪ With the information the DHCP server provides, CC-SG registers itself dynamically with the DNS server if it accepts dynamic updates.

   ▪ Please refer to *Recommended DHCP Configurations for CC-SG* (on page 161) for details.

   Static:

   ▪ If you choose Static, type Primary DNS, Secondary DNS, Domain Suffix, IP address, and Subnet mask in the appropriate fields.

   ▪ Specify only one Default gateway, not both.

7. Click the Adapter Speed drop-down arrow and select a line speed from the list. Make sure your selection agrees with your switch's adapter port setting.

8. If you selected Auto in the Adapter Speed field, the Adapter Mode field is disabled, with Full Duplex selected automatically. If you specified an Adapter Speed other than Auto, click the Adapter Mode drop-down arrow and select a duplex mode from the list.

9. Click Update Configuration to save your changes. CC-SG restarts.

Recommended DHCP Configurations for CC-SG

Review the following recommended DHCP configurations. Make sure that your DHCP server is set up properly before you configure CC-SG to use DHCP.

- Configure the DHCP to statically allocate CC-SG's IP address.

- Configure the DHCP and DNS servers to automatically register the CC-SG with the DNS when the DHCP allocates an IP address to CC-SG.

- Configure the DNS to accept un-authenticated Dynamic Domain Name System (DDNS) registration requests from CC-SG.

Configuring Logging Activity

You can configure CC-SG to report to external logging servers. You can specify what level of message is reported in each of the logs.

➢ **To configure CC-SG logging activity:**

1. Choose **Administration** > **Configuration**.

2. Click the **Logs** tab.

3. To assign an external log server for CC-SG to use, type the IP address in the **Server Address** field under **Primary Server**.

4. Click the **Level to Forward** drop-down arrow and select an event severity level. All events of this level or higher will be sent to the logging server.

5. To configure a second external log server, repeat steps 3 and 4 for the fields under **Secondary Server**.

6. Under **CommandCenter Log**, click the **Level to Forward** drop-down menu and select a severity level. All events of this level or higher will be reported in CC-SG's own internal log.

7. Click **Update Configuration** to save your changes.

Purging CC-SG's Internal Log

You can purge the CC-SG's internal log. This operation does not delete any events recorded on your external log servers.

Note: The Audit Trail and Error Log reports are based on CC-SG's internal log. If you purge CC-SG's internal log, these two reports will also be purged. You can also purge these reports individually. **Purge a report's data from CC-SG** *(on page 128)*

➢ *To purge CC-SG's internal log:*

1. Choose **Administration** > **Configuration**.

2. Click the **Logs** tab.

3. Click **Purge**.

4. Click **Yes**.

Configuring the CC-SG Server Time and Date

CC-SG's time and date must be accurately maintained to provide credibility for its device-management capabilities.

Important! The Time/Date configuration is used when scheduling tasks in Task Manager. Please refer to *Task Manager* **(on page 186) for details. The time set on your client PC may be different than the time set on CC-SG.**

Only the CC Super-User and users with similar privileges can configure Time and Date.

Changing the time zone is disabled in a cluster configuration.

➢ *To configure the CC-SG server time and date:*

1. Choose Administration > Configuration.

2. Click the **Time/Date** tab.

   a. **To set the date and time manually: Date**-click the drop-down arrow to select the **Month**, use the up and down arrows to select the **Year**, and then click the **Day** in the calendar area. **Time**-use the up and down arrows to set the **Hour, Minutes,** and **Seconds**, and then click the **Time zone** drop-down arrow to select the time zone in which you are operating CC-SG.

b. **To set the date and time via NTP:** Check the **Enable Network Time Protocol** checkbox at the bottom of the window, and then type the IP addresses for the **Primary NTP server** and the **Secondary NTP server** in the corresponding fields**.**

Note: Network Time Protocol (NTP) is the protocol used to synchronize the attached computer's date and time data with a referenced NTP server. When CC-SG is configured with NTP, it can synchronize its clock time with the publicly available NTP reference server and maintain correct and consistent time.

3. Click **Update Configuration** to apply the time and date changes to CC-SG.

4. Click **Refresh** to reload the new server time in the **Current Time** field.

5. Choose **System Maintenance** > **Restart** to restart CC-SG.

Modem Configuration

Use this screen to access a CC-SG G1 from a client machine over a dial-up connection. This method of accessing CC-SG can be used in emergency situations.

A modem is not available and cannot be configured on CC-SG V1 or E1 models.

Configure CC-SG

1. Choose Administration > Configuration. When the Configuration Manager screen appears, click the Modem tab.

2. Type the IP address of the CC-SG in the Server Address field.

3. Type the IP address of the client that will dial into CC-SG in the Client Address field.

4. If you are using call-back dialing, type the call-back number that CC-SG dials to connect to the client in the Client Phone field.

5. Click Update Configuration to save your changes.

Configure the Modem on Client PC

Connect a phone line to the CC-SG G1, which has a built-in modem. Optionally, remove the LAN cables.

On the client that will be dialing in, connect a modem to the client machine, for example, a Windows XP machine. Connect a phone line to the client modem. Restart the client machine and the connected modem is discovered as new hardware. Install the modem on the client as follows, which assumes a Windows XP client machine:

1. Choose **Control Panel** > **Phone and Modem Options**.

2. Click the **Modems** tab.

3. Click **Properties**.

4. Click the **Advanced** tab.

5. Type an initialization command in **Extra initialization commands** that will be used by your modem to set the "Carrier detection" flag. For example, type **at&c** for a SoftK56 Data Fax modem. This is necessary to tell Windows not to close the started Modem connection process when the modem connection is closed from the other (dialed-in) side. Click **OK** to save your changes.

Configure the Dial-up Connection

The following procedure illustrates creating an inbound dial-up connection to CC-SG from a Windows XP client machine:

1. Choose **Start** > **My Network Places**.

2. Right-click in the window and select **Properties**.

3. Under **Network Tasks** in the **Network Connections** window, click **Create a new connection**.

4. Click **Next**, **Connect to the network at my workplace**, **Dial-up connection**.

5. Type a name for the connection to CC-SG.

6. Type the phone number used to connect to CC-SG, and then click **Next**. This is NOT the dial-back number that was configured as the **Client phone** under the **Modem** tab in **Configuration Manager** on CC-SG.

7. A smart card is not necessary to dial into CC-SG. If you are not using one, click **Do not use my smart card** for this connection, and then click **Next**.

8. Click **My use only** in the next screen to make the connection available only to yourself.

9. Click **Finish** in the last screen to save your changes.

Configure the Call-back Connection

If the CC-SG uses a call-back connection, you need to use a script file. To supply the script file for call-back:

1. Choose **Start** > **My Network Places**.

2. Click **view network connections** under **Network Tasks**.

3. Right-click the **CommandCenter** connection, and then click **Properties**.

4. Click the **Security** tab.

5. Click the **Show terminal window**.

6. Click **Run script**, and then click **Browse** to enter the dial-up script, for example, **call-back.scp**.

7. Click **OK**.

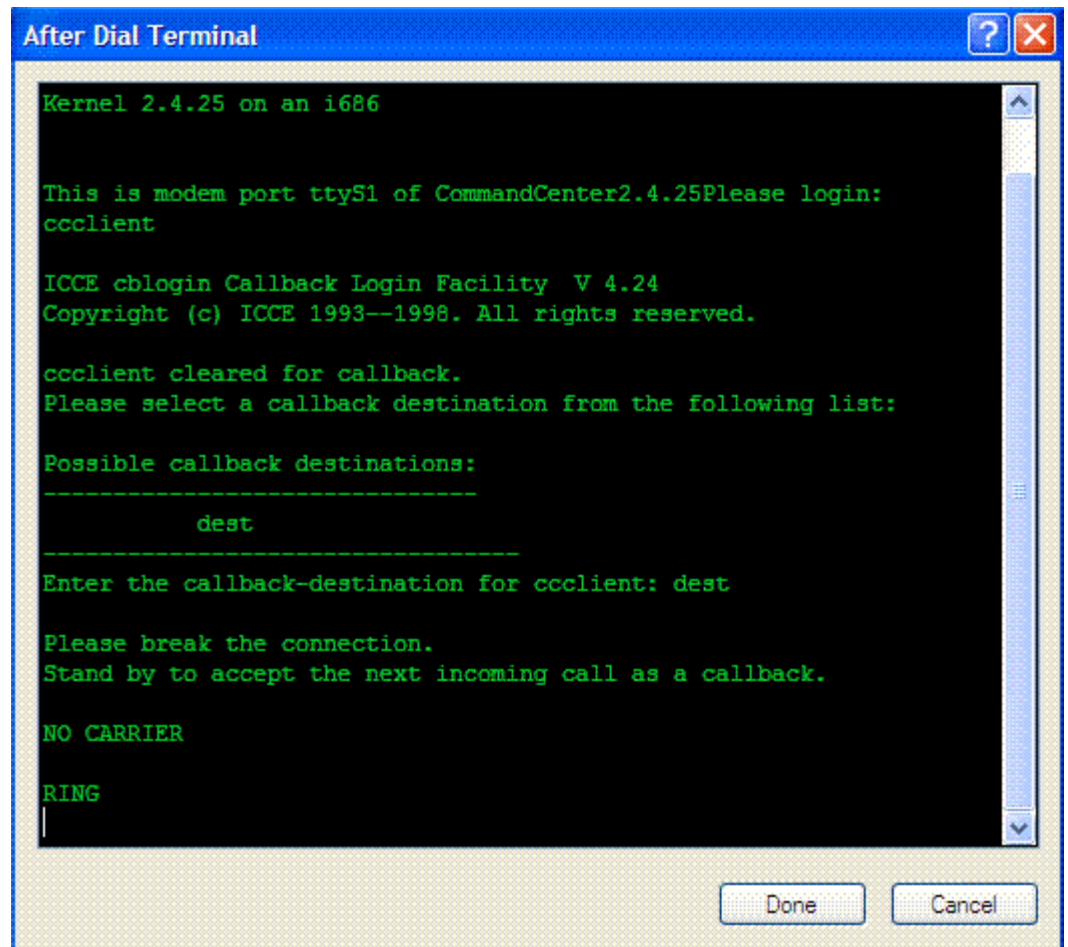   **Call-back Script File Example:**

```
proc main

delay 1

waitfor "ogin:"

transmit "ccclient^M"

waitfor "client:"

transmit "dest^M"

waitfor "callback."

transmit "ATH^M"

waitfor "RING"

transmit "ATA^M"

waitfor "CONNECT"

waitfor "ogin:"

transmit "ccclient^M"

endproc
```

Connect to CC-SG with Modem

➢ *To connect to CC-SG via a Modem:*

1. Choose **Start** > **My Network Places**.

2. Click **View network connections**.

3. Double-click the dial-up connection you created.

4. Type a username of **ccclient** and password of **cbupass**.

5. If not filled in already, type the phone number used to connect to CC-SG. This is NOT the dial-back number.

6. Click **Dial**. If using call-back, the modem will dial CC-SG and then CC-SG will dial your client PC.

7. If **Show terminal window** was checked as described in **Configure the Call-back Connection** (on page 165), an After Dial Terminal appears.

After Dial Terminal

```
Kernel 2.4.25 on an i686


This is modem port ttyS1 of CommandCenter2.4.25Please login:
ccclient

ICCE cblogin Callback Login Facility  V 4.24
Copyright (c) ICCE 1993--1998. All rights reserved.

ccclient cleared for callback.
Please select a callback destination from the following list:

Possible callback destinations:
------------------------------
          dest
------------------------------------
Enter the callback-destination for ccclient: dest

Please break the connection.
Stand by to accept the next incoming call as a callback.

NO CARRIER

RING
```

Done   Cancel

8. Wait 1 or 2 minutes. Then, in a supported browser, enter the IP address of CC-SG that was configured as the **Server address** under the **Modem** tab in **Configuration Manager** on CC-SG and login to CC-SG.

Connection Modes: Direct and Proxy

About Connection Modes

CC-SG offers three connection modes for out-of-band connections to Raritan device ports: Direct, Proxy, and Both, which is a combination of Direct and Proxy.

- Direct mode allows you to connect to a node or port directly, without passing data through CC-SG. Direct mode generally provides faster connections.

- Proxy mode allows you to connect to a node or port by passing all data through CC-SG. Proxy mode increases the load on your CC-SG server, which may cause slower connections. However, proxy mode is recommended if you are more concerned about the security of the connection. You only need to keep the CC-SG TCP ports (80, 443, and 2400) open in your firewall.

- Both mode allows you to configure CC-SG to use a combination of Direct mode and Proxy mode. In Both mode, Proxy mode is the default, but you can configure CC-SG to use Direct mode when connections are made using client IP addresses in specified ranges.

Important! When CC-SG is in Proxy or Both mode, you cannot give users access to virtual media.

To Configure Direct Mode for All Client Connections

1. Choose **Administration** > **Configuration.**

2. Click the **Connection Mode** tab.

3. Select **Direct mode**.

4. Click **Update Configuration**.

To Configure Proxy Mode for All Client Connections

1. Choose **Administration** > **Configuration.**

2. Click the **Connection Mode** tab.

3. Select **Proxy mode**.

4. Click **Update Configuration**.

To Configure a Combination of Direct Mode and Proxy Mode

When you configure CC-SG to use a combination of Direct mode and Proxy mode, Proxy mode will be the default connection mode, and Direct mode will be used for the client IP addresses you specify.

1. Choose **Administration** > **Configuration**.

2. Click the **Connection Mode** tab.

3. Select **Both**.

4. In the **Net Address** and **Net Mask** fields, specify the client IP address range that should connect to nodes and ports via Direct mode, and then click **Add**.

5. Click **Update Configuration**.

Device Settings

1. Choose **Administration** > **Configuration**.

2. Click the **Device Settings** tab.

3. To update device Default Port, select a Device Type in the table and double-click the Default Port value. Type the new Default Port value and press the **Enter** key.

4. To update device timeout duration, type a new timeout duration in the **Heartbeat (sec)** field.

5. Click **Update Configuration** to save your changes. A success message appears to confirm the update of all associated device settings.

Configuring SNMP

About SNMP and CC-SG

Simple Network Management Protocol allows CC-SG to push SNMP traps (event notifications) to an existing SNMP manager on the network. You should be trained in handling SNMP infrastructure to configure CC-SG to work with SNMP.

CC-SG also supports SNMP GET/SET operations with third-party solutions, such as HP OpenView. To support the operations, you must provide SNMP agent identifier information such as these MIB-II System Group objects: sysContact, sysName, and sysLocation. These identifiers provide contact, administrative, and location information regarding the managed node. Please refer to RFC 1213 for details.

MIB Files

Because CC-SG pushes its own set of Raritan traps, you must update all SNMP managers with a custom MIB file that contains Raritan SNMP trap definitions. *SNMP Traps* (on page 258) The custom MIB file can be found on on the Raritan Support web site.

To Configure SNMP in CC-SG

1. Choose **Administration** > **Configuration**.

2. Click the **SNMP** tab.

3. To identify the SNMP agent running on CC-SG to a third-party enterprise Management Solutions, provide agent information under **Agent Configuration**. Type a **Port** for the agent (default is **161).** Type a **Read-Only Community** string (default is **public)**, and **Read-Write Community** string, (default is **private)**. Multiple community strings are allowed; separate them with a comma. Type a **System Contact**, **System Name**, and **System Location** to provide information regarding the managed node.

4. Click **Update Agent Configuration** to save your changes.

5. Select **Enable SNMP Traps** to enable sending SNMP traps from CC-SG to a SNMP host.

6. Check the checkboxes before the traps you want CC-SG to push to your SNMP hosts: Under **Trap Sources**, a list of SNMP traps grouped into two different categories: **System Log** traps, which include notifications for the status of the CC unit itself, such as a hard disk failure, and **Application Log** traps for notifications generated by events in the CC application, such as modifications to a user account. To enable traps by type, check the boxes marked **System Log** and **Application Log.** Individual traps can be enabled or disabled by checking their corresponding checkboxes Use **Select All** and **Clear All** to enable all traps or clear all checkboxes. Refer to the MIB files for the list of SNMP traps that are provided. Please refer to **MIB Files** for details.

7. Type the **Trap Destination Host** IP address and **Port** number used by SNMP hosts in the **Trap Destinations** panel. Default port is **162**.

8. Type the **Community** string and **Version** (**v1** or **v2**) used by SNMP hosts in the **Trap Destinations** panel.

9. Click **Add** to add this destination host to the list of configured hosts. There is no limit to the number of managers that can be set in this list.

10. Click **Update Trap Configuration** to save your changes.

Configuring CC-SG Clusters

What is a CC-SG Cluster?

A CC-SG cluster uses two CC-SG nodes, one Primary node and one Secondary node, for backup security in case of Primary node failure. Both nodes share common data for active users and active connections, and all status data is replicated between the two nodes.

Devices in a CC-SG cluster must be aware of the IP of the Primary CC-SG node in order to be able to notify the Primary node of status change events. If the Primary node fails, the Secondary node immediately assumes all Primary node functionality. This requires initialization of the CC-SG application and user sessions and all existing sessions originating on the Primary CC-SG node will terminate. The devices connected to the Primary node will recognize that the Primary node is not responding and will respond to requests initiated by the Secondary node.

Requirements for CC-SG Clusters

- The primary and secondary nodes in a cluster must be running the same firmware version, on the same hardware version (G1, V1, or E1).

- CC-SG must in **Primary/Backup** mode to be used for clustering. Clustering will not work with an Active/Active configuration. Please refer to *About Network Setup* **(on page 155)** for details.

- Date, time, and time zone settings are not replicated from the Primary Node to the Secondary Node. You must configure these settings in each CC-SG before you create the cluster.

About CC-SG Clusters and CC-NOC

In a cluster configuration, only the Primary node communicates with CC-NOC. Whenever a CC-SG becomes the Primary node, it sends its IP address, in addition to the IP address of the Secondary node, to CC-NOC.

Create a Cluster

In the event of a failover, the administrator should send an email to all CC-SG users, notifying them to use the IP address of the new Primary CC-SG node.

If the Primary and Secondary Nodes lose communication with one another, the Secondary Node will assume the role of the Primary Node. When connectivity resumes, you may have two Primary Nodes. You should then remove a Primary Node and reset it as a Secondary Node.

Important: You should backup your configuration on both CC-SG units before creating a cluster.

➢ *1. Set Primary CC-SG Node*

1. Choose **Administration** > **Cluster Configuration**.

2. Click **Discover CommandCenters** to scan and display all CC-SG appliances on the same subset as the one you are currently using. Alternatively, you can add a CC-SG, perhaps from a different subnet, by specifying an IP address in **CommandCenter address** in the bottom of the window, and then clicking **Add CommandCenter**.

3. Type a name for this cluster in **Cluster Name**. If you do not provide a name now, a default name will be provided, such as **cluster192.168.51.124**, when the cluster is created.

4. Click **Create Cluster**. A message appears.

5. Click **Yes**. The CC-SG you are currently using becomes the Primary node.

> ➢ *2. Set Secondary CC-SG Node*

1. Click **Discover CommandCenters** to scan and display all CC-SG appliances on the same subset as your one you are currently using. Alternatively, you can add a CC-SG, perhaps from a different subnet, by specifying an IP address in **CommandCenter address** in the bottom of the window. Click **Add CommandCenter**.

2. To add a Secondary Node, or backup CC-SG node, select a CC-SG unit with **Standalone** status from the Cluster Configuration table. The version number must match the primary node's version.

3. Type a valid user name and password for the backup node in the **Backup username** and **Password** fields.

4. Click **Join "Backup" Node**.

5. A confirmation message appears. Click **Yes** to assign Secondary status to the selected node.

    Important! Once you begin the Join process, do not perform any other functions in CC-SG until the Join process has completed.

6. The newly selected Secondary node restarts. This process takes several minutes. When restart is complete, a confirmation message appears.

7. Choose **Administration** > **Cluster Configuration** to view the updated Cluster Configuration table.

Remove Secondary CC-SG Node

Removing a Secondary, or Backup, Node removes the designation of Secondary Node. It does not delete the Secondary CC-SG unit from your configuration.

> ➢ *To remove Secondary Node status from a CC-SG unit:*

1. Select the Secondary CC-SG Node in the Cluster Configuration table.

2. Click **Remove "Backup" Node.**

3. Click **Yes** to remove Secondary Node status.

Remove Primary CC-SG Node

Removing a cluster does not delete the Primary CC-SG unit from your configuration; it simply removes the designation of Primary Node. Remove Cluster is only available when no backup nodes exist.

➢ *To remove Primary Node status from a CC-SG unit:*

1. Select the Primary CC-SG Node in the Cluster Configuration table.

2. Click **Remove Cluster.**

3. Click **Yes** to remove Primary Node status.

Recover a Failed CC-SG Node

When a node fails and failover occurs, the failed node will recover in Waiting status. Once a node is in Waiting status it can be started in Standalone mode or Backup mode.

1. Select the Waiting node in the Cluster Configuration table.

2. Add it as a backup node by clicking **Join "Waiting" Node.**

3. A confirmation message appears. Click **Yes** to assign Secondary status to the selected node.

4. The secondary node restarts. This process takes several minutes. When restart completes, a confirmation message appears.

Advanced Cluster Settings

You cannot chang the time zone in a cluster configuration.

➢ *To configure advanced cluster settings:*

1. Select the Primary node.

2. Click **Advanced**. The **Advanced Settings** window appears.

3. For **Time Interval**, enter how often CC-SG should check its connection with the other node.

> Note: Setting a low Time Interval will increase the network traffic generated by heartbeat checks. You may want to set higher intervals for clusters with nodes located far apart from each other.

4. For **Failure Threshold**, enter the number of consecutive heartbeats that must pass without a response before a CC-SG node is considered failed.

5. For **Recover After**, enter the number of consecutive heartbeats that must successfully be returned before a failed connection is considered recovered.

6. Click **OK** to save your changes.

Security Manager

The Security Manager is used to manage how CC-SG provides access to users. Within Security Manager you can configure authentication methods, SSL access, AES Encryption, strong password rules, lockout rules, the login portal, certificates, and access control lists.

Remote Authentication

Please refer to *Remote Authentication* (on page 107) for detailed instructions on configuring remote authentication servers.

AES Encryption

You can configure CC-SG to require AES 128 encryption between your client and the CC-SG server. When AES encryption is required, all users must access CC-SG using an AES-enabled client. If AES encryption is required, and you try to access CC-SG with a non-AES browser, you will not be able to connect to CC-SG.

Check Your Browser for AES Encryption

If you do not know if your browser uses AES, check with the browser manufacturer.

You may also want to try navigating to the following web site using the browser whose encryption method you want to check: https://www.fortify.net/sslcheck.html. This web site will detect your browser's encryption method and display a report. Raritan is not affiliated with this web site.

Require AES Encryption between Client and CC-SG

In Security Manager, you can configure CC-SG to require AES-encryption for sessions between the client and the CC-SG server.

1. Choose **Administration** > **Security**.

2. Open the **Encryption** tab.

3. Check the **Require AES Encryption between Client and Server** check box.

4. A message appears to alert you that your clients must use AES encryption to connect to CC-SG once this option is selected. Click **OK** to confirm.

   ▪ The **Key Length** field displays 128. 128-bit encryption will be required between your client and the CC-SG server.

   ▪ The **Browser Connection Protocol** field displays HTTPS/SSL selected.

5. Click **Update** to save your changes.

Configure Browser Connection Protocol: HTTP or HTTPS/SSL

In Security Manager, you can configure CC-SG to use either regular HTTP connections from clients, or to require HTTPS/SSL connections. You must restart CC-SG for changes to this setting to take effect.

1. Choose **Administration** > **Security**.

2. Open the **Encryption** tab.

3. Select the **HTTP** or **HTTP/SSL** option to specify the Browser Connection Protocol you want clients to use when connecting to CC-SG.

4. Click **Update** to save your changes.

Setting the Port Number for SSH Access to CC-SG

In Security Manager, you can set the port number you want to use for SSH access to CC-SG. Please refer to **SSH Access to CC-SG** (on page 196) for details.

➢ *To set the port number for SSH access to CC-SG:*

1. Choose **Administration** > **Security**.

2. In the **Encryption** tab, type the port number for accessing CC-SG via SSH in the **SSH Server Port** field.

3. Click **Update** to save your changes.

Login Settings

The **Login Settings** tab enables you to configure the **Strong Password Settings** and **Lockout Settings**.

View login settings

1. Choose **Administration** > **Security**.

2. Click the **Login Settings** tab.

Require strong passwords for all users

1. Choose **Administration** > **Security**.

2. Open the **Login Settings** tab.

3. Check the **Strong Passwords Required for All Users** checkbox.

4. Select a **Maximum Password Length**. Passwords must contain fewer than the maximum number of characters.

5. Select a **Password History Depth**. The number specifies how many previous passwords are kept in the history and cannot be reused. For example, if **Password History Depth** is set to 5, users cannot reuse any of their previous 5 passwords.

6. Select a **Password Expiration Frequency**. All passwords expire after a set number of days. After a password expires, users will be asked to choose a new password the next time they log in.

7. Select **Strong Password Requirements**:

   - Passwords must contain at least one lower case letter.

   - Passwords must contain at least one upper case letter.

   - Passwords must contain at least one number.

   - Passwords must contain at least one special character (for example, an exclamation point or ampersand).

8. Click **Update** to save your changes.

About CC-SG Passwords

All passwords must meet every criteria that the administrator configures. After configuring strong password rules, all future passwords must meet these criteria. All existing users must change their passwords at their next logins if the new criteria are stronger than the previous criteria. Strong password rules apply only to user profiles stored locally. Password rules on an authentication server must be managed by the authentication server.

In addition, any four contiguous characters in the user name and the password cannot match.

Strong password rules require users to observe strict guidelines when creating passwords, which makes the passwords more difficult to guess and, in theory, more secure. Strong passwords are not enabled in CC-SG by default. A strong password that includes all strong password parameters is always required for the CC Super-User.

You can use the **Message of the Day** feature to provide advanced notice to users when the strong password rules will be changing and what the new criteria are.

Lockout Settings

Administrators can lock out CC-SG, CC-NOC users, and SSH users after a specified number of failed login attempts. This feature applies to users who are authenticated and authorized locally by CC-SG. It does not apply to users who are remotely authenticated by external servers. Please refer to *Configuring Remote Authentication* (see "Remote Authentication" on page 107) for details.

> *Note: By default, the **admin** account is locked out for five minutes after three failed login attempts. For **admin**, the number of failed login attempts before lockout and after lockout is not configurable.*

➢ *To enable lockout:*

1. Choose Administration > Security.

2. Open the Login Settings tab.

3. Check Lockout Enabled.

4. The default number of Failed Login Attempts before a user is locked out is 3. You can change this value by entering a number from 1 to 10.

5. Choose a Lockout Strategy:

- Lockout for Period: specify the period of time, in minutes, the user will be locked out before they can login again. The default number is 5 minutes. You can specify a period from 1 minute up to 1440 minutes (24 hours). After the time expires, the user can login again. At any time during the lockout period, an administrator can override this value and allow the user to log back into CC-SG.

- Lockout Until Admin Allows Access: users are locked out until an administrator unlocks the user account.

6. (Optional) Type an email address in the Lockout Notification Email field. Notification is sent to this email address when lockout has occurred. If the field is blank, notification is not sent.

7. (Optional) Type a phone number in the Administrator's Telephone field. The phone number will display in the notification email that is sent when lockout occurs.

8. Click Update to save your changes.

➢ *To disable lockout:*

When you disable lockout, all users currently locked out of CC-SG will be allowed to login.

1. Choose Administration > Security.

2. Open the Login Settings tab.

3. Clear the Lockout Enabled checkbox.

4. Click Update to save your changes.

Allow Concurrent Logins per Username

You can permit more than one concurrent CC-SG session with the same username.

1. Choose **Administration** > **Security.**

2. Open the **Login Settings** tab.

- Check **Super User** if you want to allow more than one simultaneous login with the CC Super User account.

- Check **System Administrators** if you want to allow concurrent logins by users in the **System Administrators** user group.

- Check **Other Users** if you want to allow concurrent logins by all other users.

3. Click **Update** to save your changes.

Configuring the Inactivity Timer

You can configure the inactivity timer to specify how long a CC-SG session can remain inactive before the user is logged out of CC-SG.

If a user has any connections to nodes open, the session is considered active, and the user will not be logged out when the inactivity timer expires.

➢ *To configure the inactivity timer:*

1. Choose **Administration** > **Security**

2. Open the **Login Settings** tab.

3. Type the desired time limit in the **Inactivity Time** field.

4. Click **Update** to save your changes.

Portal

Portal settings allow administrators to configure a logo and an access agreement to greet users when they access CC-SG.

➢ *To configure the portal settings:*

1. Choose **Administration** > **Security**.

2. Open the **Portal** tab.

Logo

A small graphic file can be uploaded to CC-SG to act as a banner on the login page. The maximum size of the logo is 998 by 170 pixels.

➢ *To upload a logo:*

1. Click **Browse** in the **Logo** area of the Portal tab. An Open dialog appears.

2. Select the graphic file you want to use as your logo in the dialog, and then click **Open**.

3. Click **Preview** to preview the logo. The selected graphic file appears to the right.

4. Click **Update** to save your changes.

Restricted Service Agreement

A message can be configured to appear to the left of the login fields on the login screen. This is intended for use as a Restricted Service Agreement, or a statement users agree to upon accessing the CC-SG. A user's acceptance of the Restricted Service Agreement is noted in the log files and the audit trail report.

➢ *To add a restricted service agreement to the CC-SG login screen:*

1. Select **Require Acceptance of Restricted Service Agreement** to require users to check an agreement box on the login screen before they are allowed to enter their login information.

2. Enter your message:

    a. Select **Restricted Service Agreement Message** if you want to enter the banner text directly.

      ▪ Type an agreement message in the text field provided. The maximum length of the text message is 10,000 characters.

      ▪ Click the **Font** drop-down menu and select a font for the message.

      ▪ Click the **Size** drop-down menu and select a font size for the message.

    b. Select **Restricted Service Agreement Message File** if you want to load a message from a text (.TXT) file.

      ▪ Click **Browse**. A dialog window appears.

      ▪ In the dialog window, select the text file with the message you want to use, and then click **Open**. The maximum length of the text message is 10,000 characters.

      ▪ Click **Preview** to preview the text contained in the file. The preview appears in the banner message field above.

3. Click **Update** to save your changes. The updates will appear on the login screen the next time a user accesses CC-SG.

Certificates

In the Certificate tab, you can generate a certificate signing request (CSR) to be sent to a certificate authority to apply for a digital identity certificate, generate a self signed certificate, or import and export certificates and their private keys.

Certificate Tasks

*Note: The button at the bottom of the screen will change from **Export** to **Import** to **Generate**, depending on which certificate option is selected.*

➢ *Export Current Certificate and Private Key*

1. Choose **Administration** > **Security**.

2. Click the **Certificate** tab.

3. Select **Export current certificate and private key**.

4. Click **Export.**

   The certificate appears in the **Certificate** panel and the private key appears in **Private Key** panel.

5. In each panel, select the text, and then press CTRL+C to copy it. You can then paste the text wherever needed.

➢ *Generate Certificate Signing Request, and Import Pasted Certificate and Private Key*

The CSR will be submitted to the Certificate Server who will issue a signed certificate. A root certificate will also be exported from the Certificate Server and saved in a file. Once you receive the signed certificate from the certificate signing authority, you can import the signed certificate, root certificate, and private key.

1. Choose **Administration** > **Security**.

2. Click the **Certificate** tab.

3. Click **Generate Certificate Signing Request**, and then click **Generate.** The Generate Certificate Signing Request window appears.

4. Type the requested data into the fields.

   a. Encryption Mode: If **Require AES Encryption between Client and Server** is selected in the Administration > Security > Encryption, AES-128 is the default. If AES is not required, 3DES is the default.

   b. Private Key Length: 1024 is the default.

   c. Validity Period (days): Maximum 4 numeric characters.

   d. Country Code: CSR tag is Country Name.

   e. State or Province: Maximum 64 characters. Type in the whole state or province name. Do not abbreviate.

    f.   City/Locality: CSR tag is Locality Name. Maximum 64 characters.

    g.   Registered Company Name: CSR tag is Organization Name. Maximum 64 characters.

    h.   Division/Department Name: CSR tag is Organization Unit Name. Maximum 64 characters.

    i.   Fully Qualified Domain Name: CSR tag is Common Name. The Registered Company name must own the domain name for CSRs. The signing service will reject the request if the Registered Company does not own the domain name.

    j.   Challenge Password: Maximum 64 characters.

    k.   Administrator Email Address: Type in the email address of the administrator who is responsible for the certificate request.

5. Click **OK** to generate the CSR. The CSR and Private Key appear in the corresponding fields of the **Certificate** screen.

6. Select the text in the Certificate Request box, and then press CTRL+C to copy it. Using an ASCII editor such as Notepad, paste the CSR into a file and save it with a **.cer** extension.

7. Select the text in the Private Key box, and then press CTRL+C to copy it. Using an ASCII editor such as Notepad, paste the Private Key into a file and save it with a **.txt** extension.

8. Submit the **.cer file** to the Certificate Server to obtain a signed certificate.

9. Download or export the root certificate from the Certificate Server and save it to a file with a **.cer** extension. This is a different certificate from the signed certificate that will be issued by the Certificate Server in the next step.

10. Click **Browse** next to **CA file** and select the root certificate file.

11. Once you receive the signed certificate from the Certificate Server, select **Import pasted certificate and private key**.

12. Copy the text of the signed certificate, and then press CTRL+V to paste it into the Certificate box.

13. Copy the text of the Private Key previously saved as a .txt file, and then press CTRL+V to paste it into the Private Key box.

14. Type **raritan** in the **Password** field if the CSR was generated by CC-SG. If a different application generated the CSR, use the password for that application.

Note: *If the imported certificate is signed by a root and subroot CA (certificate authority), using only a root or subroot certificate will fail. To resolve this, copy and paste both root and subroot certificate into one file, and then import it.*

➢ *Generate Self Signed Certificate Request*

1. Choose **Administration** > **Security**.

2. Click the **Certificate** tab.

3. Select **Generate Self Signed Certificate**, and then click **Generate**. The **Generate Self Signed Certificate** window appears.

4. Type the requested data into the fields.

   a. Encryption Mode: If **Require AES Encryption between Client and Server** is selected in the Administration > Security > Encryption, AES-128 is the default. If AES is not required, 3DES is the default.

   b. Private Key Length: 1024 is the default.

   c. Validity Period (days): Maximum 4 numeric characters.

   d. Country Code: CSR tag is Country Name.

   e. State or Province: Maximum 64 characters. Type in the whole state or province name. Do not abbreviate.

   f. City/Locality: CSR tag is Locality Name. Maximum 64 characters.

   g. Registered Company Name: CSR tag is Organization Name. Maximum 64 characters.

   h. Division/Department Name: CSR tag is Organization Unit Name. Maximum 64 characters.

   i. Fully Qualified Domain Name: CSR tag is Common Name. The Registered Company name must own the domain name for CSRs. The signing service will reject the request if the Registered Company does not own the domain name.

   j. Challenge Password: Maximum 64 characters.

   k. Administrator Email Address: Type in the email address of the administrator who is responsible for the certificate request.

5. Click **OK** to generate the certificate. The Certificate and Private Key appear encrypted in the corresponding fields of the **Certificate** screen.

Access Control List

An IP Access Control List specifies ranges of client IP addresses for which you want to deny or allow access to CC-SG. Each entry in the Access Control List becomes a rule that determines whether a user in a certain group, with a certain IP address, can access CC-SG. You can also set rules that apply to the whole CC-SG system (select System instead of a user group) at an operating system level. Once you create rules, you can arrange them in the list to specify the order in which they are applied. Rules at the top of the list take precedence over rules in lower positions in the list.

➢ *To view the Access Control List:*

1. Choose Administration > Security.

2. Open the Access Control List tab.

➢ *To add a rule to the Access Control List:*

1. Choose Administration > Security.

2. Open the Access Control List tab.

3. Click the Add Row icon to add a row to the table.

4. Specify a range of IP addresses to apply the rule to by typing the starting IP value in the Starting IP field, and the ending IP value in the Ending IP field.

5. Click the Group drop-down arrow to select a user group to apply the rule to. Selecting System will apply the rule to the

6. Click the Action drop-down arrow and select Allow or Deny to specify whether the specified users in the IP range can access CC-SG.

7. Click Update to save your changes.

➢ *To add a rule to the Access Control List that allows or denies access at an operating system level:*

1. Choose Administration > Security.

2. Open the Access Control List tab.

3. Click the Add Row icon to add a row to the table.

4. Specify a range of IP addresses to apply the rule to by typing the starting IP value in the Starting IP field, and the ending IP value in the Ending IP field.

5. Choose Group > System.

6. Click the Action drop-down arrow and select Allow or Deny to specify whether the specified users in the IP range can access CC-SG.

7. Click Update to save your changes.

➢ **To change the order in which CC-SG applies rules:**

1. Choose Administration > Security.

2. Open the Access Control List tab.

3. Select a rule you want to move up or down in the list.

4. Click the up or down arrow until the rule is in position.

5. Click Update to save your changes.

➢ **To remove a rule from the Access Control List:**

1. Choose Administration > Security.

2. Open the Access Control List tab.

3. Select the rule you want to remove, and then click the Remove Row icon.

4. Click Update to save your changes.

Notification Manager

Use Notification Manager to configure an external SMTP server so notifications can be sent from CC-SG. Notifications are used to email reports that have been scheduled, email reports if users are locked out, and to email status of failed or successful scheduled tasks. *Task Manager* (on page 186) After configuring the SMTP server, you can elect to send a test email to the designated recipient and notify the recipient of the result of the test.

Configure an external SMTP server

1. Choose **Administration** > **Notifications**.

2. Check the **Enable SMTP Notification** checkbox.

3. Type the SMTP host in the **SMTP host** field. For hostname rules, please refer to *Terminology/Acronyms* (on page 2).

4. Type a valid SMTP port number in the **SMTP port** field.

5. Type a valid account name that can be used to log in to the SMTP server in the **Account name** field.

6. Type the account name's password in the **Password** and **Re-enter Password** fields.

7. Type a valid email address that will identify messages from CC-SG in the **From** field.

8. Type the number of times emails should be re-sent should the send process fail in the **Sending retries** field.

9. Type the number of minutes, from 1-60, that should elapse between sending retries in the **Sending retry interval (minutes)** field.

10. Check **Use SSL** if you want emails to be sent securely using Secure Sockets Layer (SSL).

11. Click **Test Configuration** to send a test email to the SMTP account specified. You should check to make sure that the email arrives.

12. Click **Update Configuration** to save your changes.

Task Manager

Use Task Manager to schedule CC-SG tasks on a daily, weekly, monthly, or yearly basis. A task can be scheduled to run only once or periodically on a specified day of the week and at a specified interval. For example, you could schedule device backups to occur every three weeks on Fridays, or schedule a particular report to be emailed to one or more recipients every Monday.

Note: Task Manager uses the server time that is set on CC-SG for scheduling - not the time on your client PC. The server time is displayed in the upper right corner of each CC-SG screen.

Task Types

These tasks can be scheduled:

- Backup CC-SG
- Backup Device Configuration (individual device or device group)
- Copy Device Configuration (individual device or device group)
- Group Power Control
- Outlet Power Control
- Purge Logs
- Restart Device
- Restore Device Configuration (does not apply to device groups)
- Upgrade Device Firmware (individual device or device group).
- Generate all reports (HTML or CSV format)

Scheduling Sequential Tasks

You may want to schedule tasks sequentially to confirm that expected behavior occurred. For example, you may want to schedule an Upgrade Device Firmware task for a given device group, and then schedule an Asset Management Report task immediately after it to confirm that the correct versions of firmware were upgraded.

Email Notifications for Tasks

Upon completion of a task, an email message can be sent to a specified recipient. You can specify where and how the email is sent, such as if it is sent securely via SSL, in the *Notification Manager* (on page 185).

Scheduled Reports

Scheduled reports are sent via email to the recipients that you specify.

All reports that have a **Finished** status are stored on CC-SG for 30 days. You can view the finished reports in HTML format by selecting **Scheduled Reports** on the **Reports** menu. Please refer to *Scheduled Reports* (on page 138) for details.

Schedule a Task

This section covers most tasks that can be scheduled. Please refer to *Schedule a Device Firmware Upgrade Task* (see "Schedule a Device Firmware Upgrade" on page 190) for details on scheduling device firmware upgrades.

➢ **To schedule a task:**

1. Choose **Administration** > **Tasks**.

2. Click **New**.

3. In the **Main** tab, type a name (1-32 characters, alphanumeric characters or underscores, no spaces) and description for the task.

4. Click the **Task Data** tab.

5. Click the **Task Operation** drop-down menu and select the task you want to schedule. Note that the fields requiring data will vary according to the task selected. Please refer to the following sections for details on each task:

   ▪ *Backup CC-SG* (on page 141)

   ▪ *Backup Device Configuration* (on page 39)

   ▪ *Copy Device Configuration* (on page 42)

   ▪ *Group Power Control* (see "Node Group Power Control" on page 17)

   ▪ Outlet Power Control: Please refer to the CC-SG User Guide.

   ▪ *Purge Logs* (see "Configuring Logging Activity" on page 161)

   ▪ *Restart Device* (on page 42)

   ▪ *Restore Device Configuration* (see "Restore Device Configurations" on page 40) (does not apply to device groups)

   ▪ *Generate all reports* (see "Reports" on page 127)

   ▪ *Upgrade Device Firmware* (see "Schedule a Device Firmware Upgrade" on page 190) (individual device or device group)

6. Click the **Recurrence** tab. The **Recurrence** tab is disabled for *Upgrade Device Firmware tasks* (see "Schedule a Device Firmware Upgrade" on page 190).

7. In the **Period** field, click the radio button that corresponds to the period of time at which you want the scheduled task to recur.

   a. **Once:** Use the up and down arrows to select the **Start time** at which the task should begin.

b. **Periodic:** Use the up and down arrows to select the **Start time** at which the task should begin. Type the number of times the task should be executed in the **Repeat Count** field. Type the time that should elapse between repetitions in the **Repeat Interval** field. Click the drop-down menu and select the unit of time from the list.

c. **Daily:** Click the radio button next to **Every day** if you want the task to repeat 7 days per week. Click the radio button next to **Every weekday** if you want the task to repeat each day from Monday through Friday.

d. **Weekly:** Use the up and down arrows to select how many weeks should elapse between task executions, then check the checkbox next to each day on which the task should recur each week that it runs.

e. **Monthly:** Type the date on which the task should execute in the **Days** field, and then check the checkbox next to each month in which the task should recur on the specified date.

f. **Yearly:** Click the drop-down menu and select the month in which the task should execute from the list. Use the up and down arrows to select the day in that month on which the task should execute.

8. For **Daily**, **Weekly**, **Monthly**, and **Yearly** tasks, you must add a start and end time for the task in the **Range of recurrence** section. Use the up and down arrows to select the **Start at** time and **Start date**. Click the radio button next to **No end date** if the task should recur as specified indefinitely. Or, click the radio button next to **End date**, and then use the up and down arrows to select the date at which the task should stop recurring.

9. Click the **Retry** tab.

10. If a task fails, CC-SG can retry the task at a later time as specified in the **Retry** tab. Type the number of times CC-SG should retry to execute the task in the Retry count field. Type the time that should elapse between retries in the **Retry Interval** field. Click the drop-down menu and select the unit of time from the list.

Important: If you are scheduling a task to upgrade SX or KX devices, set the Retry Interval for more than 20 minutes, because it takes approximately 20 minutes to successfully upgrade these devices.

11. Click the **Notification** tab.

12. Specify email addresses to which a notification should be sent upon task success or failure. By default, the email address of the user currently logged in is available. User email addresses configured in the User Profile. To add another email address, click **Add**, type the email address in the window that appears, and then click **OK**. By default, email is sent if the task is successful. To notify recipients of failed tasks, check the **On Failure** checkbox.

13. Click **OK** to save your changes.

Schedule a Device Firmware Upgrade

You can schedule a task to upgrade multiple devices of the same type, such as KX or SX, within a device group. Once the task begins, an Upgrade Device Firmware report is available in the Reports > Scheduled Reports menu to view the upgrade status in real time. This report is also emailed if you specify the option in the Notification tab.

Please refer to the Raritan User Guide for each device for estimated upgrade times.

➢ *To schedule a Device Firmware Upgrade:*

1. Choose Administration > Tasks.

2. Click New.

3. In the Main tab, type a name and description for the task. The Name you choose will be used to identify the task and the report associated with the task.

4. Open the Task Data tab.

5. Specify the device upgrade details:

   a. Task Operation: Select Upgrade Device Firmware.

   b. Device Group: Select the device group that contains the devices you want to upgrade.

   c. Device Type: Select the type of device you want to upgrade. If you need to upgrade more than one device type, you must schedule a task for each type.

   d. Concurrent Upgrades: Specify the number of devices that should begin the file transfer portion of the upgrade simultaneously. Maximum is 10. As each file transfer completes, a new file transfer will begin, ensuring that only the maximum number of concurrent transfers occurs at once.

    e.   Upgrade File: Select the firmware version you want to upgrade to. Only available upgrade files that are appropriate for the device type selected will display as options.

6. Specify the time period for the upgrade:

    a.   Start Date/Time: Select the date and time at which the task begins. The start date/time must be later than the current date/time.

    b.   Restrict Upgrade Window and Latest Upgrade Start Date/Time: If you must finish all upgrades within a specific window of time, use these fields to specify the date and time after which no new upgrades can begin. Select Restrict Upgrade Window to enable the Latest Upgrade Start Date/Time field.

7. Specify which devices will be upgraded, and in what order. Place higher priority devices at the top of the list.:

    a.   In the Available list, select each device you want to upgrade, and click Add to move it to the Selected list.

    b.   In the Selected list, select a device and use the arrow buttons to move the devices into the order in which you want upgrades to proceed.

8. Open the Retry tab. Specify whether failed upgrades should be retried.

    a.   Retry Count: Type the number of times CC-SG should retry a failed upgrade.

    b.   Retry Interval: Enter the time that should elapse between retries. Default times are 30, 60, and 90 minutes. These are the optimal retry intervals.

9. Open the Notification tab. Specify email addresses that should receive notifications of success and failure. By default, the email address of the user currently logged in is available. User email addresses are configured in the User Profile.

    a.   Click Add, type the email address in the window that appears, and then click OK.

    b.   Select On Failure if you want an email sent if an upgrade fails.

    c.   Select On Success if you want an email sent when all upgrades complete successfully

10. Click OK to save your changes.

When the task starts running, you can open the Upgrade Device Firmware report any time during the scheduled time period to view the status of the upgrades. Please refer to *Upgrade Device Firmware Report* (on page 139) for details.

View a Task, Details of a Task, and Task History

If a task is changed or updated, its prior history no longer applies and the Last Execution Date will be blank.

➢ *To view a task:*

1. Choose **Administration** > **Tasks**.

2. To search for tasks, use the up and down buttons to select the date range you want to search. You can filter the list further by selecting one or more (**CTRL+click**) tasks, status, or owner from each list. Click **View Tasks** to view the list of tasks.

   ▪ To delete a task, select the task, and then click **Delete**.

   Note: You cannot delete a task that is currently running.

   ▪ To view the history of a task, select the task, and then click **Task History**.

   ▪ To view details of a task, double-click a task.

   ▪ To change a scheduled task, select the task, and then click **Edit** to open the Edit Task window. Change the task specification as needed, and then click **Update**. Please refer to **Create a New Task** for tab descriptions.

   ▪ To create a new task based on a previously configured task, select the task you want to copy, and then click **Save As** to open the Save As Task window. The tabs are populated with the information from the previously configured task. Change the task specifications as needed, and then click **Update**. Please refer to *Schedule a New Task* (see "Schedule a Task" on page 188) and *Schedule a Device Firmware Upgrade task* (see "Schedule a Device Firmware Upgrade" on page 190) for tab descriptions.

CommandCenter NOC

Adding a CommandCenter NOC (CC-NOC) to your setup will expand your target management capabilities by providing monitoring, reporting, and alert services for your serial and KVM target systems. Please refer to Raritan's CommandCenter NOC documentation for details on installing and operating CC-NOC.

To create a valid connection between the CC-SG and the CC-NOC, you should synchronize the time settings on each. CC-NOC and CC-SG are required to be configured to use an NTP server.

Add a CC-NOC

You must provide the passcodes generated to the CC-NOC administrator, who must configure them in CC-NOC within five minutes. Avoid transmitting the passcodes over email or other electronic means to avoid a possible interception by automated systems. A phone call or exchange of written codes between trusted parties is better protection against automated interception.

1. On the **Access** menu, click **CC-NOC Configuration**.

2. Click **Add**.

3. Select a software version of CC-NOC you want to add, and then click **Next**. Version 5.1 has fewer integration features than 5.2 and later, and only requires adding a name and an IP address. Please refer to the Raritan Support web site for details on CC-NOC 5.1.

4. Type a descriptive name for the CC-NOC in the **Name** field. Maximum length is 50 alphanumeric characters.

5. Type the IP address or hostname of the CC-NOC in the **CC-NOC IP/Hostname** field. This is a required field. For hostname rules, please refer to *Terminology/Acronyms* (on page 2).

6. To retrieve daily information on targets in the CC-NOC database, type a discovery range in the **IP Range From** and **IP Range To** fields. CC-SG will request that CC-NOC send events for devices in this IP range to CC-SG. This range is related to the discovery range configured in CC-NOC. Please refer to Raritan's **CommandCenter NOC Administrator Guide** for details. Type a range, keeping the following rules in mind:

IP Address Range	Description
If CC-SG range entered here is a subset of the range configured in CC-NOC…	…then, CC-NOC returns all known target device information within this range.
If CC-SG range entered here includes a partial list (non-null intersection) of the range configured in CC-NOC…	…then, CC-NOC returns all known target device information within the intersecting range.
If CC-SG range is a superset of the range configured in CC-NOC…	…then, CC-NOC returns all known target device information within this range. Essentially, CC-NOC returns targets that are defined in the CC-NOC range.
If CC-SG range does not overlap the range configured in CC-NOC…	…then, CC-NOC will not return any target device information at all.

Note: Use the CC-NOC Synchronization Report to view targets that CC-SG is subscribing to. The report also displays any new targets that have been discovered by CC-NOC. Please refer to ***CC-NOC Synchronization Report*** (on page 139) for details.

1. Specify a **Synchronization Time** to schedule when the target information is retrieved from the CC-NOC database. This will refresh the databases as targets are discovered or become unmanaged. The default is the current time as set on the client machine. You may want to schedule synchronization during an off-peak time so synchronization will not affect the performance of other processes.

2. In the **Heartbeat Interval** field, enter how often, in seconds, CC-SG sends a heartbeat message to CC-NOC. This confirms if CC-NOC if still up and available. Default is **60** seconds. Valid range is **30-120** seconds.

3. In the **Failed Heartbeat Attempts** field, enter the number of consecutive heartbeats that must pass without a response before a CC-NOC node is considered unavailable. Default is **2** heartbeats. Valid range is **2-4** heartbeats.

4. Click **Next**.

5. Either copy and paste the passcodes into CC-NOC fields if you are the CC-NOC administrator, or submit the two passcodes to the CC-NOC administrator.

Important: To increase security, you must enter the passcodes in CC-NOC within five minutes after they are generated on CC-SG. This will minimize the window of opportunity for intruders to breach the system with a brute-force attack. Avoid transmitting the passcodes over email or other electronic means to avoid a possible interception by automated systems. A phone call or exchange of written codes between trusted parties is better protection against automated interception.

Once the certificate exchange process is complete, a secure channel has been established between CC-NOC and CC-SG. The CC-NOC data will be copied to CC-SG. Click **OK** to complete the process. If the process does not complete within **5** minutes, it times out and data is not saved in CC-SG and any stored certificates are deleted. You must repeat the procedure.

Note: CommandCenter NOC can only be added to standalone CC-SG units or primary nodes of clustered CC-SG units.

Edit a CC-NOC

➢ *To edit a CC-NOC*

1. Choose **Access** > **CC-NOC Configuration**.

2. Highlight a CC-NOC in the list, and then click **Edit**.

3. Change the configuration as needed.

Launch CC-NOC

➢ *To launch CC-NOC from CC-SG:*

1. Choose **Access** > **CC-NOC Configuration**.

2. In the CC-NOC Configuration screen, select an available CC-NOC.

3. Click **Launch**. This will connect you to a configured CC-NOC.

Delete a CC-NOC

1. Choose **Access** > **CC-NOC Configuration**.

2. Select the CC-NOC you want to delete from CC-SG, and then click **Delete**. A confirmation message appears.

3. Click **Yes** to delete the CC-NOC. A message appears when the CC-NOC has been deleted.

SSH Access to CC-SG

Use Secure Shell (SSH) clients, such as Putty or OpenSHH Client, to access a command line interface to SSH (v2) server on CC-SG. Only a subset of CC-SG commands is provided via SSH to administer devices and CC-SG itself.

The SSH client user is authenticated by the CC-SG in which existing authentication and authorization policies are applied to the SSH client. The commands available to the SSH client are determined by the permissions for the user groups to which the SSH client user belongs.

Administrators who use SSH to access CC-SG cannot logout a CC Super-User SSH user, but are able to log out all other SSH client users, including System Administrators.

➢ **To access CC-SG via SSH:**

1. Launch an SSH client, such as PuTTY.

2. Specify the IP address of the CC-SG and specify **22** for the port, and open the connection. You can configure the port for SSH access in Security Manager. Please refer to *Configuring Security* (see "Security Manager" on page 174) for details.

3. Log in with your CC-SG username and password.

4. A shell prompt appears. Type **ls** to display all commands available. You can type **?** or **help** to display descriptions and format for typing all commands.
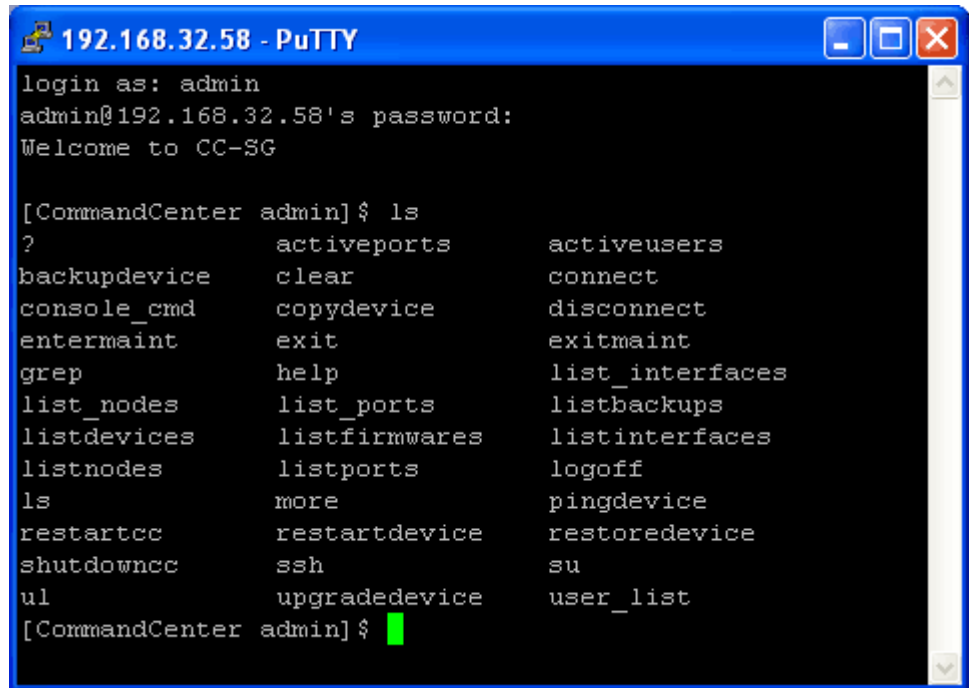
SSH Commands

The following table describes all commands available in SSH. You must be assigned the appropriate privileges in CC-SG to access each command.

Typing a command followed by the **-h** switch displays help for that command, such as **listfirmwares -h.**

Command Description
`activeports` List active ports.
`activeusers` List active users.
`backup device < [-host <host>] | [-id <device_id>] > backup_name [description]` Backup device configuration.

```clear```   Clear screen.
```connect [-d <device_name>] [-e <escape_char>] <[-i``` ```<interface_id>]	[-n <port_name>]	[port_id]>``` Establish a connection to a serial port. If <port_name> or <device_name> contains spaces it should be surrounded by quotes.
``copydevice <[-b <backup_id>]	[source_device_host]>``` ```target_device_host``` Copy device configuration

```disconnect <[-u <username>] [-p <port_id>] [-id```
 ```<connection_id>]>```
 	
 Close port connection.

```entermaint minutes [message]```   Place CC-SG in maintenance mode.
```exitmaint```   Remove CommandCenter from maintenance mode.
```grep search_term```   Search text from piped output stream.
```help```   View help screen.
``listbackups <[-id <device_id>]	[host]>``` List available device configuration backups.
```listdevices```   List available devices.
``listfirmwares [[-id <device_id>]	[host]]``` List firmware versions available for upgrade.
```listinterfaces [-id <node_id>]```   List all interfaces.
```listnodes```   List all nodes.
``listports [[-id <device_id>]	[host]]``` List all ports.
```logoff [-u <username>] message```   Logoff user

`ls` List commands
`more [-p <page_size>]` Make paging
`pingdevice <[-id <device_id>]	[host]>` Ping device
`restartcc minutes [message]` Restart CC-SG
`restartdevice <[-id <device_id>]	[host]>` Restart device
`restoredevice <[-host <host>]	[-id <device_id>]>` `[backup_id]` Restore device configuration
`shutdowncc minutes [message]` Shutdown CC-SG.
`ssh [-e <escape_char>] <[-id <device_id>]	[host]>` Open SSH connection to an SX device
`su [-u <user_name>]` Change a user.
`upgradedevice <[-id <device_id>]	[host]>` Upgrade device firmware
`exit` Exit SSH session.

Command Tips
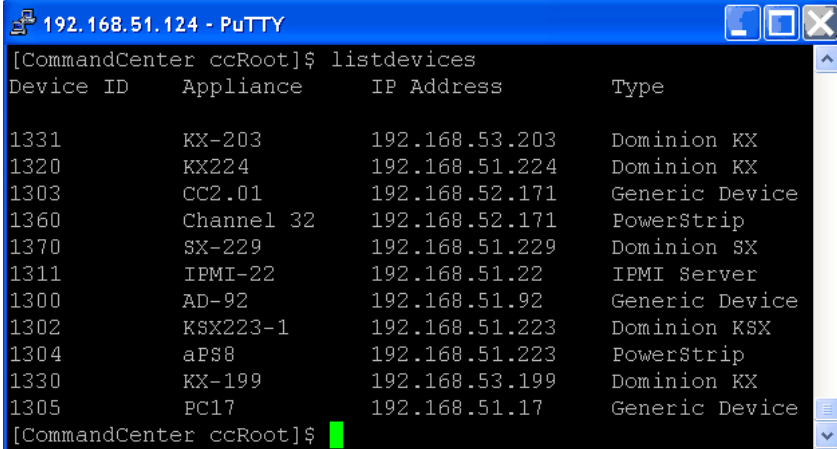
- For commands that pass an IP address, such as `upgradedevice`, you can substitute the hostname for an IP address. For hostname rules, please refer to *Terminology/Acronyms* (on page 2).

- The `copydevice` and `restartdevice` commands apply only to some Raritan devices, for example, Dominion SX. IPMI servers, generic devices are not supported by these commands.

Create an SSH Connection to an SX Device

You can create an SSH connection to an SX device to perform administrative operations on the device. Once connected, the administrative commands supported by the SX device are available.
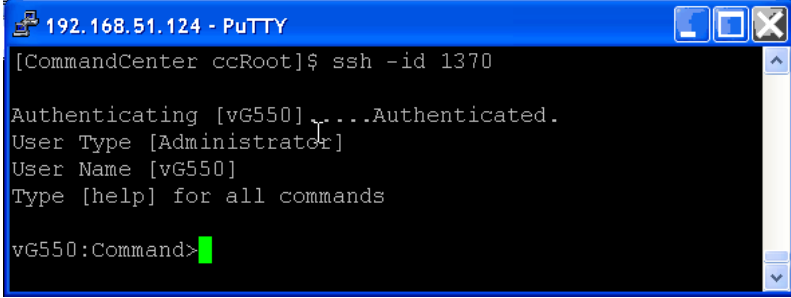
Note: Before you connect, ensure that the SX device has been added to the CC-SG.

1. Type `listdevices` to ensure the SX has been added to CC-SG.

```
192.168.51.124 - PuTTY
[CommandCenter ccRoot]$ listdevices
Device ID    Appliance      IP Address        Type

1331         KX-203         192.168.53.203    Dominion KX
1320         KX224          192.168.51.224    Dominion KX
1303         CC2.01         192.168.52.171    Generic Device
1360         Channel 32     192.168.52.171    PowerStrip
1370         SX-229         192.168.51.229    Dominion SX
1311         IPMI-22        192.168.51.22     IPMI Server
1300         AD-92          192.168.51.92     Generic Device
1302         KSX223-1       192.168.51.223    Dominion KSX
1304         aPS8           192.168.51.223    PowerStrip
1330         KX-199         192.168.53.199    Dominion KX
1305         PC17           192.168.51.17     Generic Device
[CommandCenter ccRoot]$
```

2. Connect to the SX device by typing `ssh -id <device id>`. For example, using the figure above as an example, you can connect to SX-229 by typing `ssh -id 1370`.

```
192.168.51.124 - PuTTY
[CommandCenter ccRoot]$ ssh -id 1370

Authenticating [vG550] .....Authenticated.
User Type [Administrator]
User Name [vG550]
Type [help] for all commands

vG550:Command>
```

Use SSH to Connect to a Node via a Serial Out of Band Interface

You can use SSH to connect to a node through its associated serial out-of-band interface. The SSH connection is in proxy mode.

1. Type `listinterfaces` to view the node ids and associated interfaces.

2. Type `connect -i <interface_id>` to connect to the node associated with the interface.

3. Once connected to the node, type the default Escape keys of '~' followed by a dot '.' At the prompt that displays, you can enter specific commands or aliases.

Command	Alias	Description
`quit`	q	Terminates connection and returns to SSH prompt.
`get_write`	gw	Gets Write Access. Allows SSH user to execute commands at target server while browser user can only observe proceedings.
`get_history`	gh	Gets History. Displays the last few commands and results at target server.
`send_break`	sb	Sends Break. Breaks the loop in target server initiated by browser user.

help	?,h	Prints help screen.

Exit an SSH Session

To exit the entire SSH connection to CC-SG, type `exit`.

Serial Admin Port

The serial admin port on CC-SG can be connected directly to a Raritan serial device, such as Dominion SX or KSX.

You can connect to the SX or KSX via the IP address using a terminal emulation program, such as HyperTerminal or PuTTY. Set the baud rate in the terminal emulation program to match the SX or KSX baud rate.

➢ *G1 Serial Admin Port:*

➢ *V1 Serial Admin Port:*

➢ *E1 Serial Admin Port:*

About Terminal Emulation Programs

HyperTerminal is available on many Windows OS. HyperTerminal is not available on Windows Vista.

PuTTY is a free program you can download from the internet.

Web Services API

The Web Services Application Programming Interface (WS API) is not currently available for activation. Please refer to http://www.raritan.com/web-services-api for updated information about this feature.

Chapter 16 Diagnostic Console

The Diagnostic Console is a non-graphical interface that provides local access to CC-SG. You can **access Diagnostic Console from a serial or KVM port** (see "Accessing Diagnostic Console via VGA/Keyboard/Mouse Port" on page 205), or from a **Secure Shell (SSH) client** (see "Accessing Diagnostic Console via SSH" on page 205), such as PuTTY or OpenSSH Client.

Diagnostic Console comprises two interfaces: **Status Console** (see "About Status Console" on page 206) and **Administrator Console** (see "About Administrator Console" on page 207).

Note: When you access Diagnostic Console via SSH, the Status Console and the Administrator Console inherit the appearance settings from your SSH client and keyboard bindings. These appearance settings may differ from this documentation.

In This Chapter

Accessing Diagnostic Console via VGA/Keyboard/Mouse Port

1. Attach a VGA monitor plus PS2 keyboard and mouse to the rear of the CC-SG unit.

2. Press RETURN to display a login prompt on the screen.

Accessing Diagnostic Console via SSH

1. Launch an SSH client, such as PuTTY, on a client PC that has network connectivity to the CC-SG.

2. Specify the IP address, or IP hostname (if CC-SG has been registered with a DNS server) of the CC-SG, and specify 23 for the port.

3. Click the button that allows you to connect. A window opens, prompting you for a login.

➢ **To accessing Status Console**

A password is not required to access the Status Console, but password usage can be enforced.

- At the login prompt, type **status**. The read-only Status Console appears.

```
+-----------------------------------------------------------------------+
|Mon Dec 11 EST          CommandCenter Secure Gateway          22:27:58|
|+ Message of the Day: ------------------------------------------------+|
||CommandCenter Secure Gateway                                        ||
||                                                                    ||
||Centralized access and control for your global IT infrastructure    ||
||                                                                    ||
||                                                                    ||
|+-------------------------------------------------------------------+|
|System Information:                                                    |
|   Host Name      : CommandCenter.localdomain                         |
|   CC-SG Version  : 3.1.0.5.1        Model         :  CC-SG-V1        |
|   CC-SG Serial # : ACC6500009       Host ID       :  00304856F118    |
|Server Information:                                                    |
|   CC-SG Status   : Up               DB Status      :  Responding     |
|   Web Status     : Responding/Unsecured                             |
|   Cluster Status : standalone        Cluster Peer  :  Not Configured |
|Network Information:                                                   |
| Dev  Link  Auto    Speed Duplex         IPAddr    RX Pkts   TX Pkts  |
| eth0  yes   on    100Mb/s  Full    192.168.0.192    55285        11  |
| eth1  no    on    Unknown! Unknown!                                  |
|                                                                      |
|                                                                      |
|                            Help: <F1>  Exit: <ctl+Q> or <ctl+C>|
+-----------------------------------------------------------------------+
```

This screen dynamically displays information about the health of the system and whether CC-SG and its sub-components are working.

The time in the upper-right corner of the screen is the last time at which the CC-SG data was polled.

Information on this screen updates approximately every 5 seconds.

- Type **CTRL-L** to clear the current screen and reload with updated information. You can update the screen a maximum of once per second.

- Pressing **CTRL-Q** or **CTRL-C** to exit the screen.

- The Status Console does not accept any other inputs or screen navigation. All other inputs are ignored.

The following table describes the statuses for CC-SG and the CC-SG database:

Status	Description
CC-SG Status: Up	CC-SG is available.
CC-SG Status: Down	CC-SG may be in the process of rebooting. If the Down status is continual, try restarting CC-SG.
CC-SG Status: Restarting	CC-SG is in the process of restarting.
DB Status: Responding	CC-SG's database is available.
DB Status: Down	CC-SG may be in the process of rebooting.

About Status Console

You can use the Status Console to ascertain the health of CC-SG, the various services CC-SG uses, and the attached network.

By default, Status Console does not require a password.

Accessing Status Console

➢ **To access Status Console:**

1. Type **status** at the **login** prompt.

2. The current system information appears.

About Administrator Console

The Administrator Console allows you to set some initial parameters, provide initial networking configuration, debug log files, and perform some limited diagnostics and restarting CC-SG.

The default login for the Administrator Console is:

- Username: **admin**
- Password: **raritan**

The Diagnostic Console **admin** account is separate and distinct from the CC Super User **admin** account and password used in the Java-based CC-SG Admin Client and the html-based Access Client. Changing one of these passwords does not affect the other.

Accessing Administrator Console

All information displayed in the Administrator Console is static. If the configuration changes through the CC-SG GUI or the Diagnostic Console, you must re-login to Administrator Console after the changes have taken effect to view them in Administrator Console

1. At the login prompt, type **admin**.

2. Type the CC-SG password. The default password is **raritan**. On first login, this password expires, and you must choose a new one. Type this password and when prompted, type a new password. Please refer to *Diagnostic Console Passwords (Admin)* **(see** "Diagnostic Console Password Settings" **on page 226)** for information on setting password strength.

The main Administrator Console screen appears.

```
 File  Operation

 CC-SG Administrator Console: Welcome:
Welcome to the Administration (Admin) section of the Diagnostic Console

The menus in this area will let you:
   - Do initial system set-up / installation.
   - Configure and control Diagnostic Services.
   - Preform emergency repairs.
   - Collected some diagnostic information.

There are more navigation aids in the Admin Console.
The top title bar offers you a series of menus and sub-menus.
Short-cut to this menu bar is <ctl+X> (or using your mouse).



Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Navigating Administrator Console

The following table provides the various navigation means within the Diagnostic Console menus. For some sessions, the mouse may also be used to navigate. However, the mouse may not work in all SSH clients or on the KVM console.

PRESS	To
CTRL+C or CTRL+Q	To exit Diagnostic Console.
CTRL+L	Clear screen and redraw the information (but the information itself is not updated nor refreshed).
TAB	Move to next available option.
SPACE	Select current option.
ENTER	Select current option.
ARROW	Move to different fields within an option.

Editing Diagnostic Console Configuration

The Diagnostic Console can be accessed via the serial port (COM1), VGA/Keyboard/Mouse (KVM) port, or from Secure Shell (SSH) clients. For each port type, you can configure whether or not **status** or **admin** logins are allowed, and whether field support can also access Diagnostic Console from the port. For SSH clients, you can also configure which port number should be used, as long as no other CC-SG service is using the desired port.

Important: Be careful not to completely lock out all Admin or Field Support access.

➢ *To edit Diagnostic Console configuration:*

1. Choose **Operation** > **Diagnostic Console Config**.

2. Determine how you want the Diagnostic Console configured and accessible.

   There are three Diagnostic Console Access mechanisms: Serial Port (COM1), KVM Console, SSH (IP network). The Diagnostic Console offers three services: Status Display, Admin Console, Raritan Field Support. This screen allows the selection of which services are available via the various access mechanisms.

3. Type the port number you want to set for SSH access to Diagnostic Console in the **Port** field. The default port is **23**.

```
  File   Operation

┌ CC-SG Administrator Console: Diagnostic Console Configuration: ─┐
 This screen lets you configure what Diagnostic Console Services
 (Status, Admin and Raritan Field Support) are available via what
 Access Methods or Ports (Serial Console, KVM port, SSH).
 [Note: Be careful not to lock out access to Admin Console.]


   ┌ Ports: ──┐┌ Status: ──┐┌ Admin: ──┐┌ Raritan Access: ─┐
    [X] Serial  [X] Status   [X] Admin    [X] Field Support
    [X] KVM     [X] Status   [X] Admin    [X] Field Support
    [X] SSH     [X] Status   [X] Admin    [ ] Field Support  Port: [23    ]




                                                        < Save >

 Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

4. Click **Save**.

Editing Network Interfaces Configuration (Network Interfaces)

In Network Interface Configuration, you can perform initial setup tasks, such as setting the hostname and IP address of the CC-SG.

1. Choose **Operation** > **Network Interfaces** > **Network Interface Config**.

2. If the network interfaces have already been configured, you will see a **Warning** message stating that you should use the CC-SG GUI (administrator's Director Client) to configure the interfaces. If you want to continue, click **YES**.

```
 File   Operation

 ┌ CC-SG Administrator Console: Network Interface Configuration: ───┐
 Hostname:        [CommandCenter.localdomain                      ]
 Domain Suffix:   [localdomain                                    ]
 Primary DNS:     [                    ]   Secondary DNS: [              ]

                  Mode:    <o> Primary/Backup
                           < > Active/Active

 Configuration:   < > DHCP           Configuration:      < > DHCP
                  <o> STATIC                             <o> STATIC

 IP Address:  [192.168.0.192    ]  IP Address:   [                ]
 Netmask:     [255.255.255.0    ]  Netmask:      [                ]
 Gateway:     [                 ]  Gateway:      [                ]
 Adapter Speed:    <o> AUTO              Adapter Speed:    <o> AUTO
 Adapter Duplex:   <o> FULL              Adapter Duplex:   <o> FULL

                                                     < Save >

 Help: <F1> //   Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

3. Type your hostname in the **Host Name** field. After you save, this field will be updated to reflect the Fully-Qualified Domain Name (FQDN), if known. For hostname rules, please refer to *Terminology/Acronyms* (on page 2).

4. In the **Mode** field, select either **Primary/Backup Mode** or **Active/Active Mode.** See *About Network Setup* **(on page 155)** for details.

   ▪ In the Configuration Field, select either DHCP or Static.

   ▪ If you choose DHCP and your DHCP server has been configured appropriately, the DNS information, the domain suffix, IP address, default gateway and subnet mask will be automatically populated once you save, and you exit and re-enter Admin Console.

- If you choose **Static**, type an **IP Address** (required), **Netmask** (required), **Default Gateway** (optional), **Primary DNS** (optional) and **Secondary DNS** (optional), and Domain Name in **Domain Suffix** (optional).

- Even if DHCP is being used to determine the IP configuration for an interface, a properly formatted **IP address** and **Netmask** must be provided.

5. In the **Adapter Speed** select a line speed. The other values of 10, 100, and 1000 Mbps are on a scrollable list (where only one value is visible at any given time) and the ██ keys are used to navigate to them. Press the SPACEBAR key to select the option displayed.

6. If you did not select **AUTO** for **Adapter Speed**, click **Adapter Duplex** and use the ██ keys to select a duplex mode (**FULL** or **HALF**) from the list, if applicable. While a duplex mode can be selected at any time, it only has meaning and takes effect when **Adapter Speed** is not **AUTO**.

7. Repeat these steps for the second network interface if you selected **Active/Active Mode.**

8. Select **Save**. CC-SG will restart, logging off all CC-SG GUI users and terminating their sessions. A **Warning** screen will be presented informing of the impending network reconfiguration and associated CC-SG GUI user impact. Select <**YES**> to proceed.

   System progress can be monitored in a Diagnostic Console Status Screen. On the KVM port, another terminal session can be selected by typing <**ALT**>+<**F2**> and logging in as **status.** You may return to the original terminal session by typing <**ALT**>+<**F1**>. There are six available terminal sessions on <**F1**> through <**F6**>.

Ping an IP Address (Network Interfaces)

Use ping to check that the connection between CC-SG computer and a particular IP address is working correctly.

Note: Some sites explicitly block ping requests. Verify that the target and intervening network allow pings if a ping is unsuccessful.

1. Choose Operation > Network Interfaces > Ping.

2. Enter the IP address or hostname (if DNS is appropriately configured on the CC-SG) of the target you want to check in the Ping Target field.

3. (Optional) Select:

Option	Description
Show other received ICMP packets	Verbose output, which lists other received ICMP packets in addition to ECHO_RESPONSE packets. Rarely seen.
No DNS Resolution	Does not resolve addresses to host names.
Record Route	Records route. Sets the IP record route option, which will store the route of the packet inside the IP header.
Use Broadcast Address	Allows pinging a broadcast message.
Adaptive Timing	Adaptive ping. Interpacket interval adapts to round-trip time, so that effectively not more than one unanswered probes present in the network. Minimal interval is 200 msec.

4. (Optional) Type values for how many seconds the ping command will execute, how many ping requests are sent, and the size for the ping packets (default is 56, which translates into 64 ICMP data bytes when combined with 8 bytes of ICMP header data). If left blank, defaults will be used.

5. Click Ping. If the results show a series of replies, the connection is working. The time shows you how fast the connection is. If you see a "timed out" error instead of a reply, the connection between your computer and the domain is not working. Please refer to *Trace Route* (see "Editing Static Routes (Network Interfaces)" on page 214) for details.

6. Press CTRL+C to terminate the ping session.

Note: Press CTRL+Q to display a statistics summary for the session so far and continue to ping the destination.

Using Traceroute (Network Interfaces)

Traceroute is often used for network troubleshooting. By showing a list of routers traversed, it allows you to identify the path taken from your computer to reach a particular destination on the network. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes. This can help identify routing problems or firewalls that may be blocking access to a site.

➢ *To perform a traceroute on an IP address or hostname:*

1. Choose **Operation** > **Network Interfaces** > **Traceroute**.

2. Enter the IP address or hostname of the target you wish to check in the **Traceroute Target** field.

3. (Optional) Select:

Option	Description
Verbose	Verbose output, which lists received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs.
No DNS Resolution	Does not resolve addresses to host names.
Use ICMP (vs. normal UDP)	Use ICMP ECHO instead of UDP datagrams.

4. (Optional) Type values for how many hops the traceroute command will use in outgoing probe packets (default is 30), the UDP destination port to use in probes (default is 33434), and the size for the traceroute packets. If left blank, defaults will be used.

5. Click **Traceroute** in the bottom right-hand corner of the window.

6. Press **CTRL+C** or **CTRL+Q** to terminate the traceroute session. A **Return?** prompt appears; press **ENTER** to return to the Traceroute menu. The **Return?** prompt also appears when Traceroute terminates due to "destination reached" or "hop count exceeded" events occur.

Editing Static Routes (Network Interfaces)

In Static Routes, you can view the current IP routing table and modify, add, or delete routes. Careful use and placement of static routes may actually improve the performance of your network, allowing you to conserve bandwidth for important business applications and may be useful for Active/Active network settings where each interface is attached to a separate IP domain. Please refer to *About Network Setup* (on page 155) for details. Click with the mouse or use the **TAB**, arrow keys to navigate and press the **Enter** key to select a value.

➢ *To view or change static routes:*

1. Choose **Operation** > **Network Interfaces** > **Static Routes**.

2. The current IP routing table is displayed. You can add a host or network route, or delete a route. The **Refresh** button updates the routing information in the above table.

```
  File  Operation

┌ CC-SG Administrator Console: Static Routes: ─────────────────
│This screen allows you to manage your IP routing table.
│You can see the routes currently in effect, add routes,
│and delete routes.
│
│  ┌ Destination      Gateway          Netmask          Interface    Flags ┐
│  │192.168.51.0      *                255.255.255.0    eth0             U │
│  │<default>         192.168.51.126   0.0.0.0          eth0            UG │
│  │                                                                       │
│  │                                                                       │
│  │                                                                       │
│  │                                                                       │
│  │                                                                       │
│  └───────────────────────────────────────────────────────────────────────┘
│
│ < Add Host Route > < Add Network Route > < Delete Route > < Refresh >

 Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Viewing Log Files in Diagnostic Console (Admin)

You can view one or more log files simultaneously via LogViewer, which allows browsing through several files at once, to examine system activity.

The Logfile list is only updated when the associated list becomes active, as when a user enters the logfile list area, or when a new sorting option is selected. File names are either preceded by a timestamp indicating how recently the logfile has received new data or the file size of the logfile.

➢ *Timestamp and file size abbreviations:*

Timestamps:

- s = seconds
- m = minutes
- h = hours
- d = days

File sizes:

- B = Bytes
- K = Kilobytes (1,000 bytes)
- M = Megabytes (1,000,000 bytes)
- G = Gigabytes (1,000,000,000 bytes)

➢ *To view log files:*

1. Choose **Operation** > **Admin** > **System Logfile Viewer**.

2. The Logviewer screen is divided into 4 main areas.

   - List of Logfiles currently available on the system. If list is longer than the display window, the list can be scrolled using the arrow keys.

   - Logfile List sort criteria. Logfiles can be shown sort by their Full File Name, the most recently changed logfile or by the largest logfile size.

   - Viewer Display options.

   - Export / View selector.

3. Click with the mouse or use the arrow keys to navigate and press the **SPACEBAR** key to select a log file, marking it with an **X**. You can view more than one log file at a time.

```
 File  Operation

 CC-SG Administrator Console: System Logfile Viewer:
 ┌ Logfile(s) to View: ───────────────────────────┐
 │ [ ]  10h ./boot.log                             │   ┌ Sort Logfile list by: ┐
 │ [ ]   9m ./cron                                 │   │ <o> Full File Name     │
 │ [ ]   7m ./messages                             │   │ < > Recent Change      │
 │ [ ]  16h ./pgsql                                │   │ < > File Size          │
 │ [ ]  10h ./rpmpkgs                              │   └────────────────────────┘
 │ [ ]  38m ./secure                               │
 │ [ ]  16h sg/ShellCommandExecutor.log            │   Viewer Display Options:
 │ [ ]   2s sg/httpd/access_log                    │    <o> Individual Windows
 │ [ ]  10h sg/httpd/access_log.1                  │    < > Merged Windows
 │ [ ]  10h sg/httpd/error_log                     │    Initial Buffer:[5000    ]
 │ [ ]   1d sg/install/anaconda.log                │
 │ [ ]   1d sg/install/ccinstall.log               │    [X] Remember Selected Items
 │ [ ]   1d sg/install/dmi.log                     │    [X] Use Default Color Scheme
 │ [ ]   1d sg/install/install.log                 │    [X] Use Default Filters
 │ [ ]   1d sg/install/install.log.syslog          │
 └─────────────────────────────────────────────────┘          < Export > < View >

 Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

➢ *To sort the Logfiles to View list:*

The **Sort Logfile list by** options control the order in which logfiles are displayed in the **Logfile to View** list.

Option	Description
Individual Windows	Display the selected logs in separate sub-windows.
Merged Windows	Merge the selected logs into one display window.
Initial Buffer	Sets initial buffer or history size. **5000** is default. This system is configured to buffer all the new information that comes along.
Remember Selected Items	If this box is checked, the current logfile selections (if any) will be remembered. Otherwise, selection is reset each time a new Logfile list is generated. This is useful if you want to step thorough files.

Use Default Color Scheme	If this box is checked, some of the logfiles will be viewed with a standard color scheme. Note: multitail commands can be used to change the color scheme once the logfile(s) are being viewed.
Use Default Filters	If this box is checked, some of the logfiles will have automatic filters applied.
Export	This option packages up all the selected logfiles and makes them available via Web access so that they can be retrieved and forwarded to Raritan Technical Support. Access to the contents of this package is not available to customer. Exported logfiles will be available for up to 10 days, and then the system will automatically delete them.
View	View the selected log(s).

When **View** is selected with Individual Windows, the LogViewer displays:

- While viewing log files, press **Q, CTRL-Q** or **CTRL+C** to return to the previous screen.

- You can change colors in a log file to highlight what is important.
  Type **c** to change colors of a log file and select a log from the list.

```
Toggle colors: select window
00 sg/jboss/console.log
01 ./messages
02 sg/httpd/access_log
Press ^G to abort
```

- Type **i** for info to display system information.

Note: System load is static as of the start of this Admin Console session - use the TOP utility to dynamically monitor system resources.

➢ **To filter a log file with a regular expression:**

1. Type **e** to add or edit a regular expression and select a log from the list if you have chosen to view several.

```
Select window (reg.exp. editi
)00 sg/jboss/console.log
01 ./messages
02 sg/httpd/access_log
Press ^G to abort
```

2. Type **a** to add a regular expression. For example, to display information on the **WARN** messages in **sg/jboss/console.log** log file, enter **WARN** and select **match**.

> **Note**: This screen also shows the Default Filter Scheme for console.log, which removes most of the Java heap messages.

```
50064K->45311K(324096K), 0.4177820 secs]

      Edit reg.exp.
      sg/jboss/console.log
      add, edit, delete, quit, move Down, move Up, reset counter
      nv Unloading class |Full GC |\[GC                        601

00] s                                                              46:02
Dec 1                                                              HTTP
D:1


              I



01] .                                                              46:02

      Edit regular expression:
      WARN

      Usage of regexp? (match, v do not match
      Color, Bell, bell + colorize, execute)

02] s                                                              46:02
```

Restarting CC-SG with Diagnostic Console

You can restart CC-SG, which will log off all current CC-SG users and terminate their sessions to remote target servers.

Important: It is HIGHLY recommended to restart CC-SG in the Java-based Admin client, unless it is absolutely necessary to restart it from Diagnostic Console. Please refer to *Restart CC-SG* **(on page 145) for details. Restarting CC-SG in Diagnostic Console will NOT notify users that it is being restarted.**

➢ *To restart CC-SG with Diagnostic Console:*

1. Choose **Operation** > **Admin** > **CC-SG Restart**.

2. Either click **Restart CC-SG Application** or press **ENTER.** Confirm the restart in the next screen to proceed.

```
 File  Operation

 CC-SG Administrator Console: CC-SG Restart: ─────────────
CC-SG Restart.

This operation will restart the CC-SG Application.

This will log-off all currently active CC-SG GUI users of the system
and terminate any sessions to remote targets that they might have.

They will get no notification that this event will happen.

   [It is better to use the CC-SG GUI to do this -- it will provide a
    count-down timer and notification of session termination.]


< Restart CC-SG Application >  < Cancel >



Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Rebooting CC-SG with Diagnostic Console

This option will reboot the entire CC-SG, which simulates a power cycle. Users will not receive a notification. CC-SG, SSH, and Diagnostic Console users (including this session) will be logged off. Any connections to remote target servers will also be terminated.

➢ **To reboot CC-SG**

1. Choose **Operation** > **Admin** > **CC-SG System Reboot**.

2. Either click **REBOOT System** or press **ENTER** to reboot CC-SG. Confirm the reboot in the next screen to proceed.

```
 File  Operation

 CC-SG Administrator Console: CC-SG System Reboot: ─────────────
 CC-SG System Reboot.

 This operation will reboot the entire system (simulating a power cycle).

 This will log-off all currently active CC-SG GUI, CC-SG SSH and Diagnostic
 Console users (including this session) to this system and terminate any
 sessions to remote targets that they might have.  This could also impact
 cluster operations (if so configured).

 Users will get no notification that this event will happen.



 < REBOOT System >  < Cancel >



 Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Powering Off the CC-SG System from Diagnostic Console

This option will power off the CC-SG unit. Logged-in users will not receive a notification. CC-SG, SSH, and Diagnostic Console users (including this session) will be logged off. Any connections to remote target servers will also be terminated.

The only way to power the CC-SG unit back on is to press the power button on the front panel of the unit.

➢ **To power off the CC-SG:**

1. Choose **Operation** > **Admin** > **CC-SG System Power OFF**.

2. Either click **Power OFF the CC-SG** or press **ENTER** to remove AC power from the CC-SG. Confirm the power down operation in the next screen to proceed.

```
 File  Operation

┌ CC-SG Administrator Console: Power OFF: ─────────────────────────────
CC-SG Power OFF.

This operation will turn the AC Power OFF for this CC-SG Unit.

The only way to bring the unit back online is by pressing the
Front Panel Power Button.

All active sessions will be terminated and no notification will given.

The system may take a couple of minutes before it actually powers off.
Please be patient!


< Power OFF the CC-SG >  < Cancel >



Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Resetting CC Super User Password with Diagnostic Console

This option will reset the password for the CC Super User account to the factory default value.

Factory default password: **raritan**

Note: This is not the password for the Diagnostic Console admin user. Please refer to **Diagnostic Console Passwords (Admin)** *(see "Diagnostic Console Password Settings" on page 226) for details.*

➢ *To reset the CC-SG GUI admin password:*

1. Choose Operation > Admin > CC-SG ADMIN Password Reset.

2. Either click Reset CC-SG GUI Admin Password or press ENTER to change the admin password back to factory default. Confirm the password reset in the next screen to proceed.

```
  File  Operation

┌ CC-SG Administrator Console: CC-SG ADMIN Password Reset: ─────────────
CC-SG Administrator Password Reset.

This operation will reset the password for the ADMIN account of the
CC-SG GUI to the initial Factory Default value.

[Note: This is *NOT* the admin password for Diagnostic Console!
See: ADMIN->DiagCon Passwords->Account Configuration to
change the Diagnostic Console admin password.]




< Reset CC-SG GUI Admin Password > < Cancel >



Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Resetting CC-SG Factory Configuration (Admin)

This option will reset all or parts of the CC-SG system back to their factory default values. All active CC-SG users will be logged off without notification, and SNMP processing will stop. It is highly recommended that CC-SG be placed in **Maintenance Mode** prior to initiating this operation. If possible, reset CC-SG from within the administrator's Admin Client, rather than from the Diagnostic Console. The Admin Client Reset option can perform all functions listed here, except for resetting Network values.

1. Choose **Operation** > **Admin** > **Factory Reset**. The following screen with seven **Reset Options** appears.

```
 File  Operation

 CC-SG Administrator Console: Factory Reset:
Factory Reset.

This operation will restore the system to initial Factory Configuration.
This will log-off all currently active CC-SG GUI sessions to this system
and may terminate any sessions to remote targets that they might have.
This could also impact cluster operations (if so configured).
Users will get no notification that this event will happen.
                      Reset Options:
                [X] Full CC-SG Database Reset
                [X] Preserve CC-SG Personality during Reset
                [X] Network Reset
                [X] SNMP Reset
                [X] Firmware Reset
                [X] Install Firmware into CC-SG DB
                [X] Diagnostic Console Reset

< RESET System > < Cancel >


Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Option	Description
Full CC-SG Database Reset	Selecting this option completes removes the existing CC-SG Database and builds a new version from scratch loading it with all the Factory Default values.

Preserve CC-SG Personality during Reset	This option is only valid and effective if the previous option is also selected. As the CC-SG Database is rebuilt (in the previous option), the following values are migrated to the new version of the database (if they can be read and are available; otherwise default values will be used). An attempt to keep the following information is made. Default value in brackets.
	Secure Communication [unsecured] between PC Clients and CC-SG
	Strong Password Check [off] select if strong password enforcement is enabled.
	Direct vs. Proxy Connections [Direct] selects if PC clients use direct or proxy connections to Out-of-Band nodes
	Inactivity Timer [1800] the time before idle sessions log out
	Modem Setting [10.0.0.1/10.0.0.2/<none>] the setting for the modem Server IP Address, Client IP Address, and callback phone number.
Network Reset	This option sets the networking back to Factory Defaults:
	Host name = CommandCenter
	Domain name = localdomain
	Mode = Primary/Backup
	Configuration = Static
	IP Address = 192.168.0.192
	Netmask = 255.255.255.0
	Gateway = <none>
	Primary DNS = <none>
	Secondary DNS = <none>
	Adapter Speed = Auto

SNMP Reset	Resets SNMP configuration to Factory Defaults
	Port: 161
	Read-only Community: public
	Read-write Community: private
	System Contact, Name, Location: <empty>
	SNMP Trap Configuration
	SNMP Trap Destinations
Firmware Reset	Removes uploaded Firmware files and restores the default versions into filesystem repository. Does not change the CC-SG DB.
Install Firmware into CC-SG DB	Loads Firmware files found in the filesystem-based repository into the CC-SG DB.
Diagnostic Console Reset	Restores Diagnostic Console to Factory Configuration, Account Settings and Defaults

Diagnostic Console Password Settings

This option provides the ability to configure the strength of passwords (status and admin) and allows you to configure password attributes, such as, the setting maximum number of days that must lapse before you need to change the password, which should be done via the Account Configuration menu. The operation in these menus only applies to Diagnostic Console accounts (status and admin) and passwords - it has no effect on the regular CC-SG GUI accounts or passwords.

➢ *Password Configuration*

1. Choose **Operation** > **Admin** > **DiagCon Passwords** > **Password Configuration**.

2. In the Password History Depth field, type the number of passwords that will be remembered. The default setting is **5**.

```
 File  Operation

 CC-SG Administrator Console: Password Settings: ──────
Use this screen to update how all subsequent Diagnostic Console (only!)
password operations will work.  You can set the type of passwords (regular,
strong or random) that the system will let the user use on any subsequent
password change operation.  Also, the number of passwords henceforth that
the system will remember and not let the user duplicate or reuse.

Password Configuration:

  Password History Depth:[5   ]

  Password Type & Parameters:
   <o> Regular
   < > Random  Size:[20  ] Retries:[10  ]
   < > Strong  Retries:[3   ] DiffOK:[4  ] MinLEN:[9   ]
               Digits:  [-1 ] Upper: [-1 ] Lower: [-1 ] Other:[-1 ]

                                                         < Update >


Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

3. Select either **Regular**, **Random**, or **Strong** for the **admin** and **status** (if enabled) passwords.

Password setting	Description
Regular	These are standard. Passwords must be longer than 4 characters with few restrictions. This is the system default password configuration.
Random	Provides randomly generated passwords. Configure the maximum password size in bits (minimum is 14, maximum is 70, default is 20) and number of retries (default is 10), which is the number of times you will be asked if you want to accept the new password. You can either accept (by typing in the new password twice) or reject the random password. You cannot select your own password.

Strong	Enforce strong passwords.
	Retries is the number of times you are prompted before an error message is issued.
	DiffOK is how many characters can be the same in the new password relative to the old.
	MinLEN is the minimum length of characters required in the password. Specify how many Digits, Upper-case letters, Lower-case letters, and Other (special) characters are required in the password.
	Positive numbers indicate the maximum amount of "credit" of this character class can be accrued towards the "simplicity" count.
	Negative numbers implies that the password MUST have at least that many characters from this given class. Thus, numbers of -1 means that every password must have at least one digit in it.

Account Configuration

By default, the **status** account does not require a password, but you can configure it to require one. Other aspects of the **admin** password can be configured and the Field Support accounts can be enabled or disabled.

➢ *To configure accounts:*

1. Choose **Operation** > **Admin** > **DiagCon Passwords** > **Account Configuration**.

2. In the screen that appears, you can view the settings for each account, **Status**, **Admin**, **FS1** and **FS2**.

```
  File  Operation

┌ CC-SG Administrator Console: Account Settings: ──────────────────
│Account Configuration:
│Field: \ User: Status:        Admin:         FS1:          FS2:
│User Name:     status         admin          fs1           fs2
│Last Changed:  Dec 12, 2006   Dec 12, 2006   Dec 13, 2006  Dec 13, 2006
│Expire:        Never          Never          Never         Never
│
│Mode:          < > Disabled                  < > Disabled  <o> Disabled
│               < > Enabled                   <o> Enabled   < > Enabled
│               <o> NoPassword
│Min Days:      [0        ]    [0        ]
│Max Days:      [99999  ]      [99999  ]
│Warn:          [7        ]    [7        ]
│Max # Logins:  [-1        ]   [2        ]     [1        ]   [0        ]
│Update Param:   <UPDATE>       <UPDATE>        <UPDATE>      <UPDATE>
│New Password:  <New Password> <New Password>
│
│                                   < RESET to Factory Password Configuration >
│

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

This screen is split into three main areas:

- The top displays read-only information about the accounts on the system.

- The middle section displays the various parameters related and pertinent to each ID, along with a set of buttons, to allow the parameters to be updated or new passwords provided for the accounts.

- The final area restores the password configuration to Factory Defaults (or how the system was initially shipped).

3. If you want to require a password for the **Status** account, select **Enabled** underneath it.

4. For the **Admin** and **Status** accounts, you can configure:

Setting	Description
User \ User Name	(Read-only). This is the current user name or ID for this account.
Last Changed	(Read-only). This is the date of the last password change for this account.
Expire	(Read-only). Tells the day that this account must change its password.

Mode	A configurable option if the account is disabled (no login allowed), or enabled (authentication token required), or access is allowed and no password is required. (Do not lock out both the Admin and FS1 accounts at the same time, or you cannot use Diagnostic Console.)
Min Days	The minimum number of days after a password has been changed before it can be changed again. Default is **0**.
Max Days	The maximum number of days the password will stay in affect. Default is **99999**.
Warning	The number of days that warning messages are issued before the password expires.
Max # of Logins	The maximum number of concurrent logins the account will allow. Negative numbers indicate no restrictions (**-1** is the default for status login). **0** means no one can log in. A positive number defines the number of concurrent users who can be logged in (**2** is the default for admin login).
UPDATE	Saves any changes that have been made for this ID.
New Password	Enter a new password for the account.

Displaying Disk Status (Utilities)

This option displays status of CC-SG disks, such as size of disks, if they are active and up, state of the RAID-1, and amount of space currently used by various file systems.

➢ **To display disk status of the CC-SG:**

1. Choose **Operation** > **Utilities** > **Disk Status**.

2. Either click **Refresh** or press **Enter** to refresh the display. Refreshing the display is especially useful when upgrading or installing, and you want to see the progress of the RAID disks as they are being rebuilt and synchronized.

```
 File  Operation

┌ CC-SG Administrator Console: Disk Status: ─────────────────────────
│ Personalities : [raid1]
│ md1 : active raid1 sdb2[1] sda2[0]
│       78043648 blocks [2/2] [UU]
│
│ md0 : active raid1 sdb1[1] sda1[0]
│       104320 blocks [2/2] [UU]
│
│ Filesystem           Size  Used Avail Use% Mounted on
│ /dev/mapper/svg-root  4.9G  115M  4.5G   3% /
│ /dev/md0              99M  9.0M   85M  10% /boot
│ /dev/mapper/svg-opt   5.8G  334M  5.2G   6% /opt
│ /dev/mapper/svg-sg    2.9G  195M  2.6G   7% /sg
│ /dev/mapper/svg-DB    8.7G  286M  8.0G   4% /sg/DB
│ /dev/mapper/svg-tmp   2.0G  339M  1.6G  18% /tmp
│ /dev/mapper/svg-usr   2.0G  580M  1.3G  31% /usr
│ /dev/mapper/svg-var   7.7G  133M  7.2G   2% /var
│                                            < Refresh >
│
├────────────────────────────────────────────────────────────────────
│ Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

*Note: The disk drives are fully synchronized and full RAID-1 protection is available when you see a screen as shown above. The status of both **md0** and **md1** arrays are [**UU**]).*

Viewing Top Display with Diagnostic Console

Top Display allows you to view the list of processes and their attributes that are currently running on CC-SG, as well as overall system health.

➢ **To display the processes running on CC-SG:**

1. Choose **Operation** > **Utilities** > **Top Display**.

2. View the total running, sleeping, total number, and processes that have stopped.

```
top - 20:19:27 up 1 day, 23:33,  6 users,  load average: 0.55, 0.27, 0.20
Tasks: 117 total,   1 running, 116 sleeping,   0 stopped,   0 zombie
Cpu(s):  5.6% us,  8.6% sy,  0.0% ni, 85.7% id,  0.0% wa,  0.0% hi,  0.0% si
Mem:   2076088k total,  1351804k used,   724284k free,   245720k buffers
Swap:  2031608k total,        0k used,  2031608k free,   795588k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
20271 sg        16   0  275m  26m  11m S  1.7  1.3   0:14.09 jsvc
 4990 root      23   0  5452 3460 1780 S  0.3  0.2   4:30.55 status-poller.p
12634 admin     16   0  2584  960  748 R  0.3  0.0   0:00.01 top
    1 root      16   0  2280  544  468 S  0.0  0.0   0:00.79 init
    2 root      34  19     0    0    0 S  0.0  0.0   0:00.24 ksoftirqd/0
    3 root       5 -10     0    0    0 S  0.0  0.0   0:00.68 events/0
    4 root       5 -10     0    0    0 S  0.0  0.0   0:00.00 khelper
    5 root      15 -10     0    0    0 S  0.0  0.0   0:00.00 kacpid
   25 root       5 -10     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
   35 root      15   0     0    0    0 S  0.0  0.0   0:00.12 pdflush
   36 root      15   0     0    0    0 S  0.0  0.0   0:01.13 pdflush
   38 root      13 -10     0    0    0 S  0.0  0.0   0:00.00 aio/0
   26 root      15   0     0    0    0 S  0.0  0.0   0:00.00 khubd
   37 root      15   0     0    0    0 S  0.0  0.0   0:00.02 kswapd0
  111 root      25   0     0    0    0 S  0.0  0.0   0:00.00 kseriod
  181 root       5 -10     0    0    0 S  0.0  0.0   0:00.00 ata/0
  183 root      22   0     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_0
```

3. Type **h** to view a help screen for the top command. **F1** for help is not operational here.

Displaying NTP Status (Utilities)

You can display the status of the NTP time daemon if it is configured and running on CC-SG. The NTP Daemon can only be configured in the CC-SG administrator's GUI, the Director Client.

➢ **To display status of the NTP daemon on the CC-SG:**

1. Choose **Operation** > **Utilities** > **NTP Status Display**.

▪ NTP is not enabled or not configured properly:

```
  File   Operation

 ┌ CC-SG Administrator Console: NTP Status: ─────────────────────────────

 NTP Daemon does not appear to be running




























                                                              < Refresh >


 Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

▪ NTP is properly configured and running:

```
  File   Operation

 ┌ CC-SG Administrator Console: NTP Status: ─────────────────────────────
 NTP Daemon PID=17735
 synchronised to NTP server (81.0.239.181) at stratum 3
    time correct to within 143 ms
    polling server every 64 s


 -----------

 client    127.127.1.0
 client    81.0.239.181
 client    152.118.24.8
      remote            local       st poll reach  delay    offset     disp
 ==========================================================================
 =127.127.1.0      127.0.0.1       10   64  377 0.00000  0.000000 0.03061
 *81.0.239.181     192.168.51.40    2   64  377 0.13531 -0.026990 0.05887
 =152.118.24.8     192.168.51.40    3   64  377 0.39163 -0.039222 0.07307
                                                              < Refresh >


 Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Appendix A Specifications for G1, V1, and E1

In This Chapter

G1 Model

G1 General Specifications

Form Factor	1U
Dimensions (DxWxH)	22.1"x 17.32" x 1.75" 563 mm x 440 mm x 44 mm
Weight	24.07lb (10.92kg)
Power	Redundant, hot-swappable power supplies, auto-sensing 110/220 V - 2.0A
Mean Time Between Failure (MTBF)	38,269 hours
KVM Admin Port	(DB15 + PS2 Keyboard/Mouse)
Serial Admin Port	DB9
Console Port	N/A

G1 Hardware Specifications

Processor	Intel® Pentium® III 1 GHz
Memory	512 MB
Network Interfaces	(2) 10/100 Ethernet (RJ45)
Hard Disk & Controller	(2) 40-GB IDE @7200 rpm, RAID 1
CD/ROM Drive	CD/ROM 40x Read Only

G1 Environmental Requirements

Operating	
Humidity	20% - 85% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (est.)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A
Non-Operating	
Temperature	0 - 30° C; 32° - 104° F
Humidity	10% - 90% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (est.)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

V1 Model

V1 General Specifications

Form Factor	1U
Dimensions (DxWxH)	24.21"x 19.09" x 1.75" 615 mm x 485 mm x 44 mm
Weight	23.80lb (10.80kg)
Power	Single Supply (1 x 300 watt)
Operating Temperature	10° - 35° (50°- 95°)
Mean Time Between Failure (MTBF)	36,354 hours
KVM Admin Port	(DB15 + PS2 or USB Keyboard/Mouse)
Serial Admin Port	DB9
Console Port	(2) USB 2.0 Ports

V1 Hardware Specifications

Processor	AMD Opteron 146
Memory	2 GB
Network Interfaces	(2) 10/100/1000 Ethernet (RJ45)
Hard Disk & Controller	(2) 80-GB SATA @ 7200 rpm, RAID 1
CD/ROM Drive	DVD-ROM

V1 Environmental Requirements

Operating	
Humidity	8% - 90% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (Estimated)
Vibration	5-55-5 HZ, 0.38 mm, 1 minutes per cycle; 30 minutes for each axis(X,Y,Z)
Shock	N/A

Non-Operating	
Temperature	-40° - +60° (-40°-140°)
Humidity	5% - 95% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (Estimated)
Vibration	5-55-5 HZ, 0.38mm,1 minutes per cycle; 30 minutes for each axis (X,Y,Z)
Shock	N/A

E1 Model

E1 General Specifications

Form Factor	2U
Dimensions (DxWxH)	27.05"x 18.7" x 3.46"-687 mm x 475 mm x 88 mm
Weight	44.09 lbs-20 kg
Power	SP502-2S Hot-Swappable 500W 2U power supply
Operating Temperature	0-50° C
Mean Time Between Failure (MTBF)	53,564 hours
KVM Admin Port	PS/2 keyboard and mouse ports, 1 VGA port
Serial Admin Port	Fast UART 16550 serial port
Console Port	(2) USB 2.0 Ports

E1 Hardware Specifications

Processor	(2) AMD Opteron 250 2.4G 1MB processors
Memory	4 GB
Network Interfaces	Intel PRO/1000 PT Dual Port Server Adapter
Hard Disk & Controller	(2) WD740ADFD SATA 74GB 10K RPM 16MB cache
CD/ROM Drive	DVD-ROM

E1 Environmental Requirements

Operating	
Humidity	5-90%, non-condensing
Altitude	Sea level to 7,000 feet
Vibration	10 Hz to 500 Hz sweep at 0.5 g constant acceleration for one hour on each of the perpendicular axes X, Y, and Z

Shock	5 g for 11 ms with a ½ sine wave for each of the perpendicular axes X, Y, and Z
Non-Operating	
Temperature	-40°-70° C
Humidity	5-90%, non-condensing
Altitude	Sea level to 40,000 feet
Vibration	10 Hz to 300 Hz sweep at 2 g constant acceleration for one hour on each of the perpendicular axes X, Y, and Z
Shock	30 g for 11 ms with a ½ sine wave for each of the perpendicular axes X, Y, and Z

Appendix B CC-SG and Network Configuration

In This Chapter

About this Appendix

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.

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 dropped if all access to the CC-SG is via HTTPS addresses.

Ports 5000 and 51000 can be dropped 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 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

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 target communication is whether:

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

Communication Direction	Port Number	Protocol	Configurable?
Client to CC-SG via Proxy to Target	2400 (on CC-SG)	TCP	no
Client to Raritan Target (Direct Mode)	5000 (on device)	TCP	yes
Client to Dominion SX to (Direct Mode)	51000	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
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* (on page 167) 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.

Appendix C User Group Privileges

Menu > Sub-menu	Menu Item	Required Privilege	Description
Secure Gateway	**This menu is available for all users.**		
	My Profile	None*	
	Message of the Day	None*	
	Print	None*	
	Logout	None*	
	Exit	None*	
Users	**This menu and the User tree are available only for users with the User Management privilege.**		
> User Manager	> Add User	User Management	
	(Editing users)	User Management	Via User Profile
	> Delete User	User Management	
	> Delete User from Group	User Management	
	> Logout User(s)	User Management	
	> Bulk Copy	User Management	
> User Group Manager	> Add User Group	User Management	
	(Editing user groups)	User Management	Via User Group Profile
	> Delete User Group	User Management	
	> Assign Users to Group	User Management	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> Logout Users	User Management	
Devices	**This menu and the Devices tree is available only for users with any one of the following privileges:** Device, Port and Node Management Device Configuration and Upgrade Management		
	Discover Devices	Device, Port and Node Management	
> Device Manager	> Add Device	Device, Port and Node Management	
	(Editing devices)	Device, Port and Node Management	Via Device Profile
	> Delete Device	Device, Port and Node Management	
	> Bulk Copy	Device, Port and Node Management	
	> Upgrade Device	Device Configuration and Upgrade Management	
>> Configuration	>> Backup	Device Configuration and Upgrade Management	
	>> Restore	Device Configuration and Upgrade Management	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	>> Copy Configuration	Device Configuration and Upgrade Management	
	> Restart Device	Device, Port and Node Management or Device Configuration and Upgrade Management	
	> Ping Device	Device, Port and Node Management or Device Configuration and Upgrade Management	
	> Pause Management	Device, Port and Node Management or Device Configuration and Upgrade Management	
	> Device Power Manager	Device, Port and Node Management	
	> Launch Admin	Device, Port and Node Management or Device Configuration and Upgrade Management	
	> Launch User Station Admin		

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> Disconnect Users	Device, Port and Node Management or Device Configuration and Upgrade Management	
	> Topological View	Device, Port and Node Management	
> Change View	> Create Custom View	Device, Port and Node Management or Device Configuration and Upgrade Management	
	> Tree View	Device, Port and Node Management or Device Configuration and Upgrade Management	
> Port Manager	> Connect	Device, Port and Node Management	
	> Configure Ports	Device, Port and Node Management	
	> Bookmark Port	Device, Port and Node Management	
	> Disconnect Port	Device, Port and Node Management	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> Bulk Copy	Device, Port and Node Management	
	> Delete Ports	Device, Port and Node Management	
> Port Sorting Options	> By Port Name	Device, Port and Node Management or Device Configuration and Upgrade Management	
	> By Port Status	Device, Port and Node Management or Device Configuration and Upgrade Management	
Nodes	**This menu and the Nodes tree is available only for users with any one of the following privileges:** Device, Port and Node Management Node In-Band Access Node Out-of-Band Access Node Power Control		
	Add Node	Device, Port and Node Management	
	(Editing Nodes)	Device, Port and Node Management	Via the Node Profile
	Delete Node	Device, Port and Node Management	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	\<interfaceName\>	In-Band Access or Out-of-Band Access	
	Disconnect	In-Band Access or Out-of-Band Access	
	Power Control	Power Control	
	Group Power Control	Power Control	
> Node Sorting Options	> By Node Name	Any of the following: Device, Port and Node Management or In-Band Access or Out-of-Band Access or Power Control	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> By Node Status	Any of the following: Device, Port and Node Management or Node In-Band Access or Node Out-of-Band Access or Node Power Control	
> Chat	> Start Chat	Node In-Band Access or Node Out-of-Band Access or Node Power Control	
	> Show Chat Session	Node In-Band Access or Node Out-of-Band Access or Node Power Control	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> End Chat Session	Node In-Band Access or Node Out-of-Band Access or Node Power Control	
> Change View	> Create Custom View	Any of the following: Device, Port and Node Management or Node In-Band Access or Node Out-of-Band Access or Node Power Control	
	> Tree View	Any of the following: Device, Port and Node Management or Node In-Band Access or Node Out-of-Band Access or Node Power Control	

Menu > Sub-menu	Menu Item	Required Privilege	Description
Associations	**This menu is available only for users with the User Security Management privilege**		
	> Associations	User Security Management	Includes ability to add, modify and delete.
	> Device Group	User Security Management	Includes ability to add, modify and delete.
	> Node Group	User Security Management	Includes ability to add, modify and delete.
	> Policies	User Security Management	Includes ability to add, modify and delete.
Reports	**This menu is available for all users.**		
	Audit Trail	CC Setup and Control	
	Error Log	CC Setup and Control	
	Access Report	CC Setup and Control	
	Availability Report	Device, Port and Node Management or Device Configuration and Upgrade Management	
> Users	> Active Users	User Management	
	> Locked Out Users	CC Setup and Control	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> User Data	To view all user data: User Management To view your own user data: None	
	> Users in Groups	User Management	
	> Group Data	User Security Management	
> Devices	Asset Management	Device, Port and Node Management	
> Nodes	> Node Asset Report	Device, Port and Node Management	
	> Active Nodes	Device, Port and Node Management	
	> Node Creation	Device, Port and Node Management	
> Ports	> Query Port	Device, Port and Node Management	
	> Active Ports	Device, Port and Node Management	
> Active Directory	AD Users Group Report		
	Scheduled Reports	CC Setup and Control	
	CC-NOC Synchronization	CC Setup and Control	

Menu > Sub-menu	Menu Item	Required Privilege	Description
Access			
	CC-NOC Configuration	CC Setup and Control	
Administration	**This menu is available only for users with one of the following privilege(s):** CC Setup and Control Combination of Device, Port and Node Management, User Management, and User Security Management		
	Guided Setup	All of the following: Device, Port and Node Management, User Management, and User Security Management	
	Message of the Day Setup	CC Setup and Control	
	Applications	CC Setup and Control	
	Firmware	Device, Port and Node Management	
	Configuration	CC Setup and Control	
	Security	CC Setup and Control	
	Notifications	CC Setup and Control	
	Tasks	CC Setup and Control	
	Compatibility Matrix	Device Configuration and Upgrade Management	

Menu > Sub-menu	Menu Item	Required Privilege	Description
System Maintenance			
	Backup	CC Setup and Control	
	Restore	CC Setup and Control	
	Reset	CC Setup and Control	
	Restart	CC Setup and Control	
	Upgrade	CC Setup and Control	
	Shutdown	CC Setup and Control	
> Maintenance Mode	> Enter Maintenance Mode	CC Setup and Control	
	> Exit Maintenance Mode	CC Setup and Control	
View		None*	
Window		None*	
Help		None*	

*None means that no particular privilege is required. Any user who has access to CC-SG will be able to view and access these menus and commands.

Appendix D SNMP Traps

CC-SG provides the following SNMP traps:

SNMP Trap	Description
ccUnavailable	CC-SG application is unavailable
ccAvailable	CC-SG application is available
ccUserLogin	CC-SG user logged in
ccUserLogout	CC-SG user logged out
ccPortConnectionStarted	CC-SG session started
ccPortConnectionStopped	CC-SG session stopped
ccPortConnectionTerminated	CC-SG session terminated
ccImageUpgradeStarted	CC-SG image upgrade started
ccImageUpgradeResults	CC-SG image upgrade results
ccUserAdded	New user added to CC-SG
ccUserDeleted	User deleted from CC-SG
ccUserModified	CC-SG user has been modified
ccUserAuthenticationFailure	CC-SG user authentication failure
ccLanCardFailure	CC-SG detected a LAN Card Failure
ccHardDiskFailure	CC-SG detected a hard disk failure
ccLeafNodeUnavailable	CC-SG detected a connection failure to a leaf node
ccLeafNodeAvailable	CC-SG detected a leaf node that is reachable
ccIncompatibleDeviceFirmware	CC-SG detected a device with incompatible firmware
ccDeviceUpgrade	CC-SG has upgraded the firmware on a device
ccEnterMaintenanceMode	CC-SG entered Maintenance Mode
ccExitMaintenanceMode	CC-SG exited Maintenance Mode
ccUserLockedOut	CC-SG user has been locked out

≡≡ Raritan.
When you're ready to take control®

258

ccDeviceAddedAfterCCNOCNotification	CC-SG has added a device after receiving a notification from CC-NOC
ccScheduledTaskExecutionFailure	The reason why the execution of a scheduled task failed
ccDiagnosticConsoleLogin	User has logged into the CC-SG Diagnostic Console
ccDiagnosticConsoleLogout	User has logged out of the CC-SG Diagnostic Console
ccNOCAvailable	CC-SG has detected that CC-NOC is available
ccNOCUnavailable	CC-SG has detected that CC-NOC is unavailable
ccUserGroupAdded	A new user group has been added to CC-SG
ccUserGroupDeleted	CC-SG user group has been deleted
ccUserGroupModified	CC-SG user group has been modified
ccSuperuserNameChanged	CC-SG Superuser password has changed
ccSuperuserPasswordChanged	CC-SG Superuser password has changed
ccLoginBannerChanged	CC-SG login banner has changed
ccMOTDChanged	CC-SG Messsage of the Day (MOTD) has changed

Appendix E Troubleshooting

To launch CC-SG from your web browser, it requires a Java plug-in. If your machine has an incorrect version, CC-SG will guide you through the installation steps. If your machine does not have a Java plug-in, CC-SG cannot automatically launch. In this case, you must uninstall or disable your old Java version and provide serial port connectivity to CC-SG to ensure proper operation.

- If the CC-SG applet does not load, check your web browser settings.
  - In Internet Explorer: Ensure Java (Sun) is enabled.
  - Open Java Plug-in in Control Panel, and adjust the settings for your browser.
- If you have problems adding devices, ensure the devices have the correct firmware versions.
- If the network interface cable is disconnected between the device and CC-SG, wait for the configured heartbeat minutes, and then plug the network interface cable back in. During the configured heartbeat period, the device operates in standalone mode and can be accessed through RRC, MPC, or RC.
- If you receive an error message that states your client version is different from the server version and that behavior may be unpredictable, you should restart and empty the cache of your browser.

In This Chapter

Client Browser Requirements

For a complete list of supported browsers, please refer to the **Compatibility Matrix** on the Raritan Support web site.

Appendix F Two-Factor Authentication

CC-SG can be configured to point to a RSA RADIUS Server that supports two-factor authentication via an associated RSA Authentication Manager. CC-SG acts as a RADIUS client and sends user authentication requests to RSA RADIUS Server. The authentication request includes user id, a fixed password, and a dynamic token code.

In This Chapter

Supported Environments for Two-Factor Authentication

The following two-factor authentication components are known to work with CC-SG.

- RSA RADIUS Server 6.1 on Windows Server 2003

- RSA Authentication Manager 6.1 on Windows Server 2003

- RSA Secure ID SID700 hardware token.

  Earlier RSA product versions should also work with CC-SG, but they have not been verified.

Two-Factor Authentication Setup Requirements

The following tasks must be completed for two-factor authentication setup. Please consult the RSA documentation for details.

1. Import tokens.

2. Create a CC-SG user and assign a token to the user.

3. Generate a user password.

4. Create an agent host for the RADIUS server.

5. Create an agent host (type: Communication Server) for CC-SG.

6. Create a RADIUS CC-SG client.

Two-Factor Authentication Known Issues

The RSA RADIUS "New PIN" mode that requires a challenge password/PIN will not work. Instead, all users in this scheme must be assigned fixed passwords.

Appendix G FAQs

Question	Answer
General	
What is CC-SG?	CC-SG is a network management device for aggregating and integrating multiple servers and network equipment typically deployed in a datacenter and which are connected to a Raritan IP-enabled product.
Why would I need CC-SG?	As you deploy more and more datacenter servers and devices, their management becomes exponentially complex. CC-SG allows a systems administrator or manager to access and manage all servers, equipment, and users from a single device.
What is CommandCenter NOC?	CommandCenter NOC is a network monitoring device for auditing and monitoring the status of servers, equipment and Raritan devices that CC-SG provides access to.
Which Raritan products does CC-SG support?	Please refer to the CC-SG Compatibility Matrix on the Raritan Support web site.
How does CC-SG integrate with other Raritan Products?	CC-SG uses a unique and proprietary search and discovery technology that identifies and connects to selected Raritan devices with a known network address. Once CC-SG is connected and configured, the devices connected to CC-SG are transparent, and operation and administration is extremely simple.
Is PDA access possible?	Yes, as long as the PDA has a Java-enabled browser and supports 128-bit (or lower strength for some geographies) SSL encryption. Call Raritan Tech Support for further information. No testing has been done in this area.
Is the status of CC-SG limited by the status of the devices which it proxies?	No. Because CC-SG software resides on a dedicated server, even if a device being proxied by the CC-SG is turned off, you will still be able to access CC-SG.
Can I upgrade to newer versions of CC-SG software as they become available?	Yes. Contact your authorized Raritan sales representative or Raritan, Inc. directly.

Question	Answer
How many nodes and/or Dominion units and/or IP-Reach units can be connected to CC-SG?	There is no specified limit to the number of nodes and/or Dominion and/or IP-Reach units that can be connected, but the number is not limitless: the performance of the processor and the amount of memory on the hosting server will determine how many nodes can actually be connected.
Is there any way to optimize the performance of Microsoft Internet Explorer if it is my preferred web browser?	To improve the performance of Microsoft IE when accessing the console, disable the "JIT compiler for virtual machine enabled," "Java logging enabled," and "Java console enabled" options. On the main menu bar, select **Tools > Internet Options > Advanced**. Scroll down until you see the above items and make sure that they are **not** checked.
What do I do if I am unable to add a console/serial port to CC-SG?	Assuming the console/serial device is a Dominion, ensure that the following conditions are met: - The Dominion unit is active. - The Dominion unit has not reached the maximum number of configured user accounts.
Which version of Java will Raritan's CC-SG be supporting?	For server and client side minimum Java requirements, please refer to the Compatibility Matrix on http://www.raritan.com/support. Click Firmware Upgrades and then CommandCenter Secure Gateway.
An administrator added a new node to the CC-SG database and assigned it to me, how can I see it in my Nodes tree?	To update the tree and see the newly assigned node, click the **Refresh** shortcut button on the toolbar. Remember that refreshing CC-SG will close all of your current console sessions.

Question	Answer
How will the Windows desktop be supported in the future?	Accessing CC-SG from outside the firewall can be achieved by configuring the right ports on the firewall. The following ports are standard ports: 80: for HTTP access via web browser 443: for HTTPS access via web browser 8080: for CC-SG server operations 2400: for Proxy mode connections 5001: for IPR/DKSX/DKX/ P2-SC event notification If there is firewall between two cluster nodes, the following ports should be opened for cluster to be worked properly: 8732: for cluster nodes heartbeat 5432: for cluster nodes DB replication
What are some design guidelines for large-scale systems? Any constraints or assumptions?	Raritan provides two models for server scalability: the datacenter model and the network model. The datacenter model uses Paragon to scale to thousands of systems in a single datacenter. This is the most effective and cost-efficient way to scale a single location. It also supports the network model with IP-Reach and the IP User Station (UST-IP). The network model scales through use of the TCP/IP network and aggregates access through CC-SG, so users don't have to know IP addresses or the topology of access devices. It also provides the convenience of single sign-on.
Authentication	
How many user accounts can be created for CC-SG?	Check your licensing restrictions. There is no specified limit to the number of user accounts that can be created for CC-SG, but the number is not limitless. The size of the database, the performance of the processor, and the amount of memory on the hosting server will determine how many user accounts can actually be created.
Can I assign specific node access to a specific user?	Yes, if you have Administrator permissions. Administrators have the ability to assign specific nodes per user.

Question	Answer
If we had more than 1,000 users, how would this be managed? Do you support Active Directory?	CC-SG works with Microsoft Active Directory, Sun iPlanet or Novell eDirectory. If a user account already exists in an authentication server, then CC-SG supports remote authentication using **AD/TACACS+ /RADIUS/LDAP** authentication.
What options are available for authentication with directory services and security tools such as LDAP, AD, RADIUS, etc.	CC-SG permits local authentication as well remote authentication. Remote authentication servers supported include: AD, TACACS+, RADIUS, and LDAP.
Security	
Sometimes when I try to log on, I receive a message that states my "login is incorrect" even though I am sure I am entering the correct username and password. Why is this?	There is a session-specific ID that is sent out each time you begin to log on to CC-SG. This ID has a time-out feature, so if you do not log on to the unit before the time-out occurs, the session ID becomes invalid. Performing a **Shift-Reload** refreshes the page from CC-SG. Or, you may close the current browser, open a new browser, and log on again. This provides an additional security feature so that no one can recall information stored in the web cache to access the unit.
How is a password secure?	Passwords are encrypted using MD5 encryption, which is a one-way hash. This provides additional security to prevent unauthorized users from accessing the password list.
Sometimes I receive a "No longer logged in" message when I click any menu in CC-SG, after leaving my workstation idle for a period of time. Why?	CC-SG times each user session. If no activity happens for a pre-defined period of time, CC-SG logs the user out. The length of the time period is pre-set to 60 minutes, but it can be reconfigured. It is recommended that users **exit** CC-SG when they finish a session.
As Raritan has root access to server, this may potentially cause issue with government bodies. Can customers also have root access or can Raritan provide a method of auditability / accountability?	No party will have root access to server once the unit is shipped out of Raritan, Inc.

266

Question	Answer
Is SSL encryption internal as well as external (not just WAN, but LAN, too)?	Both. The session is encrypted regardless of source, LAN or WAN.
Does CC-SG support CRL List, that is, LDAP list of invalid certificates?	No.
Does CC-SG support Client Certificate Request?	No.
Accounting	
The event times in the Audit Trail report seem incorrect. Why?	Log event times are logged according to the time settings of the client computer. You can adjust the computer's time and date settings.
Can audit/logging abilities track down who switched on or off a power plug?	Direct power switch-off is not logged, but power control through CC-SG can be logged to audit logs.
Performance	
As a CC-SG Administrator, I added over 500 nodes and assigned all of them to me. Now it takes a long time to log on to CC-SG.	When you, as Administrator, have many nodes assigned to you, CC-SG downloads all information for all nodes during the logging process, which slows the process considerably. It is recommended that Administrator accounts used primarily to manage CC-SG configuration/settings do not have many nodes assigned to them.
What is the bandwidth usage per client?	Remote access to a serial console over TCP/IP is about the same level of network activity as a telnet session. However, it is limited to the RS232 bandwidth of the console port itself, plus SSL/TCP/IP overhead. The Raritan Remote Client (RRC) controls remote access to a KVM console. This application provides tunable bandwidth from LAN levels down to something suitable for a remote dial-up user.
Grouping	

Question	Answer
Is it possible to put a given server in more than one group?	Yes. Just as one user can belong to multiple groups, one device can belong to multiple groups. For example, a Sun in NYC could be part of Group Sun: "Ostype = Solaris" and Group New York: "location = NYC"
What impact to other usage that would be blocked through the active usage of the console port, for example, some UNIX variants not allowing admin over network interfaces?	A console is generally considered a secure and reliable access path of last resort. Some UNIX systems allow root login only on the console. For security reasons, other systems might prevent multiple logins, so that if the administrator is logged in on the console, other access is denied. Finally, from the console, the administrator can also disable the network interfaces when/if necessary to block all other access. Normal command activity on the console has no greater impact than the equivalent command run from any other interface. However, since it is not dependent upon the network, a system that is too overloaded to be able to respond to a network login may still support console login. So, another benefit of console access is the ability to troubleshoot and diagnose system and network problems.
How do you recommend handling the issue of CIMs being moved / swapped at the physical level with changes to the logical database?	Each CIM includes a serial number and target system name. Our systems assume that a CIM remains connected to its named target when its connection is moved between switches. This movement is automatically reflected in the system configuration and is propagated to CC-SG. If, instead, the CIM is moved to another server, an administrator must rename it.
Interoperability	
How does CC-SG integrate with Blade Chassis products?	CC-SG can support any device with a KVM or serial interface as a transparent pass-through.

Question	Answer
To what level is CC-SG able to integrate with 3rd party KVM tools, down to 3rd party KVM port level or simply box level?	3rd party KVM switch integration is typically done through keyboard macros when the 3rd party KVM vendors do not publicize the communications protocols for the 3rd party KVM switches. Depending on the capability of the 3rd party KVM switches, the tightness of integration will vary.
How would I mitigate the restriction of four simultaneous paths through any IP-Reach box, including the roadmap for the potential 8-path box?	Currently, the best possible implementation is to aggregate IP-Reach boxes with CC-SG. In the future, Raritan plans to increase simultaneous access paths per box. These plans have yet to complete development as other projects have taken priority, but we welcome comments about the market demand and use cases of an 8-path solution.
Authorization	
Can authorization be achieved via RADIUS/TACACS/LDAP?	LDAP and TACACS are used for remote authentication only, not authorization.
User Experience	
Regarding console management via network port or local serial port (for example, COM2): What happens to the logging, does CC-SG capture local management or is this lost?	Logging on to CC-SG through the CC-SG console itself is the same as gaining the root privilege of the operating system (Linux) upon with CC-SG is running. Syslog will record such event, but what the user types at the CC-SG console itself will be lost.

Appendix H Keyboard Shortcuts

The following keyboard shortcuts can be used in the Java-based Admin Client.

Operation	Keyboard Shortcut
Refresh	F5
Print panel	Ctrl + P
Help	F1
Insert row in Associations table	Ctrl + I

Appendix I Naming Conventions

This appendix includes information about the naming conventions used in CC-SG. Please comply with the maximum character lengths when naming all the parts of your CC-SG configuration.

CC-SG Limits	
Field in CC-SG:	**Number of Characters CC-SG Allows**
Device Name	32
Device Group	40
Port Name	32
User Name	20
User Group Name	64
Password (not strong password)	16
Password (strong password)	Configurable Minimum: 8 Maximum: 64 Default minimum: 8 Default maximum: 16
Category Name	64
Element Name	31
Node Name	66
Node Group Name	40
Policy Name	56

Raritan.
When you're ready to take control®

Index

➤ **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

➤ **Beijing**

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

➤ **Europe**

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

➤ **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

➤ **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

➤ **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

➤ **Shanghai**

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

➤ **Taiwan**

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

➤ **United Kingdom**

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