



CommandCenter Secure Gateway

Administrators Guide
Release 4.0

Copyright © 2008 Raritan, Inc.

CCA-0H-E

July 2008

255-80-5140-00

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

© Copyright 2008 Raritan, Inc., CommandCenter®, Dominion®, Paragon® and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. Java® is a registered trademark of Sun Microsystems, Inc. Internet Explorer® is a registered trademark of Microsoft Corporation. Netscape® and Netscape Navigator® are registered trademarks of Netscape Communication Corporation. All other trademarks or registered trademarks are the property of their respective holders.

FCC Information

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

VCCI Information (Japan)

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

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



Contents

What's New in the CC-SG Administrators Guide	xiv
---	------------

How-To: CC-SG Essentials	xv
---------------------------------	-----------

Configuring and Enforcing Strong Passwords	xv
Upgrading CC-SG to a New Firmware Version	xvi
Controlling Power to a Node Group and Monitoring the Power Control Operation	xviii
Node Group Power Control	xviii
Power Status Messages	xix
Upgrading Multiple Devices Within a Limited Time Period	xix
Assign a default custom view of nodes for all users	xxi

Chapter 1 Introduction	1
-------------------------------	----------

Prerequisites	1
Terminology/Acronyms	2
Client Browser Requirements	4

Chapter 2 Accessing CC-SG	5
----------------------------------	----------

Browser-Based Access via the CC-SG Admin Client	5
JRE Incompatibility	6
Thick Client Access	6
Install the Thick Client	6
Use the Thick Client	7
CC-SG Admin Client	8

Chapter 3 Getting Started	10
----------------------------------	-----------

Confirming IP Address	10
Setting CC-SG Server Time	10
Checking the Compatibility Matrix	11
Checking and Upgrading Application Versions	11

Chapter 4 Configuring CC-SG with Guided Setup	13
--	-----------

Before You Use Guided Setup	13
Associations in Guided Setup	14
Create Categories and Elements	14
Device Setup	14
Discover and Add Devices	15

Contents

Creating Groups.....	16
Add Device Groups and Node Groups.....	16
User Management	18
Add User Groups and Users	19

Chapter 5 Associations, Categories, and Elements 21

About Associations	21
Association Terminology	21
Associations - Defining Categories and Elements	22
How to Create Associations	23
Association Manager	23
Add a Category.....	23
Edit a Category.....	23
Delete a Category.....	24
Add an Element.....	24
Edit an Element	24
Delete an Element	25

Chapter 6 Devices, Device Groups, and Ports 26

Viewing Devices.....	27
The Devices Tab.....	27
Device and Port Icons	27
Port Sorting Options	28
Device Profile Screen	29
Topology View	30
Right Click Options in the Devices Tab	30
Searching for Devices.....	31
Wildcards for Search	31
Wildcard Examples.....	31
Discovering Devices	31
Adding a Device.....	33
Add a KVM or Serial Device	33
Add a PowerStrip Device.....	34
Add a Dominion PX Device	35
Editing a Device	36
Editing a PowerStrip Device or a Dominion PX Device.....	36
Adding Notes to a Device Profile	36
Adding Location and Contacts to a Device Profile	37
Deleting a Device.....	37
Configuring Ports	38
Configure a Serial Port	38
Configure a KVM Port.....	39
Nodes Created by Configuring Ports.....	39

Editing a Port	40
Deleting a Port	41
Bulk Copying for Device Categories and Elements	41
Upgrading a Device	41
Backing Up a Device Configuration	42
Restoring Device Configurations	43
Restore a Device Configuration (KX, KSX, KX101, SX, IP-Reach)	43
Restore All Configuration Data Except Network Settings to a KX2, KSX2, or KX2-101 Device	44
Restore Only Device Settings or User and User Group Data to a KX2, KSX2, or KX2-101 Device	44
Restore All Configuration Data to a KX2, KSX2, or KX2-101 Device	45
Save, Upload, and Delete Device Backup Files	45
Copying Device Configuration	46
Restarting a Device	46
Pinging the Device	47
Pausing CC-SG's Management of a Device	47
Resuming Management	47
Device Power Manager	48
Launching a Device's Administrative Page	48
Disconnecting Users	49
Special Access to Paragon II System Devices	49
Paragon II System Controller (P2-SC)	49
IP-Reach and UST-IP Administration	50
Device Group Manager	50
Add a Device Group	50
Edit a Device Group	53
Delete a Device Group	54

Chapter 7 Managed Powerstrips 55

Configuring Powerstrips that are Managed by Another Device in CC-SG	56
Configuring PowerStrips Connected to KX, KX2, KX2-101, KSX2, and P2SC	57
Add a PowerStrip Device Connected to a KX, KX2, KX2-101, KSX2, or P2SC Device ...	57
Move a KX, KX2, KX2-101, KSX2, or P2SC's PowerStrip to a Different Port	57
Delete a PowerStrip Connected to a KX, KX2, KX2-101, KSX2, or P2SC Device	58
Configuring PowerStrips Connected to SX 3.0 and KSX	58
Add a PowerStrip Connected to an SX 3.0 or KSX device	58
Delete a PowerStrip Connected to an SX 3.0 or KSX Device	59
Change a PowerStrip's Device or Port Association (SX 3.0, KSX)	59
Configuring Powerstrips Connected to SX 3.1	60
Add a Powerstrip Connected to an SX 3.1 Device	60
Move an SX 3.1's Powerstrip to a Different Port	61
Delete a PowerStrip Connected to an SX 3.1 Device	61
Configuring Outlets on a Powerstrip	61

Chapter 8 Nodes, Node Groups, and Interfaces 63

Nodes and Interfaces Overview	63
About Nodes	63

Node Names.....	64
About Interfaces.....	64
Viewing Nodes.....	64
Nodes Tab.....	64
Node Profile.....	65
Node and Interface Icons.....	67
Service Accounts.....	68
Service Accounts Overview.....	68
Add, Edit, and Delete Service Accounts.....	68
Change the Password for a Service Account.....	69
Assign Service Accounts to Interfaces.....	70
Adding, Editing, and Deleting Nodes.....	70
Add a Node.....	70
Nodes Created by Configuring Ports.....	71
Edit a Node.....	71
Delete a Node.....	72
Adding Location and Contacts to a Node Profile.....	72
Adding Notes to a Node Profile.....	73
Configuring the Virtual Infrastructure in CC-SG.....	73
Terminology for Virtual Infrastructure.....	73
Virtual Nodes Overview.....	74
Add a Control System with Virtual Hosts and Virtual Machines.....	74
Add a Virtual Host with Virtual Machines.....	76
Edit Control Systems, Virtual Hosts, and Virtual Machines.....	78
Delete Control Systems and Virtual Hosts.....	79
Delete a Virtual Machine Node.....	80
Delete a Virtual Infrastructure.....	80
Synchronizing the Virtual Infrastructure with CC-SG.....	80
Synchronize the Virtual Infrastructure Now.....	80
Enable or Disable Daily Synchronization of the Virtual Infrastructure.....	81
Reboot or Force Reboot a Virtual Host Node.....	81
Accessing the Virtual Topology View.....	82
Connecting to a Node.....	82
Pinging a Node.....	83
Adding, Editing, and Deleting Interfaces.....	83
Add an Interface.....	83
Edit an Interface.....	90
Delete an Interface.....	90
Bookmarking an Interface.....	91
Configuring Direct Port Access to a Node.....	92
Bulk Copy for Node Categories and Elements.....	92
Using Chat.....	92
Adding, Editing, and Deleting Node Groups.....	93
Node Groups Overview.....	93
Add a Node Group.....	94
Edit a Node Group.....	97
Delete a Node Group.....	97

Chapter 9 Users and User Groups 98

The Users Tab	99
Default User Groups	100
CC Super-User Group	100
System Administrators Group.....	100
CC Users Group	100
Adding, Editing, and Deleting User Groups.....	101
Add a User Group.....	101
Edit a User Group.....	102
Delete a User Group.....	103
Configuring Access Auditing for User Groups	103
Adding, Editing, and Deleting Users	104
Add a User	104
Edit a User	105
Delete a User.....	106
Assigning a User to a Group.....	106
Deleting a User From a Group.....	107
Your User Profile.....	107
Change your password.....	107
Change your default search preference	107
Change the CC-SG default font size	108
Change your email address.....	108
Change the CC-SG Super User's Username	108
Logging Users Out.....	108
Bulk Copying Users	109

Chapter 10 Policies for Access Control 110

Adding a Policy	111
Editing a Policy	112
Deleting a Policy	113
Support for Virtual Media	114
Assigning Policies To User Groups	114

Chapter 11 Custom Views for Devices and Nodes 115

Types of Custom Views	115
View by Category	115
Filter by Node Group	115
Filter by Device Group.....	115
Using Custom Views in the Admin Client	116
Custom Views for Nodes.....	116
Custom Views for Devices.....	118

Chapter 12 Remote Authentication 122

Authentication and Authorization (AA) Overview.....	122
Flow for Authentication.....	122
User Accounts.....	123
Distinguished Names for LDAP and AD.....	123
Specify a Distinguished Name for AD.....	123
Specify a Distinguished Name for LDAP.....	123
Specify a Username for AD.....	124
Specify a Base DN.....	124
Specifying Modules for Authentication and Authorization.....	124
Establishing Order of External AA Servers.....	124
AD and CC-SG Overview.....	125
Adding an AD Module to CC-SG.....	125
AD General Settings.....	126
AD Advanced Settings.....	127
AD Group Settings.....	128
AD Trust Settings.....	129
Editing an AD Module.....	130
Importing AD User Groups.....	130
Synchronizing AD with CC-SG.....	131
Synchronize All User Groups with AD.....	132
Synchronize All AD Modules.....	133
Enable or Disable Daily Synchronization of All AD Modules.....	133
Change the Daily AD Synchronization Time.....	134
About LDAP and CC-SG.....	134
Add an LDAP (Netscape) Module to CC-SG.....	134
LDAP General Settings.....	134
LDAP Advanced Settings.....	135
Sun One LDAP (iPlanet) Configuration Settings.....	136
OpenLDAP (eDirectory) Configuration Settings.....	136
About TACACS+ and CC-SG.....	137
Add a TACACS+ Module.....	137
TACACS+ General Settings.....	137
About RADIUS and CC-SG.....	138
Add a RADIUS Module.....	138
RADIUS General Settings.....	138
Two-Factor Authentication Using RADIUS.....	139

Chapter 13 Reports 140

Using Reports.....	140
Sort Report Data.....	140
Resize Report Column Width.....	140
View Report Details.....	140
Navigate Multiple Page Reports.....	141
Print a Report.....	141
Save a Report to a File.....	141
Purge a Report's Data From CC-SG.....	142

Hide or Show Report Filters	142
Audit Trail Report	142
Error Log Report	143
Access Report.....	144
Availability Report	145
Active Users Report	145
Locked Out Users Report	145
All Users Data Report	146
User Group Data Report	146
Device Asset Report	147
Device Group Data Report	147
Query Port Report.....	147
Node Asset Report.....	149
Active Nodes Report.....	150
Node Creation Report.....	150
Node Group Data Report	150
AD User Group Report	151
Scheduled Reports	151
Upgrade Device Firmware Report	152
CC-NOC Synchronization Report	152

Chapter 14 System Maintenance **153**

Maintenance Mode	153
Scheduled Tasks and Maintenance Mode	153
Entering Maintenance Mode.....	153
Exiting Maintenance Mode	154
Backing Up CC-SG	154
Saving and Deleting Backup Files	155
Save a Backup File.....	155
Delete a Backup File	156
Restoring CC-SG	156
Resetting CC-SG	157
Restarting CC-SG	159
Upgrading CC-SG.....	160
Clear the Browser's Cache	161
Clear the Java Cache	162
CC-SG Shutdown	162
Restarting CC-SG after Shutdown.....	162
Powering Down CC-SG	163
Ending CC-SG Session	163
Log Out of CC-SG	163
Exit CC-SG	163

Chapter 15 Advanced Administration **164**

Configuring a Message of the Day	164
Configuring Applications for Accessing Nodes.....	165
About Applications for Accessing Nodes.....	165
Checking and Upgrading Application Versions	165

Add an Application.....	166
Delete an Application.....	167
Configuring Default Applications.....	167
About Default Applications	167
View the Default Application Assignments	167
Set the Default Application for an Interface or Port Type.....	167
Managing Device Firmware	168
Upload Firmware	168
Delete Firmware	168
Configuring the CC-SG Network.....	168
About Network Setup.....	169
About CC-SG LAN Ports	169
What is Primary/Backup mode?	170
What is Active/Active mode?	172
Recommended DHCP Configurations for CC-SG.....	174
Configuring Logging Activity	174
Purge CC-SG's Internal Log.....	175
Configuring the CC-SG Server Time and Date	175
Connection Modes: Direct and Proxy	176
About Connection Modes	176
Configure Direct Mode for All Client Connections.....	176
Configure Proxy Mode for All Client Connections	177
Configure a Combination of Direct Mode and Proxy Mode.....	177
Device Settings.....	177
Configuring Custom JRE Settings	178
Configuring SNMP	179
MIB Files.....	180
Configuring CC-SG Clusters.....	181
What is a CC-SG Cluster?.....	181
Requirements for CC-SG Clusters	181
About CC-SG Clusters and CC-NOC	181
Create a Cluster.....	181
Remove Secondary CC-SG Node.....	183
Remove Primary CC-SG Node.....	183
Recover a Failed CC-SG Node	183
Advanced Cluster Settings	183
Security Manager.....	184
Remote Authentication	184
AES Encryption.....	184
Configure Browser Connection Protocol: HTTP or HTTPS/SSL.....	185
Set the Port Number for SSH Access to CC-SG.....	185
Login Settings.....	186
Configure the Inactivity Timer.....	189
Portal	189
Certificates.....	190
Access Control List.....	193
Notification Manager.....	195
Configure an External SMTP Server	195
Task Manager.....	196
Task Types	196
Schedule Sequential Tasks	196
Email Notifications for Tasks	196

Scheduled Reports	197
Find and View Tasks	197
Schedule a Task.....	197
Schedule a Device Firmware Upgrade.....	199
Change a Scheduled Task	201
Reschedule a Task.....	201
Schedule a Task that is Similar to Another Task.....	202
Delete a Task.....	202
CommandCenter NOC	202
Add a CC-NOC.....	202
Edit a CC-NOC.....	204
Launch CC-NOC.....	204
Delete a CC-NOC.....	205
SSH Access to CC-SG	205
Get Help for SSH Commands	206
SSH Commands and Parameters	207
Command Tips	209
Create an SSH Connection to a Serial-Enabled Device	210
Use SSH to Connect to a Node via a Serial Out-of-Band Interface.....	211
End SSH Connections.....	212
Serial Admin Port.....	213
About Terminal Emulation Programs.....	213
Finding Your CC-SG Serial Number.....	213
Web Services API.....	214

Chapter 16 Diagnostic Console 216

Accessing Diagnostic Console	216
Access Diagnostic Console via VGA/Keyboard/Mouse Port.....	216
Access Diagnostic Console via SSH.....	216
Status Console.....	218
About Status Console.....	218
Access Status Console.....	218
Administrator Console	218
About Administrator Console.....	218
Access Administrator Console.....	219
Navigate Administrator Console.....	219
Edit Diagnostic Console Configuration.....	219
Edit Network Interfaces Configuration (Network Interfaces)	220
Ping an IP Address.....	221
Use Traceroute	223
Edit Static Routes	224
View Log Files in Diagnostic Console	225
Restart CC-SG with Diagnostic Console.....	229
Reboot CC-SG with Diagnostic Console.....	229
Power Off CC-SG System from Diagnostic Console.....	230
Reset CC Super-User Password with Diagnostic Console	231
Reset CC-SG Factory Configuration (Admin)	232
Diagnostic Console Password Settings.....	234
Diagnostic Console Account Configuration	235

Configure Remote System Monitoring	237
Configure Historical Data Trending	238
Display Disk Status.....	238
View Top Display with Diagnostic Console	239
Display NTP Status	240

Appendix A Specifications for V1 and E1 242

V1 Model.....	242
V1 General Specifications	242
V1 Environmental Requirements.....	242
E1 Model.....	243
E1 General Specifications	243
E1 Environmental Requirements.....	243

Appendix B CC-SG and Network Configuration 245

Required Open Ports for CC-SG Networks: Executive Summary.....	245
CC-SG Communication Channels	246
CC-SG and Raritan Devices.....	246
CC-SG Clustering.....	247
Access to Infrastructure Services.....	248
PC Clients to CC-SG	248
PC Clients to Nodes	249
CC-SG and Client for IPMI, iLO/RILOE, DRAC, RSA	249
CC-SG and SNMP.....	250
CC-SG and CC-NOC.....	250
CC-SG Internal Ports.....	251
CC-SG Access via NAT-enabled Firewall	251
RDP Access to Nodes	251
VNC Access to Nodes	251
SSH Access to Nodes	252
Remote System Monitoring Port.....	252

Appendix C	User Group Privileges	253
<hr/>		
Appendix D	SNMP Traps	261
<hr/>		
Appendix E	Troubleshooting	263
<hr/>		
Appendix F	Two-Factor Authentication	264
<hr/>		
	Supported Environments for Two-Factor Authentication.....	264
	Two-Factor Authentication Setup Requirements.....	264
	Two-Factor Authentication Known Issues	264
Appendix G	FAQs	265
<hr/>		
	General FAQs.....	265
	Authentication FAQs.....	267
	Security FAQs.....	268
	Accounting FAQs.....	269
	Performance FAQs.....	269
	Grouping FAQs.....	270
	Interoperability FAQs.....	271
	Authorization FAQs.....	271
	User Experience FAQs.....	272
Appendix H	Keyboard Shortcuts	273
<hr/>		
Appendix I	Naming Conventions	274
<hr/>		
Index		275
<hr/>		

What's New in the CC-SG Administrators Guide

The following sections have changed or information has been added to the CommandCenter Secure Gateway User Guide based on enhancements and changes to the equipment and/or user documentation.

- **JRE Incompatibility** (on page 6)
- **Add a Dominion PX Device** (on page 35)
- **Editing a PowerStrip Device or a Dominion PX Device** (on page 36)
- **Adding Notes to a Device Profile** (on page 36)
- **Adding Location and Contacts to a Device Profile** (on page 37)
- **Configuring Powerstrips That Are Managed by Another Device in CC-SG** (on page 56)
- **Service Accounts** (on page 68)
- **Adding Location and Contacts to a Node Profile** (on page 72)
- **Adding Notes to a Node Profile** (on page 73)
- **Configuring the Virtual Infrastructure in CC-SG** (on page 73)
- **Synchronizing the Virtual Infrastructure with CC-SG** (on page 80)
- **Reboot or Force Reboot a Virtual Host Node** (on page 81)
- **Accessing the Virtual Topology View** (on page 82)
- **Interfaces for In-Band Connections** (on page 85)
- **Delete an Interface** (on page 90)
- **Configuring Access Auditing for User Groups** (on page 103)
- **Upgrading CC-SG** (on page 160)
- **Resetting CC-SG** (on page 157)
- **Device Settings** (on page 177)
- **Configuring Custom JRE Settings** (on page 178)
- **Configuring SNMP** (on page 179)
- **Configure Remote System Monitoring** (on page 237)
- **Configure Historical Data Trending** (on page 238)
- **CC-SG Communication Channels** (on page 246)

Please see the Release Notes for a more detailed explanation of the changes applied to this version of the CommandCenter Secure Gateway.

How-To: CC-SG Essentials

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

In This Chapter

Configuring and Enforcing Strong Passwords.....	xv
Upgrading CC-SG to a New Firmware Version.....	xvi
Controlling Power to a Node Group and Monitoring the Power Control Operation.....	xviii
Upgrading Multiple Devices Within a Limited Time Period	xix
Assign a default custom view of nodes for all users	xxi

Configuring and Enforcing Strong Passwords

1. Choose Administration > Security.
2. Click the Login Settings tab.
3. Select 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 five 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 lowercase letter.
 - Passwords must contain at least one uppercase 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.

See **Login Settings** (on page 186) for more details on login security.

Upgrading 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.

CC-SG version 4.0 is not compatible with G1 hardware. Do not upgrade a CC-SG G1 unit to version 4.0.

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

Only users with the CC Setup and Control privilege can upgrade CC-SG.

You should back up CC-SG before upgrading.

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

CC-SG will reboot as part of the upgrade process. 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. Log into the CC-SG Admin Client using an account that has the CC Setup and Control privilege.
3. Enter Maintenance Mode. See **Entering Maintenance Mode** (on page 153).
4. Once CC-SG is in maintenance mode, choose System Maintenance > Upgrade.
5. Click Browse. Navigate to and select the CC-SG firmware file (.zip) then click Open.
6. Click OK to upload the firmware file to CC-SG.

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

7. Click OK to exit CC-SG.

8. Clear the browser cache, then close the browser window. See **Clear the Browser's Cache** (on page 161).
 9. Clear the Java cache. See **Clear the Java Cache** (on page 162).
 10. You must wait for the upgrade to complete before logging into CC-SG again. You can monitor the upgrade in the Diagnostic Console.
 - a. Access Diagnostic Console using the admin account. See **Access Administrator Console** (on page 219).
 - b. Choose Admin > System Logfile Viewer. Select sg/upgrade.log then choose View to view the upgrade log.
 - c. Wait for the upgrade process to run. The upgrade process is complete when you see the "Upgrade completed" message in the upgrade log.
 - d. The server must reboot. The reboot process begins when you see the "Linux reboot" message in the upgrade.log. The server will shut down and reboot.
 11. Wait a few minutes while CC-SG reboots, then launch a new web browser window.
 12. Log into the CC-SG Admin Client using an account that has the CC Setup and Control privilege.
 13. 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.
 14. Exit Maintenance Mode. See **Exiting Maintenance Mode** (on page 154).
- Back up the CC-SG. See **Backing Up CC-SG** (on page 154).

Controlling Power to a Node Group and Monitoring 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 on which they are mounted or if you need to perform other types of maintenance on a node group.

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

1. Click the Nodes tab.
2. Choose Nodes > 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 on which you want to perform power control, 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. Arrange the interfaces in the Selected list in the order you would like CC-SG to perform the power operation. Select an interface in the Selected list and click the up and down arrows to move the interface into the desired sequence.
6. Click the Operation drop-down arrow, and select Power On, Power Off, Power Cycle, Graceful Shutdown, or Suspend from the list.
7. If you selected Power On, Power Off, Graceful Shutdown, or Suspend 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.
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 that you can monitor progress.

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

Power Status Messages

The Power Status Messages window opens 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:**

- When a power control operation fails, an alert message containing information about the failed operation appears.
- The status bar at the bottom of your browser window displays an alert message when the entire operation completes successfully.
- Alert messages appear only for failed operations. Alert messages do not appear for successful operations.

Upgrading 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.

See 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. Click 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 to which you want to upgrade. Only available upgrade files that are appropriate for the device type selected will appear 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. Specify whether failed upgrades should be retried.
 - a. Click the Retry tab.
 - b. Retry Count: Type the number of times CC-SG should retry a failed upgrade.
 - c. 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. 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 the Notification tab.
 - b. Click Add, type the email address in the window that opens, and then click OK.
 - c. Select On Failure if you want an email sent if an upgrade fails.
 - d. 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. See **Upgrade Device Firmware Report** (on page 152).

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.

► **To assign a default custom view of nodes 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. Select the System Wide checkbox, and then click Save.

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

See **Custom Views** (see "Custom Views for Devices and Nodes" on page 115) 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 see Raritan's **CommandCenter Secure Gateway User Guide**.

In This Chapter

Prerequisites.....	1
Terminology/Acronyms.....	2
Client Browser Requirements.....	4

Prerequisites

Before configuring a CC-SG according to the procedures in this document, see Raritan's **CommandCenter Secure Gateway 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 - 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 - Java-based client for CC-SG useable by both normal access users and administrators. It is the only client that permits administration.

Associations - relationships 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 before adding devices and ports in CC-SG.

Category - 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) - 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 must be rebooted after connecting to a CIM.

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

Device Group - 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 - Raritan products such as Dominion KX, Dominion KX II, Dominion SX, Dominion KSX, IP-Reach, Paragon II System Controller, and 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. Check the CC-SG Compatibility Matrix on the Raritan Support web site for a list of supported devices.

Elements - values of a category. For example, the "New York City" element belongs to the "Location" category, and 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). See **Raritan's Paragon II User Guide**.

Hostname - can be used if DNS server support is enabled. See **About Network Setup** (on page 169).

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 a user group's access within the CC-SG network. 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 - target systems, such as servers, desktop PCs, and other networked equipment, that CC-SG users can access.

Interfaces - the different ways a Node can be accessed, whether through an out-of-band solution such as a Dominion KX2 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 - connection points between a Raritan device and a node. Ports exist only on Raritan devices, and they identify a pathway from that device to a node.

SASL (Simple Authentication and Security Layer) - 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.

Client Browser Requirements

For a complete list of supported browsers, see the Compatibility Matrix on the Raritan Support web site.

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, see 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.
- Diagnostic Console: Provides emergency repair and diagnostics only and is not a replacement for the browser-based GUI to configure and operate CC-SG. See **Diagnostic Console** (on page 216).

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

In This Chapter

Browser-Based Access via the CC-SG Admin Client	5
Thick Client Access	6
CC-SG Admin Client.....	8

Browser-Based Access via the CC-SG Admin Client

The CC-SG Admin client is a Java-based client that provides a GUI for both administrative and access tasks, depending on your permissions.

1. Using a supported Internet browser, type the URL of the CC-SG and then type /admin: `https://IP address/admin`, for example, **`https://10.0.3.30/admin`** (`https://10.0.3.30/admin`).

*If you see the JRE Incompatibility Warning window, select the JRE version that is appropriate for your client computer and install it. Once JRE is installed, try this procedure again. See **JRE Incompatibility** (on page 6).*

Or, you can continue without installing a new JRE version.

2. If you see a Restricted Service Agreement, read the agreement text and select the I Understand and Accept the Restricted Service Agreement checkbox.
3. Type your Username and Password and click Log In.
4. Upon valid login, the CC-SG Admin Client opens.

JRE Incompatibility

If you do not have the minimum required version of JRE installed on your client computer, you will see a warning message before you can access the CC-SG Admin Client. The JRE Incompatibility Warning window opens when CC-SG cannot find the required JRE file on your client computer.

If you see the JRE Incompatibility Warning window, select the JRE version that is appropriate for your client computer and install it, or you can continue without installing a new JRE version.

You must launch CC-SG again once JRE is installed.

Administrators can configure the JRE minimum version that is recommended and the message that appears in the JRE Incompatibility Warning window. See **Configuring Custom JRE Settings** (on page 178).

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 opens. 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 opens.
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 select the Secure Socket Layer (SSL) checkbox. If the CC-SG is not configured for secure browser connections, you must deselect 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 select the Secure Socket Layer SSL checkbox in the thick client's IP address specification window. If the HTTP option is selected, deselect 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 two ways to access it on your client computer, based on 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.

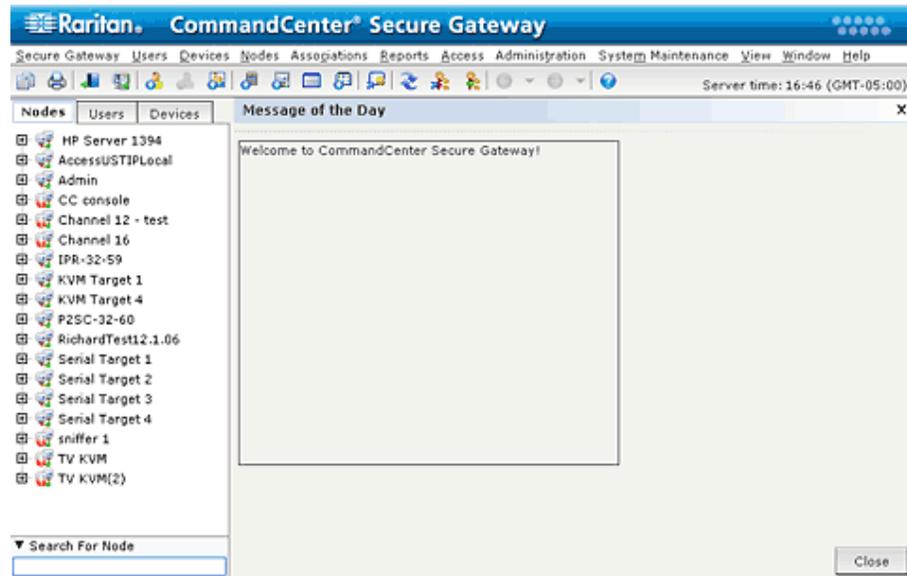
► Java 1.5

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 (alphabetically) 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 shortcut buttons for executing common commands.
- **Operation and Configuration menu bar:** These menus contain commands to operate and configure CC-SG. You can 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 based on 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. See **Task Manager** (on page 196). 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, proceed to Guided Setup. See **Configuring CC-SG with Guided Setup** (on page 13).

In This Chapter

Confirming IP Address.....	10
Setting CC-SG Server Time	10
Checking the Compatibility Matrix	11
Checking and Upgrading Application Versions	11

Confirming IP Address

1. Choose Administration > Configuration.
2. Click the Network Setup tab.
3. Check that the network settings are correct, and make changes if needed. See **About Network Setup** (on page 169). **Optional.**
4. Click Update Configuration to submit your changes.
5. Click Restart Now to confirm your settings and restart CC-SG.

Setting 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. See *Task Manager* (on page 196). 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.
- a. To set the date and time via NTP: Select 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 to 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.

Checking 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 support only the current and previous firmware versions for Raritan devices at the time of release. You can view the compatibility matrix on the Raritan Support web site.

- ▶ **To check the Compatibility Matrix:**
 - Choose Administration > Compatibility Matrix.

Checking and Upgrading Application Versions

Check and upgrade the CC-SG applications, including 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, see the Compatibility Matrix on the Raritan Support website.

The best practice is to enter Maintenance Mode before upgrading applications. See **Entering Maintenance Mode** (on page 153).

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. See **Add an Application** (on page 166).
3. Click Browse, locate and select the application upgrade file from the dialog that appears 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.

Note: Users who were logged in during the upgrade must log out of CC-SG then log in again to ensure that the new version of the application is launched.

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 four tasks:

- Associations - Define the categories and elements that you use to organize your equipment. See **Associations in Guided Setup** (on page 14).
- Device Setup - Discover devices in your network and add them to CC-SG. Configure device ports. See **Device Setup** (on page 14).
- Create Groups - Categorize the devices and nodes that CC-SG manages into groups and create full access policies for each group. See **Creating Groups** (on page 16).
- User Management - 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. See **User Management** (on page 18).

See **Naming Conventions** (on page 274) for details on CC-SG's rules for name lengths.

In This Chapter

Before You Use Guided Setup	13
Associations in Guided Setup	14
Device Setup	14
Creating Groups	16
User Management	18

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

► **To create categories and elements in Guided Setup:**

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 into which you want to organize your equipment, such as “Location.”
 3. In the Applicable for field, indicate whether you want the category to be available for devices, nodes, or both. Click the Applicable for drop-down menu and 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.
 - To delete an element, select its row, and then click the Delete Row icon .
 5. Repeat these steps until you have added all the elements within the category to the Elements table.
 6. To create another category, click Apply to save this category, and then repeat the steps in this section to add additional categories.
- Optional**
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 on to 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.

► To discover and add devices in Guided Setup:

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 Ctrl key while you click device types to select multiple device types.
4. Select the Broadcast discovery checkbox if searching for devices on the same subnet on which CC-SG resides. Deselect the Broadcast discovery checkbox to discover devices across all subnets.
5. Click Discover.
6. When the discovery is complete, a confirmation message appears. Click OK.
7. If CC-SG has discovered devices of the specified type and in the specified address range, the devices appear in a table in the bottom section of the Discover Devices panel. 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, select the Allow Direct Device Access checkbox if you want to allow local access to the device. Deselect 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, 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, select 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, select the Apply to Nodes checkbox.
20. If you want to add another device, click Apply to save this device, and repeat these steps. **Optional.**
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.

Creating 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

► **To add device groups and node groups in Guided Setup:**

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. Select 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. To add another device group, click Apply to save this group and repeat these steps. **Optional.**
 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. To remove a node from the group, select the node name in the Selected list and 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. See **Policies for Access Control** (on page 110).
 - d. Deselect 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. To add another node group, click Apply to save this group and repeat these steps. **Optional.**
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.

► To add user groups and users in Guided Setup:

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 select 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. Select 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 and 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. 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. Select the checkbox that corresponds with each Active Directory module you want to associate with the user group.
9. To add another user group, click Apply to save this group and repeat these steps. **Optional.**
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. Select the Login Enabled checkbox if you want the user to be able to log in to CC-SG.

13. Select 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. Select 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. 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.
- Optional.**

Chapter 5 Associations, Categories, and Elements

In This Chapter

About Associations	21
Association Manager	23

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 - the relationships between categories, elements of a category, and nodes and devices.
- Category - 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 - 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 will 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. See **Configuring CC-SG with Guided Setup** (on page 13).
- Association Manager allows you to work only with associations, and does not automate any configuration tasks. You can use Association Manager to edit your Associations after using Guided Setup, too. See **Association Manager** (on page 23).

Association Manager

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

Add a Category

▶ **To add a category:**

1. Choose Associations > Association.
2. Click Add. The Add Category window opens.
3. Type a category name in the Category Name field. See **Naming Conventions** (on page 274) 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

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

▶ **To edit a category:**

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 opens.
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.

► **To delete a category:**

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 opens.
4. Click Yes to delete the category.

Add an Element

► **To 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. See **Naming Conventions** (on page 274) 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

► **To edit an element:**

1. Choose Associations > 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 opens.
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.

► **To delete an element:**

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, Device Groups, and Ports

To add Raritan PowerStrip Devices that are connected to other Raritan devices to CC-SG, see **Managed PowerStrips** (on page 55).

*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. See **Nodes, Node Groups, and Interfaces** (on page 63).*

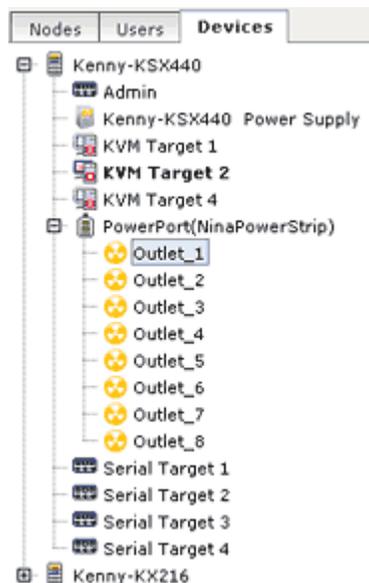
In This Chapter

Viewing Devices	27
Searching for Devices	31
Discovering Devices	31
Adding a Device	33
Editing a Device.....	36
Editing a PowerStrip Device or a Dominion PX Device	36
Adding Notes to a Device Profile.....	36
Adding Location and Contacts to a Device Profile	37
Deleting a Device	37
Configuring Ports.....	38
Editing a Port	40
Deleting a Port.....	41
Bulk Copying for Device Categories and Elements	41
Upgrading a Device	41
Backing Up a Device Configuration.....	42
Restoring Device Configurations.....	43
Copying Device Configuration	46
Restarting a Device	46
Pinging the Device.....	47
Pausing CC-SG's Management of a Device	47
Resuming Management	47
Device Power Manager	48
Launching a Device's Administrative Page	48
Disconnecting Users.....	49
Special Access to Paragon II System Devices.....	49
Device Group Manager	50

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 + or - to expand or collapse the list of ports.

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

Icon	Meaning
	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.

► **To sort the ports in the Devices tab:**

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.

Device Profile Screen

When you select a device in the Devices tab, the Device Profile screen appears, displaying information about the selected device.

When a device is down, the information in the Device Profile screen is read-only. You can delete a device that is down. See **Deleting a Device** (on page 37).

The screenshot shows the 'Device Profile' configuration window. At the top, there is an information icon and the text 'Please provide device properties to change.' Below this, the 'Device Name' is 'KX2-432-53-191'. The 'Device IP or Hostname' is '192.168.53.191', 'Subnet Mask' is '255.255.255.0', and 'Heartbeat (seconds)' is '600'. The 'TCP Port' is '5000', 'Default Gateway' is '192.168.53.126', 'Encryption' is 'Unknown', and 'Firmware Version' is '2.0.20.5.6903'. The 'Description' field contains 'Dominion KX2 model DKX2-432 ver. 2.0.20.1.6740'. Below the description are tabs for 'Associations', 'Location & Contacts', and 'Notes'. The 'Associations' tab is active, showing a table with columns 'Category', 'Element', and 'Apply To Nodes'. The table contains one row: 'US States and territories', 'CALIFORNIA', and a checked box. At the bottom right are 'OK' and 'Cancel' buttons.

Category	Element	Apply To Nodes
US States and territories	CALIFORNIA	<input checked="" type="checkbox"/>

The Device Profile includes tabs that contain information about the device.

▶ **Associations tab**

The Associations tab contains all categories and elements assigned to the node. You can change the associations by making different selections. See **Associations, Categories, and Elements** (on page 21).

▶ **Location & Contacts tab**

The Location & Contacts tab contains information about a device's location and contact information, such as phone numbers, that you may need when working on a device. You can change the information in the fields by typing in new information. See **Adding Location and Contacts to a Device Profile** (on page 37).

▶ **Notes tab**

The Notes tab contains a tool that enables users to leave notes about a device for other users to read. All notes display in the tab with the date, username, and IP address of the user who added the note.

If you have the Device, Port, and Node Management privilege, you can clear all notes from the node profile by clicking Clear.

See **Adding Notes to a Device Profile** (on page 36).

Topology View

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

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

▶ **To open the topology view:**

1. Click the Devices tab and select the device whose topological view you want to see.
2. Choose Devices > Device Manager > Topology View. The Topology View for the selected device appears.
 - Click + or - to expand or collapse the view.

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.

Searching 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 107).

► **To search for a device:**

- At the bottom of the Devices Tab, type a search string in Search For Device field, then press the Enter key.
- Wildcards are supported in the search string. See ***Wildcards for Search*** (on page 31).

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.

Discovering Devices

Discover Devices initiates a search for all 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. Clear 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. Select the Include IPMI Agents checkbox 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 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. The Add Device page is different for different device types. See the instructions on adding each device type CC-SG discovered.
 - For KVM or Serial devices, see **Add a KVM or Serial Device** (on page 33).
 - For Powerstrips, see **Add a PowerStrip Device** (on page 34).
 - For Dominion PX powerstrips on the IP network, see **Add a Dominion PX Device** (on page 35).
9. Click Apply to add a discovered device and continue to the next discovered device. Click OK to add the current discovered device and stop the process of adding the discovered devices.

Adding 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. The Add Device screen is used to add devices whose properties you know and can provide to CC-SG. To search for devices to add, use the Discover Devices option. See **Discovering Devices** (on page 31).

To add Raritan PowerStrip Devices that are connected to other Raritan devices to CC-SG, see **Managed Powerstrips** (on page 55).

► **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. Depending on the device type you select, you will see a slightly different Add Device page.
 - For instructions on adding KVM or serial devices, see **Add a KVM or Serial Device** (on page 33).
 - For instructions on adding Powerstrip devices, see **Add a PowerStrip Device** (on page 34).
 - For instructions on adding Dominion PX devices, see **Add a Dominion PX Device** (on page 35).

Add a KVM or Serial Device

KVM and serial devices may support 256 bit AES encryption, but CC-SG does not support this level of encryption. Make sure the device is set to the default encryption mode "auto-negotiate." The device will negotiate down to a 128 bit level to function with CC-SG.

1. Type a name for the device in the Device name field. See **Naming Conventions** (on page 274) 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. See **Terminology/Acronyms** (on page 2) for hostname rules.
3. Type the number of the TCP communication port used to communicate with the device in the TCP Port Number field. The maximum is five numeric characters. The default port number for most Raritan devices is 5000.
4. Type the name used to log into 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 Direct Device 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. Type a short description of this device in the Description field.
Optional.
9. Select the Configure all ports checkbox to automatically add all ports on this device to the Devices tab and to 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. See **Associations, Categories, and Elements** (on page 21).
11. 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, select the Apply to Nodes checkbox.
12. If you do not see the Category or Element values you want to use, you can add more through the Associations menu. See **Associations, Categories, and Elements** (on page 21).
13. 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.
14. 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. See **Upgrading a Device** (on page 41).

Add a PowerStrip Device

The process of adding a PowerStrip Device to CC-SG varies, based on which Raritan device the powerstrip is connected to physically. See **Managed PowerStrips** (on page 55).

To add a Dominion PX that is not connected to another Raritan device, see **Add a Dominion PX Device** (on page 35).

Add a Dominion PX Device

Dominion PX devices are powerstrips that are connected only to your IP network. A Dominion PX device is not managed by another Raritan device. If you want to add a powerstrip that is managed by another Raritan device, there is a different procedure. See **Managed PowerStrips** (on page 55).

1. Type a name for the device in the Device name field. See **Naming Conventions** (on page 274) 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. See **Terminology/Acronyms** (on page 2) for hostname rules.
3. Type the name used to log into this device in the Username field. The user must have administrative access.
4. Type the password needed to access this device in the Password field. The user must have administrative access.

Warning: If you change the password on the PX, you must delete and re-add the PX device in CC-SG. CC-SG will lose connectivity with the Dominion PX device if the username or password changes.

5. Type a short description of this device in the Description field.
Optional.
6. Select the Configure All Outlets checkbox to automatically add all outlets on this Dominion PX to the Devices tab.
7. A list of Categories and Elements can be configured to better describe and organize this device.
 - For each Category listed, 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 do not see the Category or Element values you want to use, you can add others. See **Associations, Categories, and Elements** (on page 21).
8. 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.

Editing 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.

Editing a PowerStrip Device or a Dominion PX Device

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

► **To edit a powerstrip device:**

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, click the Node hyperlink to open the Node Profile.
5. If an outlet is associated with a node, select the outlet, and then click Power Control to open the Power Control screen for the associated node.
6. To delete an outlet, deselect the checkbox next to the outlet name.
7. To configure an outlet, select the checkbox next to the outlet name.
8. Click OK to save your changes. A message appears when the device has been modified.

Adding Notes to a Device Profile

You can use the Notes tab to add notes about a device for other users to read. All notes display in the tab with the date, username, and IP address of the user who added the note.

If you have the Device, Port, and Node Management privilege, you can clear all notes that display in the Notes tab.

► **To add notes to the device profile:**

1. Select a device in the Devices tab. The Device Profile page opens.

2. Click the Notes tab.
3. Type your note in the New Note field.
4. Click Add. Your note appears in the Notes list.

► **To clear all notes:**

1. Click the Notes tab.
2. Click Clear Notes.
3. Click Yes to confirm. All notes are deleted from the Notes tab.

Adding Location and Contacts to a Device Profile

Enter details about the location of the device and contact information for the people who administer or use the device.

► **To add location and contacts to a device profile:**

1. Select a device in the Devices tab. The Device Profile page opens.
2. Click the Location & Contacts tab.
3. Enter Location information.
 - Department: Maximum 64 characters.
 - Site: Maximum 64 characters.
 - Location: Maximum 128 characters.
4. Enter Contacts information.
 - Primary Contact Name and Secondary Contact Name: Maximum 64 characters.
 - Telephone Number and Cell Phone: Maximum 32 characters.
5. Click OK to save your changes.

Deleting 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 confirmation message that appears. The KSX device will restart. Once the device has been paused, you can delete it from CC-SG.

► **To delete a device:**

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.

Configuring Ports

If all ports of a device were not automatically added by selecting Configure all ports when you added the device, use the Configure Ports screen to add individual ports or a set of ports on the device to CC-SG.

Once you configure ports, a node is created in CC-SG for each port, and the default interface is also created. See **Nodes Created by Configuring Ports** (on page 39).

Configure a Serial Port

► **To configure a serial port:**

1. Click the Devices tab and select a serial 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 serial port you want to configure.
4. Type a name in the Port Name field. For ease of use, name the port after the target that is connected to the port. See **Naming Conventions** (on page 274) 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.

Configure a KVM Port

► **To 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. See **Naming Conventions** (on page 274) 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.

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. See **Naming Conventions** (on page 274).

Editing a Port

You can edit ports to change various parameters, such as port name, access application, and serial port settings. The changes you can make vary, based on port type and device type.

► **To edit a KVM or serial port name or access application:**

Some ports support only one access application, so you cannot change the access application preference.

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.

► **To edit a KSX2 or KSX serial port's settings, such as baud rate, flow control, or parity/data bits:**

1. Click the Devices tab and select the serial port you want to edit, or just select the device that contains the port you want to edit.
2. Choose Devices > Device Manager > Launch Admin. The device's administrative page opens.
3. Click Port Configuration.
4. Click the serial port you want to edit.
5. Edit the port settings.
6. Click OK to save your changes. Close the administrative page and return to CC-SG.

► **To edit an SX serial port's settings, such as baud rate, flow control, or parity/data bits:**

1. Click the Devices tab and select a port you want to edit. The Port Profile page opens.
2. Edit the port settings.
3. Click OK to save your changes.

Deleting a Port

Delete a port to remove the port entry from a Device. When a port is down, the information in the Port Profile screen is read-only. You can delete a port that is down.

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.

► **To delete a port:**

1. Click the Devices tab and select a device whose ports you want to delete.
2. Choose Devices > Port Manager > Delete Ports.
3. Select the checkbox of the port you want to delete.
4. Click OK to delete the selected port. A message appears when the port has been deleted.

Bulk Copying 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. Note that categories and elements are the only properties copied in this process.

► **To bulk copy device categories and elements:**

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. Select the device and click < to remove it from the Selected Devices list.
6. Click OK to bulk copy. A message appears when the device categories and elements have been copied.

Upgrading a Device

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

Important: 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.

► **To upgrade a device:**

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.

Backing Up a 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.

The maximum number of backup files that can be stored on CC-SG is 3 per device. If you need more backups, you can save a backup file to your network then delete it from CC-SG. Or, you can opt to allow CC-SG to delete the oldest backup file for you. This option will appear as an alert when you attempt to do a fourth backup. See **Restore All Configuration Data to a KX2, KSX2, or KX2-101 Device** (on page 45).

Each device may back up different components of the configuration. See the User Guide for the device you want to back up for details.

Note: When you back up 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.

► **To backup a device configuration:**

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. Type a short description of the backup in the Description field.
Optional.
5. Click OK to back up the device configuration. A message appears when the device configuration has been backed up.

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, KSX2, and KX2-101 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. You can use the Protected option to restore a backup of one device to another device of the same model (KX2, KSX2, and KX2-101 only).
- 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 Data 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.

► **To restore a full backup device configuration:**

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, KSX2, or KX2-101 Device

The Protected restore option allows you to restore all configuration data in a backup file, except network settings, to a KX2, KXSX2, or KX2-101 device. You can use the Protected option to restore a backup of one device to another device of the same model (KX2, KXSX2, and KX2-101 only).

► **To restore all configuration data except network settings to a KX2, KXSX2, or KX2-101 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, KXSX2, or KX2-101 Device

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

► **To restore only device settings or user and user group data to a KX2, KXSX2, or KX2-101 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 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, KSX2, or KX2-101 Device

The Full restore option allows you to restore all configuration data in a backup file to a KX2, KSX2, or KX2-101 device.

▶ To restore all configuration data to a KX2, KSX2, or KX2-101 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.

Save, Upload, and Delete Device Backup Files

You can save the device backup files in the Restore Device Configuration page to a location on your network or local machine. If you need to make space for new backups to be stored on CC-SG, you can delete device backup files. You can also upload device backup files saved on your network back to CC-SG to use them to restore a device configuration.

▶ Save a device backup file from CC-SG:

1. Click the Devices tab and select a device.
2. Choose Devices > Device Manager > Configuration > Restore.
3. Select the device backup file you want to save. Click Save to File.
4. Navigate to the location where you want to save the file. Click Save.

▶ Delete a device backup file from CC-SG:

1. Click the Devices tab and select a device.
2. Choose Devices > Device Manager > Configuration > Restore.
3. Select the device backup file you want to delete. Click Delete.
4. Click Yes to confirm.

▶ Upload a device backup file to CC-SG:

1. Click the Devices tab and select a device.
2. Choose Devices > Device Manager > Configuration > Restore.

3. Click Upload. Navigate to and select the device backup file. The file type is .rfp. Click Open.

The device backup file uploads to CC-SG and appears in the page.

Copying Device Configuration

You can copy configurations from one Dominion SX device to one or more other SX devices.

Configuration can be copied only between SX units. The SX units must each have the same number of ports.

► **To copy a Dominion SX device configuration:**

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.

Restarting a Device

Use the Restart Device function to restart a device.

► **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.

Pinging the Device

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

▶ **To ping a device:**

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.

Pausing CC-SG's Management of a Device

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

▶ **To pause CC-SG management of a device:**

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.

Resuming Management

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

▶ **To resume CC-SG's management of a paused device:**

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 device's active state.

Device Power Manager

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

Before using the Device Power Manager, a physical connection must 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 SX serial port or the KSX dedicated power port that is providing management of the PowerStrip.

► **To view the device power manager:**

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.

Launching a Device's Administrative Page

If available for the device selected, the Launch Admin command provides access to the device's administrator interface.

► **To launch a device's administrative page:**

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.

Disconnecting Users

Administrators can terminate any user's session on 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 into the device as well as those who are connected to the device via CC-SG.

► **To disconnect users from a device:**

1. Click the Devices tab and select the device from which you want to disconnect users.
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 the users 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. See 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 from CC-SG:**

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 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 with which you want to work 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. See **Policies for Access Control** (on page 110).

Add a Device Group

► **To add a device group:**

1. Choose Associations > Device Groups. The Device Groups Manager window opens. Existing device groups appear in the left panel.
2. Click the New Group icon  in the toolbar. The Device Group: New panel appears.
3. In the Group name field, type a name for a device group you want to create. See **Naming Conventions** (on page 274) 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 choose 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 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 can 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.
 - 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 are available here.
 - 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 appear 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. It is not editable; it is used for writing descriptions in the Short Expression field.

- 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.
 - 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 requires only a single rule, 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 needs to satisfy only 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 before the rest of the description is compared to the node. Parenthetical groups can be nested inside other parenthetical groups.
 - Example1: If you want to describe devices that belong to the engineering department, create a rule that says Department = Engineering. This will become Rule0. 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 must create three rules. Department = Engineering (Rule0) Location = Philadelphia (Rule1) Memory = 1GB (Rule2). These rules must 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. Make this comparison first by enclosing it parentheses: (Rule0|Rule1). Since the devices 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.
- To remove a row from the table, select the row, and then click the Remove Selected Row icon .
 - 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 opens, 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. Select the Create Full Access Policy for Group checkbox to create a policy for this device group that allows access to all devices in the group at all times with control permission.
- d. To add another device group, click Apply to save this group, then repeat these steps. **Optional.**
- e. If you have finished adding device groups, click OK to save your changes.

Describe Method versus Select Method

Use the describe method when you want your group to be based on some attribute of the node or devices, such as the categories and elements. The advantage of the describe method is that when you add more devices or nodes with the same attributes as described, they will be pulled into the group automatically.

Use the select method when you just want to create a group of specific nodes manually. New nodes and devices added to CC-SG are not pulled into these groups automatically. You must manually add the new nodes or devices to the group after you add them to CC-SG.

These two methods cannot be combined.

Once a group is created with one method, you must edit it using the same method. Switching methods will overwrite the current group settings.

Edit a Device Group

► To edit a device group:

1. Choose Associations > Device Groups. The Device Groups Manager window opens.
2. Existing device groups appear in the left panel. Select the Device Group whose name you want to edit. The Device Group Details panel appears.

3. Type a new name for the device group in the Group Name field.
Optional.
4. Edit the device group's included devices using the Select Device or Describe Devices tabs. See **Add a Device Group** (on page 50).
5. Click OK to save your changes.

Delete a Device Group

► **To delete a device group:**

1. Choose Associations > Device Groups. The Device Groups Manager window opens.
2. Existing device groups appear 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 appears.

Chapter 7 Managed Powerstrips

There are two ways to configure power control using powerstrips in CC-SG.

1. All supported Raritan-brand powerstrips can be connected to another Raritan device and added to CC-SG as a Powerstrip device. Raritan-brand powerstrips include Dominion PX and RPC powerstrips. Check the Compatibility Matrix for supported versions. To configure this type of managed powerstrip in CC-SG , you must know to which Raritan device the powerstrip is physically connected. See **Configuring Powerstrips That Are Managed by Another Device in CC-SG** (on page 56).
2. Dominion PX powerstrips can be connected directly to the IP network and added to CC-SG as a PX device. If you have PX powerstrips connected directly to the IP network, they do not need to be connected to another Raritan device.

With both methods, you must add Managed Powerstrip interfaces to nodes to create power associations between the outlets and the nodes they power. See **Interfaces for Managed Powerstrip Connections** (on page 86).

► Special Note about Dominion PX

Regardless of which method you choose to configure a PX, you should configure all power associations using a single method, that is, as a powerstrip of the managed device or as a PX device, but not both.

In addition, you can connect the PX to a managing device and configure power associations, and also connect the same PX device to the IP network so that you can use the PX web client to view and collect power data. See the Raritan **Dominion PX User Guide**, located in the Support section of the Raritan website under Firmware and Documentation.

In This Chapter

Configuring Powerstrips that are Managed by Another Device in CC-SG56	
Configuring PowerStrips Connected to KX, KX2, KX2-101, KSX2, and P2SC	57
Configuring PowerStrips Connected to SX 3.0 and KSX	58
Configuring Powerstrips Connected to SX 3.1	60
Configuring Outlets on a Powerstrip.....	61

Configuring Powerstrips that are Managed by Another Device in CC-SG

In CC-SG, managed powerstrips can be connected to one of the following devices:

- Dominion KX
- Dominion KX2
- Dominion KX2-101
- Dominion SX 3.0
- Dominion SX 3.1
- Dominion KSX
- Dominion KSX2
- Paragon II/Paragon II System Controller (P2SC)

You must know which Raritan device the managed powerstrip is connected to physically.

*Note: You can also have a Dominion PX powerstrip that is connected to your IP network, but not connected to any other Raritan device. See **Managed PowerStrips** (on page 55) for details on configuring power control for these powerstrips.*

► To configure managed powerstrips in CC-SG:

1. Complete all physical connections between the device, the powerstrip, and the nodes that are powered by the powerstrip. See 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. See the section that corresponds to the device the powerstrip is connected to:
 - **Configuring PowerStrips Connected to KX, KX2, KX2-101, KSX2, and P2SC** (on page 57)
 - **Configuring PowerStrips Connected to SX 3.0 and KSX** (on page 58)
 - **Configuring PowerStrips Connected to SX 3.1** (on page 60).
3. Configure outlets. See **Configuring Outlets on a PowerStrip** (on page 61).
4. Associate each outlet with the node that it powers. See **Interfaces for Managed Powerstrip Connections** (on page 86).

Configuring PowerStrips Connected to KX, KX2, KX2-101, KSX2, and P2SC

CC-SG automatically detects PowerStrips connected to KX, KX2, KX2-101, KSX2, and P2SC devices. You can perform the following tasks in CC-SG to configure and manage PowerStrips connected to these devices.

- **Add a PowerStrip Device Connected to a KX, KX2, KX2-101, KSX2, or P2SC Device** (on page 57)
- **Move a KX, KX2, KX2-101, KSX2, or P2SC's PowerStrip to a Different Port** (on page 57)
- **Delete a PowerStrip Connected to a KX, KX2, KX2-101, KSX2, or P2SC Device** (on page 58)

Add a PowerStrip Device Connected to a KX, KX2, KX2-101, KSX2, or P2SC Device

When you add a KX, KX2, KX2-101, KSX2, or P2SC device that is connected to a PowerStrip to CC-SG, the PowerStrip is added automatically. The PowerStrip will appear in the Devices tab, beneath the device to which it is connected.

Next Steps:

1. Configure outlets. See **Configuring Outlets on a PowerStrip** (on page 61).
2. Associate each outlet with the node that it powers. See **Interfaces for Managed Powerstrip Connections** (on page 86).

Move a KX, KX2, KX2-101, KSX2, or P2SC's PowerStrip to a Different Port

When you physically move a PowerStrip from one KX, KX2, KX2-101, KSX2, or P2SC device or port to another KX, KX2, KX2-101, KSX2, 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 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. See the **Raritan P2SC User Guide**.*

Delete a PowerStrip Connected to a KX, KX2, KX2-101, KSX2, or P2SC Device

You cannot delete a PowerStrip connected to a KX, KX2, KX2-101, KSX2, or P2SC device from CC-SG. You must physically disconnect the PowerStrip from the device to delete the PowerStrip from CC-SG. When you physically disconnect the PowerStrip from the 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** (on page 58)
- **Delete a PowerStrip Connected to an SX 3.0 or KSX Device** (on page 59)
- **Change a PowerStrip's Device or Port Association (SX 3.0, KSX)** (on page 59)

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. Click the Device type drop-down menu and select Select PowerStrip.
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 select the SX 3.0 or KSX device that is connected to this power strip.
7. Click the Managing Port drop-down menu and select the port on the SX 3.0 or KSX device to which this power strip is connected.
8. Type a short description of this PowerStrip in the Description field.
Optional.
9. Select 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 **Configuring Outlets on a Powerstrip** (on page 61). **Optional.**

10. For each Category listed, click the Element drop-down menu and select the element you want to apply to the device. Select the blank item in the Element field for each Category you do not want to use. See **Associations, Categories, and Elements** (on page 21).
Optional.
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 **Configuring Outlets on a PowerStrip** (on page 61).
2. Associate each outlet with the node that it powers. See **Interfaces for Managed Powerstrip Connections** (on page 86).

Delete a PowerStrip Connected to an SX 3.0 or KSX Device

You can visually delete a powerstrip connected to an SX 3.0, KSX, or P2SC device even if the powerstrip is still physically connected. If you physically disconnect a powerstrip from the SX 3.0, KSX, or P2SC device with which it is associated, the powerstrip still appears in the Devices tab beneath that device. 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.
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 Connected to an SX 3.1 Device** (on page 60)
- **Move an SX 3.1's Powerstrip to a Different Port** (on page 61)
- **Delete a Powerstrip Connected to an SX 3.1 Device** (on page 61)

Add a Powerstrip Connected to an SX 3.1 Device

The procedure for adding a powerstrip connected to an SX 3.1 device varies, based 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 yet been added to CC-SG:

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 appear in the Devices tab beneath the SX 3.1 device to which it is connected.

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 **Configuring Ports** (on page 38).
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 to which the PowerStrip is connected, 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 **Configuring Outlets on a PowerStrip** (on page 61).
2. Associate each outlet with the node that it powers. See **Interfaces for Managed Powerstrip Connections** (on page 86).

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 and add it to the new SX 3.1 port. See **Delete a Powerstrip Connected to an SX 3.1 Device** (on page 61) and **Add a Powerstrip Device Connected to an SX 3.1 Device** (see "Add a Powerstrip Connected to an SX 3.1 Device" on page 60).

Delete a PowerStrip Connected to an SX 3.1 Device

You can visually delete a powerstrip connected to an SX 3.1 device even if the powerstrip is still physically connected. If you physically disconnect the powerstrip from the SX 3.1 device with which it is associated, the powerstrip still appears in the Devices tab beneath that device. To remove it from display, you must delete the powerstrip.

► **To delete a powerstrip connected to an SX 3.1 device:**

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.

Configuring Outlets on a Powerstrip

Before associating Powerstrip outlets with nodes, you must configure the outlets by adding the Managed Powerstrip interface to the node. See **Interfaces for Managed Power Strip connections** (see "Interfaces for Managed Powerstrip Connections" on page 86).

► **To configure outlets from the PowerStrip profile:**

1. In the Devices tab, click the + next to the device that is connected to the PowerStrip.
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 appear 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.

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.
2. Click the + next to the PowerStrip.
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. See Raritan's **CommandCenter Secure Gateway User Guide** for details on connecting to nodes.

In This Chapter

Nodes and Interfaces Overview	63
Viewing Nodes.....	64
Service Accounts.....	68
Adding, Editing, and Deleting Nodes.....	70
Adding Location and Contacts to a Node Profile	72
Adding Notes to a Node Profile	73
Configuring the Virtual Infrastructure in CC-SG	73
Synchronizing the Virtual Infrastructure with CC-SG	80
Reboot or Force Reboot a Virtual Host Node.....	81
Accessing the Virtual Topology View	82
Connecting to a Node.....	82
Pinging a Node	83
Adding, Editing, and Deleting Interfaces	83
Bookmarking an Interface.....	91
Configuring Direct Port Access to a Node.....	92
Bulk Copy for Node Categories and Elements.....	92
Using Chat	92
Adding, Editing, and Deleting Node Groups.....	93

Nodes and Interfaces Overview

About Nodes

Each node represents a target that is accessible through CC-SG, via either 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. Nodes can also be created automatically by selecting 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 edit these nodes, ports, and interfaces at any time.

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.

See **Naming Conventions** (on page 274) for details on CC-SG's rules for name lengths.

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 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, but only 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.

Viewing Nodes

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

Nodes Tab

When you click the Nodes tab, all nodes to which you have access appear 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.

See **Custom Views for Devices and Nodes** (on page 115) for details on viewing the Nodes tab in different ways.

Node Profile

Click a Node in the Nodes tab to open the Node Profile page. The Node Profile page includes tabs that contain information about the node.

Node Profile
Please provide node properties.

Node Name: *
Sample Virtual Machine Node

Description:
virtual machine

Interfaces | Associations | Location & Contacts | Notes | Audit | Virtual Machine Data

Default Interface: *
Test-MiniXP-2

Type	Name	Status	Availability	Raritan Device
In-Band - VNC	Test-MiniXP-2	Up	Idle	192.168.43.185
VMW Viewer	Test-MiniXP-2	Up	Idle	
VMW Power	Test-MiniXP-2	Up	Power On	

Add Edit Delete

OK Cancel

▶ **Interfaces tab**

The Interfaces tab contains all the node's interfaces. You can add, edit, and delete interfaces on this tab, and select the default interface. Nodes that support virtual media include an additional column that shows whether virtual media is enabled or disabled.

▶ **Associations tab**

The Associations tab contains all categories and elements assigned to the node. You can change the associations by making different selections.

See **Associations, Categories, and Elements** (on page 21).

▶ **Location & Contacts tab**

The Location & Contacts tab contains information about a device's location and contact information, such as phone numbers, that you may need when working on a device. You can change the information in the fields by typing in new information.

See **Adding Location and Contacts to a Node Profile** (on page 72).

▶ **Notes tab**

The Notes tab contains a tool that enables users to leave notes for about a device for other users to read. All notes display in the tab with the date, username, and IP address of the user who added the note.

If you have the Device, Port, and Node Management privilege, you can clear all notes from the node profile. Click the Clear button.

See **Adding Notes to a Node Profile** (on page 73).

▶ **Audit tab**

You can view the reasons that a node was accessed in the Audit tab. Users must enter a reason for access before connecting to a node when node auditing has been enabled for the user group.

The Audit tab is hidden if the feature is disabled, or if no reasons for access have been entered.

See **Configuring Access Auditing for User Groups** (on page 103).

▶ **Control System Data tab**

Control system server nodes, such as VMware's Virtual Center, include the Control System Data tab. The Control System Data tab contains information from the control system server that is refreshed when the tab opens. You can access a topology view of the virtual infrastructure, link to associated node profiles, or connect to the control system and open the Summary tab.

► Virtual Host Data tab

Virtual host nodes, such as VMware's ESX servers, include the Virtual Host Data tab. The Virtual Host Data tab contains information from the virtual host server that is refreshed when the tab opens. You can access a topology view of the virtual infrastructure, link to associated node profiles, or connect to the virtual host and open the Summary tab. If you have Device, Port, and Node Management permission, you can Reboot and Force Reboot the virtual host server.

► Virtual Machine Data tab

Virtual machine nodes, such as VMware's Virtual Machines, include the Virtual Machine Data tab. The Virtual Machine Data tab contains information from the virtual machine that is refreshed when the tab opens. You can access a topology view of the virtual infrastructure, link to associated node profiles, or connect to the virtual host and open the Summary tab.

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.

Service Accounts

Service Accounts Overview

Service accounts are special login credentials that you can assign to multiple interfaces. You can save time by assigning a service account to a set of interfaces that often require a password change. You can update the login credentials in the service account, and the change is reflected in every interface that uses the service account.

Service accounts cannot be used for Out-of-Band interfaces or Managed Powerstrip interfaces.

- For DRAC, iLO, and RSA interfaces, the login credentials apply to the embedded processor card, not the underlying OS.
- For RDP, SSH, and Telnet interfaces, the login credentials apply to the OS.
- For VNC interfaces, the login credentials apply to the VNC server.
- For Web Browser interfaces, the login credentials apply to the form available at the URL specified in the interface.

► To view service accounts:

- Choose Nodes > Service Accounts. The Service Accounts dialog appears.

Field	Description
Service Account Name	This name is used to identify the service account in the interface dialogs and in the Assign Service Account page.
Username	This username is used as part of the login credentials when the service account is assigned to an interface.
Password	This password is used as part of the login credentials when the service account is assigned to an interface.
Retype Password	This field is used to ensure the password is typed correctly.
Description	This description can contain any extra information you want to add about the service account.

Add, Edit, and Delete Service Accounts

► To add a service account:

1. Choose Nodes > Service Accounts. The Service Accounts dialog appears.



2. Click the Add Row icon  to add a row to the table.
3. Enter a name for this service account in the Service Account Name field.
4. Enter the username in the Username field.
5. Enter the password in the Password field.
6. Re-type the password in the Retype Password field.
7. Enter a description of this service account in the Description field.
8. Click OK.

► **To edit a service account:**

1. Choose Nodes > Service Accounts. The Service Accounts dialog appears.
2. Find the service account you want to edit.
3. Edit the fields. You cannot edit the Service Account Name.

Note: CC-SG updates all interfaces that use the service account to use the new login credentials when you change the username or password.

4. Click OK.

► **To delete a service account:**

1. Choose Nodes > Service Accounts. The Service Accounts dialog appears.
2. Select the service account you want to delete.



3. Click the Delete Row button. 
4. Click OK.

Change the Password for a Service Account

► **To change the password for a service account:**

1. Choose Nodes > Service Accounts. The Service Accounts dialog appears.
2. Find the service account whose password you want to change.
3. Enter the new password in the Password field.
4. Re-type the password in the Retype Password field.
5. Click OK.

Note: CC-SG updates all interfaces that use the service account to use the new login credentials when you change the username or password.

Assign Service Accounts to Interfaces

You can assign a service account to multiple interfaces. Each interface that is assigned the service account uses the same login information for connections.

CC-SG updates all interfaces that use the service account to use the new login credentials when you change the username or password.

You can also select a service account when you configure an interface. See **Adding, Editing, and Deleting Interfaces** (on page 83).

You must have the Device, Port, and Node Management privilege to assign service accounts to interfaces. See **Adding, Editing, and Deleting User Groups** (on page 101).

► **To assign a service account to interfaces:**

1. Choose Nodes > Assign Service Accounts. The Assign Service Accounts page opens.
2. In the Service Account Name field, select the service account you want to assign to the nodes.
3. In the Available list, select the interfaces you want to assign the service account to. Use Ctrl+click or Shift+click to select multiple interfaces at once.

*Tip: Type a node name in the Find field to highlight it in the list. Type * after a partial name to highlight all similar names in the list.*

Click the column headers to sort the lists alphabetically.

4. Click Add to move the selected interfaces into the Selected list.
5. Click OK. The service account is assigned to all nodes in the Selected list.

Note: CC-SG updates all interfaces that use the service account to use the new login credentials when you change the username or password.

Adding, Editing, and Deleting Nodes

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. See **Naming Conventions** (on page 274) for details on CC-SG's rules for name lengths.
4. Type a short description for this node in the Description field.
Optional.
5. You must configure at least one interface. Click Add in the Interfaces area of the Add Node screen to add an interface. See **Add an Interface** (on page 83).
6. A list of Categories and Elements can be configured to better describe and organize this node. See **Associations, Categories, and Elements** (on page 21). **Optional.**
 - 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 them through the Associations menu. See **Associations, Categories, and Elements** (on page 21).
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. See **Naming Conventions** (on page 274).

Edit a Node

You can edit a node to change its 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.

3. Click OK to save your changes.

Delete a Node

Deleting a node removes 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.

Adding Location and Contacts to a Node Profile

Enter details about the location of the node, and contact information for the people who administer or use the node.

► **To add location and contacts to a node profile:**

1. Select a node in the Nodes tab. The Node Profile page opens.
2. Click the Location & Contacts tab.
3. Enter Location information.
 - Department: Maximum 64 characters.
 - Site: Maximum 64 characters.
 - Location: Maximum 128 characters.
4. Enter Contacts information.
 - Primary Contact Name and Secondary Contact Name: Maximum 64 characters.
 - Telephone Number and Cell Phone: Maximum 32 characters.
5. Click OK to save your changes.

Adding Notes to a Node Profile

You can use the Notes tab to add notes about a node for other users to read. All notes appear in the tab with the date, username, and IP address of the user who added the note.

If you have the Device, Port, and Node Management privilege, you can clear all notes that appear in the Notes tab.

► **To add notes to the node profile:**

1. Select a node in the Nodes tab. The Node Profile page opens.
2. Click the Notes tab.
3. Type your note in the New Note field.
4. Click Add. Your note appears in the Notes list.

► **To clear all notes:**

1. Click the Notes tab.
2. Click Clear Notes.
3. Click Yes to confirm. All notes are deleted from the Notes tab.

Configuring the Virtual Infrastructure in CC-SG

Terminology for Virtual Infrastructure

CC-SG uses the following terminology for virtual infrastructure components.

Term	Definition	Example
Control System	The Control System is the managing server. The Control System manages one or more Virtual Hosts.	VMware's Virtual Center
Virtual Host	The Virtual Host is the physical hardware that contains one or more Virtual Machines.	VMware's ESX
Virtual Machine	A Virtual Machine is a virtual "server" that resides on a Virtual Host. A Virtual Machine can be relocated from one Virtual Host to a different Virtual Host.	VMware's Virtual Machine or VM

Term	Definition	Example
VI Client interface	Control system nodes and virtual host nodes have a VI Client interface that provides access to the virtualization system's infrastructure client application.	VMware's Virtual Infrastructure Web Access
VMW Viewer interface	Virtual machine nodes have a VMW Viewer interface that provides access to the virtual machine's viewer application.	VMware's Virtual Machine Remote Console
VMW Power interface	Virtual machine nodes have a VMW Power interface that provides power control for the node through CC-SG.	N/A

Virtual Nodes Overview

You can configure your virtual infrastructure for access in CC-SG. The Virtualization page offers two wizard tools, Add Control System wizard and Add Virtual Host wizard, that help you add control systems, virtual hosts, and their virtual machines properly.

Once you complete the configuration, all control systems, virtual hosts, and virtual machines are available for access as nodes in CC-SG. Each type of virtual node is configured with an interface for access and an interface for power.

- Control system nodes and virtual host nodes are configured with a VI Client interface. The VI Client interface provides access to the virtualization system's infrastructure client. For VMware control centers, the VI Client interface provides access to the control center server via VMware Virtual Infrastructure Web Access. For VMware ESX servers, the VI Client interface provides access to the ESX server via VMware Virtual Infrastructure Web Access.
- Virtual machine nodes are configured with a VMW Viewer interface and a VMW Power interface. The VMW Viewer interface provides access to the virtual machine's viewer application. For VMware virtual machines, the VMW Viewer interface provides access to the virtual machine remote console. The VMW Power interface provides power control for the node through CC-SG.

Add a Control System with Virtual Hosts and Virtual Machines

When you add a control system, a wizard guides you through adding the virtual hosts and virtual machines included in the control system.

► **To add a control system with virtual hosts and virtual machines:**

1. Choose Nodes > Virtualization.
2. Click Add Control System.

3. Hostname/IP Address: Enter the IP Address or hostname of the control system. Maximum 64 characters.
4. Connection Protocol: Specify HTTP or HTTPS communications between the control system and CC-SG.
5. TCP Port: Enter the TCP port. The default port is 443.
6. Check Interval (seconds): Enter the time in seconds that should elapse before timeout between the control system and CC-SG.
7. Enter authentication information:
 - To use a service account for authentication, select the Use Service Account Credentials checkbox. Select the service account to use in the Service Account Name menu.

or

 - Enter a Username and Password for authentication. Maximum 64 characters each.
8. To allow users who access this control system to automatically log into the VI Client interface, select the Enable Single Sign On For VI Client checkbox. **Optional.**
9. Click Next. CC-SG discovers the control system's virtual hosts and virtual machines.
10. Select the Configure checkbox next to each virtual machine to add it to CC-SG. Each associated virtual host will also be configured. One node will be created for each virtual machine. Only one virtual host node will be added, even if the virtual host is associated with multiple virtual machines.
11. To add a VNC, RDP, or SSH interface to the virtual host node and the virtual machine node, select the checkboxes next to each virtual machine. **Optional.**
12. Click Next. CC-SG displays a list of interface types that will be added. You can add names and login credentials for each type.
13. For each interface type, enter a name and login credentials. The name and login credentials will be shared by all the interfaces added to each virtual machine node and virtual host node configured. **Optional.**

Leave these fields blank if you prefer to add names and login credentials to each interface individually.

The interface will take the name of the node if the field is left blank.

- a. Enter names for interfaces. Maximum 32 characters.

- Virtual Host VI Client Interfaces
 - VMware Viewer Interfaces
 - Virtual Power Interfaces
 - RDP, VNC, and SSH Interfaces, if specified
- b. Enter login credentials, if needed. Some interface types do not require login credentials.:
- To use a Service Account, select the Use Service Account Credentials checkbox then select the name of the service account.
- or
- Enter a username and password for the interface type. Maximum 64 characters each.
1. Click OK.
- CC-SG creates:
- One node for each virtual machine. Each virtual machine node has a VMW Viewer interface, a VMW Power interface, and any other in-band interfaces you specified. Virtual machine nodes are named with their virtual machine names from the virtual host systems.
 - One node for each virtual host. Each virtual host node has a VI Client interface. Virtual Host nodes are named with their IP addresses or host names.
 - One node for the control system. The control system node has a VI Client interface. Control System nodes are named VMware Virtual Center.

Add a Virtual Host with Virtual Machines

When you add a virtual host, a wizard guides you through adding the virtual machines included in the virtual host.

► **To add a virtual host with virtual machines:**

1. Choose Nodes > Virtualization.
2. Click Add Virtual Host.
3. Choose Nodes > Virtualization.
4. Click Add Virtual Host.
5. Hostname/IP Address: Enter the IP Address or hostname of the virtual host. Maximum 64 characters.
6. Connection Protocol: Specify HTTP or HTTPS communications between the virtual host and CC-SG.

7. TCP Port: Enter the TCP port. The default port is 443.
8. Check Interval (seconds): Enter the time in seconds that should elapse before timeout between the virtual host and CC-SG.
9. Enter authentication information:
 - To use a service account for authentication, select the Use Service Account Credentials checkbox. Select the service account to use in the Service Account Name menu.

or

 - Enter a Username and Password for authentication. Maximum 64 characters each.
10. To allow users who access this virtual host to automatically login to the VI Client interface, select the Enable Single Sign On For VI Client checkbox. **Optional.**
11. Click Next. CC-SG discovers the virtual host's virtual machines.
12. Select the Configure checkbox next to each virtual machine to add it to CC-SG. Each associated virtual host will also be configured. One node will be added for each virtual machine. Only one virtual host node will be added, even if the virtual host is associated with multiple virtual machines.
13. To add a VNC, RDP, or SSH interface to the virtual host node and the virtual machine node, select the checkboxes next to each virtual machine. **Optional.**
14. Click Next. CC-SG displays a list of interface types that will be added. You can add names and login credentials for each type.
15. For each interface type, enter a name and login credentials. The name and login credentials will be shared by all the interfaces added to each virtual machine node and virtual host node configured. **Optional.**

Leave these fields blank if you prefer to add names and login credentials to each interface individually.

The interface will take the name of the node if the field is left blank.

- a. Enter names for interfaces. Maximum 32 characters.
 - VI Client Interfaces
 - VMware Viewer Interfaces
 - Virtual Power Interfaces
 - RDP, VNC, and SSH Interfaces, if specified
- b. Enter login credentials, if needed. Some interface types do not require login credentials.:

- To use a Service Account, select the Use Service Account Credentials checkbox then select the name of the service account.

or

- Enter a username and password for the interface type. Maximum 64 characters each.

16. Click OK.

CC-SG creates:

- One node for each virtual machine. Each virtual machine node has a VMW Viewer interface, a VMW Power interface, and any other in-band interfaces you specified. Virtual machine nodes are named with their virtual machine names from the virtual host systems.
- One node for each virtual host. Each virtual host node has a VI Client interface. Virtual host nodes are named with their IP addresses or host names.

Edit Control Systems, Virtual Hosts, and Virtual Machines

You can edit the control systems, virtual hosts, and virtual machines configured in CC-SG to change their properties. You can delete virtual machine nodes from CC-SG by deselecting the Configure checkbox for the virtual machine.

► **To edit control systems, virtual hosts, and virtual machines:**

1. Choose Nodes > Virtualization.
2. Select the control system or virtual host you want to edit.
3. Click Edit.
4. Change the information as needed. See **Add a Control System with Virtual Hosts and Virtual Machines** (on page 74) and **Add a Virtual Host with Virtual Machines** (on page 76) for complete field descriptions.
5. Click Next.
6. To delete a virtual machine from CC-SG, deselect the Configure checkbox. To add VNC, RDP, or SSH interfaces to the virtual host node and the virtual machine node, select the checkboxes next to each virtual machine.

*You cannot remove SSH, VNC and RDP interfaces from virtual machine nodes or virtual host nodes from this page. You must delete the interfaces from the node profile. See **Delete an Interface** (on page 90).*

7. Click Next. If you chose to delete virtual machines, a message appears to alert you.
8. For each interface type, enter a name and login credentials. The name and login credentials will be shared by all the interfaces added to each virtual machine node and virtual host node configured.

Optional. You can leave these fields blank if you prefer to add names and login credentials to each interface individually.

 - a. Enter names for interfaces (maximum 32 characters).
 - Virtual Host VI Client Interfaces
 - VMware Viewer Interfaces
 - Virtual Power Interfaces
 - RDP, VNC, and SSH Interfaces, if specified
 - b. Enter login credentials:
 - To use a Service Account, select the Use Service Account Credentials checkbox then select the name of the service account.

or

 - Enter a username and password for the interface type. Maximum 64 characters each.
1. Click OK.

Delete Control Systems and Virtual Hosts

You can delete control systems and virtual hosts from CC-SG.

When you delete a control system, the virtual hosts and virtual machines associated with it are not deleted.

When you delete a virtual host, the control systems and virtual machines associated with it are not deleted.

Virtual machine nodes are not automatically deleted when their associated control systems or virtual hosts are deleted. See **Delete a Virtual Machine Node** (on page 80).

► **To delete control systems and virtual hosts:**

1. Choose Nodes > Virtualization.
2. Select the control systems and virtual hosts you want to delete from the list. Use Ctrl+click to select multiple items.
3. Click Delete.

Delete a Virtual Machine Node

There are two ways to delete virtual machine nodes:

- Use the Delete Node feature. See **Delete a Node** (on page 72).
- Deselect the Configure checkbox for the virtual machine. See **Edit Control Systems, Virtual Hosts, and Virtual Machines** (on page 78).

Delete a Virtual Infrastructure

Follow these steps to delete a whole virtual infrastructure from CC-SG, including the control system, virtual hosts, and virtual machines.

► **To delete a virtual infrastructure:**

1. Delete all virtual machine nodes by deselecting the Configure checkbox for each virtual machine. See **Edit Control Systems, Virtual Hosts, and Virtual Machines** (on page 78).
2. Delete the control system and virtual hosts. See **Delete Control Systems and Virtual Hosts** (on page 79).

All components of the virtual infrastructure are deleted, including control system nodes, virtual host nodes, and virtual machine nodes and their interfaces.

Synchronizing the Virtual Infrastructure with CC-SG

Synchronization ensures that the CC-SG has the most up-to-date information about your virtual infrastructure. Synchronization updates information specific to each virtual machine node and virtual infrastructure topology information.

You can configure an automatic daily synchronization of all control systems and virtual hosts configured. You can also perform a synchronization of selected control systems and virtual hosts at any time.

Synchronize the Virtual Infrastructure Now

You can perform a synchronization of CC-SG with your virtual infrastructure.

When you select a control system for synchronization, the associated virtual hosts will also be synchronized, whether or not you select the virtual hosts.

► **To synchronize the virtual infrastructure now:**

1. Choose Nodes > Virtualization.

2. In the list of nodes, select the nodes you want to synchronize. Use Ctrl+click to select multiple items.
3. Click Synchronize. If the virtual infrastructure had changed since the last synchronization, the information in CC-SG updates.
 - The Configured in Secure Gateway column shows the number of virtual machines or hosts that are configured in CC-SG.
 - The Last Synchronization Date shows the date and time of the synchronization.
 - The Node Status column shows the status of the virtual node.

Enable or Disable Daily Synchronization of the Virtual Infrastructure

You can configure an automatic synchronization of CC-SG with your virtual infrastructure. The automatic synchronization occurs daily at the time you specify.

► **To enable daily synchronization of the virtual infrastructure:**

1. Choose Nodes > Virtualization.
2. Select the Enable Daily Automatic Synchronization checkbox.
3. Enter the time when you want the daily synchronization to occur in the Start Time field.
4. Click Update.

► **To disable daily synchronization of the virtual infrastructure:**

1. Choose Nodes > Virtualization.
2. Deselect the Enable Daily Automatic Synchronization checkbox.
3. Click Update.

Reboot or Force Reboot a Virtual Host Node

You can reboot or force reboot the virtual host server. A Reboot operation performs a normal reboot of the virtual host server when it is in maintenance mode. A Force Reboot operation forces the virtual host server to reboot, even if the server is not in maintenance mode.

To access these commands, you must have the Node In-Band Access and Node Power Control privilege. You must also be in a user group that is assigned a policy to access the node you want to reboot or force reboot.

► **To reboot or force reboot a virtual host node:**

1. Select the virtual host node you want to reboot or force reboot.
2. Click the Virtual Host Data tab.

3. Click Reboot or Force Reboot.

Accessing the Virtual Topology View

The Topology View is a tree structure that shows the relationships of the control system, virtual hosts, and virtual machines associated with the selected node.

You must have the Device, Port, and Node Management privilege to open the topology view.

► **Open the topology view from the virtual node profile:**

1. In the node profile, click the tab that contains virtualization information about the node: Virtual Machine Data tab, Virtual Host Data tab or Control System tab, depending on the node type.
2. Click the Topology View link. The topology view opens in a new window. Virtual nodes that are configured in CC-SG display as links.
 - Double-click a node's link to open the node profile for the virtual node.
 - Double-click an interface link to either connect to the node.
 - Double-click a virtual power interface link to open the Power Control page for the node.

Connecting to a Node

Once a node has an interface, you can connect to that node through the interface in several different ways. See Raritan's **CommandCenter Secure Gateway User Guide**.

► **To connect to a node:**

1. Click the Nodes tab.
2. Select the node to which you want to connect and:
 - In the Interfaces table, click the name of the interface with which you want to connect.or
 - In the Nodes tab, expand the list of interfaces underneath the node to which you want to connect. Double-click the name of the interface to which you want to connect, or right-click the interface and select Connect.

Pinging 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.

Adding, Editing, and Deleting Interfaces

Add an Interface

*Note: Interfaces for virtual nodes, such as control system, virtual hosts, and virtual machines, can only be added using the Virtualization tools under Nodes > Virtualization. See **Configuring the Virtual Infrastructure in CC-SG** (on page 73).*

► **To 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 opens.

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

In-Band Connections:

- 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.

See **Interfaces for In-Band Connections** (on page 85).

Out-of-Band Connections:

- 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).

See **Interfaces for Out-of-Band KVM, Out-of-Band Serial Connections** (on page 85).

Power Control Connections:

- 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: 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.

See **Interfaces for DRAC, RSA and ILO Processor Power Control Connections** (see "Interfaces for DRAC, RSA, and ILO Processor Power Control Connections" on page 86) and **Interfaces for IPMI Power Control Connections** (on page 87).

Managed Powerstrip Connections:

- Managed PowerStrip: Select this item to create a power control connection to a node powered through a Raritan PowerStrip or Dominion PX device.

See **Interfaces for Managed Powerstrip Connections** (on page 86).

Web Browser Connections:

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

See **Web Browser Interface** (on page 88).

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. See **Naming Conventions** (on page 274) for details on CC-SG's rules for name lengths.

Interfaces for In-Band Connections

In-band connections include RDP, VNC, SSH, RSA KVM, iLO Processor KVM, DRAC KVM, and TELNET.

Telnet is not a secure access method. All usernames, passwords, and traffic are transmitted in clear text.

► **To add an interface for in-band connections:**

1. Type the IP Address or Hostname for this interface in the IP Address/Hostname field.
2. Type a TCP Port for this connection in the TCP Port field. **Optional.**
3. For RDP interfaces, select Console or Remote User. When a Console user accesses a node, all other users are disconnected. Multiple Remote Users can access a node simultaneously.
4. Enter authentication information:
 - To use a service account for authentication, select the Use Service Account Credentials checkbox. Select the service account to use in the Service Account Name menu.

or

 - Enter a Username and Password for authentication. For VNC interfaces, only a password is required.
5. Select the Keyboard layout for your language.
6. Type a description of this interface in the Description field. **Optional.**
7. Click OK to save your changes.

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

► **To add an Interface for out-of-band KVM or 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 that a device must be added to CC-SG before it appears 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. Type a description of this interface in the Description field. **Optional.**
5. Click OK to save your changes.

Interfaces for DRAC, RSA, and ILO Processor Power Control Connections

► **To add an interface 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. Type a TCP Port for this connection in the TCP Port field. **Optional.**
3. Enter authentication information:
 - To use a service account for authentication, select the Use Service Account Credentials checkbox. Select the service account to use in the Service Account Name menu.or
 - Enter a Username and Password for authentication.
4. Type a description of this interface in the Description field. **Optional.**
5. Click OK to save your changes.

Interfaces for Managed Powerstrip 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.

► **To add an interface for managed powerstrip connections:**

1. Managing Device:
 - Select the Raritan device to which the Power Strip is connected. The device must be added to CC-SG.or
 - Select Dominion PX if this power control interface uses a PX device on the IP network that is not connected to another Raritan device.
2. Managing Port: select the port on the Raritan device to which the Power Strip is connected. This field is disabled when you select PX as the Managing Device.
3. Power Strip Name: select the Power Strip or PX device that provides power to the node. The power strip or PX device 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. **Optional.**

5. Type a description of this interface in the Description field.
6. Click OK to save your changes.

Interfaces for IPMI Power Control Connections

► **To add an interface 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. Enter authentication information:
 - To use a service account for authentication, select the Use Service Account Credentials checkbox. Select the service account to use in the Service Account Name menu.or
 - Enter a Username and Password for authentication. **Optional.**
6. Type a description of this interface in the Description field.
7. 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. See **Example: Adding a Web Browser Interface to a PX Node** (on page 89). 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 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.

► **To add a web browser interface:**

1. The default name for a Web Browser Interface is Web Browser. You can change the name in the Name field. See **Naming Conventions** (on page 274) 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. Enter authentication information: **Optional**.
 - To use a service account for authentication, select the Use Service Account Credentials checkbox. Select the service account to use in the Service Account Name menu.or
 - Enter a Username and Password for authentication. Type the username and password that will allow access to this interface.

Note: Do not enter authentication information 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. See **Tips for Adding a Web Browser Interface** (on page 89).

5. Type a description of this interface in the Description field. **Optional.**
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. See 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. Then you can add a Web Browser Interface that enables users to access the Dominion PX's Web-based administration application to the node.

▶ **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 saving changes to the Add Node or Node Profile screen, the name of the interface(s) also appears 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 and select the node with the interface you want to edit. The Node Profile page opens.
2. In the Interfaces tab, select the row of the interface you want to edit.
3. Click Edit.
4. Edit the fields as needed. See **Add an Interface** (on page 83) for field details. Some fields are read-only.
5. Click OK to save your changes.

Delete an Interface

You cannot delete a VMW Viewer interface or a VMW Power interface from a virtual machine node.

► **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.

Bookmarking an Interface

If you frequently access a node via a particular interface, you can bookmark it so that 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 the Enter key 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 appears in the Bookmark Name field. You can change the name, which will appear in your Favorites list in Internet Explorer.
5. Click OK. The Add Favorite window opens.
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.

► **To get bookmark URLs for all nodes:**

- You can get bookmark URLs for all nodes in the Node Asset Report. See **Node Asset Report** (on page 149).

Configuring Direct Port Access to a Node

You can configure Direct Port Access to a node using the Bookmark Node Interface feature.

See ***Bookmarking an Interface*** (on page 91).

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.

▶ **To bulk copy node categories and elements:**

1. Click the Nodes tab and select a node.
2. Choose 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.
 - Select the node in the Selected Nodes list and click the left arrow button to remove it from the list.
4. Click OK to bulk copy. A message appears when the node categories and elements have been copied.

Using 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.

Adding, Editing, and Deleting Node Groups

Node Groups Overview

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. See **Adding a Policy** (on page 111). Nodes can be grouped manually, using the Select method, or by creating a Boolean expression that describes a set of common attributes, using the Describe method.

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. See **Associations, Categories, and Elements** (on page 21) for details on creating categories and elements.

► To view node groups:

- Choose Associations > Node Groups. The Node Groups Manager window appears. A list of existing node groups is displayed on the left, while details about the selected node group appear 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 appear, 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. See **Users and User Groups** (on page 98).
 - 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 opens, 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 appears
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. See **Naming Conventions** (on page 274) 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.

Describe Method versus Select Method

Use the describe method when you want your group to be based on some attribute of the node or devices, such as the categories and elements. The advantage of the describe method is that when you add more devices or nodes with the same attributes as described, they will be pulled into the group automatically.

Use the select method when you just want to create a group of specific nodes manually. New nodes and devices added to CC-SG are not pulled into these groups automatically. You must manually add the new nodes or devices to the group after you add them to CC-SG.

These two methods cannot be combined.

Once a group is created with one method, you must edit it using the same method. Switching methods will overwrite the current group settings.

Select Nodes

► To add a node group with the Select Nodes option:

1. Click the Select Nodes tab.
2. Click the Device Name drop-down menu and select a device to filter the Available list to display only 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. To remove a node from the group, select the node name in the Selected list and 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, select the Create Full Access Policy For This Group checkbox.
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

► To add a node group with the Describe Nodes option:

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 appear 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.
 - 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 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 must create three rules. Department = Engineering (Rule0) Location = Philadelphia (Rule1) Memory = 1GB (Rule2). These rules must 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. Make this comparison first by enclosing it parentheses: (Rule0|Rule1). Since the devices 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 opens, 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, select the Create Full Access Policy For This Group checkbox.
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

► **To delete a node group:**

1. Choose Associations > Node Group. The Node Groups Manager window opens.
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.

You can also configure CC-SG to use external authentication. See **Remote Authentication** (on page 122).

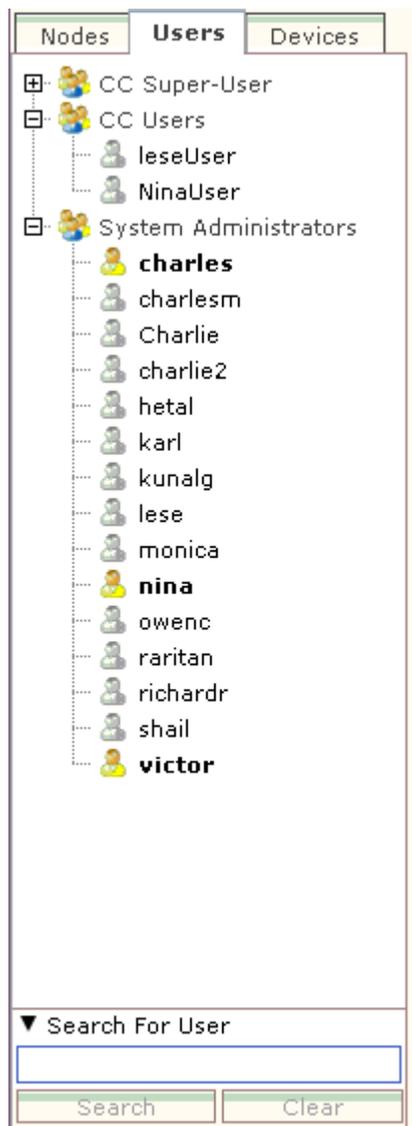
You must also create policies for access that you can assign to user groups. See **Policies for Access Control** (on page 110).

In This Chapter

The Users Tab	99
Default User Groups	100
Adding, Editing, and Deleting User Groups.....	101
Configuring Access Auditing for User Groups.....	103
Adding, Editing, and Deleting Users.....	104
Assigning a User to a Group	106
Deleting a User From a Group	107
Your User Profile	107
Logging Users Out.....	108
Bulk Copying Users	109

The Users Tab

Click the Users tab to display all user groups and users in CC-SG.



Users are nested underneath the user groups to which they belong. User groups with users assigned to them appear in the list with a + symbol next to them. Click the + to expand or collapse the list. 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 default user groups: 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 lowercase letter.
- Passwords must contain at least one uppercase 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.

Adding, Editing, and Deleting User Groups

Add a User Group

Creating user groups first will help you organize users when the users 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. See **User Group Privileges** (on page 253).

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. See **Naming Conventions** (on page 274) for details on CC-SG's rules for name lengths.
3. Type a short description for the group in the Description field.
Optional.
4. Click the Privileges tab.
5. Select the checkbox that corresponds with 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. Select 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. See **Policies for Access Control** (on page 110) for details 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. 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. **Optional.**
 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 user group:**

1. Click the Users tab.
2. Click the user group in the Users tab. The User Group Profile appears.
3. Type a new name for the user group in the User Group Name field. **Optional.**
4. Type a new description for the user group in the Description field. **Optional.**
5. Click the Privileges tab.
6. Select the checkbox that corresponds to each privilege you want to assign to the user group. Deselect 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 click Remove.
12. Click OK to save your changes.

Delete a User Group

You can delete a user group if it does not have any members.

► **To delete a User Group:**

1. Click the Users tab.
2. Click the user group you want to delete.
3. Choose Users > User Group Manager > Delete User Group.
4. Click OK to delete the User Group.

Configuring Access Auditing for User Groups

You can require members of a user group to enter the reason why they are accessing the node before access is permitted. A dialog will appear to all users in the user groups you select. Users must enter the reason for access before the node connection is made. This feature applies to all types of access with all interface types, including power control.

The reasons for access are logged in the Audit Trail and in the Node Profile's Auditing tab.

► **To configure access auditing for user groups:**

1. Choose Users > Node Auditing.
2. Select the Require Users to Enter Access Information When Connecting to a Node checkbox.
3. In the Message to Users field, enter a message that users will see when attempting to access a node. A default message is provided. 256 character maximum.
4. Move the user groups to enable access auditing for the group into the Selected list by clicking the arrow buttons. Use Ctrl+click to select multiple items.

*Tip: Type the name of a user group in the Find field to highlight it in the list. Type * after a partial name to highlight all similar names in the list.*

Click the column headers to sort the lists alphabetically.

5. Click Update.

Adding, Editing, and Deleting Users

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. See **Naming Conventions** (on page 274) for details on CC-SG's rules for name lengths.
4. Select the Login Enabled checkbox if you want the user to be able to log in to CC-SG.
5. Select the Check Remote Authentication checkbox 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: See **Naming Conventions** (on page 274) 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. See **Advanced Administration** (on page 164) for details on strong passwords.*

7. Select the Force Password Change on Next Login checkbox to force the user to change the assigned password the next time they log in.
8. Select the Force Password Change Periodically checkbox to specify how often the user will be forced to change their password.
9. If selected, 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. In the Telephone Number field, type the user's telephone number.

12. Click the User Groups drop-down menu and select the group to which the user will be added.
13. 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. See **Assigning a User to a Group** (on page 106).

► **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. Deselect the Login enabled checkbox to prevent this user from logging into CC-SG. Select the Login enabled checkbox to allow this user to log into CC-SG.
3. Select the Remote Authentication only checkbox 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. See **Advanced Administration** (on page 164) for details on strong passwords.*

5. Select the Force Password Change on Next Login checkbox 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. See ***Deleting a User From a Group*** (on page 107) 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.

Assigning a User to a Group

Use this command to assign an existing user to another group. Users assigned in this way will be added to the 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 to which you want to assign a users.
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.
 - Select the users you want to remove from the Users in group list, and then click the < button to remove them.
 - 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.

Deleting 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 belongs to only 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 the 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

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 CC Super User 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 the Change Password (For Local Authentication Only) checkbox.
3. Type your current password in the Old Password field.
4. Type your new password in the New Password field. A message 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.

Logging Users Out

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 log out of 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 log out 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 Copying 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 receiving the affiliations have existing group affiliations, the existing 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 the 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 to the Selected Users list.
 - Select the user in the Selected Users list, and then click < to remove the user.
 - Click << to remove all users from the Users in group list.
 4. Click OK to copy.

Chapter 10 Policies for Access Control

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. See **Assigning Policies To User Groups** (on page 114).

CC-SG 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. See **Configuring CC-SG with Guided Setup** (on page 13).

► To control access using policies:

- Create Node Groups to organize the nodes you want to create access rules for. See **Add a Node Group** (on page 94).
- Create Device Groups to organize the devices you want to create access rules for. See **Add a Device Group** (on page 50).
- Create a policy for a node or device group specifying when access to that node or device group can occur. See **Adding a Policy** (on page 111).
- Apply the policy to a user group. See **Assigning Policies To User Groups** (on page 114).

In This Chapter

Adding a Policy	111
Editing a Policy	112
Deleting a Policy	113
Support for Virtual Media	114
Assigning Policies To User Groups	114

Adding 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. See **Connection Modes: Direct and Proxy** (on page 176).*

► **To add a policy:**

1. Choose Associations > Policies. The Policy Manager window opens.
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. See **Naming Conventions** (on page 274) 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 to which this policy governs access.
6. Click the Node Group drop-down arrow and select the Node Group to which this policy governs access.
7. If the policy will cover only one type of group, select a value only for that type.
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. Select 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.

Editing a Policy

When you edit a policy, the changes do not affect users who are currently logged into CC-SG. The changes will go into effect at the next login.

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 out of CC-SG until you exit Maintenance Mode, when users can log in again. See **Maintenance Mode** (on page 153).

► **To edit a policy:**

1. On the Associations menu, click Policies. The Policy Manager window opens.
2. Click the Policy Name drop-down arrow, and then select the policy you want to edit from the list.
3. To edit the name of the policy, click Edit. An Edit Policy window opens. Type a new name for the policy in the field, and then click OK to change the name of the policy. **Optional.**
4. Click the Device Group drop-down arrow, and select the Device Group to which this policy governs access.
5. Click the Node Group drop-down arrow and select the Node Group to which this policy governs access.
6. If the policy will cover only one type of group, select a value only 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. Select 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.

Deleting a Policy

You can delete a policy that is no longer needed.

► **To delete a policy:**

1. Choose Associations > Policies. The Policy Manager window opens.
2. Click the Policy Name drop-down arrow, and then select the policy you want to delete.
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 KX2, KSX2, and KX2-101 devices. For detailed instructions on accessing virtual media with your device, see:

- **Dominion KX II User Guide**
- **Dominion KSX II User Guide**
- **Dominion KXII-101 User Guide**

See **Adding a Policy** (on page 111) for details on creating policies to assign virtual media permission to user groups in CC-SG.

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. See **Users and User Groups** (on page 98) 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.....	115
Using Custom Views in the Admin Client.....	116

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 appear 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 appear 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 appear 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

► **To add a custom view for nodes:**

1. Click the Nodes tab.
2. Choose Nodes > Change View > Create Custom View. The Custom View screen appears.
3. In the Custom View panel, click Add. The Add Custom View window opens.
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. In the Available list, select the item you want to include in the custom view, and then click Add to add the item to the list. Repeat this step to add as many items as you want.
 - b. Arrange the items in the Selected list in the order you would like each grouping to display in the Nodes tab. Select an item and click the up and down arrow buttons to move the item into the desired sequence.
 - c. If you must remove an item from the list, select it and click Remove.
8. Click Save. A message confirms that the custom view has been added.
9. To apply the new custom view, click Set Current.

Apply a Custom View for Nodes

► **To apply a custom view to the nodes list:**

1. Choose Nodes > Change View > 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.

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. Choose Nodes > 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

► To change a custom view's name:

1. In the Custom View panel, click Edit. The Edit Custom View window opens.
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. In the Available list, select the item you want to include in the custom view, and then click Add to add the item to the list. Repeat this step to add as many items as you want.
 - b. Arrange the items in the Selected list in the order you would like each grouping to display in the Nodes tab. Select an item and click the up and down arrow buttons to move the item into the desired sequence.
 - c. If you must remove an item from the list, select it and click Remove.
2. Click Save. A message confirms that the custom view has been added.
3. To apply the new custom view, click Set Current.

Delete a Custom View for Nodes

► To delete a custom view for nodes:

1. Click the Nodes tab.

2. Choose Nodes > 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.

Assign a Default Custom View for Nodes

► **To assign a default custom view for nodes:**

1. Click the Nodes tab.
2. Choose Nodes > 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 log in, 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.

► **To assign a default custom view of nodes 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. Select the System Wide checkbox, and then click Save.

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

Custom Views for Devices

Add a Custom View for Devices

► **To add a custom view for devices:**

1. Click the Devices tab.

2. Choose Devices > Change View > 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. In the Available list, select the item you want to include in the custom view, and then click Add to add the item to the list. Repeat this step to add as many items as you want.
 - b. Arrange the items in the Selected list in the order you would like each grouping to display in the Nodes tab. Select an item and click the up and down arrow buttons to move the item into the desired sequence.
 - c. If you must remove an item from the list, select it and click Remove.
8. Click Save. A message confirms that the custom view has been added.
9. To apply the new custom view, click Set Current.

Apply a Custom View for Devices

► **To apply a custom view to the devices list:**

1. Choose Devices > Change View > 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. 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.

► To change a custom view's name:

1. In the Custom View panel, click Edit. The Edit Custom View window opens.
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. In the Available list, select the item you want to include in the custom view, and then click Add to add the item to the list. Repeat this step to add as many items as you want.
 - b. Arrange the items in the Selected list in the order you would like each grouping to display in the Nodes tab. Select an item and click the up and down arrow buttons to move the item into the desired sequence.
 - c. If you must remove an item from the list, select it and click Remove.
2. Click Save. A message confirms that the custom view has been added.
3. To apply the new custom view, click Set Current.

Delete a Custom View for Devices

► To 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.

Assign a Default Custom View for Devices

► **To 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.

► **To assign a default custom view of devices 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. Select the System Wide checkbox, and then click Save.

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

Chapter 12 Remote Authentication

In This Chapter

Authentication and Authorization (AA) Overview	122
Distinguished Names for LDAP and AD	123
Specifying Modules for Authentication and Authorization	124
Establishing Order of External AA Servers	124
AD and CC-SG Overview	125
Adding an AD Module to CC-SG	125
Editing an AD Module	130
Importing AD User Groups	130
Synchronizing AD with CC-SG	131
About LDAP and CC-SG	134
Add an LDAP (Netscape) Module to CC-SG	134
About TACACS+ and CC-SG	137
Add a TACACS+ Module	137
About RADIUS and CC-SG	138
Add a RADIUS Module	138

Authentication and Authorization (AA) Overview

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.

LDAP implementations use LDAP v3.

Flow for Authentication

When remote authentication is enabled, authentication and authorization follow these steps:

1. The user logs into CC-SG with the appropriate username and password.
2. CC-SG connects to the external server and sends the username and password.

3. Username 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 username entered matches a group that has been created in CC-SG or imported from AD, and grants privileges according to 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. See **Users and User Groups** (on page 98) for details on adding users who will be remotely authenticated.

Note: If remote authentication is used, users must 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 usernames 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.

Specify 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)

Specify 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)

Specify 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.

Specify 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.

Specifying Modules for Authentication and Authorization

Once you have added all the external servers as modules in CC-SG, 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. Click the Authentication tab. All configured external Authorization and Authentication Servers appear 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.

Establishing 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. Click the Authentication tab. All configured external Authorization and Authentication Servers appear 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.

AD and CC-SG Overview

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.

Do not add duplicate AD modules. If your users see a message that says "You are not a member of any group" when attempting to login, you may have configured duplicate AD modules. Check the modules you have configured to see if they describe overlapping domain areas.

Adding 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. See *Configuring the CC-SG Network* (on page 168).

► **To add an AD 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 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 must add the information that allows CC-SG to query the AD server.

Do not add duplicate AD modules. If your users see a message that says "You are not a member of any group" when attempting to login, you may have configured duplicate AD modules. Check the modules you have configured to see if they describe overlapping domain areas.

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 select the Use default CC-SG DNS checkbox to use the DNS configured in the Configuration Manager section of CC-SG. See **Advanced Administration** (on page 164).
3. Select the Anonymous Bind checkbox 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 depends 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. Maximum length is 32 characters.
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. Select the Secure Connection for LDAP checkbox 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 the Filter field 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.

- Select the Use Bind checkbox 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.

- Select the Use Bind After Search checkbox 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
<code>dc=raritan,dc=com</code>	The search query for the user in the group will be made over the whole directory structure.
<code>cn=Administrators,cn=Users,dc=raritan,dc=com</code>	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 the Filter field 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.
 - Outgoing: information will be trusted going to the selected domain.
 - 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. Select the Authentication checkbox if you want CC-SG to use the AD module for authentication of users. Select the Authorization checkbox if you want CC-SG to use the AD module for authorization of users.
5. Click Update to save your changes.

Editing 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. Click the Authentication tab. All configured external Authorization and Authentication Servers appear 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. See **AD General Settings** (on page 126), **AD Advanced Settings** (on page 127), **AD Group Settings** (on page 128), and **AD Trust Settings** (on page 129).
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. See **Synchronize All User Groups with AD** (on page 132) and **Synchronize All AD Modules** (on page 133).

Importing AD User Groups

You must specify Group settings in the AD module before you can import groups from the AD server. See **AD Group Settings** (on page 128).

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. See **Synchronize All User Group with AD** (see "Synchronize All User Groups with AD" on page 132) and **Synchronize All AD Modules** (on page 133).

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. See **Advanced Administration** (on page 164).*

► **To import AD user groups:**

1. Choose Administration > Security.

2. Click the Authentication tab. All configured Authorization and Authentication Servers appear 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.

Synchronizing AD with CC-SG

There are several methods for synchronizing the information on CC-SG with the information on 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. See **Synchronize All AD Modules** (on page 133). This synchronization is necessary only when you are using AD for authorization.
- On Demand Synchronization: You can perform two types of synchronization whenever you choose:
 1. **All Active Directory Modules:** 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 necessary only when you are using AD for authorization. See **Synchronize All AD Modules** (on page 133).

2. **All User Groups:** 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 by running the on-demand synchronization of all modules, to update access information. See **Synchronize All User Groups with AD** (on page 132).

Synchronize All User Groups with AD

You should synchronize all user groups if you have made a change to a user group, such as moving a user group from one AD module to another. (You can also change the AD association of a user group manually, in the User Group Profile's Active Directory Associations tab.)

If you have made changes to users or domain controllers, you should synchronize all AD modules. See **Synchronize All AD Modules** (on page 133).

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. Choose Administration > Security.
2. Click the Authentication tab. All configured Authorization and Authentication Servers appear in a table.
3. Select the AD server whose user groups you want to synchronize with the user groups in CC-SG.
4. In the On Demand Synchronization list, select All User Groups, then click the arrow button.
5. 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 then click OK.

A confirmation message appears when all imported user groups in the selected module have been successfully synchronized.

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. Choose Administration > Security.
2. Click the Authentication tab. All configured Authorization and Authentication Servers appear in a table.
3. 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.

Enable or Disable Daily Synchronization of All AD Modules

► **To enable daily synchronization of all AD modules:**

1. Choose Administration > Security.
2. Click the Authentication tab. All configured Authorization and Authentication Servers appear 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. Click the Authentication tab. All configured Authorization and Authentication Servers appear in a table.
3. Deselect 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. Select the Authentication tab. Ensure that the Daily synchronization of All Modules checkbox is selected.
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. See **Terminology/Acronyms** (on page 2) for hostname rules.
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=Netscape Root. Separate the values with commas but do not use spaces before or after the comma. The values can include spaces, for example, 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. Select the Use bind after search checkbox 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>

Parameter Name	Open LDAP Parameters
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 must 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. See *Users and User Groups* (on page 98).

Add a TACACS+ Module

► **To 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. See *Terminology/Acronyms* (on page 2) for hostname rules.
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. Maximum length is 128 characters.

5. Click OK to save your changes. The new TACACS+ module appears in the Security Manager screen under External AA Servers.
6. Select 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 must 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. See **Users and User Groups** (on page 98).

Add a RADIUS Module

► **To 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. See **Terminology/Acronyms** (on page 2) for hostname rules.
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. Select 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, users logs into CC-SG by first typing their usernames in the Username field, then typing their fixed passwords, and then the dynamic token value in the Password field.

Configuration of CC-SG is identical to standard RADIUS remote authentication described above. See ***Two-Factor Authentication (on page 264)***.

Chapter 13 Reports

In This Chapter

Using Reports.....	140
Audit Trail Report.....	142
Error Log Report.....	143
Access Report.....	144
Availability Report.....	145
Active Users Report.....	145
Locked Out Users Report.....	145
All Users Data Report.....	146
User Group Data Report.....	146
Device Asset Report.....	147
Device Group Data Report.....	147
Query Port Report.....	147
Node Asset Report.....	149
Active Nodes Report.....	150
Node Creation Report.....	150
Node Group Data Report.....	150
AD User Group Report.....	151
Scheduled Reports.....	151
Upgrade Device Firmware Report.....	152
CC-NOC Synchronization Report.....	152

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 the Enter key 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

There are two printing options in CC-SG. You can print a report page as it appears in your screen (print a screenshot), or you can print a full report, including all details for each item.

Note: Printing options work for all CC-SG pages.

▶ **To print a screenshot of a report:**

1. Generate the report you want to print.
2. Choose Secure Gateway > Print Screen.

▶ **To print all report details:**

1. Generate the report you want to print. Make sure to select All in the Entries to Display field.
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 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 data that appears in the Audit Trail and Error Log reports. Purging these reports deletes all data that satisfy the search criteria used. For example, if you search for all Audit Trail entries from March 26, 2008 through March 27, 2008, only those records will be purged. Entries earlier than March 26 or later than March 27 will remain in the Audit Trail.

Purged data is removed from CC-SG permanently.

► **To purge a report's data from CC-SG:**

1. Generate the report whose data you want to delete from CC-SG.
2. Click Purge.
3. Click Yes to confirm.

Hide or Show 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 hide or show 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 into CC-SG
- When a user logs out of 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 Time and End Date and Time fields. Click each component of the default date (month, day, year, hour, minute) to select it 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 Type, Message, Username, and User IP address fields. Wildcards are accepted in these fields.
 - To limit the report to a type of message, select a type in the Message Type field.
 - 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. In the Entries to Display field, select the number of entries to display in the report screen.
5. Click Apply to generate the report.
 - To purge the records in the report, click Purge. See ***Purge a report's data from CC-SG*** (on page 142).

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 Time and End Date and Time fields. Click each component of the default date (month, day, year, hour, minute) to select it 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. In the Entries to Display field, select the number of entries to display in the report screen.
 5. Click Apply to generate the report.
 - Click **Purge** (see "Purge a Report's Data From CC-SG" on page 142) to delete the Error Log. See **Purge a Report's Data from CC-SG** (on page 142)

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 Devices or Nodes.
3. Set the date and time range for the report in the Start Date and Time and End Date and Time fields. Click each component of the default date (month, day, year, hour, minute) to select it 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(s) field.
 - To limit the report to a particular node, type the port name in the Node name(s) field.
 - To limit the report to a particular user's activities, type the user's username in the Username(s) field.
 - To limit the report to a particular IP address's activities, type the user's IP address in the IP address(es) 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.

▶ **To generate the Availability Report:**

1. Choose Reports > Availability Report.
2. Select Nodes or Devices.
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 the report. See **Lockout settings** (on page 187).

▶ **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 you want to unlock then click Unlock User.

All Users Data Report

The User Data report displays certain data on all users in the CC-SG database.

▶ **To generate the All Users Data report:**

- Choose Reports > Users > All User Data.
 - The User Name field displays the user names of all CC-SG users.
 - 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 option is selected in the User Profile. See **Add a User** (on page 104).
 - The Password Expiration field displays the number of days that the user can use the same password before being forced to change it. See **Add a User** (on page 104).
 - The Groups field displays the user groups to which the user belongs.
 - The Privileges field displays the CC-SG privileges assigned to the user. See **User Group Privileges** (on page 253).
 - 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.

User Group Data Report

The User Group Data report displays data on users and the groups with which they are associated.

▶ **To generate the User Group Data report:**

1. Choose Reports > Users > User Group Data.
2. Double-click the User Group to view the assigned policies.

Device Asset Report

The Device Asset report displays data on devices currently managed by CC-SG.

▶ **To generate the Device Asset report:**

- Choose Reports > Devices > Device Asset Report. The report is generated for all devices.

▶ **To filter the report data by device type:**

- Select a device type then click Apply. The report is generated again with the selected filter applied.
 - Devices whose versions do not comply with the Compatibility Matrix will appear in red text in the Device Name field.

Device Group Data Report

The Device Group Data report displays device group information.

▶ **To generate the Device Group Data report:**

1. Choose Reports > Users > Device Group Data.
2. Double-click a row to display the list of devices in the group.

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	

State Type	Port State	Definition
	Down	Connection to port is not possible since the device is down and unavailable.
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. 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). See Raritan's **Paragon II User Guide**. **Optional**.
4. Select Paused Ports or Locked Ports to include ports that are paused or locked. Paused ports occur when a CC-SG management of a device is paused. Locked ports occur when a device is being upgraded. **Optional**.
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.

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 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, select a parameter from corresponding menu.
 - If you select Devices, select the devices in the Available list whose node assets you want to include in the report then click Add to move them to the Selected list.
3. Click Apply to generate the report. The Node Asset Report generates.

▶ **To get bookmark URLs for nodes:**

1. Generate the Node Asset report then double-click a node to view the details dialog.
2. Click Save to File. All report information is saved to a .csv file.
3. The URL column contains direct links to each node. You can use this information to create a web page with links to each node, instead of bookmarking each node individually. See ***Bookmarking an Interface*** (on page 91).

Active Nodes Report

The Active Nodes report includes the name and type of each active interface, the connection mode, the associated device, a timestamp, the current user, 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:**

- Choose Reports > Nodes > Active Nodes. The Active Nodes report generates if there are currently active nodes.

▶ **To disconnect a node from an active session:**

- In the Active Nodes report, select the node you want to disconnect 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. Select All Nodes or Potential Duplicates. Potential Duplicates limits the report to only those nodes that have been flagged as potential duplicates.
3. If you selected All Nodes, set the date range for the report in the Start Date and Time and End Date and Time fields. Click each component of the default date (month, day, year, hour, minute) to select it then click the up and down arrows to reach the desired number.
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

Node Group Data Report

The Node Group Data report displays node group information.

▶ **To generate the Node Group Data report:**

1. Choose Reports > Users > Node Group Data.

2. Double-click a row to display the list of nodes in the group.

AD User Group Report

The AD Users Group report displays all users in groups that were imported into CC-SG from AD servers that have been configured for both authentication and authorization. The report does not include users who were added to the AD user groups locally via CC-SG.

► **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. Select the checkbox that corresponds to each AD server you want 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 then click Add to move the user groups to the Selected list.
4. Click Apply to generate the report.

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. Scheduled reports can be viewed in HTML format only. See **Task Manager** (on page 196).

► **To access scheduled reports:**

1. Choose Reports > Scheduled Reports.
2. Select a Report Type.
3. Select a Report Owner.
4. 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.
5. Set the date range for the report in the Start Date and Time and End Date and Time fields. Click each component of the default date (month, day, year, hour, minute) to select it then click the up and down arrows to reach the desired number.
6. Click Apply. The list of scheduled reports is generated.

► **To view a scheduled report:**

1. Select the report in the list.
2. Click View Report.

► **To delete a scheduled report:**

1. Select the reports you want to delete. Use Ctrl+click and Shift+click to select multiple reports.
2. Click Delete Reports.
3. Click Yes to confirm.

Upgrade Device Firmware Report

The Upgrade Device Firmware report is located 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.

See **Scheduled Reports** (on page 151) for details on viewing the report.

CC-NOC Synchronization Report

The CC-NOC Synchronization report lists all targets and their IP addresses that the CC-SG subscribes to and that are monitored by a CC-NOC on a particular discovery date. Any new targets that are discovered in the configured range are displayed here as well. See **Add a CC-NOC (on page 202)**. You can 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 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 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	153
Entering Maintenance Mode.....	153
Exiting Maintenance Mode	154
Backing Up CC-SG.....	154
Saving and Deleting Backup Files.....	155
Restoring CC-SG.....	156
Resetting CC-SG	157
Restarting CC-SG.....	159
Upgrading CC-SG	160
CC-SG Shutdown	162
Restarting CC-SG after Shutdown	162
Powering Down CC-SG.....	163
Ending CC-SG Session	163

Maintenance Mode

Maintenance mode restricts access to CC-SG so that an administrator can perform various operations, such as upgrading CC-SG, without disruption.

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 available only on standalone CC-SG units that are not in cluster configurations. 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. See **Task Manager** (on page 196). When CC-SG exits Maintenance Mode, scheduled tasks will be executed as soon as possible.

Entering Maintenance Mode

1. Choose System Maintenance > Maintenance Mode > Enter Maintenance Mode.
2. Password: Type your password. Only users with the CC Setup and Control privilege can enter maintenance mode.

3. Broadcast message: Type the message that will display to users who will be logged out of CC-SG.
4. 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.
5. Click OK.
6. Click OK in the confirmation dialog box.

Exiting Maintenance Mode

1. Choose System Maintenance > Maintenance Mode > Exit Maintenance Mode.
2. Click OK to exit Maintenance Mode.
3. A message appears when CC-SG has exited Maintenance Mode. All users will now be able to access CC-SG normally.

Backing Up 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.

► **To backup CC-SG:**

1. Choose System Maintenance > Backup.
2. Type a name for this backup in the Backup Name field.
3. Type a short description for the backup in the Description field.
Optional.
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. Select 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 backup files.
 - Standard - Creates a backup of only critical data on CC-SG. This backup includes CC-SG configuration information, Device and Node configurations, and User configurations. This produces the smallest backup files.
5. To save a copy of this backup file to an external server, select the Backup to Remote Location checkbox. **Optional.**
 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 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. See **Restoring CC-SG** (on page 156).

Saving and Deleting Backup Files

Use the Restore CommandCenter screen to save and delete backups stored on CC-SG. 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 do not need saves space on the CC-SG.

Save a Backup File

1. Choose System Maintenance > Restore Command Center.
2. In 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 to copy the backup file to the specified location.

Delete a Backup File

1. In 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.

Restoring CC-SG

You can restore CC-SG using a backup file that you created.

► **To restore CC-SG:**

1. Choose System Maintenance > Restore. The Restore CommandCenter screen appears, displaying a list of backup files available to CC-SG. You can see 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. 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. **Optional.**
 - a. Click Upload.
 - 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 backup file appears in the Available Backups table.
3. Select the backup file 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 - Restores only 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. Select 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 (min.)" field. This gives users time to complete their work and log out.
 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 before restoring its configuration from the selected backup. When the restore occurs, all other users are logged out.

Resetting CC-SG

You can reset CC-SG to purge the database or to reset other components to their factory default settings. You should perform a backup and save the backup file to another location before using any reset options.

It is recommended to use the default options selected.

Option	Description
Full Database	<p>This option removes the existing CC-SG database and builds a new version with the factory default values. Network settings, SNMP settings, firmware, and diagnostic console settings are not part of the CC-SG database.</p> <p>IP-ACL settings are reset with a Full Database reset whether you select the IP ACL Tables option or not.</p> <p>When the database is removed, all devices, nodes, and users are removed. All remote authentication and authorization servers are removed.</p> <p>Your CC Super User account will be reset to default. After the reset operation is complete, you must login with the default username and password admin/raritan.</p>

Option	Description
Attempt to Save Personality Settings	<p>This option is enabled when you select Full CC-SG Database Reset.</p> <p>As the CC-SG database is rebuilt, some previously configured options are saved.</p> <ul style="list-style-type: none"> ▪ Secure Communication between PC Clients and CC-SG. ▪ Enforce Strong Passwords. ▪ Direct vs. Proxy Connections to Out-of-Band nodes. ▪ Inactivity Timer setting.
Network Settings	<p>This option changes the network settings back to factory defaults.</p> <ul style="list-style-type: none"> ▪ 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 Configuration	<p>This option resets the SNMP settings back to factory defaults.</p> <ul style="list-style-type: none"> ▪ Port: 161 ▪ Read-only Community: public ▪ Read-write Community: private ▪ System Contact, Name, Location: none ▪ SNMP Trap Configuration ▪ SNMP Trap Destinations
Default Firmware	<p>This option resets all device firmware files to factory defaults. This option does not change the CC-SG database.</p>
Upload Firmware to DB After Reset	<p>This option loads the firmware files for the current CC-SG version into the CC-SG database.</p>
Diagnostic Console	<p>This option restores Diagnostic Console settings back to factory defaults.</p>
IP-ACL Tables	<p>This option removes all entries from the IP-ACL table.</p> <p>IP-ACL settings are reset with a Full Database reset whether you select the IP ACL Tables option or not.</p>

► **To reset CC-SG:**

1. Before you reset, back up CC-SG and save the backup file to a remote location. See **Backing Up CC-SG** (on page 154).
2. Choose System Maintenance > Reset.
3. Select the reset options.
4. Type your CC-SG password.
5. Broadcast message: Type the message that will display to users who will be logged off CC-SG.
6. Enter the number of minutes (from 0-720) that should elapse before CC-SG performs the reset operation.
7. Click OK. A message appears to confirm the reset.

Restarting 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.

Upgrading 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.

CC-SG version 4.0 is not compatible with G1 hardware. Do not upgrade a CC-SG G1 unit to version 4.0.

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

Only users with the CC Setup and Control privilege can upgrade CC-SG.

You should back up CC-SG before upgrading.

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

CC-SG will reboot as part of the upgrade process. 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. Log into the CC-SG Admin Client using an account that has the CC Setup and Control privilege.
3. Enter Maintenance Mode. See **Entering Maintenance Mode** (on page 153).
4. Once CC-SG is in maintenance mode, choose System Maintenance > Upgrade.
5. Click Browse. Navigate to and select the CC-SG firmware file (.zip) then click Open.
6. Click OK to upload the firmware file to CC-SG.

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

7. Click OK to exit CC-SG.
8. Clear the browser cache, then close the browser window. See **Clear the Browser's Cache** (on page 161).
9. Clear the Java cache. See **Clear the Java Cache** (on page 162).

10. You must wait for the upgrade to complete before logging into CC-SG again. You can monitor the upgrade in the Diagnostic Console.
 - a. Access Diagnostic Console using the admin account. See **Access Administrator Console** (on page 219).
 - b. Choose Admin > System Logfile Viewer. Select sg/upgrade.log then choose View to view the upgrade log.
 - c. Wait for the upgrade process to run. The upgrade process is complete when you see the "Upgrade completed" message in the upgrade log.
 - d. The server must reboot. The reboot process begins when you see the "Linux reboot" message in the upgrade.log. The server will shut down and reboot.
11. Wait a few minutes while CC-SG reboots, then launch a new web browser window.
12. Log into the CC-SG Admin Client using an account that has the CC Setup and Control privilege.
13. 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.
14. Exit Maintenance Mode. See **Exiting Maintenance Mode** (on page 154).
15. Back up the CC-SG. See **Backing Up CC-SG** (on page 154).

Clear the Browser's Cache

These instructions may vary slightly for different browser versions.

► **To clear the browser cache in Internet Explorer 6.0:**

1. Choose Tools > Internet Options.
2. On the General tab, click Delete Files then click OK to confirm.

► **In FireFox 2.0:**

1. Choose Tools > Clear Private Data.
2. Make sure Cache is selected then click Clear Private Data Now.

Clear the Java Cache

These instructions may vary slightly for different Java versions and different operating systems.

▶ **In Windows XP with Java 1.6:**

1. Choose Control Panel > Java.
2. On the General tab, click Settings.
3. In the dialog box that opens, click Delete Files.
4. Make sure the Applications and Applets checkbox is selected then click OK.

CC-SG Shutdown

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 shut down 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. See **Diagnostic Console** (on page 216).
- Recycle the power to your CC-SG unit.

Powering 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.
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.

Ending CC-SG Session

There are two ways to end a CC-SG Session.

- Log out to end your session while keeping the client window open. See **Log Out of CC-SG** (on page 163).
- Exit to end your session and close the client window. See **Exit CC-SG** (on page 163).

Log Out of CC-SG

1. Choose Secure Gateway > Logout. The Logout window opens.
2. Click Yes to log out of CC-SG. Once you log out, the CC-SG login window opens.

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	164
Configuring Applications for Accessing Nodes	165
Configuring Default Applications	167
Managing Device Firmware.....	168
Configuring the CC-SG Network	168
Configuring Logging Activity	174
Configuring the CC-SG Server Time and Date	175
Connection Modes: Direct and Proxy	176
Device Settings.....	177
Configuring Custom JRE Settings.....	178
Configuring SNMP.....	179
Configuring CC-SG Clusters	181
Security Manager	184
Notification Manager.....	195
Task Manager.....	196
CommandCenter NOC	202
SSH Access to CC-SG	205
Serial Admin Port.....	213
Finding Your CC-SG Serial Number	213
Web Services API.....	214

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. Select the Display Message of the Day for All Users checkbox if you want the message to be displayed to all users after they log in.
Optional.
3. Select the Message of the Day Content checkbox if you want to type a message in CC-SG, or select the Message of the Day File checkbox 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 for the message text.

- c. Click the Font Size drop-down menu and select a font size for the message text.
 - 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 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.

Checking and Upgrading Application Versions

Check and upgrade the CC-SG applications, including 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, see the Compatibility Matrix on the Raritan Support website.

The best practice is to enter Maintenance Mode before upgrading applications. See **Entering Maintenance Mode** (on page 153).

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. See **Add an Application** (on page 166).
3. Click Browse, locate and select the application upgrade file from the dialog that appears 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.

Note: Users who were logged in during the upgrade must log out of CC-SG then log in again to ensure that the new version of the application is launched.

Add an Application

When you add an application to CC-SG, you must specify which device types function with the application. If a device provides both KVM and serial access, the device is listed twice, once for each method.

► **To add an application:**

1. Choose Administration > Applications.
2. Click Add. The Add Applications dialog window opens.
3. Type a name for the application in the Application name field.
4. Select the Raritan devices with which the application will function from the Available list 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 then click Remove.
5. Click OK. An Open dialog appears.
6. Navigate to and select the application file (usually a .jar or .cab file), and then click Open.
7. The selected application loads onto CC-SG.

Delete an Application

► **To 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

► **To 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

► **To 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. See ***Upgrading a Device*** (on page 41).

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.

▶ **To upload firmware to CC-SG:**

1. Choose Administration > Firmware.
2. Click Add to add a new firmware file. A search window opens.
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

▶ **To 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 170)
- **Active/Active mode:** See *What is Active/Active mode?* (on page 172)

CC-SG also allows either Static or DHCP-assigned IP addresses. See **Recommended DHCP Configurations for CC-SG** (on page 174) for best practices on using DHCP with your CC-SG.

About CC-SG LAN Ports

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.

See the tables below to check the locations of the Primary and Secondary LAN ports on your CC-SG model.

► 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

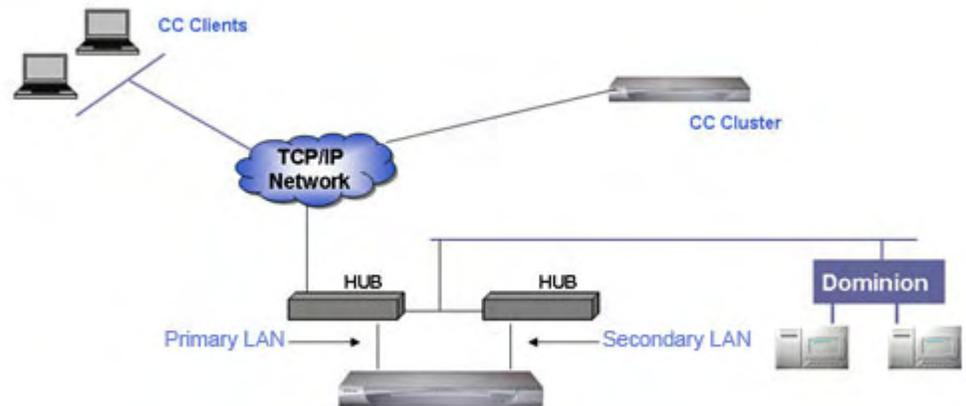
► E1 LAN Ports:

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.

See **About CC-SG LAN Ports** (on page 169) 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.
- You can attach each LAN port to a different switch or hub on the same subnetwork for reliability. **Optional.**

► 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. See **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.
- See **Recommended DHCP Configurations for CC-SG** (on page 174).

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. If your switch uses 1 Gig line speed, select Auto.
 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 later. See **Restarting CC-SG** (on page 159).
 - 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.

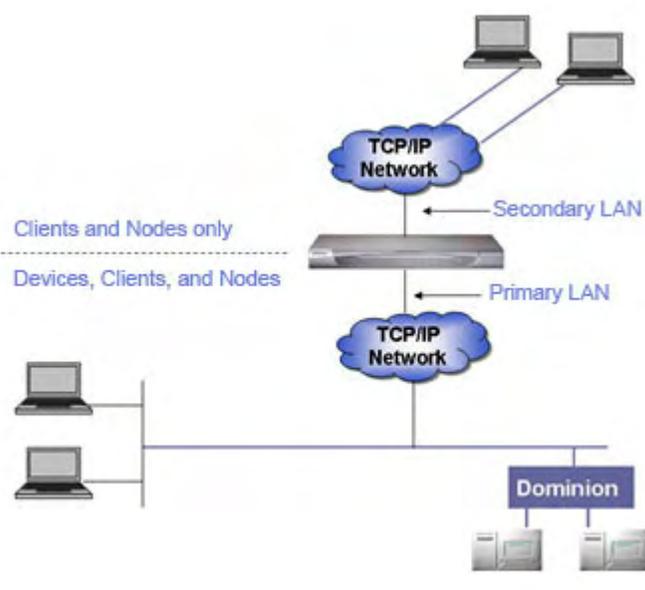
Note: If CC-SG is configured with DHCP, you can access CC-SG via the hostname after a successful registration with the DNS server.

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 will not have access.

See **About CC-SG LAN Ports** (on page 169) 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 if needed. See **Edit Static Routes** (on page 224).

► 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. See **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.
- See **Recommended DHCP Configurations for CC-SG** (on page 174).

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. If your switch uses 1 Gig line speed, select Auto.
 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 and 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.

Purge 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. See **Purge a report's data from CC-SG** (on page 142).*

► **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. See *Task Manager* (on page 196). 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.
 - a. To set the date and time via NTP: Select 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 to 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.

Connection Modes: Direct and Proxy

About Connection Modes

CC-SG offers three connection modes for in-band and out-of-band connections: Direct, Proxy, and Both.

- 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 need to keep only the CC-SG TCP ports (80, 443, and 2400) open in your firewall. Proxy mode does not use SSL between CC-SG and the KXII device for KVM data, when AES is enabled in the KXII device.
- 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.

Configure Direct Mode for All Client Connections

► **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.

Configure Proxy Mode for All Client Connections

► **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.

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.

► **To configure a combination of direct mode and proxy mode:**

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

You can configure some settings that apply to all devices, and configure each device type's default port number.

► **To configure default port number for devices:**

1. Choose Administration > Configuration.
2. Click the Device Settings tab.
3. Select a Device Type in the table and double-click the Default Port value.
4. Type the new Default Port value.
5. Click Update Configuration to save your changes.

► **To configure timeout duration for devices:**

1. Choose Administration > Configuration.
2. Click the Device Settings tab.

3. Type a new timeout duration in the Heartbeat (sec) field. The valid range is 30 seconds to 50,000 seconds.
4. Click Update Configuration to save your changes.

► **To enable or disable a warning message for all power operations:**

Select the Display Warning Message For All Power Operations checkbox to enable a warning message that alerts a user before a requested power operation occurs. Only the user who initiated the power operation sees the message. The user can cancel the power operation or confirm it by clicking Yes or No in the message.

1. Choose Administration > Configuration.
2. Click the Device Settings tab.
3. Select the Display Warning Message For All Power Operations checkbox to enable the warning message. Deselect the checkbox to disable the warning message.
4. Click Update Configuration to save your changes.

Configuring Custom JRE Settings

CC-SG will display a warning message to users who attempt to access CC-SG without the minimum JRE version that you specify. Check the Compatibility Matrix for the minimum supported JRE version. Choose Administration > Compatibility Matrix.

If a user attempting to log into CC-SG does not have the specified JRE version installed, the JRE Incompatibility Warning window opens. The window includes several options for downloading the default minimum JRE versions. You can change the message to include any text and links to download options. Users can download a new JRE version or continue to access CC-SG with the current installed JRE version.

► **To enable or disable custom JRE for login:**

1. Back up CC-SG and save the backup file to a remote location before you enable or disable this feature. See **Backing Up CC-SG** (on page 154).
2. Choose Administration > Configuration.
3. Click the Custom JRE tab.
4. Select the Enable Custom JRE for Login checkbox to enable the option. Deselect the checkbox to disable the option.

5. Enter the minimum JRE version required in the Require Minimum JRE field. You must enter the full version number, including at least three parts. For example, 1.6.0 is a correct version number. 1.6 is not a correct version number. For JRE "Update" versions, use an underscore character. For example, 1.6.0_5 is a correct version number for JRE version 1.6.0 Update 5.
 6. Click Update.
- ▶ **To customize the message in the JRE Incompatibility Warning window:**
1. Choose Administration > Configuration.
 2. Click the Custom JRE tab.
 3. Using HTML code, enter the message that appears in the JRE Incompatibility Warning window.
 4. Click Update.
- ▶ **To restore the default message and minimum JRE version:**
1. Choose Administration > Configuration.
 2. Click the Custom JRE tab.
 3. Click Restore Default.
 4. Click Update.
- ▶ **To clear the default message and minimum JRE version:**
1. Choose Administration > Configuration. Click the Custom JRE tab.
 2. Click Clear.

Configuring SNMP

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. See RFC 1213 for details.

- ▶ **To configure SNMP in CC-SG:**
1. Choose Administration > Configuration.
 2. Click the SNMP tab.

3. Select the Enable SNMP Daemon checkbox to enable SNMP operations.
4. 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.
5. Click Update Agent Configuration to save your changes.
6. Select the Enable SNMP Traps checkbox to enable sending SNMP traps from CC-SG to a SNMP host.
7. Select 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, select the boxes marked System Log and Application Log. Individual traps can be enabled or disabled by selecting their checkboxes. Use Select All and Clear All to enable all traps, or deselect all checkboxes. Refer to the MIB files for the list of SNMP traps that are provided. See MIB Files for details.
8. Type the Trap Destination Host IP address and Port number used by SNMP hosts in the Trap Destinations panel. Default port is 162.
9. Type the Community string and Version (v1 or v2) used by SNMP hosts in the Trap Destinations panel.
10. 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.
11. Click Update Trap Configuration to save your changes.

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. See **SNMP Traps** (on page 261). The custom MIB file can be found on the Raritan Support web site.

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 (V1 or E1).
- Your CC-SG network must in Primary/Backup mode to be used for clustering. Clustering will not work with an Active/Active configuration. See **About Network Setup (on page 169)**.
- 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 and 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 the Cluster Name field. If you do not provide a name now, a default name, such as cluster192.168.51.124, will be provided 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 available only 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.

► **To recover a failed CC-SG node:**

1. Select the Waiting node in the Cluster Configuration table.
2. Clicking Join “Waiting” Node to add it as a backup 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 change the time zone in a cluster configuration.

► **To configure advanced cluster settings:**

1. Select the Primary node.

2. Click Advanced. The Advanced Settings window opens.
3. For Time Interval, enter how often CC-SG should check its connection with the other nodes.

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

See **Remote Authentication** (on page 122) 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>

<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. Select the Require AES Encryption between Client and Server checkbox.
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 either use regular HTTP connections from clients or require HTTPS/SSL connections. You must restart CC-SG for changes to this setting to take effect.

► To configure browser connection protocol:

1. Choose Administration > Security.
2. Open the Encryption tab.
3. Select the HTTP or HTTPS/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.

Set 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. See **SSH Access to CC-SG** (on page 205).

► 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 allows you to configure 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. Click the Login Settings tab.
3. Select 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 five 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 lowercase letter.
 - Passwords must contain at least one uppercase 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 all 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 users, CC-NOC users, and SSH users after a specified number of failed login attempts. You can enable this feature for locally authenticated users, for remotely authenticated users, or for all users.

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. Click the Login Settings tab.
3. Select the Lockout Enabled for Local Users checkbox to enable lockout for users who are locally authenticated. Select the Lockout Enabled for Remote Users checkbox to enable lockout for users who are remotely authenticated.
4. The default number of Failed Login Attempts before a user is locked out is three. 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 five minutes. You can specify a period from 1 minute up to 1440 minutes (24 hours). After the time expires, the user can log in 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. 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. **Optional.**
 7. Type a phone number in the Administrator's Telephone field. The phone number will appear in the notification email that is sent when lockout occurs. **Optional.**
 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 log in.

1. Choose Administration > Security.
2. Open the Login Settings tab.
3. Deselect the Lockout Enabled for Local Users checkbox to disable lockout for locally authenticated users. Deselect the Lockout Enabled for Remote Users checkbox to disable lockout for remotely authenticated users.
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. Click the Login Settings tab.
 - Select the Super User checkbox to allow more than one simultaneous login with the CC Super User account.
 - Select the System Administrators checkbox to allow concurrent logins by users in the System Administrators user group.
 - Select the Other Users checkbox to allow concurrent logins by all other users.
3. Click Update to save your changes.

Configure 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. Click 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 at 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 the Require Acceptance of Restricted Service Agreement checkbox 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 opens.
 - 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.

► To 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.

► To 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 opens.
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 screen, 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.

► **To 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 opens.
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 screen, 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. Click the Access Control List tab.

► **To add a rule to the Access Control List:**

1. Choose Administration > Security.
2. Click 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 which you want to apply the rule 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 whole CC-SG 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 add a rule to the Access Control List that allows or denies access at an operating system level:**

1. Choose Administration > Security.
2. Click 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 which you want to apply the rule 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. Click 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. Click 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 that 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. See **Task Manager** (on page 196). 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. Select the Enable SMTP Notification checkbox.
3. Type the SMTP host in the SMTP host field. See **Terminology/Acronyms** (on page 2) for hostname rules.
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

Schedule 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 the email is sent and choose to send email securely via SSL in the Notification Manager. See **Notification Manager** (on page 195).

Scheduled Reports

Scheduled reports are sent via email to the recipients that you specify. You can specify either CSV or HTML for the version of the emailed report.

All reports that have a Finished status are stored in HTML format on CC-SG for 30 days. You can view the finished reports in HTML format only by selecting Scheduled Reports on the Reports menu. See **Scheduled Reports** (on page 151).

Find and View Tasks

You can view tasks in a list filtered by the criteria you choose. For each task, you can view details and history.

Note: 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 of the task you want to view.
3. Filter the list further by selecting one or more (Ctrl+click) tasks, status, or owner from each list.
4. Click View Tasks to view the list of tasks.

► **To view a task's history:**

- Select the task, and click Task History.

► **To view a task's details:**

- Double-click a task to open a dialog containing the task details.

Schedule a Task

This section covers most tasks that can be scheduled. See **Schedule a Device Firmware Upgrade** (on page 199) 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. See the following sections for details on each task:
 - **Backup CommandCenter:** See *Backing Up CC-SG* (on page 154)
 - **Backup Device Configuration:** See *Backing Up a Device Configuration* (on page 42)
 - **Copy Device Configuration:** See *Copying Device Configuration* (on page 46)
 - **Group Power Control:** See *Node Group Power Control* (on page xviii)
 - **Outlet Power Control:** See the *CC-SG User Guide*.
 - **Purge Logs:** See *Configuring Logging Activity* (on page 174).
 - **Restart Devices:** See *Restarting a Device* (on page 46)
 - **Restore Device Configuration:** See *Restoring Device Configurations* (on page 43) (does not apply to device groups)
 - **Upgrade Device Firmware (individual device or device group):** See *Schedule a Device Firmware Upgrade* (on page 199).
 - **Generate all reports:** See *Reports* (on page 140).
6. Click the Recurrence tab. The Recurrence tab is disabled for Upgrade Device Firmware tasks.
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 Every day radio button if you want the task to repeat every day of the week. Click the Every weekday radio button 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 select 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 select 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 opens, and then click OK. By default, email is sent if the task is successful. To notify recipients of failed tasks, select On Failure.
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.

See 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. Click 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 to which you want to upgrade. Only available upgrade files that are appropriate for the device type selected will appear 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. Specify whether failed upgrades should be retried.
 - a. Click the Retry tab.
 - b. Retry Count: Type the number of times CC-SG should retry a failed upgrade.

- c. **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. 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 the Notification tab.
 - b. Click Add, type the email address in the window that opens, and then click OK.
 - c. Select On Failure if you want an email sent if an upgrade fails.
 - d. 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. See **Upgrade Device Firmware Report** (on page 152).

Change a Scheduled Task

You can change a scheduled task before it runs.

► **To change a scheduled task:**

1. Select the task you want to change.
2. Click Edit.
3. Change the task specifications as needed. See **Schedule a Task** (on page 197) and **Schedule a Device Firmware Upgrade** (on page 199) for tab descriptions.
4. Click Update to save your changes.

Reschedule a Task

The Save As function in Task Manager enables you to reschedule a completed task that you want to run again. This is also a convenient way to create a new task that is similar to a completed task.

► **To reschedule a task:**

1. Choose Administration > Tasks.
2. In the Task Manager page, select the task you want to reschedule. Use the filtering criteria to search for the task.
3. Click Save As.

4. In the Save As Task window that opens, the tabs are populated with the information from the previously configured task.
5. Change the task specifications as needed. See **Schedule a Task** (on page 197) and **Schedule a Device Firmware Upgrade** (on page 199) for tab descriptions.
6. Click OK to save your changes.

Schedule a Task that is Similar to Another Task

You can use a previously configured task as a "template" to schedule a new task with similar specifications.

► **To schedule a task that is similar to another task:**

- See **Reschedule a Task** (on page 201).

Delete a Task

You can delete a task to remove it from the Task Manager. You cannot delete a task that is currently running.

► **To delete a task:**

- Select the task, then click Delete.

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. See 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 if you want to use an NTP server.

Add a CC-NOC

You must give the generated passcodes 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. See 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. See **Terminology/Acronyms** (on page 2) for hostname rules.
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. See Raritan's **CommandCenter NOC Administrator Guide**. 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 to which CC-SG is subscribing. The report also displays any new targets that have been discovered by CC-NOC. See **CC-NOC Synchronization Report** (on page 152).*

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 is 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. Enter 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. Exchange passcodes verbally or in writing.

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 five 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 be added only 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. Select 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 OpenSSH 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.

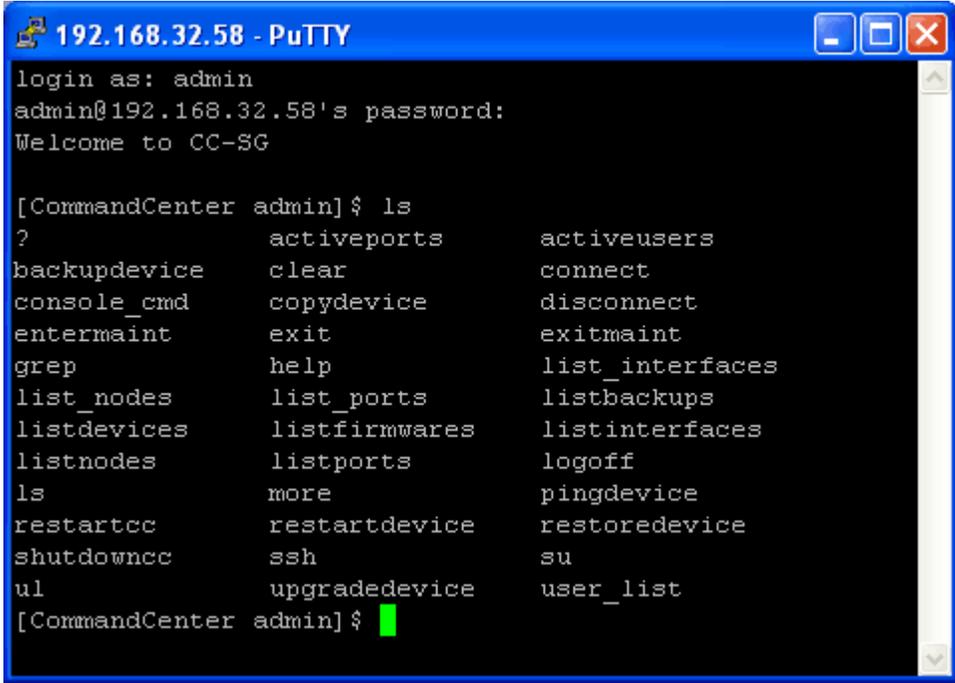
Administrators who use SSH to access CC-SG cannot log a CC Super-User SSH user out, but are able to log all other SSH client users out, including System Administrators.

► **To access CC-SG via SSH:**

1. Launch an SSH client, such as PuTTY.
2. Specify the IP address of the CC-SG.
3. Specify the SSH port number. Default is 22. You can configure the port for SSH access in Security Manager. See **Security Manager** (on page 184).
4. Open the connection.
5. Log in with your CC-SG username and password.
6. A shell prompt appears.

► **To display all SSH commands:**

- At the shell prompt, type `ls` to display all commands available.



```

192.168.32.58 - PuTTY
login as: admin
admin@192.168.32.58's password:
Welcome to CC-SG

[CommandCenter admin]$ ls
?                activeports      activeusers
backupdevice     clear            connect
console_cmd     copydevice       disconnect
entermaint      exit             exitmaint
grep            help             list_interfaces
list_nodes      list_ports       listbackups
listdevices     listfirmwares    listinterfaces
listnodes       listports        logoff
ls              more             pingdevice
restartcc       restartdevice    restoredevice
shutdowncc     ssh              su
ul              upgradedevice    user_list
[CommandCenter admin]$

```

Get Help for SSH Commands

You can get limited help for all commands at once. You can also get in-depth help on a single command at a time.

► **To get help for a single SSH command:**

1. At the shell prompt, type the command you want help for, followed by a space and `-h`. For example:

```
connect -h
```

2. Information on the command, parameters, and usage appear in the screen.

► **To get help for all SSH commands:**

1. At the shell prompt, type the following command:

```
help
```

2. A short description and example for each SSH command appears in the screen.

SSH Commands and Parameters

The following table lists all commands available in SSH. You must be assigned the appropriate privileges in CC-SG to access each command.

Some commands have additional parameters that you must type to execute the command. For more information about how to type commands, see **Command Tips** (on page 209).

▶ **To list active ports:**

```
activeports
```

▶ **To list active users:**

```
activeusers
```

▶ **To backup a device configuration:**

```
backup device <[-host <host>] | [-id <device_id>]>  
backup_name [description]
```

▶ **To clear the screen:**

```
clear
```

▶ **To establish a connection to a serial port:**

If <port_name> or <device_name> contains spaces, surround the name by quotes.

```
connect [-d <device_name>] [-e <escape_char>] <[-i  
<interface_id>] | [-n <port_name>] | [port_id]>
```

▶ **To copy a device configuration from one device to another. SX devices with same number of ports only:**

```
copydevice <[-b <backup_id>] | [source_device_host]>  
target_device_host
```

▶ **To close port connection:**

```
disconnect <[-u <username>] [-p <port_id>] [-id  
<connection_id>]>
```

▶ **To enter maintenance mode:**

```
entermaint minutes [message]
```

▶ **To exit maintenance mode:**

```
exitmaint
```

▶ **To search for text from piped output stream:**

```
grep search_term
```

▶ **To view the help screen for all commands:**

```
help
```

▶ **To list available device configuration backups:**

```
listbackups <[-id <device_id>] | [host]>
```

▶ **To list available devices:**

```
listdevices
```

▶ **To list firmware versions available for upgrade:**

```
listfirmwares [[-id <device_id>] | [host]]
```

▶ **To list all interfaces:**

```
listinterfaces [-id <node_id>]
```

▶ **To list all nodes:**

```
listnodes
```

▶ **To list all ports:**

```
listports [[-id <device_id>] | [host]]
```

▶ **To logoff a user:**

```
logoff [-u <username>] message
```

▶ **To list all commands:**

```
ls
```

▶ **To specify paging:**

```
more [-p <page_size>]
```

▶ **To ping a device:**

```
pingdevice <[-id <device_id>] | [host]>
```

▶ **To restart CC-SG:**

```
restartcc minutes [message]
```

▶ **To restart a device:**

```
restartdevice <[-id <device_id>] | [host]>
```

▶ **To restore a device configuration:**

```
restoredevice <[-host <host>] | [-id <device_id>]>  
[backup_id]
```

▶ **To shutdown CC-SG:**

```
shutdowncc minutes [message]
```

▶ **To open an SSH connection to an SX device:**

```
ssh [-e <escape_char>] <[-id <device_id>] | [host]>
```

▶ **To change a user:**

```
su [-u <user_name>]
```

▶ **To upgrade a device's firmware:**

```
upgradedevice <[-id <device_id>] | [host]>
```

▶ **To list all current users:**

```
userlist
```

▶ **To exit the SSH session:**

```
exit
```

Command Tips

- For commands that pass an IP address, such as `upgradedevice`, you can substitute the hostname for an IP address. See **Terminology/Acronyms** (on page 2) for hostname rules.
- The `copydevice` and `restartdevice` commands apply only to some Raritan devices. Dominion SX and IPMI servers are not supported by these commands.
- Parts of a command in square brackets are optional. You do not have to use that part of the command.
- Some commands contains two segments separated by the "Or" sign:
|
You must enter one of the listed parts of the command, but not both.
- Parts of a command in angle brackets show the text that you must type. Do not type the angle brackets. For example:

Command syntax	Device ID value	You should type
<code>ssh -id <device_id></code>	100	<code>ssh -id 100</code>

- The default escape character is a tilde followed by a period. For example:

~.

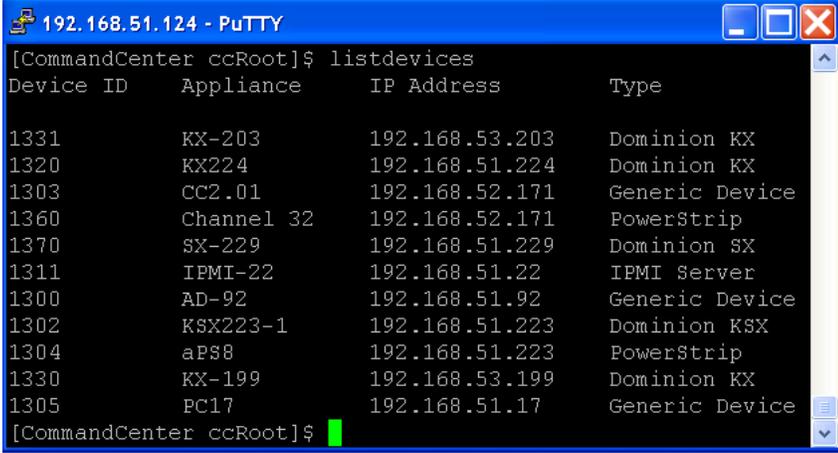
See **End SSH Connections** (on page 212) for details on using the escape character and the exit command.

Create an SSH Connection to a Serial-Enabled Device

You can create an SSH connection to a serial-enabled device to perform administrative operations on the device. Once connected, the administrative commands supported by the serial-enabled device are available.

Note: Before you connect, ensure that the serial-enabled device has been added to the CC-SG.

- Type `listdevices` to ensure the serial-enabled device has been added to CC-SG.



```

[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 device by typing `ssh -id <device_id>`.
Using the figure above as an example, you can connect to SX-229 by typing `ssh -id 1370`.



```

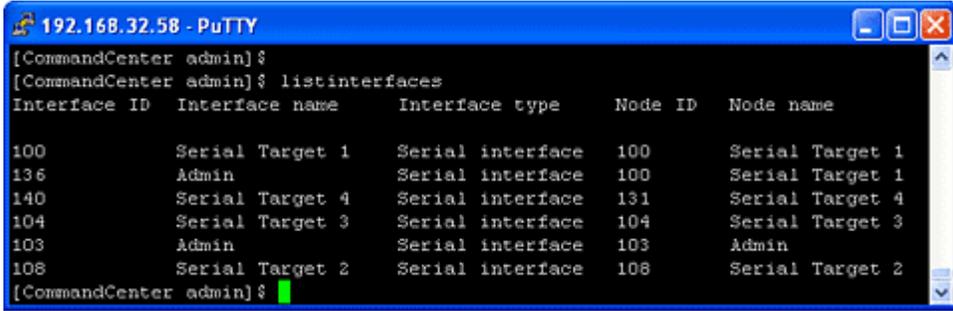
192.168.51.124 - PuTTY
[CommandCenter ccRoot]$ ssh -id 1370
Authenticating [vG550]...Authenticated.
User Type [Administrator]
User Name [vG550]
Type [help] for all commands
vG550:Command>

```

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.

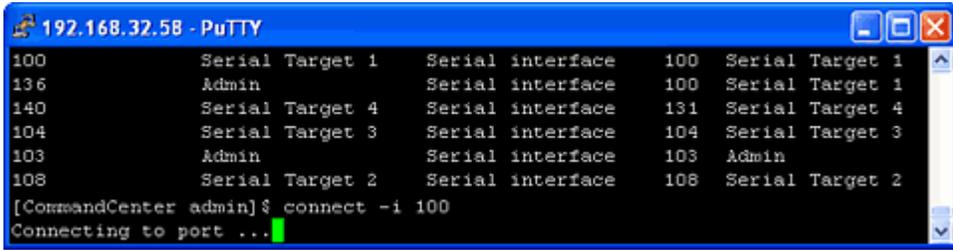


```

192.168.32.58 - PuTTY
[CommandCenter admin]$
[CommandCenter admin]$ listinterfaces
Interface ID  Interface name  Interface type  Node ID  Node name
-----
100          Serial Target 1  Serial interface 100   Serial Target 1
136          Admin            Serial interface 100   Serial Target 1
140          Serial Target 4  Serial interface 131   Serial Target 4
104          Serial Target 3  Serial interface 104   Serial Target 3
103          Admin            Serial interface 103   Admin
108          Serial Target 2  Serial interface 108   Serial Target 2
[CommandCenter admin]$

```

2. Type `connect -i <interface_id>` to connect to the node associated with the interface.



```

192.168.32.58 - PuTTY
100          Serial Target 1  Serial interface 100   Serial Target 1
136          Admin            Serial interface 100   Serial Target 1
140          Serial Target 4  Serial interface 131   Serial Target 4
104          Serial Target 3  Serial interface 104   Serial Target 3
103          Admin            Serial interface 103   Admin
108          Serial Target 2  Serial interface 108   Serial Target 2
[CommandCenter admin]$ connect -i 100
Connecting to port ...

```

3. At the prompt that appears, 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.

End SSH Connections

You can make SSH connections to CC-SG only, or you can make a connection to CC-SG and then make a connection to a port, device, or node managed by CC-SG. There are different ways to end these connections, depending on which part you want to end.

► To exit the entire SSH connection to CC-SG:

This command ends the entire SSH connection, including any port, device, or node connections made through CC-SG.

- At the prompt, type the following command and press the Enter key:

```
exit
```

► To end a connection to a port, device, or node while remaining connected to CC-SG:

You can use the escape character to end a connection to a port, device, or node while keeping your SSH connection to CC-SG open.

The default escape character is a tilde followed by a period.

- At the prompt, type the following command and press Enter:

```
~.
```

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.

► **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.

Finding Your CC-SG Serial Number

► **To find your CC-SG serial number:**

1. Log into the Admin Client.
2. Choose Help > About Raritan Secure Gateway.
3. A new window opens with your CC-SG serial number.

Web Services API

The Web Services Application Programming Interface (WS API) is not currently available for activation. See <http://www.raritan.com/web-services-api> for updated information about this feature.

You must accept the End User Agreement before adding a Web Services API client to CC-SG. You can add up to five WS-API clients. See the CC-SG Web Services SDK Guide for details on using the API.

► **To add a Web Services API:**

1. Select Access > Add Web Services API. This option is available only for users with the CC Setup and Control Privilege.
2. Read the End User Agreement.
 - You can copy and paste the text to save it, or choose Secure Gateway > Print.
 - After you complete configuration, this agreement will also be available in the Access menu.
3. Click Accept. The New Web Services API Configuration window opens.
4. Type in the data requested about your web services client.
 - Web Services Client Name: Maximum 64 characters.
 - IP Address/Hostname: Maximum 64 characters.
 - HTTPS Web Services Port: Read-only field. CC-SG uses port 9443 when trust establishment is generated.
 - Licensed Vendor Name: Maximum 64 characters.
 - Certify Vendor Name: Opens the Raritan Vendor Certification Page.
 - Client Application URL: When the URL is specified, a menu item will be available to allow access to the web services client application from CC-SG.
5. Generate a self-signed certificate.
 - a. Encryption Mode: If Require AES Encryption between Client and Server is selected in the Administration > Security > Encryption screen, 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.
6. Click Generate Certificate. The text appears in the Certificate box.
 7. Click Save to File to save the certificate to a .P12 file.
 8. Click Add to save your changes.

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 **Access Diagnostic Console via VGA/Keyboard/Mouse Port** (on page 216). Or, you can access Diagnostic Console from a Secure Shell (SSH) client, such as PuTTY or OpenSSH Client. See **Access Diagnostic Console via SSH** (on page 216).

Diagnostic Console includes two interfaces:

1. Status Console: See **About Status Console** (on page 218).
2. Administrator Console. See **About Administrator Console** (on page 218).

Note: When you access Diagnostic Console via SSH, the Status Console and the Administrator Console inherit the appearance settings of your SSH client and keyboard bindings. These appearance settings may differ from those in this documentation.

In This Chapter

Accessing Diagnostic Console	216
Status Console	218
Administrator Console	218

Accessing Diagnostic Console

Access 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 Enter to display a login prompt on the screen.

Access 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. Specify 23 for the port.
3. Click the button that allows you to connect. A window opens, prompting you for a login.

► **To access 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-U1 |
|: 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 five 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.

Status	Description
DB Status: Responding	CC-SG's database is available.
DB Status: Down	CC-SG may be in the process of rebooting.

Status Console

About Status Console

You can use the Status Console to check the health of CC-SG, the various services CC-SG uses, and the attached network.

By default, Status Console does not require a password.

Access Status Console

► **To access Status Console:**

1. At the login prompt, type status.
2. The current system information appears.

Administrator Console

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.

Access 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-log into Administrator Console after the changes have taken effect to view them in Administrator Console

► To access 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. See **Diagnostic Console Password Settings** (on page 234) for details on setting password strength.

The main Administrator Console screen appears.

Navigate Administrator Console

Use keyboard combinations to navigate Administrator Console. 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	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 bar	Select current option.
Enter	Select current option.
Arrow key	Move to different fields within an option.

Edit Diagnostic Console Configuration

The Diagnostic Console can be accessed via the serial port (COM1), VGA/Keyboard/Mouse (KVM) port, or from SSH clients. For each port type, you can configure whether or not status or admin logins are allowed, and whether field support can access Diagnostic Console from the port. For SSH clients, you can 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 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.

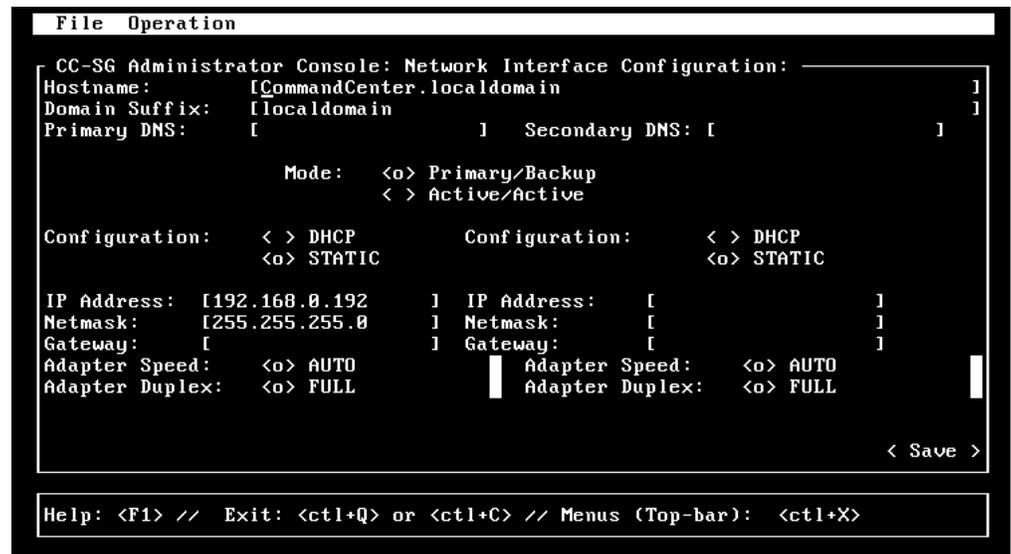
There are four Diagnostic Console Access mechanisms: Serial Port (COM1), KVM Console, SSH (IP network), and Web. The Diagnostic Console offers three services: Status Display, Admin Console, Raritan Field Support. This screen allows the selection of which services are available via the various access 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.
4. Click Save.

Edit 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 (Admin Client) to configure the interfaces. If you want to continue, click YES.



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. See **Terminology/Acronyms** (on page 2) for hostname rules.

4. In the Mode field, select either Primary/Backup Mode or Active/Active Mode. See **About Network Setup (on page 169)**.
 - 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, you must provide a properly formatted IP address and Netmask.
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 arrow keys are used to navigate to them. Press the Space bar to select the option displayed. For 1 GB line speeds, select AUTO.
6. If you did not select AUTO for Adapter Speed, click Adapter Duplex and use the arrow 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. Click Save. CC-SG will restart, logging out all CC-SG GUI users and terminating their sessions. A Warning screen will appear, informing you 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 pressing Alt+F2 and logging in as status. You may return to the original terminal session by pressing Alt+F1. There are six available terminal sessions on F1 through F6.

Ping an IP Address

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. Select: **Optional**.

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 on, 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. 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. **Optional**.
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. See **Edit Static Routes** (on page 224).
6. Press Ctrl+C to terminate the session.

Note: Press CTRL+Q to display a statistics summary for the session so far and continue to ping the destination.

Use Traceroute

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. Select: **Optional**.

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. 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. **Optional**.
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.

Edit Static Routes

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. See **About Network Setup** (on page 169). Click with the mouse or use the Tab and 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 page opens. You can add a host or network route, or delete a route. The Refresh button updates the routing information in the 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>
```

View Log Files in Diagnostic Console

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 updated only 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 preceded by a timestamp indicating either 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

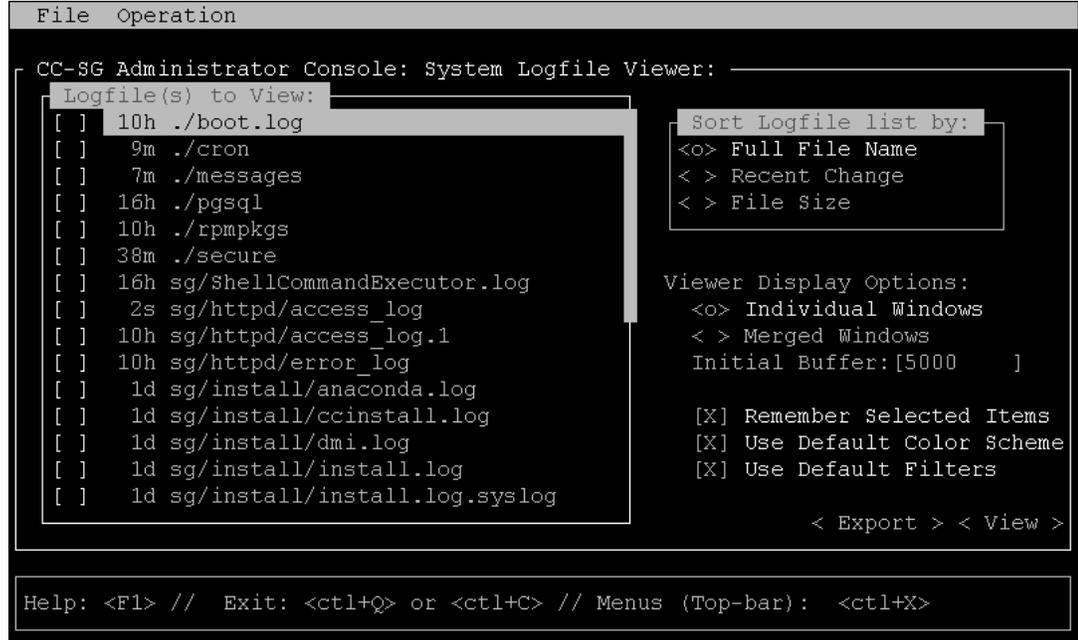
File sizes:

- 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 four 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.

- Click with the mouse or use the arrow keys to navigate and press the Space bar to select a log file, marking it with an X. You can view more than one log file at a time.



► **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: multital 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.

Option	Description
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:

```

15:30:54,366 INFO [ChannelSocket] JK: ajp13 listening on /0.0.0.0:8009
15:30:54,378 INFO [JkMain] Jk running ID=0 time=0/26 config=null
15:30:54,480 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-9443
15:30:54,756 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-0.0.0.0-8080
15:30:54,801 INFO [Server] JBoss (MX MicroKernel) [4.0.3 (build: CVSTag=JBoss_4
0 3 date=200510042324)] Started in 57s:149ms
00] sg/jboss/console.log F1/<CTRL>+<h>: help 118KB - 2006/12/13 15:32:54
3/bin ; USER=root ; COMMAND=/data/raritan/jboss/ccscripts/root-scripts/iptables_
ports.sh
Dec 13 15:30:55 CommandCenter httpd: httpd startup succeeded
Dec 13 15:30:55 CommandCenter MonitorCC[14617]: Starting httpd: ^{[60G[ ^{[0;32
mOK^{[0;39m
Dec 13 15:30:56 CommandCenter MonitorCC[14617]: startAll: Done -- JBoss:47 HTTP
D:1
01] ./messages *Press F1/<CTRL>+<h> for help* 935KB - 2006/12/13 15:32:54
02] sg/httpd/access_log F1/<CTRL>+<h>: help 538KB - 2006/12/13 15:32:54

```

- 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
```

Restart CC-SG with Diagnostic Console

Restarting CC-SG will log out all current CC-SG users and terminate their sessions to remote target servers.

Important: It is HIGHLY recommended to restart CC-SG in the Admin Client, unless it is absolutely necessary to restart it from Diagnostic Console. See *Restarting CC-SG* (on page 159). 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>

```

Reboot 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 out. Any connections to remote target servers will 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>
    
```

Power Off 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 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 off 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>

```

Reset 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. See **Diagnostic Console Password Settings** (on page 234).*

► **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>
    
```

Reset 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 out without notification and SNMP processing will stop.

It is recommended to use the default options selected.

Option	Description
Full CC-SG Database Reset	<p>This option removes the existing CC-SG database and builds a new version with the factory default values. Network settings, SNMP settings, firmware, and diagnostic console settings are not part of the CC-SG database.</p> <p>IP-ACL settings are reset with a Full Database reset whether you select the IP ACL Tables option or not.</p>

Option	Description
Preserve CC-SG Personality during Reset	<p>This option is enabled when you select Full CC-SG Database Reset.</p> <p>As the CC-SG database is rebuilt, some previously configured options are saved.</p> <ul style="list-style-type: none"> ▪ Secure Communication between PC Clients and CC-SG ▪ Enforce Strong Passwords ▪ Direct vs. Proxy Connections to Out-of-Band nodes ▪ Inactivity Timer setting
Network Reset	<p>This option changes the network settings back to factory defaults.</p> <ul style="list-style-type: none"> ▪ 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	<p>This option resets the SNMP settings back to factory defaults.</p> <ul style="list-style-type: none"> ▪ Port: 161 ▪ Read-only Community: public ▪ Read-write Community: private ▪ System Contact, Name, Location: none ▪ SNMP Trap Configuration ▪ SNMP Trap Destinations
Firmware Reset	<p>This option resets all device firmware files to factory defaults. This option does not change the CC-SG database.</p>
Install Firmware into CC-SG DB	<p>This option loads the firmware files for the current CC-SG version into the CC-SG database.</p>
Diagnostic Console Reset	<p>This option restores Diagnostic Console settings back to factory defaults.</p>
IP Access Control Lists Reset	<p>This option removes all entries from the IP-ACL table.</p> <p>IP-ACL settings are reset with a Full Database reset whether you select the IP Access Control Lists reset option or not.</p> <p>See Access Control List (on page 193).</p>

► **To reset CC-SG to the factory configuration:**

1. Choose Operation > Admin > Factory Reset.
2. Select the reset options.
3. Click Reset System.

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 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 applies only to Diagnostic Console accounts (status and admin) and passwords; it has no effect on the regular CC-SG GUI accounts or passwords.

► **To configure Diagnostic Console passwords:**

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 five.

```

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:
< > 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 four 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	<p>Enforce strong passwords.</p> <p>Retries is the number of times you are prompted before an error message is issued.</p> <p>DiffOK is how many characters can be the same in the new password relative to the old.</p> <p>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.</p> <p>Positive numbers indicate the maximum amount of “credit” of this character class can be accrued towards the “simplicity” count.</p> <p>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.</p>

Diagnostic Console 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.

- 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 lower area restores the password configuration to Factory Defaults (or to how the system was initially shipped).
- If you want to require a password for the Status account, select Enabled underneath it.
 - 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). This is the day that this account must change its password.

Setting	Description
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.

Configure Remote System Monitoring

You can enable the remote system monitoring feature to use the GKrellM tool. The GKrellM tool provides a graphical view of resource utilization on the CC-SG unit. This tool is similar to the Windows Task Manager's Performance tab.

► **1: Enable remote system monitoring for the CC-SG unit:**

1. Choose Operation > Utilities > Remote System Monitoring.
2. Select Enabled in the Remote Monitoring Service field.
3. Enter the IP address of the client PC you want to allow to monitor the CC-SG unit in the Allowed Remote Monitoring IP Addresses field. You can enter up to three IP addresses.
4. The default port for the GKrellM tool is 19150. You can change the port.
5. Select Submit.

► **2: Download the remote system monitoring client software:**

1. Navigate to www.gkrellm.net.

2. Download and install the package that is appropriate for your client PC.

▶ **3: Configure the remote system monitoring client to work with CC-SG:**

Follow the instructions in the Read Me file to set the CC-SG unit as the target to monitor.

Windows users must use the command line to locate the Gkrellm installation directory and then run the commands specified in the Read.

Configure Historical Data Trending

You can enable historical data trending to gather information about CPU utilization, memory utilization, log file size, and disk space for the system and each folder. This information is compiled into a report that you view as a web page from CC-SG. The report contains the status of the CC-SG and links to historical data.

▶ **1: Enable historical data trending:**

1. Choose Operation > Diagnostic Console Config.
2. In the Ports list, select Web.
3. In the Status list, select the Status checkbox next to Web.
4. Click Save.

▶ **2: View the historical data trending reports:**

1. Using a supported Internet browser, type this URL:
`https://<IP_address>/status` where <IP_address> is the IP address of the CC-SG. For example,
`https://10.20.3.30/status`.
2. A status page opens. This page contains the same information as the Status Console. See **Status Console** (on page 218).
 - Click the Historical CC-SG Monitors link to view information about CPU utilization, memory utilization, log file sizes, and disk space for the system and each folder. Click each graph to view details in a new page.

Display Disk Status

This option displays the status of CC-SG disks, including disk size, active and up status, 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].

View Top Display with Diagnostic Console

Top Display allows you to view the list of currently-running processes and their attributes, as well as overall system health.

► **To display the processes running on CC-SG:**

1. Choose Operation > Utilities > Top Display.

- 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

- Type **h** to view a help screen for the top command. **F1** for help is not operational here.

Display NTP Status

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 Admin Client.

► **To display status of the NTP daemon on the CC-SG:**

- 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 V1 and E1

In This Chapter

V1 Model.....	242
E1 Model.....	243

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 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°)

Operating	
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 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

Operating	
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

This appendix contains network requirements, including addresses, protocols, and ports, of a typical CC-SG deployment. It includes information about how to configure your network for both external access and internal security and routing policy enforcement. Details are provided for the benefit of a TCP/IP network administrator. The TCP/IP administrator's role and responsibilities may extend beyond that of a CC-SG administrator. This appendix will assist the administrator in incorporating CC-SG and its components into a site's security access and routing policies.

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

In This Chapter

Required Open Ports for CC-SG Networks: Executive Summary.....245
 CC-SG Communication Channels.....246

Required Open Ports for CC-SG Networks: Executive Summary

The following ports should be opened:

Port Number	Protocol	Purpose	Details
80	TCP	HTTP Access to CC-SG	Not encrypted.
443	TCP	HTTPS (SSL) Access to CC-SG	SSL/AES128 encrypted.
8080	TCP	CC-SG to PC Client	SSL/AES128 encrypted if configured.
2400	TCP	Node Access (Proxy Mode)	SSL/AES128 encrypted if configured.
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. AES128 encrypted if configured.
80 and 443 for Control System nodes 80, 443, 902, and 903 for Virtual Host and Virtual Machine Nodes	TCP	Virtual Node Access	N/A

Port Number	Protocol	Purpose	Details
51000	TCP	SX Target Access (Direct Mode)	AES128 encrypted if configured.

► **Possible exceptions to the required open ports:**

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

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

CC-SG Communication Channels

Each communication channel is documented. For each communication channel, the table includes:

- The symbolic IP Addresses used by the communicating parties. These addresses must be allowed over any communication path between the entities.
- 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.
- The Port Number and Protocol used by CC-SG.
- Whether the port is Configurable, which means the Admin Client or Diagnostic Console provides a field where you can change the port number to a different value from the default listed if there are conflicts with other applications on the network or for security reasons.
- Details about the method of communication, the message that is passed via the communication channel, or its encryption.

CC-SG and Raritan Devices

A main role of CC-SG is to manage and control Raritan devices, such as Dominion KX II. 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?	Details
CC-SG to Local Broadcast	5000	UDP	yes	heartbeat
CC-SG to Remote LAN IP	5000	UDP	yes	heartbeat

Communication Direction	Port Number	Protocol	Configurable?	Details
CC-SG to Raritan Device	5000	TCP	yes	RDM protocol RC4/AES128 encrypted
Raritan Device to CC-SG	5001	UDP	no	heartbeat
CC-SG to Dominion PX	623	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 has 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?	Details
CC-SG to Local Broadcast	10000	UDP	no	heartbeat
CC-SG to Remote LAN IP	10000	UDP	no	heartbeat
CC-SG to CC-SG	5432	TCP	no	From HA-JDBC on Primary to Backup PostgreSQL DB server. Not encrypted.
CC-SG to CC-SG	8732	TCP	no	Primary-Backup server synch clustering control data exchange. MD5 encrypted.
CC-SG to CC-SG	3232	TCP	no	Primary-Backup SNMP synch configuration changes forwarding. Not encrypted.

Access to Infrastructure Services

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

Communication Direction	Port Number	Protocol	Configurable?	Details
DHCP server to CC-SG	68	UDP	no	IPv4 DHCP standard
CC-SG to DHCP server	67	UDP	no	IPv4 DHCP standard
NTP server to CC-SG	123	UDP	no	NTP standard
CC-SG to DNS	53	UDP	no	DNS standard

PC Clients to CC-SG

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

- Admin or Access Client via a web browser. CC-SG supports SSL v2, SSL v3, and TLS v1 for browser connections. You can configure these encryption methods in your browser
- Command Line Interface (CLI) via SSH
- Diagnostic Console

Communication Direction	Port Number	Protocol	Configurable?	Details
PC Client to CC-SG	443	TCP	no	Client-server communication. SSL/AES128 encrypted if configured.
PC Client to CC-SG	80	TCP	no	Client-server communication. SSL/AES128 encrypted if configured.
PC Client to CC-SG	8080	TCP	no	Client-server communication. SSL/AES128 encrypted if configured.
PC Client to CLI SSH	22	TCP	yes	Client-server communication. SSL/AES128 encrypted if configured.
PC Client to Diagnostic Console	23	TCP	yes	Client-server communication. SSL/AES128 encrypted if configured.

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 methods such as VNC, RDP, or SSH.

Another facet of PC client to node communication is whether:

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

Communication Direction	Port Number	Protocol	Configurable?	Details
Client to CC-SG via Proxy to Node	2400 (on CC-SG)	TCP	no	Client-server communication. SSL/AES128 encrypted if configured.
Client to Raritan Device to Out-of-Band KVM Node (Direct Mode)	5000 (on Raritan Device)	TCP	yes	Client-server communication. SSL/AES128 encrypted if configured.
Client to Raritan Dominion SX Device to Out-of-Band Serial Node (Direct Mode)	51000 (on Raritan Device)	TCP	yes	Client-server communication. SSL/AES128 encrypted if configured.

CC-SG and 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?	Details
CC-SG to IPMI	623	TCP	no	IPMI standard
CC-SG to iLO/RILOE (uses HTTP ports)	80 or 443	TCP	no	Vendor standard

Communication Direction	Port Number	Protocol	Configurable?	Details
CC-SG to DRAC	80 or 443	TCP	no	Vendor standard
CC-SG to RSA	80 or 443	TCP	no	Vendor standard

CC-SG and 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?	Details
SNMP Manager to CC-SG	161	UDP	yes	SNMP standard
CC-SG to SNMP Manager	162	UDP	yes	SNMP standard

CC-SG and 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?	Details
CC-SG to CC-NOC	9443	TCP	no	NOC web services. SSL/AES128 encrypted.

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 PAT (Port Address Translation), then Proxy mode should be used for all connections that use this firewall. The firewall must 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.

Connections using the firewall must be configured to use Proxy mode. See **Connection Modes: Direct and Proxy** (on page 176). CC-SG will connect to the various targets 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.

RDP Access to Nodes

Port 3389 must be open for RDP access to nodes.

VNC Access to Nodes

Port 5800 or 5900 must be open for VNC access to nodes.

SSH Access to Nodes

Port 22 must be open for SSH access to nodes.

Remote System Monitoring Port

When the Remote System Monitoring feature is enabled, port 19150 is opened by default. See **Configuring Remote System Monitoring** (see "Configure Remote System Monitoring" on page 237).

Appendix C User Group Privileges

This table shows which privilege must be assigned for a user to have access to a CC-SG menu item.

*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.

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	
	> Logout Users	User Management	
	Node Auditing	User Management	

Appendix C: User Group Privileges

Menu > Sub-menu	Menu Item	Required Privilege	Description
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	
	>> 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	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> Launch Admin	Device, Port, and Node Management or Device Configuration and Upgrade Management	
	> Launch User Station Admin		
	> 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	
	> 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	

Appendix C: User Group Privileges

Menu > Sub-menu	Menu Item	Required Privilege	Description
Nodes	<p>This menu and the Nodes tree is available only for users with any one of the following privileges:</p> <ul style="list-style-type: none"> 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	
	<interfaceName >	In-Band Access or Out-of-Band Access	
	Disconnect	In-Band Access or Out-of-Band Access	
	Virtualization	Device, Port and Node Management	
	Bulk Copy	Device, Port and Node Management	
	Power Control	Power Control	
	Group Power Control	Power Control	
	Service Accounts	Device, Port, and Node Management	
	Assign Service Accounts	Device, Port, and Node Management	
> Node Sorting Options	> By Node Name	<p>Any of the following:</p> <ul style="list-style-type: none"> 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	
	> 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	
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.

Appendix C: User Group Privileges

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> 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	Device, Port, and Node Management	
	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	
	> All Users Data	To view all user data: User Management To view your own user data: None	
	> User Group Data	User Management	
> Devices	> Device Asset Report	Device, Port, and Node Management	
	> Device Group Data	Device, Port, and Node Management	
	> Query Ports	Device, Port, and Node Management	
> Nodes	> Node Asset Report	Device, Port, and Node Management	
	> Active Nodes	Device, Port, and Node Management	

Menu > Sub-menu	Menu Item	Required Privilege	Description
	> Node Creation	Device, Port, and Node Management	
	> Node Group Data	Device, Port, and Node Management	
> Active Directory	AD Users Group Report		
	Scheduled Reports	CC Setup and Control	
	CC-NOC Synchronization	CC Setup and Control	
Access			
	CC-NOC Configuration	CC Setup and Control	
	Add Web Services API	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	
System Maintenance			

Appendix C: User Group Privileges

Menu > Sub-menu	Menu Item	Required Privilege	Description
	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*	

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.
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.

Appendix D: SNMP Traps

SNMP Trap	Description
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 username has changed.
ccSuperuserPasswordChanged	CC-SG Superuser password has changed.
ccLoginBannerChanged	CC-SG login banner has changed.
ccMOTDChanged	CC-SG Message of the Day (MOTD) has changed.
ccDominionPXReplaced	A Dominion PX device has been replaced with another Dominion PX device.
ccSystemMonitorNotification	CC-SG is out of memory.

Appendix E Troubleshooting

Launching CC-SG from your web browser 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 CC-SG does not load, check your web browser settings.
 - In Internet Explorer, ensure Java (Sun) is enabled.
 - Open Java Plug-in in the 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 clear the browser's cache and the Java cache and restart the browser. See **Clear the Browser's Cache** (on page 161) and **Clear the Java Cache** (on page 162).

Appendix F Two-Factor Authentication

CC-SG can be configured to point to an 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	264
Two-Factor Authentication Setup Requirements.....	264
Two-Factor Authentication Known Issues	264

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. Consult the RSA documentation.

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

In This Chapter

General FAQs.....	265
Authentication FAQs.....	267
Security FAQs	268
Accounting FAQs.....	269
Performance FAQs.....	269
Grouping FAQs.....	270
Interoperability FAQs.....	271
Authorization FAQs	271
User Experience FAQs.....	272

General 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 to which CC-SG provides access.
Which Raritan products does CC-SG support?	See the Compatibility Matrix on the Raritan website in the Support section under Firmware and Documentation.
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 known network addresses. Once CC-SG is connected and configured, the devices connected to CC-SG are transparent, and operation and administration is extremely simple.

Question	Answer
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.
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: <ul style="list-style-type: none"> - 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?	See the Compatibility Matrix on the Raritan website in the Support section under Firmware and Documentation.
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?	<p>Accessing CC-SG from outside the firewall can be achieved by configuring the right ports on the firewall. The following ports are standard ports:</p> <p>80: for HTTP access via web browser</p> <p>443: for HTTPS access via web browser</p> <p>8080: for CC-SG server operations</p> <p>2400: for Proxy mode connections</p> <p>5001: for IPR/DKSX/DKX/ P2-SC event notification</p> <p>If there is firewall between two cluster nodes, the following ports should be opened for cluster to be worked properly:</p> <p>8732: for cluster nodes heartbeat</p> <p>5432: for cluster nodes DB replication</p>
What are some design guidelines for large-scale systems? Any constraints or assumptions?	<p>Raritan provides two models for server scalability: the datacenter model and the network model.</p> <p>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).</p> <p>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.</p>

Authentication FAQs

Question	Answer
Authentication	
How many user accounts can be created for CC-SG?	<p>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.</p>

Question	Answer
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.
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, and so on?	CC-SG permits local authentication as well remote authentication. Remote authentication servers supported include: AD, TACACS+, RADIUS, and LDAP.

Security FAQs

Question	Answer
Security	
Sometimes when I try to log in, 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 into CC-SG. This ID has a time-out feature, so if you do not log into 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 in 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.

Question	Answer
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.
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 FAQs

Question	Answer
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 FAQs

Question	Answer
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 into 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.

Question	Answer
<p>What is the bandwidth usage per client?</p>	<p>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.</p> <p>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.</p>

Grouping FAQs

Question	Answer
Grouping	
<p>Is it possible to put a given server in more than one group?</p>	<p>Yes. Just as one user can belong to multiple groups, one device can belong to multiple groups.</p> <p>For example, a Sun in NYC could be part of Group Sun: "Ostype = Solaris" and Group New York: "location = NYC."</p>
<p>What impact to other usage would be blocked through the active usage of the console port, for example, some UNIX variants not allowing admin over network interfaces?</p>	<p>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.</p> <p>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.</p>

Question	Answer
How do you recommend handling the issue of CIMs being moved/swapped at the physical level with changes to the logical database? For example, what happens if I physically move a CIM with target server from one port to another (either on the same device or a different device)? What happens to the port names? What happens to the node? What happens to the interfaces?	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 ports and interfaces in CC-SG; the port name and interface name are updated to reflect the change. The interface appears beneath the node that is associated with the port. However, the node name does not change. You must rename the node manually by editing the node. This scenario assumes all ports involved were already configured. If you physically move the target server and CIM to a different and unconfigured port, you can then configure the port in CC-SG, and the node will be created automatically.

Interoperability FAQs

Question	Answer
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.
To what level is CC-SG able to integrate with third party KVM tools, down to third party KVM port level or simply box level?	Third party KVM switch integration is typically done through keyboard macros when the third party KVM vendors do not publicize the communications protocols for the third party KVM switches. Depending on the capability of the third 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 FAQs

Question	Answer
Authorization	

Question	Answer
Can authorization be achieved via RADIUS/TACACS/LDAP?	LDAP and TACACS are used for remote authentication only, not authorization.

User Experience FAQs

Question	Answer
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 into 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 this 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. 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	32
Node Name	64
Node Group Name	40
Policy Name	56

Index

A

- About Administrator Console • 216, 218
- About Applications for Accessing Nodes • 165
- About Associations • 21
- About CC-SG Clusters and CC-NOC • 181
- About CC-SG LAN Ports • 169, 170, 172
- About CC-SG passwords • 187
- About Connection Modes • 176
- About Default Applications • 167
- About Interfaces • 64
- About LDAP and CC-SG • 134
- About Network Setup • 3, 10, 169, 181, 221, 224
- About Nodes • 63
- About RADIUS and CC-SG • 138
- About Status Console • 216, 218
- About TACACS+ and CC-SG • 137
- About Terminal Emulation Programs • 213
- Access Administrator Console • xvii, 161, 219
- Access Control List • 193, 233
- Access Diagnostic Console via SSH • 216
- Access Diagnostic Console via
VGA/Keyboard/Mouse Port • 216
- Access Report • 144
- Access Status Console • 218
- Access to Infrastructure Services • 248
- Accessing CC-SG • 5
- Accessing Diagnostic Console • 216
- Accessing the Virtual Topology View • xiv, 82
- Accounting FAQs • 269
- Active Nodes Report • 150
- Active Users Report • 145
- AD Advanced Settings • 127, 130
- AD and CC-SG Overview • 125
- AD General Settings • 126, 130
- AD Group Settings • 128, 130
- AD Trust Settings • 129, 130
- AD User Group Report • 151
- Add a Category • 23
- Add a CC-NOC • 152, 202
- Add a Control System with Virtual Hosts and
Virtual Machines • 74, 78
- Add a Custom View for Devices • 118
- Add a Custom View for Nodes • 116
- Add a Device Group • 50, 54, 110
- Add a Dominion PX Device • xiv, 32, 33, 34, 35
- Add a KVM or Serial Device • 32, 33, 58, 60
- Add a Node • 70
- Add a Node Group • 94, 110
- Add a PowerStrip Connected to an SX 3.0 or
KSX device • 58
- Add a Powerstrip Connected to an SX 3.1
Device • 60, 61
- Add a PowerStrip Device • 32, 33, 34
- Add a PowerStrip Device Connected to a KX,
KX2, KX2-101, KSX2, or P2SC Device • 57
- Add a RADIUS Module • 138
- Add a TACACS+ Module • 137
- Add a User • 104, 146
- Add a User Group • 101
- Add a Virtual Host with Virtual Machines • 76, 78
- Add an Application • 12, 166
- Add an Element • 24
- Add an Interface • 71, 83, 90
- Add an LDAP (Netscape) Module to CC-SG • 134
- Add Device Groups and Node Groups • 16
- Add User Groups and Users • 19
- Add, Edit, and Delete Service Accounts • 68
- Adding a Device • 33
- Adding a Policy • 93, 110, 111, 114
- Adding an AD Module to CC-SG • 125
- Adding Location and Contacts to a Device
Profile • xiv, 30, 37
- Adding Location and Contacts to a Node
Profile • xiv, 66, 72
- Adding Notes to a Device Profile • xiv, 30, 36
- Adding Notes to a Node Profile • xiv, 66, 73
- Adding, Editing, and Deleting Interfaces • 70, 83
- Adding, Editing, and Deleting Node Groups • 93
- Adding, Editing, and Deleting Nodes • 70
- Adding, Editing, and Deleting User Groups • 70, 101
- Adding, Editing, and Deleting Users • 104
- Administrator Console • 218
- Advanced Administration • 104, 105, 126, 130, 164
- Advanced Cluster Settings • 183
- AES Encryption • 184
- All Users Data Report • 146
- Allow concurrent logins per username • 188
- Apply a Custom View for Devices • 119

- Apply a Custom View for Nodes • 116
 - Assign a Default Custom View for Devices • 121
 - Assign a Default Custom View for Nodes • 118
 - Assign a Default Custom View of Devices for All Users • 121
 - Assign a default custom view of nodes for all users • xxi, 118
 - Assign Service Accounts to Interfaces • 70
 - Assigning a User to a Group • 105, 106
 - Assigning Policies To User Groups • 110, 114
 - Association Manager • 23
 - Association Terminology • 21
 - Associations - Defining Categories and Elements • 22
 - Associations in Guided Setup • 13, 14
 - Associations, Categories, and Elements • 21, 30, 34, 35, 59, 66, 71, 93
 - Audit Trail Report • 142
 - Authentication and Authorization (AA) Overview • 122
 - Authentication FAQs • 267
 - Authorization FAQs • 271
 - Availability Report • 145
- B**
- Backing Up a Device Configuration • 42, 198
 - Backing Up CC-SG • xvii, 154, 159, 161, 178, 198
 - Before You Use Guided Setup • 13
 - Bookmarking an Interface • 91, 92, 149
 - Browser-Based Access via the CC-SG Admin Client • 5
 - Bulk Copy for Node Categories and Elements • 92
 - Bulk Copying for Device Categories and Elements • 41
 - Bulk Copying Users • 109
- C**
- CC Super-User Group • 100
 - CC Users Group • 100
 - CC-NOC Synchronization Report • 152, 203
 - CC-SG Access via NAT-enabled Firewall • 251
 - CC-SG Admin Client • 8
 - CC-SG and CC-NOC • 250
 - CC-SG and Client for IPMI, iLO/RILOE, DRAC, RSA • 249
 - CC-SG and Network Configuration • 245
 - CC-SG and Raritan Devices • 246
 - CC-SG and SNMP • 250
 - CC-SG Clustering • 247
 - CC-SG Communication Channels • xiv, 246
 - CC-SG Internal Ports • 251
 - CC-SG Shutdown • 162
 - Certificate Tasks • 191
 - Certificates • 190
 - Change a Custom View for Devices • 120
 - Change a Custom View for Nodes • 117
 - Change a PowerStrip's Device or Port Association (SX 3.0, KSX) • 58, 59
 - Change a Scheduled Task • 201
 - Change the CC-SG default font size • 108
 - Change the CC-SG Super User's Username • 108
 - Change the Daily AD Synchronization Time • 134
 - Change the Password for a Service Account • 69
 - Change your default search preference • 31, 107
 - Change your email address • 108
 - Change your password • 107
 - Check Your Browser for AES Encryption • 184
 - Checking and Upgrading Application Versions • 11, 165
 - Checking the Compatibility Matrix • 11
 - Clear the Browser's Cache • xvii, 160, 161, 263
 - Clear the Java Cache • xvii, 160, 162, 263
 - Client Browser Requirements • 4
 - Command Tips • 207, 209
 - CommandCenter NOC • 202
 - Configure a Combination of Direct Mode and Proxy Mode • 177
 - Configure a KVM Port • 39
 - Configure a Serial Port • 38
 - Configure an External SMTP Server • 195
 - Configure Browser Connection Protocol HTTP or HTTPS/SSL • 185
 - Configure Direct Mode for All Client Connections • 176
 - Configure Historical Data Trending • xiv, 238
 - Configure Proxy Mode for All Client Connections • 177
 - Configure Remote System Monitoring • xiv, 237, 252
 - Configure the Inactivity Timer • 189
 - Configuring a Message of the Day • 164

- Configuring Access Auditing for User Groups • xiv, 66, 103
 - Configuring and Enforcing Strong Passwords • xv
 - Configuring Applications for Accessing Nodes • 165
 - Configuring CC-SG Clusters • 181
 - Configuring CC-SG with Guided Setup • 10, 13, 23, 110
 - Configuring Custom JRE Settings • xiv, 6, 178
 - Configuring Default Applications • 167
 - Configuring Direct Port Access to a Node • 92
 - Configuring Logging Activity • 174, 198
 - Configuring Outlets on a Powerstrip • 56, 57, 58, 59, 60, 61
 - Configuring Ports • 38, 60
 - Configuring PowerStrips Connected to KX, KX2, KX2-101, KSX2, and P2SC • 56, 57
 - Configuring PowerStrips Connected to SX 3.0 and KSX • 56, 58
 - Configuring Powerstrips Connected to SX 3.1 • 56, 60
 - Configuring Powerstrips that are Managed by Another Device in CC-SG • xiv, 55, 56
 - Configuring SNMP • xiv, 179
 - Configuring the CC-SG Network • 125, 168
 - Configuring the CC-SG Server Time and Date • 175
 - Configuring the Virtual Infrastructure in CC-SG • xiv, 73, 83
 - Confirming IP Address • 10
 - Connecting to a Node • 82
 - Connection Modes
 - Direct and Proxy • 111, 176, 251
 - Controlling Power to a Node Group and Monitoring the Power Control Operation • xviii
 - Copying Device Configuration • 46, 198
 - Create a Cluster • 181
 - Create an SSH Connection to a Serial-Enabled Device • 210
 - Create Categories and Elements • 14
 - Creating Groups • 13, 16
 - Custom Views for Devices • 118
 - Custom Views for Devices and Nodes • xxi, 64, 115
 - Custom Views for Nodes • 116
- D**
- Default User Groups • 100
 - Delete a Backup File • 156
 - Delete a Category • 24
 - Delete a CC-NOC • 205
 - Delete a Custom View for Devices • 120
 - Delete a Custom View for Nodes • 117
 - Delete a Device Group • 54
 - Delete a Node • 72, 80
 - Delete a Node Group • 97
 - Delete a PowerStrip Connected to a KX, KX2, KX2-101, KSX2, or P2SC Device • 57, 58
 - Delete a PowerStrip Connected to an SX 3.0 or KSX Device • 58, 59
 - Delete a PowerStrip Connected to an SX 3.1 Device • 60, 61
 - Delete a Task • 202
 - Delete a User • 106
 - Delete a User Group • 103
 - Delete a Virtual Infrastructure • 80
 - Delete a Virtual Machine Node • 79, 80
 - Delete an Application • 167
 - Delete an Element • 25
 - Delete an Interface • xiv, 78, 90
 - Delete Control Systems and Virtual Hosts • 79, 80
 - Delete Firmware • 168
 - Deleting a Device • 29, 37
 - Deleting a Policy • 113
 - Deleting a Port • 41
 - Deleting a User From a Group • 106, 107
 - Describe Method versus Select Method • 53, 94
 - Describe Nodes • 95
 - Device and Port Icons • 27
 - Device Asset Report • 147
 - Device Group Data Report • 147
 - Device Group Manager • 50
 - Device Power Manager • 48
 - Device Profile Screen • 29
 - Device Settings • xiv, 177
 - Device Setup • 13, 14
 - Devices, Device Groups, and Ports • 26
 - Diagnostic Console • 5, 162, 216
 - Diagnostic Console Account Configuration • 235
 - Diagnostic Console Password Settings • 219, 231, 234
 - Disconnecting Users • 49
 - Discover and Add Devices • 15
 - Discovering Devices • 31, 33
 - Display Disk Status • 238
 - Display NTP Status • 240
 - Distinguished Names for LDAP and AD • 123

E

- E1 Environmental Requirements • 243
- E1 General Specifications • 243
- E1 Model • 243
- Edit a Category • 23
- Edit a CC-NOC • 204
- Edit a Device Group • 53
- Edit a Node • 71
- Edit a Node Group • 97
- Edit a User • 105
- Edit a User Group • 102
- Edit an Element • 24
- Edit an Interface • 90
- Edit Control Systems, Virtual Hosts, and Virtual Machines • 78, 80
- Edit Diagnostic Console Configuration • 219
- Edit Network Interfaces Configuration (Network Interfaces) • 220
- Edit Static Routes • 172, 222, 224
- Editing a Device • 36
- Editing a Policy • 112
- Editing a Port • 40
- Editing a PowerStrip Device or a Dominion PX Device • xiv, 36
- Editing an AD Module • 130
- Email Notifications for Tasks • 196
- Enable or Disable Daily Synchronization of All AD Modules • 133
- Enable or Disable Daily Synchronization of the Virtual Infrastructure • 81
- End SSH Connections • 210, 212
- Ending CC-SG Session • 163
- Entering Maintenance Mode • xvi, 12, 153, 160, 165
- Error Log Report • 143
- Establishing Order of External AA Servers • 124
- Example
 - Adding a Web Browser Interface to a PX Node • 88, 89
- Exit CC-SG • 163
- Exiting Maintenance Mode • xvii, 154, 161

F

- FAQs • 265
- Filter by Device Group • 115
- Filter by Node Group • 115
- Find and View Tasks • 197
- Finding Your CC-SG Serial Number • 213

- Flow for Authentication • 122

G

- General FAQs • 265
- Get Help for SSH Commands • 206
- Getting Started • 10
- Grouping FAQs • 270

H

- Hide or Show Report Filters • 142
- How to Create Associations • 23
- How-To
 - CC-SG Essentials • xv

I

- Importing AD User Groups • 130
- Install the Thick Client • 6
- Interfaces for DRAC, RSA, and ILO Processor Power Control Connections • 84, 86
- Interfaces for In-Band Connections • xiv, 84, 85
- Interfaces for IPMI Power Control Connections • 84, 87
- Interfaces for Managed Powerstrip Connections • 55, 56, 57, 59, 60, 61, 84, 86
- Interfaces for Out-of-Band KVM, Out-of-Band Serial Connections • 84, 85
- Interoperability FAQs • 271
- Introduction • 1
- IP-Reach and UST-IP Administration • 50

J

- JRE Incompatibility • xiv, 5, 6

K

- Keyboard Shortcuts • 273

L

- Launch CC-NOC • 204
- Launching a Device's Administrative Page • 48
- LDAP Advanced Settings • 135
- LDAP General Settings • 134
- Locked Out Users Report • 145
- Lockout settings • 145, 187
- Log Out of CC-SG • 163
- Logging Users Out • 108
- Login Settings • xvi, 186

M

Maintenance Mode • 112, 153
 Managed Powerstrips • 26, 33, 34, 35, 55, 56
 Managing Device Firmware • 168
 MIB Files • 180
 Move a KX, KX2, KX2-101, KSX2, or P2SC's
 PowerStrip to a Different Port • 57
 Move an SX 3.1's Powerstrip to a Different
 Port • 60, 61

N

Naming Conventions • 13, 23, 24, 33, 35, 38,
 39, 50, 64, 71, 84, 88, 94, 101, 104, 111,
 274
 Navigate Administrator Console • 219
 Navigate Multiple Page Reports • 141
 Node and Interface Icons • 67
 Node Asset Report • 91, 149
 Node Creation Report • 150
 Node Group Data Report • 150
 Node Group Power Control • xviii, 198
 Node Groups Overview • 93
 Node Names • 64
 Node Profile • 65
 Nodes and Interfaces Overview • 63
 Nodes Created by Configuring Ports • 38, 39,
 71
 Nodes Tab • 64
 Nodes, Node Groups, and Interfaces • 26, 63
 Notification Manager • 195, 196

O

OpenLDAP (eDirectory) Configuration Settings
 • 136

P

Paragon II System Controller (P2-SC) • 49
 Pausing CC-SG's Management of a Device •
 47
 PC Clients to CC-SG • 248
 PC Clients to Nodes • 249
 Performance FAQs • 269
 Ping an IP Address • 221
 Pinging a Node • 83
 Pinging the Device • 47
 Policies for Access Control • 18, 50, 98, 101,
 110
 Port Sorting Options • 28
 Portal • 189

Power Off CC-SG System from Diagnostic
 Console • 230
 Power Status Messages • xix
 Powering Down CC-SG • 163
 Prerequisites • 1
 Print a Report • 141
 Purge a Report's Data From CC-SG • 142,
 143, 144, 175
 Purge CC-SG's Internal Log • 175

Q

Query Port Report • 147

R

RADIUS General Settings • 138
 RDP Access to Nodes • 251
 Reboot CC-SG with Diagnostic Console • 229
 Reboot or Force Reboot a Virtual Host Node •
 xiv, 81
 Recommended DHCP Configurations for
 CC-SG • 169, 171, 173, 174
 Recover a Failed CC-SG Node • 183
 Remote Authentication • 98, 122, 184
 Remote System Monitoring Port • 252
 Remove Primary CC-SG Node • 183
 Remove Secondary CC-SG Node • 183
 Reports • 140, 198
 Require AES Encryption between Client and
 CC-SG • 185
 Require strong passwords for all users • 186
 Required Open Ports for CC-SG Networks
 Executive Summary • 245
 Requirements for CC-SG Clusters • 181
 Reschedule a Task • 201, 202
 Reset CC Super-User Password with
 Diagnostic Console • 231
 Reset CC-SG Factory Configuration (Admin) •
 232
 Resetting CC-SG • xiv, 157
 Resize Report Column Width • 140
 Restart CC-SG with Diagnostic Console • 229
 Restarting a Device • 46, 198
 Restarting CC-SG • 159, 171, 229
 Restarting CC-SG after Shutdown • 162
 Restore a Device Configuration (KX, KSX,
 KX101, SX, IP-Reach) • 43
 Restore All Configuration Data Except
 Network Settings to a KX2, KSX2, or
 KX2-101 Device • 44

Restore All Configuration Data to a KX2, KSX2, or KX2-101 Device • 42, 45
Restore Only Device Settings or User and User Group Data to a KX2, KSX2, or KX2-101 Device • 44
Restoring CC-SG • 155, 156
Restoring Device Configurations • 43, 198
Results of Adding an Interface • 90
Resuming Management • 47
Right Click Options in the Devices Tab • 30

S

Save a Backup File • 155
Save a Report to a File • 141
Save, Upload, and Delete Device Backup Files • 45
Saving and Deleting Backup Files • 155
Schedule a Device Firmware Upgrade • 197, 198, 199, 201, 202
Schedule a Task • 197, 201, 202
Schedule a Task that is Similar to Another Task • 202
Schedule Sequential Tasks • 196
Scheduled Reports • 151, 152, 197
Scheduled Tasks and Maintenance Mode • 153
Searching for Devices • 31
Security FAQs • 268
Security Manager • 184, 205
Select Nodes • 94
Serial Admin Port • 213
Service Accounts • xiv, 68
Service Accounts Overview • 68
Set the Default Application for an Interface or Port Type • 167
Set the Port Number for SSH Access to CC-SG • 185
Setting CC-SG Server Time • 10
SNMP Traps • 180, 261
Sort Report Data • 140
Special Access to Paragon II System Devices • 49
Specifications for V1 and E1 • 242
Specify a Base DN • 124
Specify a Distinguished Name for AD • 123
Specify a Distinguished Name for LDAP • 123
Specify a Username for AD • 124
Specifying Modules for Authentication and Authorization • 124
SSH Access to CC-SG • 185, 205
SSH Access to Nodes • 252

SSH Commands and Parameters • 207
Status Console • 218, 238
Sun One LDAP (iPlanet) Configuration Settings • 136
Support for Virtual Media • 114
Supported Environments for Two-Factor Authentication • 264
Synchronize All AD Modules • 130, 131, 132, 133
Synchronize All User Groups with AD • 130, 132
Synchronize the Virtual Infrastructure Now • 80
Synchronizing AD with CC-SG • 131
Synchronizing the Virtual Infrastructure with CC-SG • xiv, 80
System Administrators Group • 100
System Maintenance • 153

T

TACACS+ General Settings • 137
Task Manager • 9, 10, 151, 153, 175, 195, 196
Task Types • 196
Terminology for Virtual Infrastructure • 73
Terminology/Acronyms • 2, 33, 35, 134, 137, 138, 171, 173, 195, 203, 209, 220
The Devices Tab • 27
The Users Tab • 99
Thick Client Access • 6
Tips for Adding a Web Browser Interface • 88, 89
Topology View • 30
Troubleshooting • 263
Two-Factor Authentication • 139, 264
Two-Factor Authentication Known Issues • 264
Two-Factor Authentication Setup Requirements • 264
Two-Factor Authentication Using RADIUS • 139
Types of Custom Views • 115

U

Upgrade Device Firmware Report • xxi, 152, 201
Upgrading a Device • 34, 41, 168
Upgrading CC-SG • xiv, 160
Upgrading CC-SG to a New Firmware Version • xvi

- Upgrading Multiple Devices Within a Limited Time Period • xix
- Upload Firmware • 168
- Use SSH to Connect to a Node via a Serial Out-of-Band Interface • 211
- Use the Thick Client • 7
- Use Traceroute • 223
- User Accounts • 123
- User Experience FAQs • 272
- User Group Data Report • 146
- User Group Privileges • 101, 146, 253
- User Management • 13, 18
- Users and User Groups • 93, 98, 114, 123, 137, 138
- Using Chat • 92
- Using Custom Views in the Admin Client • 116
- Using Reports • 140

V

- V1 Environmental Requirements • 242
- V1 General Specifications • 242
- V1 Model • 242
- View by Category • 115
- View Log Files in Diagnostic Console • 225
- View login settings • 186
- View Report Details • 140
- View the Default Application Assignments • 167
- View Top Display with Diagnostic Console • 239
- Viewing Devices • 27
- Viewing Nodes • 64
- Virtual Nodes Overview • 74
- VNC Access to Nodes • 251

W

- Web Browser Interface • 84, 88
- Web Services API • 214
- What is a CC-SG Cluster? • 181
- What is Active/Active mode? • 169, 172
- What is Primary/Backup mode? • 169, 170
- What's New in the CC-SG Administrators Guide • xiv
- Wildcard Examples • 31
- Wildcards for Search • 31

Y

- Your User Profile • 107

▶ **U.S./Canada/Latin America**

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

▶ **China**

Beijing

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

Shanghai

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

GuangZhou

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

▶ **India**

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

▶ **Japan**

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

▶ **Europe**

Europe

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

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

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

▶ **Korea**

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

▶ **Melbourne, Australia**

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

▶ **Taiwan**

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