



# CC-SG

## CommandCenter Secure Gateway

Administrators Guide

Release 3.2

Copyright © 2007 Raritan, Inc.  
CCA-0F-E  
October 2007  
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 2007 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

## How-To: CC-SG Essentials 15

---

How to configure and enforce strong passwords.....	15
Upgrade CC-SG to a new firmware version.....	16
Control power to a node group and monitor the power control operation.....	17
Node Group Power Control .....	17
Power Status Messages.....	18
Upgrade multiple devices within a limited time period.....	19
Assign a Default Custom View of Nodes for All Users .....	21

## Chapter 1 Introduction 1

---

Prerequisites.....	1
Terminology/Acronyms .....	2

## Chapter 2 Accessing CC-SG 5

---

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

## Chapter 3 Getting Started 10

---

Confirm IP Address .....	10
Set the CC-SG Server Time.....	10
Check the Compatibility Matrix.....	11
Check and Upgrade Application Versions .....	12

## 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
Create Groups.....	16
Add Device Groups and Node Groups.....	17

## Contents

User Management .....	19
Add User Groups and Users .....	19
<b>Chapter 5 Associations, Categories, and Elements</b> .....	<b>22</b>
About Associations .....	22
Association Terminology .....	22
Associations--Defining Categories and Elements.....	23
How to Create Associations.....	24
Association Manager.....	24
Add a Category .....	24
Edit a Category .....	24
Delete a Category .....	25
Add an Element.....	25
Edit an Element .....	25
Delete an Element .....	26
<b>Chapter 6 Devices and Ports</b> .....	<b>27</b>
Viewing Devices .....	28
The Devices Tab .....	28
Device Profile Screen .....	29
Device and Port Icons .....	29
Port Sorting Options .....	30
Right Click Options in the Devices Tab .....	30
Search for Devices .....	30
Wildcards for Search.....	30
Wildcard Examples.....	31
Discover Devices .....	31
Add a Device.....	32
Add a KVM or Serial Device .....	33
Add a PowerStrip Device.....	34
Edit a Device .....	34
Edit a PowerStrip Device.....	34
Delete a Device .....	35
Configure Ports.....	35
Configure a Serial Port .....	35
Configure a KVM Port.....	36
Edit a Port.....	37
Delete a Port.....	37
Bulk Copy for Device Categories and Elements .....	37
Upgrade a Device .....	38
Backup Device Configuration.....	39
Restore Device Configurations.....	40
About Restoring Device Configurations.....	40
Restore a Device Configuration (KX, KSX, KX101, SX, IP-Reach).....	40

Restore All Configuration Data Except Network Settings to a KX2 Device .....	41
Restore Only Device Settings or User and User Group Data to a KX2 Device .....	41
Restore All Configuration Data to a KX2 Device .....	41
Copy Device Configuration .....	42
Restart Device .....	42
Ping Device.....	43
Pause Management .....	43
Resume Management.....	43
Device Power Manager.....	44
Launch Admin.....	44
Topological View.....	44
Disconnect Users .....	45
Special Access to Paragon II System Devices .....	45
Paragon II System Controller (P2-SC) .....	45
IP-Reach and UST-IP Administration .....	46
Device Group Manager .....	46
Add a Device Group.....	46
Edit a Device Group.....	49
Delete a Device Group.....	49
<b>Chapter 7 Managed Powerstrips .....</b>	<b>51</b>
<hr/>	
Process for Configuring Power Control in CC-SG.....	51
Configuring PowerStrips Connected to KX, KX2, and P2SC .....	52
Add a PowerStrip Device Connected to a KX, KX2, or P2SC Device .....	52
Move a KX, KX2, or P2SC's PowerStrip to a Different Port .....	52
Delete a PowerStrip Connected to a KX, KX2, or P2SC Device .....	53
Configuring PowerStrips Connected to SX 3.0 and KSX .....	53
Add a PowerStrip Connected to an SX 3.0 or KSX device.....	53
Delete a PowerStrip Connected to an SX 3.0 or KSX Device.....	54
Change a PowerStrip's Device or Port Association (SX 3.0, KSX) .....	54
Configuring PowerStrips Connected to SX 3.1.....	55
Add a PowerStrip Device Connected to an SX 3.1 Device .....	55
Move an SX 3.1's PowerStrip to a Different Port .....	56
Delete a PowerStrip Connected to a SX 3.1 Device .....	56
Configure Outlets on a PowerStrip.....	56
<b>Chapter 8 Nodes, Node Groups, and Interfaces .....</b>	<b>58</b>
<hr/>	
Viewing Nodes .....	58
Nodes Tab .....	59
Node Profile.....	59
Node and Interface Icons .....	60
Nodes and Interfaces Overview .....	60
About Nodes.....	60

## Contents

Node Names .....	60
About Interfaces .....	61
Add a Node .....	61
Nodes Created by Configuring Ports .....	62
Add an Interface .....	62
Interfaces for In-Band connections .....	64
Interfaces for Out-of-Band KVM, Out-of-Band Serial connections .....	64
Interfaces for DRAC, RSA and ILO Processor power control connections .....	64
Interfaces for Managed Power Strip connections .....	65
Interfaces for IPMI Power Control connections .....	65
Web Browser Interface .....	66
Results of Adding an Interface .....	68
Edit an Interface .....	68
Delete an Interface .....	68
Bookmark an Interface .....	69
Edit a Node .....	70
Delete a Node .....	70
Bulk Copy for Node Categories and Elements .....	71
Connect to a Node .....	71
Ping a Node .....	71
Chat .....	72
About Node Groups .....	73
Add a Node Group .....	74
Select Nodes .....	74
Describe Nodes .....	74
Edit a Node Group .....	77
Delete a Node Group .....	77

## Chapter 9 Users and User Groups 78

---

The Users Tab .....	79
Default User Groups .....	80
CC Super-User Group .....	80
System Administrators Group .....	80
CC Users Group .....	80
Add a User Group .....	81
Edit a User Group .....	82
Delete a User Group .....	83
Add a User .....	83
Edit a User .....	84
Delete a User .....	85
Assign a User to a Group .....	86
Delete a User From a Group .....	87
Your User Profile .....	87
About My Profile .....	87
Change your password .....	87

Change your default search preference .....	88
Change the CC-SG default font size .....	88
Change your email address .....	88
Change the CC-SG Super User's Username .....	88
Logout Users .....	89
Bulk Copy for Users .....	89
<b>Chapter 10 Policies for Access Control</b> .....	<b>91</b>
<hr/>	
Controlling Access Using Policies.....	91
Add a Policy .....	92
Edit a Policy.....	93
Delete a Policy.....	95
Support for Virtual Media.....	95
What is Virtual Media?.....	96
Assigning Policies To User Groups .....	98
<b>Chapter 11 Custom Views for Devices and Nodes</b> .....	<b>99</b>
<hr/>	
Types of Custom Views.....	99
View by Category.....	99
Filter by Node Group .....	99
Filter by Device Group .....	100
Using Custom Views in the Admin Client .....	100
Custom Views for Nodes .....	100
Custom Views for Devices.....	103
<b>Chapter 12 Remote Authentication</b> .....	<b>107</b>
<hr/>	
About Authentication and Authorization (AA).....	107
Flow for Authentication .....	107
User Accounts.....	108
Distinguished Names for LDAP and AD.....	108
Specifying a Distinguished Name for AD .....	109
Specifying a Distinguished Name for LDAP.....	109
Specifying a Username for AD.....	109
Specifying a Base DN.....	109
Specify Modules for Authentication and Authorization .....	109
Establish Order of External AA Servers .....	110
About AD and CC-SG.....	110
Add an AD Module to CC-SG .....	110
AD General Settings.....	111
AD Advanced Settings .....	112
AD Group Settings.....	114
AD Trust Settings .....	114

## Contents

Edit an AD Module .....	115
Import AD User Groups.....	116
Synchronize AD with CC-SG.....	117
Synchronize All User Groups with AD.....	118
Synchronize All AD Modules.....	119
Enable or Disable Daily Synchronization of All AD Modules.....	119
Change the Daily AD Synchronization Time .....	120
About LDAP and CC-SG.....	120
Add an LDAP (Netscape) Module to CC-SG .....	120
LDAP General Settings.....	121
LDAP Advanced Settings .....	122
Sun One LDAP (iPlanet) Configuration Settings.....	123
OpenLDAP (eDirectory) Configuration Settings.....	123
About TACACS+ and CC-SG .....	124
Add a TACACS+ Module.....	124
TACACS+ General Settings .....	124
About RADIUS and CC-SG .....	125
Add a RADIUS Module.....	125
RADIUS General Settings .....	125
Two-Factor Authentication Using RADIUS .....	126
Chapter 13 Reports .....	127
<hr/>	
Using Reports.....	127
Sort report data.....	127
Resize report column width.....	127
View report details.....	128
Navigate multiple page reports .....	128
Print a report display .....	128
Save a report to a file .....	128
Purge a report's data from CC-SG .....	128
Show or hide report filters .....	129

Audit Trail Report ..... 129

Error Log Report..... 130

Access Report..... 130

Availability Report..... 131

Active Users Report ..... 132

Locked Out Users Report ..... 132

User Data Report ..... 132

Users in Groups Report ..... 133

Group Data Report..... 133

AD User Group Report..... 134

Asset Management Report..... 134

Node Asset Report ..... 135

Active Nodes Report..... 135

Node Creation Report..... 136

Query Port Report ..... 136

Active Ports Report ..... 138

Scheduled Reports..... 138

Upgrade Device Firmware Report..... 139

CC-NOC Synchronization Report..... 139

**Chapter 14 System Maintenance 140**

---

Maintenance Mode..... 140

    Scheduled Tasks and Maintenance Mode..... 140

Enter Maintenance Mode ..... 141

Exit Maintenance Mode..... 141

Backup CC-SG ..... 141

Saving and Deleting Backup Files..... 143

    Save a backup file..... 143

    Delete a backup file..... 143

Restore CC-SG ..... 143

Reset CC-SG ..... 145

Restart CC-SG ..... 145

Upgrade CC-SG ..... 146

Shutdown CC-SG ..... 147

Restarting CC-SG after Shutdown ..... 147

Power Down CC-SG ..... 148

End CC-SG Session ..... 148

    Log Out of CC-SG ..... 148

    Exit CC-SG ..... 149

Chapter 15 Advanced Administration 150

---

- Configuring a Message of the Day ..... 150
- Configuring Applications for Accessing Nodes..... 151
  - About Applications for Accessing Nodes..... 151
  - Check and Upgrade Application Versions ..... 151
  - Add an Application ..... 152
  - Delete an Application ..... 153
- Configuring Default Applications ..... 153
  - About Default Applications..... 153
  - View the Default Application Assignments ..... 153
  - Set the Default Application for an Interface or Port Type ..... 153
- Managing Device Firmware..... 154
  - Upload Firmware ..... 154
  - Delete Firmware ..... 154
- Configuring the CC-SG Network..... 154
  - About Network Setup..... 155
  - About CC-SG LAN Ports ..... 155
  - What is Primary/Backup mode?..... 156
  - What is Active/Active mode? ..... 159
  - Recommended DHCP Configurations for CC-SG..... 161
- Configuring Logging Activity ..... 161
  - Purging CC-SG's Internal Log ..... 162
- Configuring the CC-SG Server Time and Date ..... 162
- Modem Configuration ..... 163
  - Configure CC-SG..... 163
  - Configure the Modem on Client PC ..... 164
  - Configure the Dial-up Connection ..... 164
  - Configure the Call-back Connection ..... 165
  - Connect to CC-SG with Modem..... 166
- Connection Modes: Direct and Proxy ..... 167
  - About Connection Modes ..... 167
  - To Configure Direct Mode for All Client Connections ..... 167
  - To Configure Proxy Mode for All Client Connections..... 167
  - To Configure a Combination of Direct Mode and Proxy Mode ..... 168
- Device Settings..... 168
- Configuring SNMP..... 169
  - About SNMP and CC-SG ..... 169
  - MIB Files..... 169
  - To Configure SNMP in CC-SG ..... 169
- Configuring CC-SG Clusters..... 170
  - What is a CC-SG Cluster? ..... 170
  - Requirements for CC-SG Clusters ..... 171
  - About CC-SG Clusters and CC-NOC..... 171
  - Create a Cluster ..... 171

Remove Secondary CC-SG Node.....	172
Remove Primary CC-SG Node.....	173
Recover a Failed CC-SG Node.....	173
Advanced Cluster Settings.....	173
Security Manager.....	174
Remote Authentication.....	174
AES Encryption .....	174
Configure Browser Connection Protocol: HTTP or HTTPS/SSL .....	175
Setting the Port Number for SSH Access to CC-SG.....	175
Login Settings .....	175
Configuring the Inactivity Timer .....	179
Portal.....	179
Certificates.....	180
Access Control List.....	184
Notification Manager.....	185
Configure an external SMTP server.....	185
Task Manager.....	186
Task Types.....	187
Scheduling Sequential Tasks .....	187
Email Notifications for Tasks .....	187
Scheduled Reports .....	187
Schedule a Task .....	188
Schedule a Device Firmware Upgrade.....	190
View a Task, Details of a Task, and Task History.....	192
CommandCenter NOC.....	193
Add a CC-NOC .....	193
Edit a CC-NOC.....	195
Launch CC-NOC .....	195
Delete a CC-NOC .....	195
SSH Access to CC-SG.....	196
SSH Commands.....	197
Command Tips .....	199
Create an SSH Connection to an SX Device.....	200
Use SSH to Connect to a Node via a Serial Out of Band Interface .....	201
Exit an SSH Session.....	202
Serial Admin Port.....	202
About Terminal Emulation Programs.....	202

Contents

Web Services API..... 203

**Chapter 16 Diagnostic Console 204**

---

    Accessing Diagnostic Console via VGA/Keyboard/Mouse Port..... 205

    Accessing Diagnostic Console via SSH ..... 205

    About Status Console..... 206

    Accessing Status Console ..... 206

    About Administrator Console ..... 207

    Accessing Administrator Console..... 207

    Navigating Administrator Console ..... 208

    Editing Diagnostic Console Configuration..... 209

    Editing Network Interfaces Configuration (Network Interfaces)..... 210

    Ping an IP Address (Network Interfaces) ..... 211

    Using Traceroute (Network Interfaces)..... 213

    Editing Static Routes (Network Interfaces)..... 214

    Viewing Log Files in Diagnostic Console (Admin) ..... 215

    Restarting CC-SG with Diagnostic Console..... 219

    Rebooting CC-SG with Diagnostic Console..... 220

    Powering Off the CC-SG System from Diagnostic Console ..... 221

    Resetting CC Super User Password with Diagnostic Console ..... 222

    Resetting CC-SG Factory Configuration (Admin) ..... 224

    Diagnostic Console Password Settings..... 226

    Account Configuration ..... 228

    Displaying Disk Status (Utilities) ..... 230

    Viewing Top Display with Diagnostic Console ..... 231

    Displaying NTP Status (Utilities)..... 232

**Appendix A Specifications for G1, V1, and E1 234**

---

    G1 Model ..... 234

        G1 General Specifications ..... 234

        G1 Hardware Specifications ..... 234

        G1 Environmental Requirements..... 235

    V1 Model ..... 235

        V1 General Specifications..... 235

        V1 Hardware Specifications ..... 236

        V1 Environmental Requirements..... 236

    E1 Model..... 237

        E1 General Specifications ..... 237

        E1 Hardware Specifications ..... 237

        E1 Environmental Requirements ..... 237

Appendix B	CC-SG and Network Configuration	239
<hr/>		
	About this Appendix .....	239
	Required Open Ports for CC-SG Networks: Executive Summary .....	239
	CC-SG Communication Channels.....	240
	CC-SG and Raritan Devices .....	241
	CC-SG Clustering.....	241
	Access to Infrastructure Services .....	242
	PC Clients to CC-SG .....	242
	PC Clients to Nodes.....	243
	CC-SG & Client for IPMI, iLO/RILOE, DRAC, RSA.....	243
	CC-SG & SNMP .....	244
	CC-SG & CC-NOC .....	244
	CC-SG Internal Ports .....	245
	CC-SG Access via NAT-enabled Firewall.....	245

## Contents

Appendix C	User Group Privileges	246
<hr/>		
Appendix D	SNMP Traps	258
<hr/>		
Appendix E	Troubleshooting	260
<hr/>		
	Client Browser Requirements .....	260
Appendix F	Two-Factor Authentication	261
<hr/>		
	Supported Environments for Two-Factor Authentication.....	261
	Two-Factor Authentication Setup Requirements.....	261
	Two-Factor Authentication Known Issues .....	262
Appendix G	FAQs	263
<hr/>		
Appendix H	Keyboard Shortcuts	270
<hr/>		
Appendix I	Naming Conventions	271
<hr/>		
Index		273
<hr/>		

# How-To: CC-SG Essentials

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

## In This Chapter

How to configure and enforce strong passwords .....	15
Upgrade CC-SG to a new firmware version .....	16
Control power to a node group and monitor the power control operation	17
Upgrade multiple devices within a limited time period .....	19
Assign a Default Custom View of Nodes for All Users .....	21

---

## How to configure and enforce strong passwords

1. Choose **Administration > Security**.
2. Open the **Login Settings** tab.
3. Check the **Strong Passwords Required for All Users** checkbox.
4. Select a **Maximum Password Length**. Passwords must contain fewer than the maximum number of characters.
5. Select a **Password History Depth**. The number specifies how many previous passwords are kept in the history and cannot be reused. For example, if **Password History Depth** is set to 5, users cannot reuse any of their previous 5 passwords.
6. Select a **Password Expiration Frequency**. All passwords expire after a set number of days. After a password expires, users will be asked to choose a new password the next time they log in.
7. Select **Strong Password Requirements**:
  - Passwords must contain at least one lower case letter.
  - Passwords must contain at least one upper case letter.

## Upgrade CC-SG to a new firmware version

- Passwords must contain at least one number.
  - Passwords must contain at least one special character (for example, an exclamation point or ampersand).
8. Click **Update** to save your changes.

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

---

## Upgrade CC-SG to a new firmware version

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

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

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

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

---

### Important!

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

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

---

➤ *To upgrade CC-SG:*

1. Download the firmware file to your client PC.
2. *Enter Maintenance Mode* (on page 141)
3. Once CC-SG is in maintenance mode, choose **System Maintenance > Upgrade**.
4. Click **Browse**. Navigate to and select the CC-SG firmware file, and then click **Open**.
5. Click **OK** to upload the firmware file to CC-SG.

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

6. Click **OK** to exit CC-SG and allow it to restart. You must wait approximately 8 minutes while CC-SG restarts.
7. Close your browser window, and then clear your browser cache.
8. After 8 minutes, open a new browser window and launch CC-SG.
9. Choose **Help > About Raritan Secure Gateway**. Check the version number to verify that the upgrade was successful.
  - If the version has not upgraded, repeat the previous steps.
  - If upgrade was successful, proceed to the next step.

*Exit Maintenance Mode* (on page 141)

---

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

---

### Node Group Power Control

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

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

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

1. Click the **Nodes** tab.
2. On the **Nodes** menu, click **Group Power Control**. The **Group Power Control** screen appears.
3. Click the **Node Group** drop-down arrow and select the node group whose power you want to control from the list.

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

4. In the **Available** list, select the specific interface that you want to perform power control on, and then click **Add** to move the interface to the **Selected** list. Repeat this step until you have added all necessary interfaces to the **Selected** list. If you must remove an interface, select the interface in the **Selected** list, and then click **Remove**.
5. You must put the interfaces in the **Selected** list into the order in which you would like CC-SG to perform the power operation. Select an interface in the **Selected** list, and then click the up and down arrows to move the interfaces into the desired sequence.
6. Click the **Operation** drop-down arrow, and select **Power On**, **Power Off**, **Power Cycle** or **Graceful Shutdown** from the list.
7. If you selected **Power On**, **Power Off** or **Graceful Shutdown** in the **Operation** field, type the number of seconds, from 0-120, that should elapse between interfaces in the **Sequence Interval (seconds)** field.
8. Click **OK** to send the power operation request through the selected interfaces. A confirmation message appears in the screen.
9. A Power Status Messages window opens to show you the status of the power control operation. Messages populate the window as new information is received about the power control operation. Keep this window open until all power control operations are complete, so you can monitor progress.

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

---

### Power Status Messages

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

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

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

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

- Power control operation request is sent.
- Power control operation fails.
- Power control operation completes successfully.

- All power control operations requested complete successfully.
- *How to get status updates if you close the Power Status Messages window:*

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

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

---

## Upgrade multiple devices within a limited time period

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

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

- *To schedule a Device Firmware Upgrade:*
  1. Choose Administration > Tasks.
  2. Click New.
  3. In the Main tab, type a name and description for the task. The Name you choose will be used to identify the task and the report associated with the task.
  4. Open the Task Data tab.
  5. Specify the device upgrade details:
    - a. Task Operation: Select Upgrade Device Firmware.
    - b. Device Group: Select the device group that contains the devices you want to upgrade.
    - c. Device Type: Select the type of device you want to upgrade. If you need to upgrade more than one device type, you must schedule a task for each type.

## Upgrade multiple devices within a limited time period

- d. Concurrent Upgrades: Specify the number of devices that should begin the file transfer portion of the upgrade simultaneously. Maximum is 10. As each file transfer completes, a new file transfer will begin, ensuring that only the maximum number of concurrent transfers occurs at once.
  - e. Upgrade File: Select the firmware version you want to upgrade to. Only available upgrade files that are appropriate for the device type selected will display as options.
6. Specify the time period for the upgrade:
    - a. Start Date/Time: Select the date and time at which the task begins. The start date/time must be later than the current date/time.
    - b. Restrict Upgrade Window and Latest Upgrade Start Date/Time: If you must finish all upgrades within a specific window of time, use these fields to specify the date and time after which no new upgrades can begin. Select Restrict Upgrade Window to enable the Latest Upgrade Start Date/Time field.
  7. Specify which devices will be upgraded, and in what order. Place higher priority devices at the top of the list.:
    - a. In the Available list, select each device you want to upgrade, and click Add to move it to the Selected list.
    - b. In the Selected list, select a device and use the arrow buttons to move the devices into the order in which you want upgrades to proceed.
  8. Open the Retry tab. Specify whether failed upgrades should be retried.
    - a. Retry Count: Type the number of times CC-SG should retry a failed upgrade.
    - b. Retry Interval: Enter the time that should elapse between retries. Default times are 30, 60, and 90 minutes. These are the optimal retry intervals.
  9. Open the Notification tab. Specify email addresses that should receive notifications of success and failure. By default, the email address of the user currently logged in is available. User email addresses are configured in the User Profile.
    - a. Click Add, type the email address in the window that appears, and then click OK.
    - b. Select On Failure if you want an email sent if an upgrade fails.

- c. Select **On Success** if you want an email sent when all upgrades complete successfully
10. Click **OK** to save your changes.

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

---

## Assign a Default Custom View of Nodes for All Users

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

1. Click the **Nodes** tab.
2. Choose **Nodes > Change View > Create Custom View**.
3. Click the **Name** drop-down arrow, and select the custom view you want assign as a system-wide default view.
4. Check the **System Wide** checkbox, and then click **Save**.

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

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



# Chapter 1 Introduction

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

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

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

## In This Chapter

Prerequisites .....	1
Terminology/Acronyms.....	2

---

## Prerequisites

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

## Terminology/Acronyms

Terms and acronyms found in this document include:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Terminology/Acronyms

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

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

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

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

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

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

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

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

## Chapter 2 Accessing CC-SG

You can access CC-SG in several ways:

- **Browser:** CC-SG supports numerous web browsers. (For a complete list of supported browsers, please refer to the Compatibility Matrix on the Raritan Support website.
- **Thick Client:** You can install a Java Web Start thick client on your client computer. The thick client functions exactly like the browser-based client.
- **SSH:** Remote devices connected via the serial port can be accessed using SSH. Please refer to *Advanced Administration* (on page 150) for details.
- **Diagnostic Console:** Provides emergency repair and diagnostics only and is not a replacement for the browser-based GUI to configure and operate CC-SG. Please refer to *Advanced Administration* (on page 150) for details.

---

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

---

### In This Chapter

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

---

### Browser-Based Access

1. Using a supported Internet browser, type this URL:  
`https://<IP_address>/admin` where <IP\_address> is the IP address of the CC-SG. For example, **`https://10.20.3.30/admin`**.
2. When the security alert window appears, click **Yes** to continue.
3. You will be warned if you are using an unsupported Java Runtime Environment version on your machine. From the window that pops up, select whether you will download the correct JRE version from the CC-SG server (if available), download it from the Sun Microsystems website, or continue with the incorrect version, and then click **OK**. The Login window appears.
4. If the Restricted Service Agreement is enabled, read the agreement text, and then check the **I Understand and Accept the Restricted Service Agreement** checkbox.

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

---

## Thick Client Access

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

---

### Install the Thick Client

- *To download the thick client from CC-SG:*
1. Launch a web browser and type this URL:  
**http(s)://<IP\_address>/install** where <IP\_address> is the IP address of the CC-SG.
    - If a security warning message appears, click **Start** to continue the download.
    - If your client computer is running Java version 1.4, a **Desktop Integration** window appears. If you want Java to add a shortcut icon for the thick client to your desktop, click **Yes**.
  2. When the download is complete, a new window in which you can specify the CC-SG IP address appears.
  3. Type the IP address of the CC-SG unit you want to access in the **IP to Connect** field. Once you have connected, this address will be available from the **IP to Connect** drop-down list. The IP addresses are stored in a properties file that is saved to your desktop.
  4. If the CC-SG is configured for secure browser connections, you must check the **Secure Socket Layer (SSL)** checkbox. If the CC-SG is not configured for secure browser connections, you must clear the **Secure Socket Layer (SSL)** checkbox. This setting must be correct or the thick client will not be able to connect to CC-SG.
  5. **To check the setting in CC-SG:** Choose **Administration > Security**. In the **Encryption** tab, look at the **Browser Connection Protocol** option. If the **HTTPS/SSL** option is selected, then you must check the **Secure Socket Layer SSL** checkbox in the thick client's IP address specification window. If the **HTTP** option is selected, then you must clear the **Secure Socket Layer SSL** checkbox in the thick client's IP address specification window.
  6. Click **Start**.

- A warning message appears if you are using an unsupported Java Runtime Environment version on your machine. Follow the prompts to either download a supported Java version, or continue with the currently installed version.
7. The login screen appears.
  8. If the Restricted Service Agreement is enabled, read the agreement text, and then select the **I Understand and Accept the Restricted Service Agreement** checkbox.
  9. Type your **Username** and **Password** in the corresponding fields, and then click **Login** to continue.

---

### Use the Thick Client

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

#### ➤ *Java 1.4.x*

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

#### ➤ *Java 1.5*

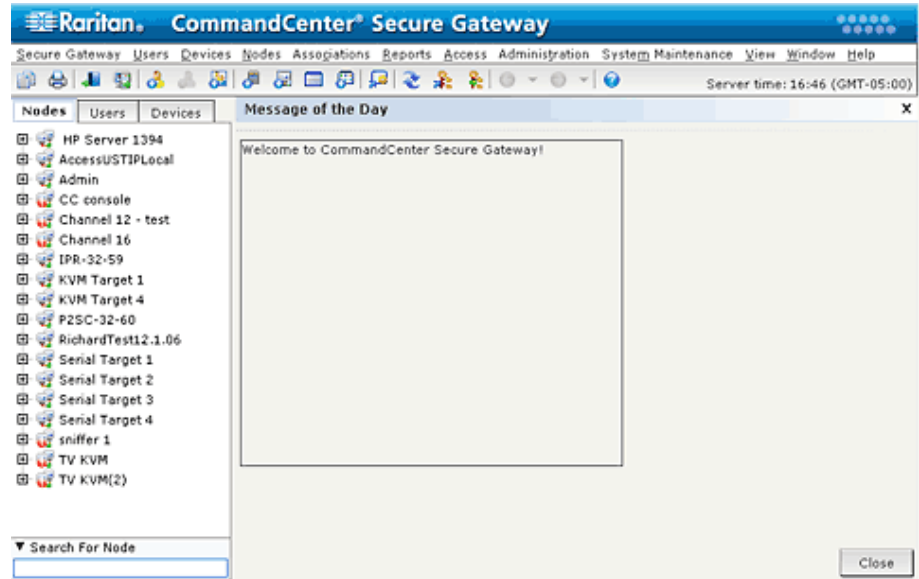
If your client computer is running **Java version 1.5**, you can:

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

---

## CC-SG Admin Client

Upon valid login, the CC-SG Admin Client appears.



- **Nodes tab:** Click the **Nodes** tab to display all known target nodes in a tree view. Click a node to view the Node Profile. Interfaces are grouped under their parent nodes. Click the + and - signs to expand or collapse the tree. Right-click an interface and select **Connect** to connect to that interface. You can sort the nodes by Node Name (alphabetical) or Node Status (Available, Busy, Unavailable). Right-click the tree view, select **Node Sorting Options**, and then select **By Node Name** or **By Node Status**.
- **Users tab:** Click the **Users** tab to display all registered Users and Groups in a tree view. Click the + and - signs to expand or collapse the tree.
- **Devices tab:** Click the **Devices** tab to display all known Raritan devices in a tree view. Different device types have different icons. Ports are grouped under their parent devices. Click the + and - signs to expand or collapse the tree. Click a port to view the Port Profile. Right-click a port and select **Connect** to connect to that port. You can sort the ports by Port Name (alphabetical) or Port Status (Available, Busy, Unavailable). Right-click the tree view, select **Port Sorting Options**, and then select **By Node Name** or **By Node Status**.
- **Quick Commands toolbar:** This toolbar offers some shortcut buttons for executing common commands.
- **Operation and Configuration menu bar:** These menus contain commands to operate and configure CC-SG. You can also access some of these commands by right-clicking on the icons in the **Nodes**, **Users**, and **Devices** Selection tabs. The menus and menu items you see are determined by your user access privileges.
- **Server time:** The current time and time zone as configured on CC-SG in Configuration Manager. This time is used when scheduling tasks in Task Manager. Please refer to *Task Manager* (on page 186) for details. This time may be different than the time your client PC uses.

# Chapter 3 Getting Started

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

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

## In This Chapter

Confirm IP Address.....	10
Set the CC-SG Server Time .....	10
Check the Compatibility Matrix .....	11
Check and Upgrade Application Versions.....	12

---

### Confirm IP Address

1. Choose **Administration > Configuration**.
2. Click the **Network Setup** tab.
3. (Optional) Check that the network setting are correct, and make changes if needed. Please refer to *About Network Setup* (on page 155) for details.
4. Click **Update Configuration** to submit your changes.
5. Click **Restart Now** to confirm your settings and restart CC-SG.

---

### Set the CC-SG Server Time

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

---

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

---

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

Changing the time zone is disabled in a cluster configuration.

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

1. Choose Administration > Configuration.

2. Click the **Time/Date** tab.
  - a. **To set the date and time manually:** **Date**-click the drop-down arrow to select the **Month**, use the up and down arrows to select the **Year**, and then click the **Day** in the calendar area. **Time**-use the up and down arrows to set the **Hour**, **Minutes**, and **Seconds**, and then click the **Time zone** drop-down arrow to select the time zone in which you are operating CC-SG.
  - b. **To set the date and time via NTP:** Check the **Enable Network Time Protocol** checkbox at the bottom of the window, and then type the IP addresses for the **Primary NTP server** and the **Secondary NTP server** in the corresponding fields.

---

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

---

3. Click **Update Configuration** to apply the time and date changes to CC-SG.
4. Click **Refresh** to reload the new server time in the **Current Time** field.

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

---

## Check the Compatibility Matrix

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

- *To check the Compatibility Matrix:*
  - On the **Administration** menu, click **Compatibility Matrix**.

---

### Check and Upgrade Application Versions

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

➤ *To check an application version:*

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

➤ *To upgrade an application:*

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

1. Save the application file to your client PC.
2. Click the **Application name** drop-down arrow and select the application that must be upgraded from the list. If you do not see the application, you must add it first. *Add an Application* (on page 152)
3. Click **Browse**, locate and select the application upgrade file from the dialog that displays, and then click **Open**.
4. The application name appears in the **New Application File** field in the **Application Manager** screen.
5. Click **Upload**. A progress window indicates that the new application is being uploaded. When complete, a new window will indicate that the application has been added to the CC-SG database and is available to use.
6. If the **Version** field does not automatically update, type the new version number in the **Version** field. The **Version** field will automatically update for some applications.
7. Click **Update**.

# Chapter 4    Configuring CC-SG with Guided Setup

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

Guided Setup is divided into 4 tasks:

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

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

## In This Chapter

Before you Use Guided Setup .....	13
Associations in Guided Setup .....	14
Device Setup .....	14
Create Groups .....	16
User Management.....	19

---

## Before you Use Guided Setup

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



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

---

## Associations in Guided Setup

---

### Create Categories and Elements

1. In the Guided Setup window, click **Associations**, and then click **Create Categories** in the left panel to open the **Create Categories** panel.
2. In the **Category Name** field, type the name of a category you want to organize your equipment into, such as "Location."
3. In the **Applicable for** field, you can indicate whether you want to category to be available for devices, nodes, or both. Click the **Applicable for** drop-down menu, and then select a value from the list.
4. In the **Elements** table, type the name of an element within the category, such as "Raritan US."
  - Click the Add New Row icon  to add more rows to the **Elements** table as needed.
  - To delete an element, select its row, and then click the Delete Row icon  to delete the selected element from the **Elements** table.
5. Repeat these steps until you have added all the elements within the category to the **Elements** table.
6. (Optional) If you want to create another category, click **Apply** to save this category, and then repeat the steps in this section to add additional categories.
7. When you have finished creating categories and elements, click **OK**. The Association Summary panel displays a list of the categories and elements that you created.
8. Click **Continue** to start the next task, **Device Setup**. Follow the steps in the next section.

---

## Device Setup

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

---

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





















































































































































































































































































































































































































































































































































