



CommandCenter® Secure Gateway



CC-SG Administrator Guide Release 3.1.1

Copyright © 2007 Raritan, Inc.

CCA-0E-E

April 2007

255-80-5140-00

This page intentionally left blank.

Copyright and Trademark Information

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

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

FCC Information

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

VCCI Information (Japan)

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

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



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

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

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

Safety Guidelines

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

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

Rack Mount Safety Guidelines

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

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

Contents

Chapter 1: Introduction	1
Prerequisites	1
Intended Audience	1
Terminology/Acronyms	1
Chapter 2: Accessing CC-SG	3
Browser-Based Access	3
Thick Client Access	4
Install the Thick Client	4
Use the Thick Client	5
CC-SG Window Components	6
Initial Configurations	7
Confirm IP Address	7
Set the CC-SG Server Time	8
Check and Upgrade CC-SG Firmware Version	9
Check and Upgrade Application Versions	10
Power Down CC-SG	10
Compatibility Matrix	11
Chapter 3: Configuring CC-SG with Guided Setup	13
Prepare to Configure CC-SG with Guided Setup	13
Guided Setup Overview	13
Start Guided Setup:	13
Associations	14
Create Categories and Elements	14
Device Setup	15
Discover and Add Devices	15
Create Groups	18
Add Device Groups and Node Groups	18
Select Devices	19
Describe Devices	19
Select Nodes	21
Describe Nodes	21
User Management	22
Add User Groups and Users	22
Chapter 4: Creating Associations	27
Associations	27
Association Terminology	27
Associations--Defining Categories and Elements	28
How to Create Associations	29
Association Manager	29
Add Category	29
Edit Category	30
Delete Category	31
Add Element	31
Edit Element	32
Delete Element	32
Chapter 5: Adding KVM and Serial Devices and Device Groups	35
The Devices Tab	35

Right Click Options in the Device Tab	35
Device and Port Icons.....	36
Search for Devices	36
Device Profile Screen.....	37
Add a Device	37
Adding a KVM or Serial Device	38
Adding a PowerStrip Device	38
Discover Devices	39
Edit Device	40
Edit PowerStrip Device	41
Delete Device	42
Configure Ports	43
Configure a Serial Port	43
Configure a KVM Port.....	45
Edit Ports	46
Delete Ports	47
Device Management	47
Bulk Copy for Device Categories and Elements	47
Upgrade Device	48
Backup Device Configuration	48
Restore Device Configurations	49
About Restoring Device Configurations	49
To Restore a Device Configuration (KX, KSX, KX101, SX, IP-Reach)	49
To Restore All Configuration Data Except Network Settings to a KX2 Device.....	49
To Restore All Configuration Data to a KX2 Device.....	50
To Restore Only Device Settings or User and User Group Data to a KX2 Device	51
To Copy Device Configuration	51
Restart Device	53
Ping Device	53
Pause Management.....	53
Resume Management	53
Device Power Manager	54
Launch Admin.....	54
Topological View.....	55
Disconnect Users.....	56
Viewing Devices	57
Tree View	57
Custom View	57
Selecting a Custom View.....	58
Add a Custom View	58
Edit a Custom View	59
Delete Custom View	59
Special Access to Paragon II System Devices	60
Paragon II System Controller (P2-SC).....	60
IP-Reach and UST-IP Administration	61
Device Group Manager	62
Add Device Group	62
Select Devices.....	63
Describe Devices.....	64
Edit Device Group.....	66
Delete Device Group	67
Chapter 6: Configuring Power Control.....	69

Process for Configuring Power Control in CC-SG	69
Configuring PowerStrips Connected to KX, KX2, and P2SC	69
Add a PowerStrip Device Connected to a KX, KX2, or P2SC Device.....	69
Move a KX, KX2, or P2SC's PowerStrip to a Different Port.....	69
Delete a PowerStrip Connected to a KX, KX2, or P2SC Device	70
Configuring PowerStrips Connected to SX 3.0 and KSX	70
Add a PowerStrip Connected to an SX 3.0 or KSX device	70
Delete a PowerStrip Connected to an SX 3.0 or KSX Device	71
Change a PowerStrip's Device or Port Association (SX 3.0, KSX).....	71
Configuring PowerStrips Connected to SX 3.1	71
Add a PowerStrip Device Connected to an SX 3.1 Device	71
Move an SX 3.1's PowerStrip to a Different Port.....	72
Delete a PowerStrip Connected to a SX 3.1 Device.....	72
Configure Outlets on a PowerStrip	72
To configure outlets from the PowerStrip profile.....	72
To configure outlets from the Configure Ports screen	72
To delete an outlet.....	72
Chapter 7: Configuring Nodes and Interfaces	75
View Nodes	75
Nodes Tree	75
Node Profile	75
Node and Interface Icons.....	75
Nodes and Interfaces Overview	76
About Nodes	76
Node Names.....	76
About Interfaces.....	76
Add Node	77
Add an Interface.....	77
For In-Band connections and DRAC, RSA, and iLO/RILOE power connections:	79
For Out-of-Band KVM, Out-of-Band Serial connections:	80
For Managed Power Strip connections:.....	81
For IPMI Power Control connections:	82
Results of Adding an Interface.....	82
Bulk Copy for Node Categories and Elements	83
Connect to a Node	83
Edit an Interface	83
Delete an Interface.....	84
Ping a Node	84
Edit a Node	84
Delete a Node	85
Chat.....	87
Node Groups.....	87
Chapter 8: Adding and Managing Users and User Groups.....	89
The Users Tree	89
Special User Groups	90
CC Super-User Group	90
System Administrators Group.....	90
CC Users Group	90
Users Not in Group	90
Add User Groups	91
Edit A User Group	93

Delete User Group	94
Add User	94
Edit a User	95
Delete User	96
Assign Users To Group.....	97
Delete Users From Group	97
Other User and User Group Functions	98
My Profile.....	98
Logout Users	99
To log out all users of a User Group:.....	99
Bulk Copy for Users.....	100
Chapter 9: Policies and Node Groups.....	101
Controlling Access Using Policies.....	101
Policy Summary.....	101
Node Groups.....	102
Add Node Groups	103
Select Nodes	104
Describe Nodes	105
Edit Node Group	107
Delete Node Group.....	107
Device Groups	108
Policy Manager	108
Add Policy.....	108
Edit a Policy	109
Delete a Policy.....	110
Support for Virtual Media	110
What is Virtual Media?.....	110
Applying Policies To User Groups	111
Chapter 10: Configuring Remote Authentication	113
Authentication and Authorization (AA)	113
Flow for Authentication	113
User Accounts	113
Distinguished Names for LDAP and AD	114
Username	114
Base DN	114
Specify Modules for Authentication and Authorization	114
Establish Order of External AA Servers.....	115
AD Configurations.....	115
Add AD Module to CC-SG	115
AD General Settings	116
AD Advanced Settings.....	118
AD Group Settings.....	119
AD Trust Settings.....	120
Edit AD Modules	122
Import AD User Groups	122
Synchronize AD User Groups.....	124
Synchronize All AD Modules	124
Set AD Synchronization Time.....	125
AD Configuration—Upgrade from CC-SG 3.0.2	125
Add LDAP (Netscape) Module to CC-SG	126
LDAP General Settings.....	127

LDAP Advanced Settings	128
Sun One LDAP (iPlanet) Configuration Settings.....	129
OpenLDAP (eDirectory) Configuration Settings.....	129
Add a TACACS+ Module	130
TACACS+ General Settings	131
Add a RADIUS Module	132
RADIUS General Settings	133
Two-Factor Authentication Using RADIUS	133
Chapter 11: Generating Reports	135
Audit Trail Report	135
Error Log Report	136
Access Report.....	137
Availability Report	139
Active Users Report	140
Locked Out Users Report.....	141
User Data Report	142
Users in Groups Report	143
Group Data Report.....	144
AD User Group Report.....	144
Asset Management Report	145
Node Asset Report.....	146
Active Nodes Report	147
Node Creation Report	148
Query Port Report.....	149
Active Ports Report	150
Scheduled Reports.....	151
CC-NOC Synchronization Report	151
Chapter 12: System Maintenance.....	153
About Maintenance Mode	153
Scheduled Tasks and Maintenance Mode.....	153
Entering Maintenance Mode.....	153
Exiting Maintenance Mode	153
Backup CC-SG.....	154
Restore CC-SG	155
Saving and Deleting Backup Files	156
To Save a backup.....	156
To Delete a backup	157
Reset CC-SG	157
Restart CC-SG	157
Upgrade CC-SG.....	158
Shut Down CC-SG	159
Restarting CC-SG after Shutdown.....	159
End CC-SG Session	159
Log Out.....	159
Exit CC-SG	159
Chapter 13: Advanced Administration.....	161
Guided Setup	161
Message of the Day Setup.....	161
Application Manager	162

Adding and Deleting Applications	162
Adding an Application:	162
Deleting an Application:	163
Default Applications	163
Firmware Manager	164
Upload Firmware	164
Delete Firmware	165
Configuration Manager	165
About Network Setup	165
About CC-SG LAN Ports	165
G1 LAN Ports	165
V1 LAN Ports	165
E1 LAN Ports	165
What is Primary/Backup mode?	166
Setup for Primary/Backup mode	166
To configure Primary/Backup mode in CC-SG	167
What is Active/Active mode?	168
Setup for Active/Active mode	168
To configure Active/Active mode in CC-SG	168
Recommended DHCP Configurations for CC-SG	169
Log Configuration	170
Configuring Logging Activity:	170
Purging CC-SG's Internal Log:	171
Inactivity Timer Configuration	171
Time/Date Configuration	172
Modem Configuration	173
Configure CC-SG	173
Configure the Modem on Client PC	173
Configure the Dial-Up Connection	174
Configure the Call-back Connection	176
Connect to CC-SG with Modem	177
Connection Modes: Direct and Proxy	179
About Connection Modes	179
To Configure Direct Mode for All Client Connections	179
To Configure Proxy Mode for All Client Connections	179
To Configure a Combination of Direct Mode and Proxy Mode	180
Device Settings	181
SNMP	181
MIB Files	181
Configuring SNMP in CC-SG	181
Cluster Configuration	182
Create a Cluster	183
Set Primary CC-SG Node	183
Set Secondary CC-SG Node	185
Remove Secondary CC-SG Node	185
Remove Primary CC-SG Node	185
Recover a Failed CC-SG Node	186
Set Advanced Settings	186
Configure Security	187
Remote Authentication	187
About CC-SG and AES Encryption	187
Check Your Browser for AES Encryption	187
Requiring AES Encryption between Client and CC-SG	187

Configuring Browser Connection Protocol: HTTP or HTTPS/SSL	188
Setting the Port Number for SSH Access to CC-SG	188
Login Settings	188
Strong Password Settings	189
Lockout Settings	190
Allow Concurrent Logins per Username	190
Portal	191
Logo	191
Restricted Service Agreement	191
Certificate	192
Export Current Certificate and Private Key	193
Generate Certificate Signing Request	193
Generate Self Signed Certificate Request	195
IP-ACL	195
Notification Manager	197
Task Manager	198
Task Types	198
Scheduling Sequential Tasks	198
Email Notifications for Tasks	198
Scheduled Reports	198
Schedule a New Task	199
View a Task, Details of a Task, and Task History	200
CommandCenter NOC	201
Add a CC-NOC	201
Edit a CC-NOC	203
Launch CC-NOC	203
Delete a CC-NOC	204
SSH Access to CC-SG	205
SSH Commands	206
Command Tips	207
Create an SSH Connection to an SX Device	208
Use SSH to Connect to a Node via a Serial Out of Band Interface	209
Exit a Session	209
Diagnostic Console	210
About Status Console	210
About Administrator Console	210
Accessing Diagnostic Console via VGA/Keyboard/Mouse Port	210
Accessing Diagnostic Console via SSH	210
Accessing Status Console	211
Accessing Administrator Console	212
Navigating Administrator Console	212
Editing Diagnostic Console Configuration	213
Editing Network Interfaces Configuration (Network Interfaces)	213
Ping an IP Address (Network Interfaces)	215
Using Traceroute (Network Interfaces)	215
Editing Static Routes (Network Interfaces)	216
Viewing Log Files (Admin)	217
Restarting CC-SG (Admin)	221
Rebooting CC-SG (Admin)	222
Powering Off the CC-SG System (Admin)	223
Resetting CC-SG GUI Admin Password (Admin)	223
To reset the CC-SG GUI admin password:	224
Resetting CC-SG Factory Configuration (Admin)	224

Diagnostic Console Passwords (Admin).....	226
Displaying Disk Status (Utilities)	228
Displaying Top Display (Utilities)	229
Displaying NTP (Network Time Protocol) Status (Utilities)	230
Serial Admin Port	231
About Terminal Emulation Programs	231
Appendix A: Specifications (G1, V1, and E1)	233
G1 Platform	233
General Specifications	233
Hardware Specifications	233
Environmental Requirements	233
V1 Platform	234
General Specifications	234
Hardware Specifications	234
Environmental Requirements	234
E1 Platform	235
General Specifications	235
Hardware Specifications	235
Environmental Requirements	235
Appendix B: CC-SG and Network Configuration	237
Introduction	237
Executive Summary	237
CC-SG Communication Channels	239
CC-SG and Raritan Devices	239
CC-SG Clustering	239
Access to Infrastructure Services	240
PC Clients to CC-SG	240
PC Clients to Nodes	241
CC-SG & Client for IPMI, iLO/RILOE, DRAC, RSA	241
CC-SG & SNMP	241
CC-SG & CC-NOC	242
CC-SG Internal Ports	242
CC-SG Access via NAT-enabled Firewall	242
Security and Open Port Scans	243
Appendix C: User Group Privileges	245
Appendix D: SNMP Traps	253
Appendix E: Troubleshooting	255
Client Browser Requirements	255
Appendix F: Two-Factor Authentication	257
Supported Environments	257
Setup Requirements	257
Known Issues	257
Appendix G: FAQs	259
Appendix H: Keyboard Shortcuts	265

Figures

Figure 1 Login Window	3
Figure 2 Thick Client IP Address Specification Window	4
Figure 3 CC-SG Window Components	6
Figure 4 Confirm IP Address	7
Figure 5 Time/Date Configuration.....	8
Figure 6 Upgrade CC-SG	9
Figure 7 CC-SG Application Manager	10
Figure 8 Compatibility Matrix	11
Figure 9 Guided Setup Window	13
Figure 10 Guided Setup – Create Categories and Elements	14
Figure 11 Guided Setup -- Discover Devices	15
Figure 12 Guided Setup – Device Discovery Results.....	16
Figure 13 Guided Setup – Add Device.....	17
Figure 14 Guided Setup—Add Device Groups, Select Devices.....	19
Figure 15 Guided Setup—Add Node Groups, Select Nodes	21
Figure 16 Guided Setup--Group Summary	22
Figure 17 Add User Group--Privileges.....	23
Figure 18 Add User Group-Policies.....	24
Figure 19 CC-SG Association Example	27
Figure 20 Association Manager Screen.....	29
Figure 21 Add Category Window	30
Figure 22 Edit Category Window	30
Figure 23 Association Manager Screen.....	31
Figure 24 Add Element Window	32
Figure 25 Edit Element Window	32
Figure 26 The Devices Tree.....	35
Figure 27 Devices Tab and Devices Profile	37
Figure 28 Add Device Screen	37
Figure 29 Discover Devices Screen	39
Figure 30 Discovered Devices List Window.....	39
Figure 31 Adding a Discovered Device.....	40
Figure 32 The Device Profile Screen	41
Figure 33 Delete Device Screen	42
Figure 34 Configure Ports Screen.....	43
Figure 35 Configure Serial Ports Screen.....	44
Figure 36 Configure Ports Screen.....	45
Figure 37 Configure KVM Port Screen.....	45
Figure 38 Ports Profile	46
Figure 39 Delete Port Screen	47
Figure 40 Upgrade Device Screen	48
Figure 41 Backup Device Configuration Screen.....	48
Figure 42 Restore Device Configuration Screen.....	49
Figure 43 Protected Restore.....	50
Figure 44 Full Restore.....	50
Figure 45 Custom Restore	51
Figure 46 Restart Device Screen	53
Figure 47 Ping Device Screen.....	53
Figure 48 Launch Admin for a KX Device.....	54
Figure 49 Topological View	55
Figure 50 Disconnect Users	56

Figure 51 Devices Tree Regular View Screen.....	57
Figure 52 Custom View Screen.....	58
Figure 53 Selecting a Custom View.....	58
Figure 54 Custom View Screen.....	59
Figure 55 Paragon Manager Application Window	60
Figure 56 IP-Reach Administration Screen.....	61
Figure 57 Device Groups Manager	62
Figure 58 Device Group: New Panel, Select Devices Tab	63
Figure 59 Describe Devices Tab.....	64
Figure 60 Device Groups Manager Screen	66
Figure 61 Device Groups Manager Screen	67
Figure 62 Delete Device Group Window.....	67
Figure 63 Delete Device Group Panel.....	68
Figure 64 Adding a PowerStrip device.....	70
Figure 65 The Nodes Tab and Nodes Profile Screen.....	75
Figure 66 Add Node Screen.....	77
Figure 67 Add Interface—In-Band iLO/RILOE KVM.....	79
Figure 68 Configuring an Out-of-Band KVM Connection.....	80
Figure 69 Configuring a Managed Power Strip Power Control Interface.....	81
Figure 70 Configuring an IPMI Power Control Interface.....	82
Figure 71 Connecting to a Node's Configured Interface	83
Figure 72 Editing an Interface.....	84
Figure 73 Edit Node Screen	85
Figure 74 Deleting a Node.....	86
Figure 75 Chat Session for a Node	87
Figure 76 The Users Tree	89
Figure 77 Add User Groups Screen	91
Figure 78 The Policies Tab on the Add User Group Screen.....	92
Figure 79 Deleting a User Group.....	94
Figure 80 Adding a User	94
Figure 81 Editing a Selected User.....	95
Figure 82 Deleting a User.....	96
Figure 83 Add Users To Group Screen	97
Figure 84 Deleting a User From A Group.....	98
Figure 85 My Profile Screen	98
Figure 86 Bulk Copy Screen	100
Figure 87 Policy Summary	101
Figure 88 The Node Group Manager	102
Figure 89 Nodes in a Group Based on Attributes.....	103
Figure 90 Adding Nodes Using Select Nodes	104
Figure 91 Describing a Node Group With Multiple Rules	105
Figure 92 Policy Manager	108
Figure 93 Adding a Policy.....	108
Figure 94 Security Manager General tab	115
Figure 95 Add Module	116
Figure 96 AD General Settings	117
Figure 97 AD Advanced Settings	118
Figure 98 AD Group Settings.....	120
Figure 99 AD Trust Settings	121
Figure 100 Importing Groups from AD Server.....	123
Figure 101 Synchronize AD User Groups	124
Figure 102 Synchronization of All AD Modules	125
Figure 103 Synchronization of All AD Modules	125

Figure 104 Add LDAP Module	126
Figure 105 LDAP General Settings	127
Figure 106 LDAP Advanced Settings	128
Figure 107 Add TACACS+ Module	130
Figure 108 TACACS+ General Settings.....	131
Figure 109 Security Manager Add Module Screen	132
Figure 110 Specifying a RADIUS Server	133
Figure 111 Audit Trail Screen.....	135
Figure 112 Audit Trail Report.....	136
Figure 113 Error Log Screen.....	136
Figure 114 Error Log Report.....	137
Figure 115 Access Report Screen	137
Figure 116 Access Report.....	138
Figure 117 Availability Report.....	139
Figure 118 Active Users Report	140
Figure 119 Locked Out Users Report.....	141
Figure 120 All Users' Data Report	142
Figure 121 Users In Groups Report	143
Figure 122 Groups Report	144
Figure 123 AD User Group Report.....	145
Figure 124 Asset Management Report	145
Figure 125 Node Asset Report Screen.....	146
Figure 126 Node Asset Report	147
Figure 127 Active Nodes Report	147
Figure 128 Node Creation Report Screen	148
Figure 129 Node Creation Report.....	148
Figure 130 Query Port Screen.....	149
Figure 131 Query Port Report.....	150
Figure 132 Active Ports Report.....	150
Figure 133 CC-NOC Synchronization Report.....	151
Figure 134 Enter Maintenance Mode	153
Figure 135 Backup CommandCenter Screen.....	154
Figure 136 Restore CommandCenter Screen.....	155
Figure 137 Saving a Backup File.....	156
Figure 138 Reset CC-SG Screen	157
Figure 139 Restart Screen.....	157
Figure 140 Upgrade CC-SG Screen	158
Figure 141 Shutdown CC-SG Screen.....	159
Figure 142 Configuring the Message of the Day	161
Figure 143 Applications Tab of the Application Manager	162
Figure 144 Adding an Application.....	162
Figure 145 A List of Default Applications.....	163
Figure 146 Firmware Manager Screen	164
Figure 147 Firmware Search Window.....	164
Figure 148 Primary/Backup Network.....	166
Figure 149 Network Setup Panel—Primary/Backup	167
Figure 150 Active/Active Network.....	168
Figure 151 Network Setup Panel—Active/Active	169
Figure 152 Configuration Manager Logs Screen	170
Figure 153 Inactivity Timer Tab.....	171
Figure 154 Configuration Manager Time/Date Screen	172
Figure 155 Configuration Manager Modem Screen	173
Figure 156 Modems Tab	174

Figure 157 Extra Initialization Commands	174
Figure 158 Create a New Connection.....	175
Figure 159 Connection Name	175
Figure 160 Phone Number to Dial	175
Figure 161 Specify Dial-up Script	176
Figure 162 Connecting to CC-SG.....	177
Figure 163 Entering username and password	177
Figure 164 After Dial Terminal.....	178
Figure 165 Connection Modes	179
Figure 166 Configuration Manager Connection Screen – Direct Mode	180
Figure 167 Configuration Settings Device Settings Screen	181
Figure 168 Configuration Settings Device Settings Screen.....	182
Figure 169 Cluster Configuration Screen	184
Figure 170 Cluster Configuration – Primary Node Set	184
Figure 171 Cluster Configuration Advanced Settings	186
Figure 172 Secure Client Connections	188
Figure 173 Login Settings	188
Figure 174 Portal Settings	191
Figure 175 Login Portal With Restricted Service Agreement.....	192
Figure 176 Security Manager Certificate Screen	193
Figure 177 Generate Certificate Signing Request Screen	194
Figure 178 Certificate Request Generated	194
Figure 179 Generate Self Signed Certificate Window	195
Figure 180 Security Manager IP-ACL Screen.....	196
Figure 181 Notification Manager	197
Figure 182 Task Manager.....	199
Figure 183 Add CC-NOC Configuration Screen	202
Figure 184 CC-SG Commands via SSH.....	205
Figure 185 Listing Devices on CC-SG.....	208
Figure 186 Access SX Device via SSH	208
Figure 187 Listinterfaces in SSH.....	209
Figure 188 Connecting to a Node via a Serial Out-of-Band Interface	209
Figure 189 Login to Diagnostic Console	210
Figure 190 Status Console.....	211
Figure 191 Administrator Console.....	212
Figure 193 Edit Diagnostic Console Configuration	213
Figure 194 Editing Network Interfaces	214
Figure 195 Editing Static Routes	216
Figure 196 Selecting Log Files to View	217
Figure 197 Selecting Log Files to View	218
Figure 198 Changing Colors in Log Files	219
Figure 199 Displaying Information.....	219
Figure 200 Adding Expressions in Log Files	219
Figure 201 Specifying a Regular Expression for a Log File.....	220
Figure 202 Restarting CC-SG in Diagnostic Console.....	221
Figure 203 Rebooting CC-SG in Diagnostic Console	222
Figure 204 Power Down CC-SG in Diagnostic Console.....	223
Figure 205 Admin Password Reset for CC-SG GUI in Diagnostic Console.....	224
Figure 206 Reset CC-SG Factory Configuration	224
Figure 207 Configuring Password Settings.....	226
Figure 208 Configuring Accounts	227
Figure 209 Displaying Disk Status of CC-SG in Diagnostic Console	229
Figure 210 Displaying CC-SG Processes in Diagnostic Console.....	229

Figure 211 NTP not configured in CC-SG GUI	230
Figure 212 NTP running on the CC-SG GUI	230
Figure 213 Serial Admin Port on G1	231
Figure 214 Serial Admin Port on E1	231
Figure 215 Serial Admin Port on E1	231
Figure 216 CC-SG Deployment Elements	238

This page intentionally left blank.

Chapter 1: Introduction

Congratulations on your purchase of CommandCenter Secure Gateway (CC-SG), Raritan's convenient and secure method for managing various UNIX servers, firewalls, routers, load balancers, Power Management devices, and Windows servers.

CC-SG provides central management and administration, using a set of serial and KVM appliances. It is designed to operate in a variety of environments, from high-density Data Centers to Service Provider environments to corporate environments handling large remote offices.

CC-SG, when used in conjunction with Raritan's Dominion or IP-Reach port-level management appliances, streamlines and simplifies the management of the target devices (referred to as "nodes"), easing administration of data center equipment by connecting to the IP network and presenting the serial console and KVM ports of all the nodes within the managed network.

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.

Intended Audience

This document is intended for administrators who typically have all available privileges. Please refer to **Appendix C: User Group Privileges**. Users who are not administrators usually have fewer privileges, such as being granted only the Nodes Access privileges. Those users should refer to Raritan's **CommandCenter Secure Gateway User Guide** for additional information.

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.
- **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,

etc. that are managed by CC-SG. These devices control the target servers and systems that are connected to them.

- **Director Client**—A Java-based client for CC-SG useable by both normal access users and administrators. It is the only client that permits administration.
- **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 additional information.
- **Hostname**—A hostname can be used if DNS server support is enabled. Please refer to About Network in **Chapter 13: Advanced Administration** for additional information. The hostname and its Fully-Qualified Domain Name (FQDN = Hostname + Suffix) cannot exceed 257 characters. It can consist of any number of components, as long as they are separated by “.”. Each component has a maximum size of 63 characters and the first character must be alphabetic. The remaining characters can be alphabetic, numeric, or “-” (hyphen or minus). The last character of a component may not be “-”. While the system preserves the case of the characters entered into the system, the FQDN is case-insensitive when used.
- **iLO/RILOE**—Hewlett Packard’s Integrated Lights Out/Remote Insight Lights Out servers that can be managed by CC-SG. Targets of an iLO/RILOE device are powered on/off and recycled directly. iLO/RILOE devices cannot be discovered by CC-SG; they have to be manually added as nodes.
- **In-band Access**—going through the TCP/IP network to correct or troubleshoot a target in your network. KVM and Serial devices can be accessed via these in-band applications: **RemoteDesktop Viewer, SSH Client, RSA Client, VNC Viewer**.
- **IPMI Servers** (Intelligent Platform Management Interface)—servers that can be controlled by CC-SG. IPMI are discovered automatically but can be added manually as well.
- **Out-of-Band Access**—using applications such as Raritan Remote Console (RRC), Raritan Console (RC), or Multi-Platform Client (MPC) to correct or troubleshoot a KVM or serial managed node in your network.
- **Policies**—define the permissions, type of access, and to which nodes and devices a user group can access. Policies are applied to a user group and have several control parameters to determine the level of control, such as date and time of access.
- **Nodes**—are the target systems, such as servers, desktop PCs, or 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. Please refer to **Chapter 13: Advanced Administration** for additional information.
- **User Groups**—sets of users that share the same level of access and privileges. For example, the default user group **System Administrators** has full access to all configuration tasks and target nodes.

Chapter 2: Accessing CC-SG

Once you have configured CC-SG with an IP address, the CC-SG unit can be placed at its final destination. Make all necessary hardware connections to make the unit operational.

You can access CC-SG in several ways, each described in this chapter:

- **Browser:** CC-SG supports numerous web browsers. (For a complete list of supported browsers and platforms, please refer to the **Compatibility Matrix** on <http://www.raritan.com/support>. On the **Support** page, click **Firmware Upgrades**, and then click **CommandCenter Secure Gateway**.)
- **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 [Chapter 13: Advanced Administration](#) for additional information.
- **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 [Chapter 13: Advanced Administration](#) for additional information.

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

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.



Figure 1 Login Window

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

1. To download the thick client from CC-SG, launch a web browser and type this URL: **http(s)://<IP_address>/install** where <IP_address> is the IP address of the CC-SG.
2. If a security warning message appears, click **Start** to continue the download.
3. 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**.
4. When the download is complete, a new window in which you can specify the CC-SG IP address appears.

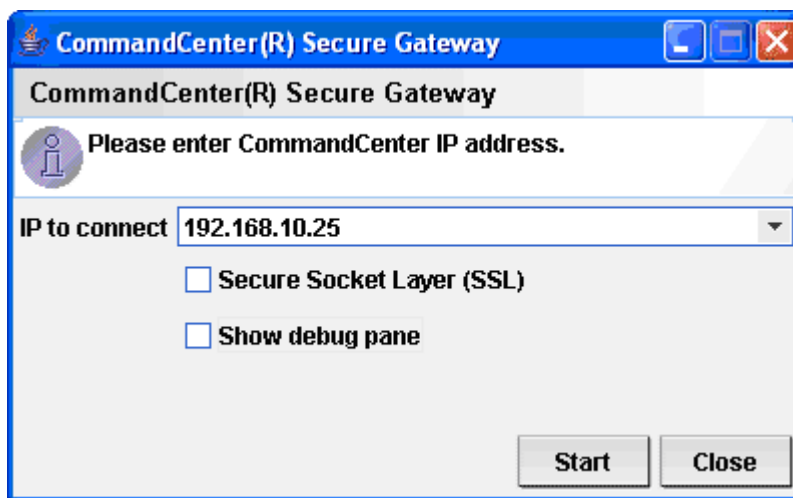


Figure 2 Thick Client IP Address Specification Window

5. 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.
6. 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.
 - **To check the setting in CC-SG:** On the **Administration** menu, click **Security**. In the **General** tab, look at the **Browser Connection Protocol** field. 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.
7. 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.
8. The login screen appears, and the thick client looks and behaves just like the browser-based Java client. If the Restricted Service Agreement is enabled, read the agreement text, and then check 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:

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

CC-SG Window Components

Upon valid login, the CC-SG application window appears.

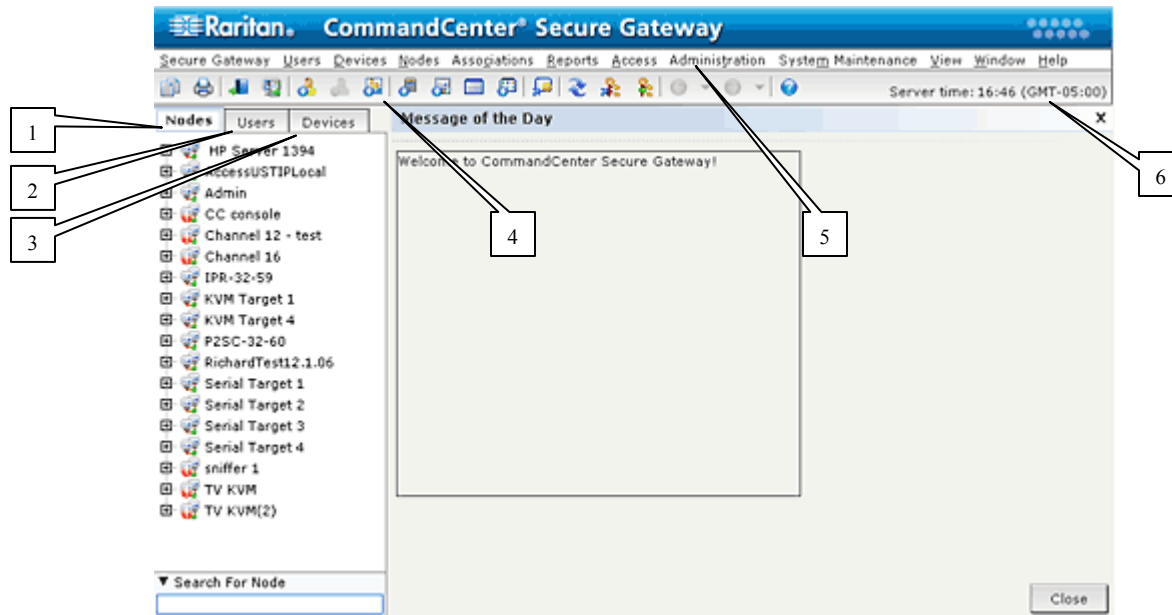


Figure 3 CC-SG Window Components

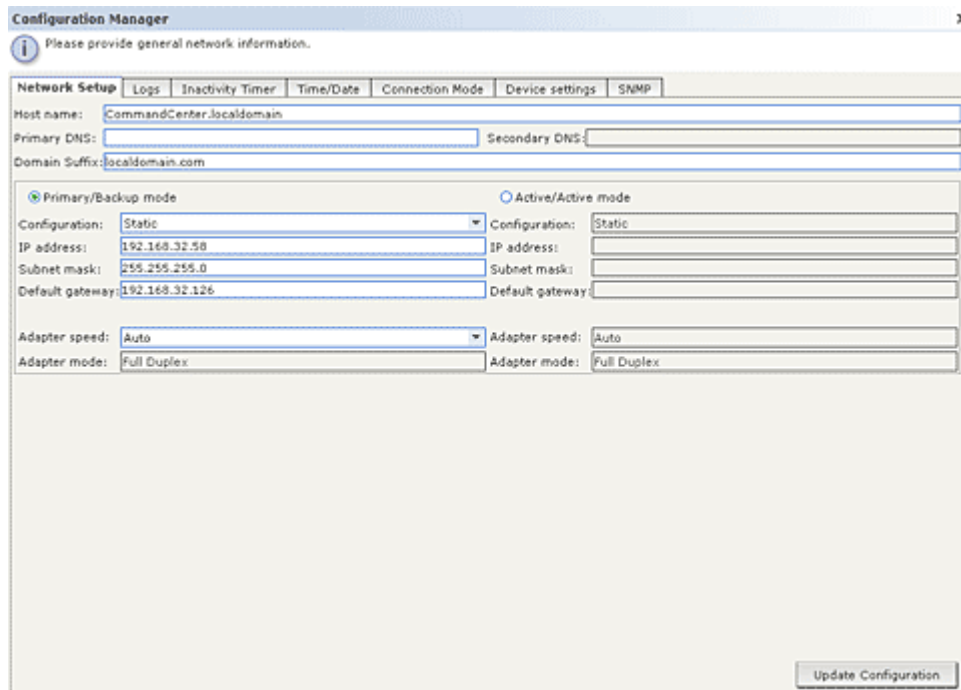
1. **Nodes tab:** Click the **Nodes** tab to display all known target nodes in a tree view. Click a node to view the Node Profile. Interfaces are grouped under their parent nodes. Click the + and - signs to expand or collapse the tree. Right-click an interface and select **Connect** to connect to that 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**.
2. **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.
3. **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**.
4. **Quick Commands toolbar:** This toolbar offers some shortcut buttons for executing common commands.
5. **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.
6. **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 Management in **Chapter 13: Advanced Administration** for additional information. This time may be different than the time used by the client.

Initial Configurations

Upon first login, 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.

Confirm IP Address

1. On the **Administration** menu, click **Configuration** to open the **Configuration Manager** screen.
2. Click the **Network Setup** tab.



The screenshot shows the 'Configuration Manager' window with the 'Network Setup' tab selected. The window has a title bar with 'Configuration Manager' and a close button. Below the title bar is a message: 'Please provide general network information.' The 'Network Setup' tab is active, showing fields for 'Host name' (CommandCenter.localdomain), 'Primary DNS' (empty), 'Secondary DNS' (empty), and 'Domain Suffix' (localdomain.com). There are two radio buttons: 'Primary/Backup mode' (selected) and 'Active/Active mode'. Under 'Primary/Backup mode', there are two columns of settings. The left column has 'Configuration' (Static), 'IP address' (192.168.32.58), 'Subnet mask' (255.255.255.0), and 'Default gateway' (192.168.32.126). The right column has 'Configuration' (Static), 'IP address' (empty), 'Subnet mask' (empty), and 'Default gateway' (empty). Below these are 'Adapter speed' (Auto) and 'Adapter mode' (Full Duplex) for both columns. An 'Update Configuration' button is at the bottom right.

Figure 4 Confirm IP Address

3. (Optional) Check that the network setting are correct, and make changes if needed. Please refer to [About Network Setup](#) 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

1. Log onto CC-SG.
2. On the **Administration** menu, click **Configuration** to open the **Configuration Manager** screen.
3. Click the **Time/Date** tab.

Configuration Manager

Please provide Time/Date settings.

Network Setup | Logs | Inactivity Timer | **Time/Date** | Connection Mode | Device settings | SNMP

Date: December 2006

Sun	Mon	Tue	Wed	Thu	Fri	Sat
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Time: 17:01:37

Current time: 17:01:37

Hour: 16

Minutes: 59

Seconds: 57

Time zone: (GMT-05:00) US/Eastern

☐ Enable Network Time Protocol (NTP)

Primary server:

Secondary server:

Update Configuration

Figure 5 Time/Date Configuration

4. On the **Administration** menu, click **Configuration** to open the **Configuration Manager** screen.
5. 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.

6. Click **Update Configuration** to apply the time and date changes to CC-SG.
7. Click **Refresh** to reload the new server time in the **Current Time** field.
8. On the **Maintenance** menu, click **Restart** to restart CC-SG.

Check and Upgrade CC-SG Firmware Version

1. Login to CC-SG.
2. On the **Help** menu, click **About Raritan Secure Gateway**. A pop-up window containing the firmware version number appears. Click **OK**.
3. If the version is not current, you must upgrade your firmware. You can download the firmware upgrade file from the Raritan website. Save the firmware upgrade file to your client PC.
4. Switch to Maintenance Mode. Please refer to **About Maintenance Mode** in Chapter 12: System Maintenance for additional information.
5. On the **System Maintenance** menu, click **Upgrade**.

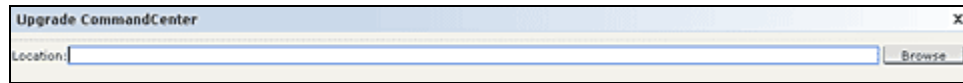


Figure 6 Upgrade CC-SG

6. Click **Browse**, locate and select the firmware upgrade file from the dialog that displays, and then click **Open**.
7. Click **OK** in the Upgrade CommandCenter screen.

Note: If you have acquired the firmware as a zip file, unzip the files and follow the instructions in the included README file.

Check and Upgrade Application Versions

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

1. On the **Administration** menu, click **Applications**.

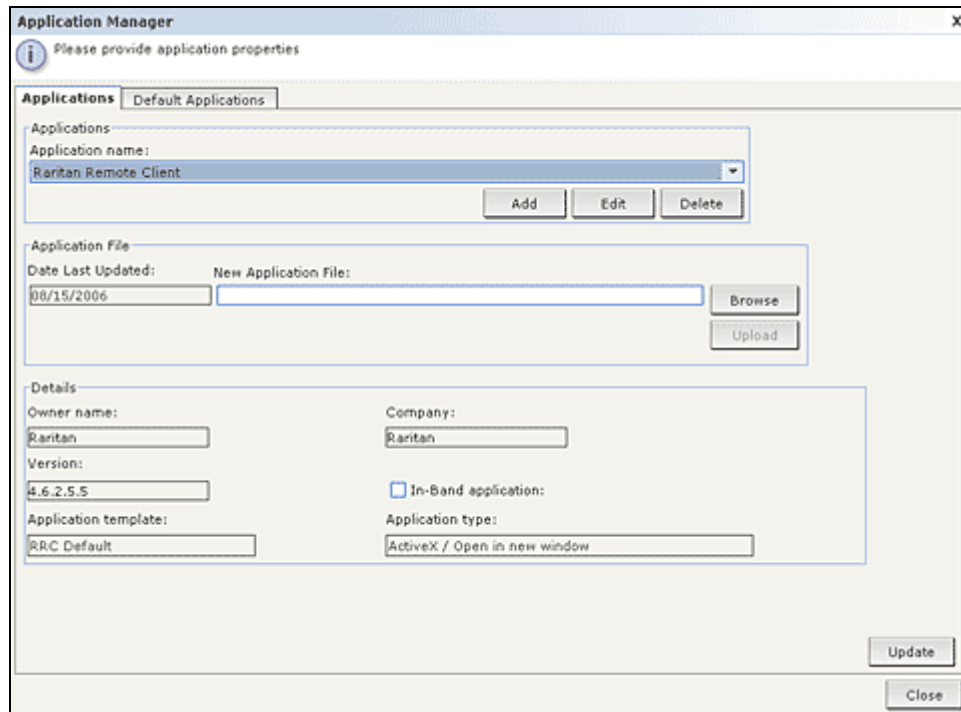


Figure 7 CC-SG Application Manager

2. Click the **Application name** drop-down arrow and select an application from the list. Note the number in the **Version** field.
3. If the application version is not current, you must upgrade the application. You can download the application upgrade file from the Raritan website. Save the application upgrade file to your client PC. (For a complete list of supported application versions, please refer to the **Compatibility Matrix** on <http://www.raritan.com/support>. On the **Support** page, click **Firmware Upgrades**, and then click **CommandCenter Secure Gateway**.)
4. Click the **Application name** drop-down arrow and select the application that must be upgraded from the list.
5. Click **Browse**, locate and select the application upgrade file from the dialog that displays, and then click **Open**.
6. The application name will appear in the **New Application File** field in the **Application Manager** screen.
7. 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.
8. 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.
9. Click **Update**.

Power Down CC-SG

If CC-SG loses AC power while it is up and running, it will remember the last power state. Once AC power is restored, CC-SG automatically reboots. However, if CC-SG loses AC power when it is powered off, it will remain powered off when AC power is restored.

Important: Do not hold the POWER button to forcibly power down CC-SG. The recommended way to power down CC-SG is to use the following procedure.

To power down the CC-SG:

1. Remove the bezel and firmly tap the **POWER** button. On G1 units, the **POWER** button is on the back of the unit.
2. Wait approximately one minute while CC-SG gracefully powers down.

Note: Users logged into CC-SG via Diagnostic Console will receive a short broadcast message when the CC-SG unit is powered down. Users logged into CC-SG via a web browser or SSH will not receive a message when the CC-SG unit is powered down.

3. If you must remove the AC power cord, let the power down process finish completely before removing the power cord. This is required for CC-SG to complete all transactions, close the databases, and place the disk drives into a safe state for power removal.

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.

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

Compatibility Matrix

Device:

Device	Versions	
ERIC	04.02.00	04.01.00
Dominion SX	2.5.6	2.4.5
Paragon II System Controller	1.11	1.11
Dominion KX101	1.0.1	1.0.0
Dominion KSX	3.22	3.21
Dominion KX	1.4.0	1.3.0
IP-Reach	3.21	3.20

Application:

Name	Version
Sun JRE	1.4.2_05
Raritan Console	2.7.19
SSH_rci	1.0
VNC_rci	1.0
RDP_rci	1.0
RILOE	2.52
RILOEII	1.16
MPC	4.6.1
Raritan Remote Client	4.6.1
iLO	1.82

You can view latest cross product compatibility matrix online by clicking on the URL below:

http://www.raritan.com/support/sup_upgrades.aspx

Close

Figure 8 Compatibility Matrix

This page intentionally left blank.

Chapter 3: Configuring CC-SG with Guided Setup

Prepare to Configure CC-SG with 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.

Guided Setup Overview

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.

Start Guided Setup:

On the **Administration** menu, click **Guided Setup**. The Guided Setup window appears. The left panel of the window lists the **Guided Tasks** in a tree view. The right side of the window displays the active task's panel.

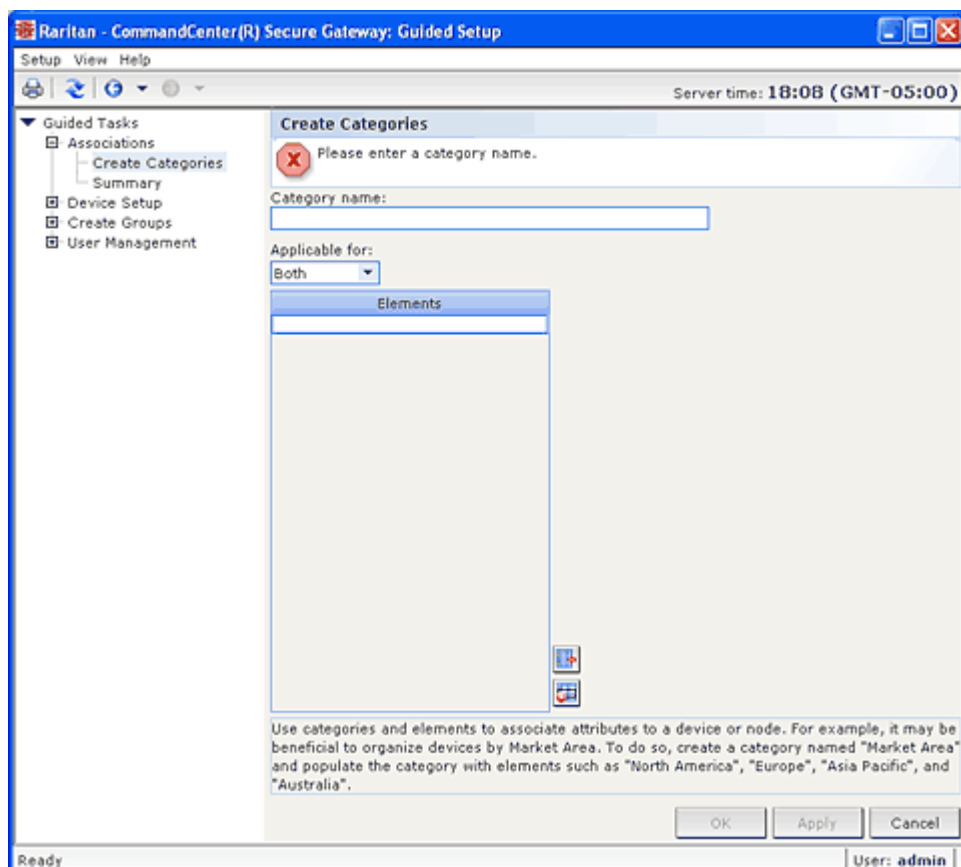


Figure 9 Guided Setup Window

Guided Setup is divided into 4 tasks, which are each explained in the following sections:

- [Associations](#)—Define the categories and elements that you use to organize your equipment.
- [Device Setup](#)—Discover devices in your network and add them to CC-SG. Configure device ports.

- **Create Groups**—Categorize the devices and nodes that CC-SG manages into groups and create full access policies for each group.
- **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.


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, to organize equipment by location, you can create a Category called “Location,” and Elements named for each server’s location, such as “Philadelphia,” “New York,” and “New Orleans.”

Create Categories and Elements

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

Figure 10 Guided Setup – Create Categories and Elements

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 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.
- Repeat these steps until you have added all the elements within the category to the **Elements** table.
 - 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.
 - 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.
 - Click **Continue** to start the next task, **Device Setup**. Follow the steps in the next section.

Device Setup

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

Important: Ensure that no other users are logged into the device during CC-SG configuration.

Discover and Add Devices

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

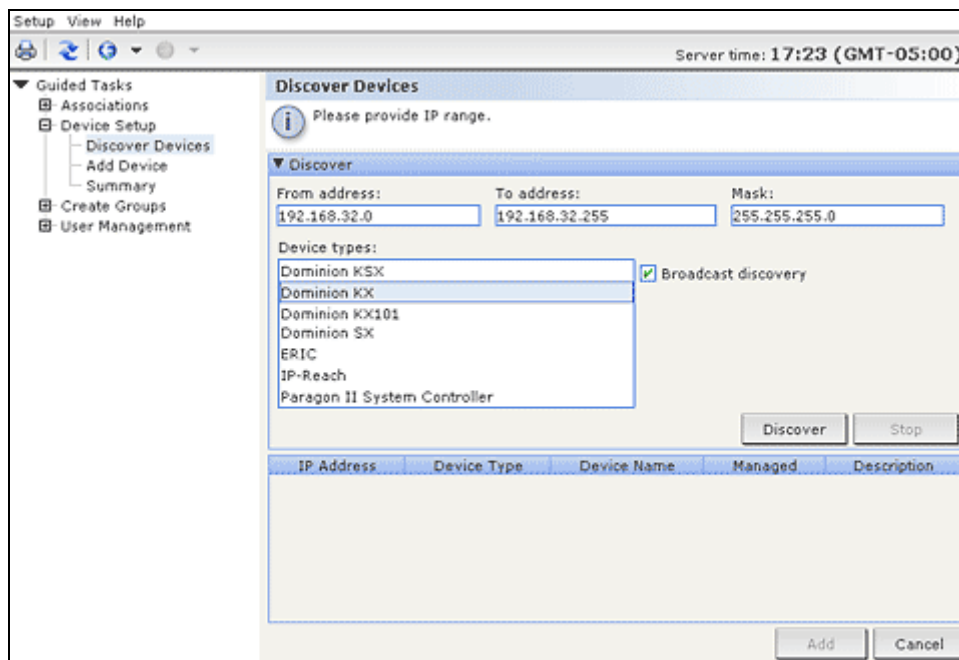


Figure 11 Guided Setup -- Discover Devices

- Type the IP address range in which you want to search for devices in the **From address** and **To address** fields.
- Type the subnet mask in which you want to search for devices in the **Mask** field.
- In the **Device types** list, select the type of device you want to search for in the range specified. Press and hold down the **CONTROL** key while you click device types to select multiple device types.

5. Check **Broadcast discovery** if searching for devices on the same subnet on which CC-SG resides. Uncheck **Broadcast discovery** to discover devices across all subnets.
6. Click **Discover**.
7. When the discovery is complete, a confirmation message pops up. Click **OK** in the confirmation message.
8. If CC-SG has discovered devices of the specified type and in the specified address range, the devices display in a table in the bottom section of the **Discover Devices** panel. You can click the black arrow at the top of the panel to hide the top section, expanding your view of the discovery results in the bottom section of the panel.

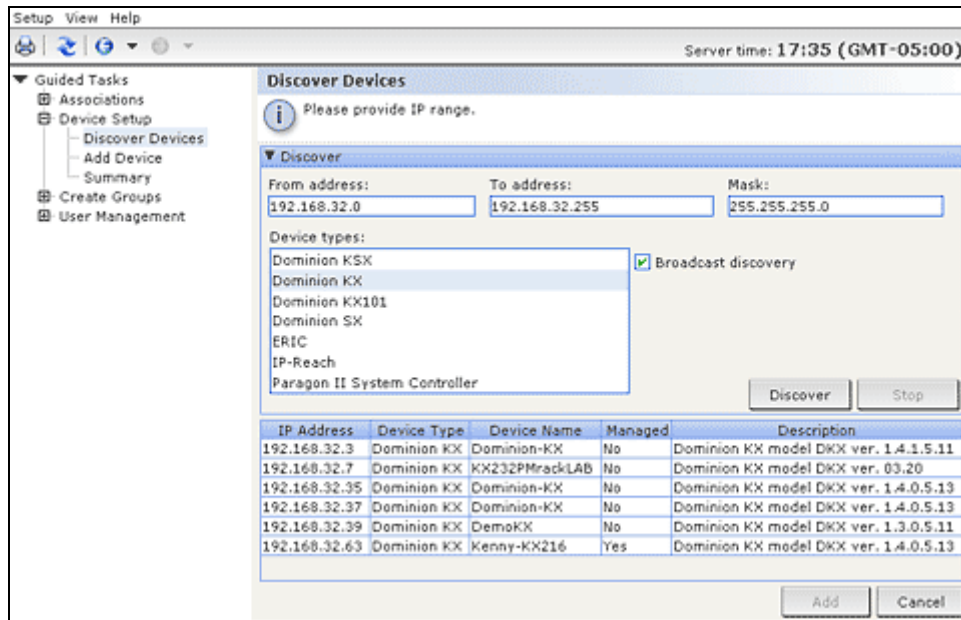


Figure 12 Guided Setup – Device Discovery Results

9. 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.

Add Device

Please provide values for the required device parameters.

Device type:
Dominion KSX

Device name:
Kenny32-KSX

Device IP or Hostname:
192.168.32.61

TCP port number:
5000

Username:

Password:

Heartbeat timeout (sec):
0

Description:
Dominion KSX model RX440 ver. 3.22.5.3

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

OK Apply Cancel

Figure 13 Guided Setup – Add Device

10. You can change the **Device name** and **Description** by typing new information in the corresponding fields.
11. 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.
12. The **TCP Port Number** field will be populated automatically based on the device type.
13. Type the **Username** and **Password** you created when you prepared the device to be added to CC-SG in the corresponding fields.
14. In the **Heartbeat timeout** field, type the number of seconds that should elapse before timeout between the device and CC-SG.
15. If you are adding a Dominion SX device, check the **Local access: Allowed** checkbox if you want to allow local access to the device. Clear the **Local access: Allowed** checkbox if you do not want to allow local access to the device.
16. 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.
17. If you are adding an IPMI Server, type an **Interval** that is used to check for availability, and an **Authentication Method**, which needs to match what has been configured on the IPMI Server, in the corresponding fields.
18. If you want to configure all available ports on the device, check the **Configure all ports** checkbox. CC-SG will add all ports on the device to CC-SG and create a node for each port.
19. 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.

20. If you want the Element to apply to the device and to the nodes connected to the device, check the **Apply to Nodes** checkbox.
21. If you want to add another device, click **Apply** to save this device, and then repeat the steps in this section to add additional devices.
22. When you have finished adding devices, click **OK**. The **Device Summary** panel displays a list of the devices that you added.
23. Click **Continue** to start the next task, **Create Groups**. Follow the steps in the next section.

Create Groups

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

Add Device Groups and Node Groups

1. The **Devices Groups Manager** panel opens when you click **Continue** at the end of the Device Setup task. You can also click **Create Groups**, and then click **Add Devices Groups** in the **Guided Tasks** tree view in the left panel to open the **Devices Groups Manager** panel.
2. In the **Group name** field, type a name for a device group you want to create.
3. There are two ways to add devices to a group, **Select Devices** and **Describe Devices**. The Select Devices tab allows you to select which devices you want to assign to the group by selecting them from the list of available devices. The Describe Devices tab allows you to specify rules that describe devices, and the devices whose parameters follow those rules will be added to the group.

Select Devices

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

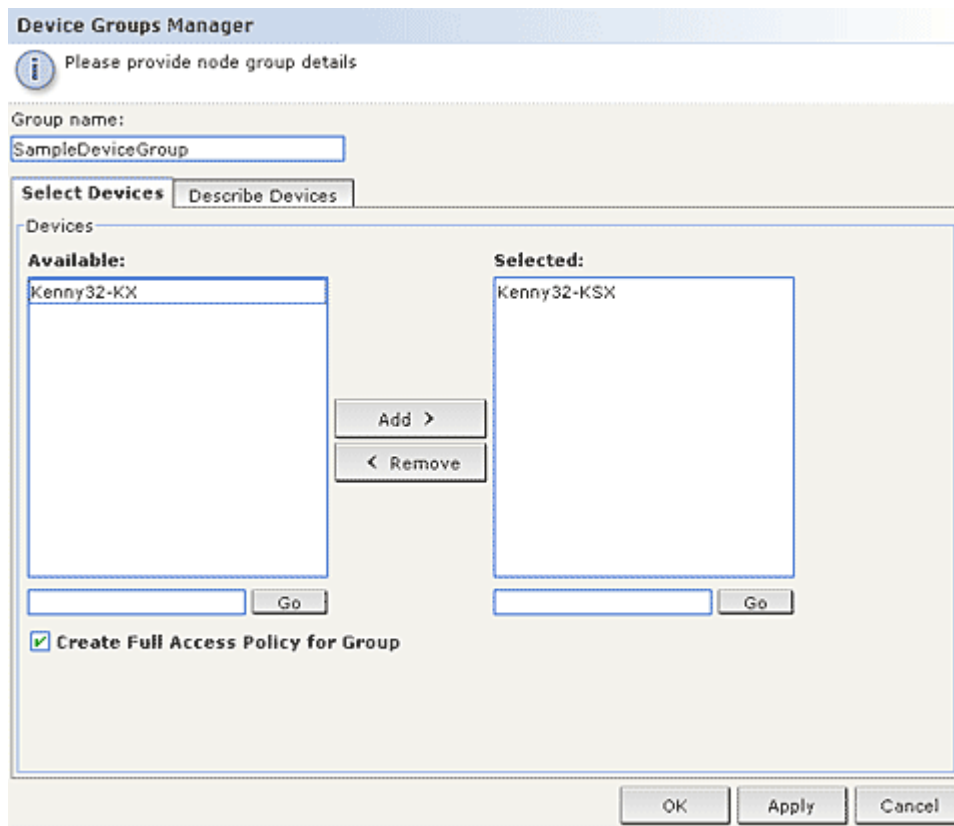



Figure 14 Guided Setup—Add Device Groups, Select Devices

- 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.
- If you want 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.
- d. Check the **Create Full Access Policy for Group** checkbox if you want to create a policy for this device group that allows access to all nodes and devices in the group at all times with control permission.
- e. If you want to add another device group, click **Apply** to save this group, and then repeat the steps in this section to add additional device groups.
- f. 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.

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

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

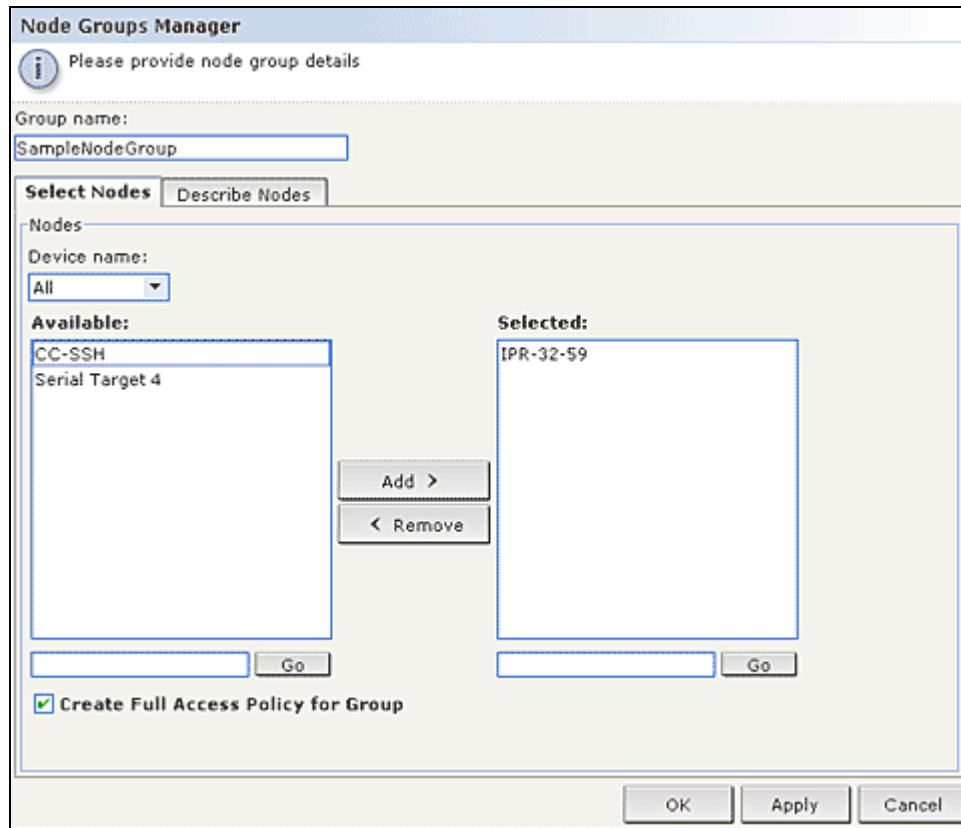



Figure 15 Guided Setup—Add Node Groups, Select Nodes

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

- 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.
- Click the Add New Row icon  to add a row to the table.
- 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. Please refer to [Chapter 9: Policies](#) for additional information.
- Check the **Create Full Access Policy for Group** checkbox if you want to create a policy for this node group that allows access to all nodes in the group at all times with control permission.
- If you want to add another node group, click **Apply** to save this group, and then repeat the steps in this section to add additional node groups.

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

Group Summary		
Group Name	Group Type	Policy Name
TestGroup	Node	Access TestGroup
TestDeviceGroup	Device	Access TestDeviceGroup

Continue Exit

Figure 16 Guided Setup--Group Summary

- g. 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

1. 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.
2. 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.
3. In the **Description** field, type a description of the user group.
4. Click the **Privileges** tab, and then check the checkboxes that correspond to the **Privileges**, or types of CC-SG activities, that you want to assign to the user group.

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

Add User Group

i Choose usergroup properties to add.

User Group Name:
Sample User Group

Description:

Privileges		Device/Node Policies	Active Directory Associations
Selected	Privilege		
<input type="checkbox"/>	CC Setup And Control		
<input type="checkbox"/>	Device Configuration And Upgrade Management		
<input checked="" type="checkbox"/>	Device, Port and Node Management		
<input checked="" type="checkbox"/>	User Management		
<input checked="" type="checkbox"/>	User Security Management		

Node Access

Selected	Privilege
<input checked="" type="checkbox"/>	Node Out-of-band Access
<input checked="" type="checkbox"/>	Node In-band Access
<input checked="" type="checkbox"/>	Node Power Control

Figure 17 Add User Group--Privileges

- Click the **Policies** tab.

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

Figure 18 Add User Group-Policies

8. 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. If you want to associate remotely authenticated users with Active Directory modules, click the **Active Directory Associations** tab. Check the checkbox that corresponds with each Active Directory module you want to associate with the user group.
10. If you want to add another user group, click **Apply** to save this group, and then repeat the steps in this section to add additional user groups.
11. 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.
12. In the **Username** field, type the name that the user you want to add will use to log in to CC-SG.
13. Check the **Login Enabled** checkbox if you want the user to be able to log in to CC-SG.
14. Check the **Remote Authentication** checkbox only if you want the user to be authenticated by an outside server, such as TACACS+, RADIUS, LDAP, or AD. If you are using remote authentication, a password is not required. The **New Password** and **Retype New Password** fields will be disabled when **Remote Authentication** is checked.
15. In the **New Password** and **Retype New Password** fields, type the password that the user will use to log in to CC-SG.
16. 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.
17. Check the **Force Password Change Periodically** checkbox if you want to specify how often the user will be forced to change the password.
18. 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.
19. In the **Email address** field, type the user's email address.

20. Click the **User Group** drop-down arrow and select the user group to which you want to assign the user from the list.
21. 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.
22. When you have finished adding users, click **OK**. The **User Summary** panel displays a list of the user groups and users that you added.

This page intentionally left blank.

Chapter 4: Creating Associations

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. The figure below shows a custom view created using this example. You can customize the CC-SG to organize and display your servers however you like.

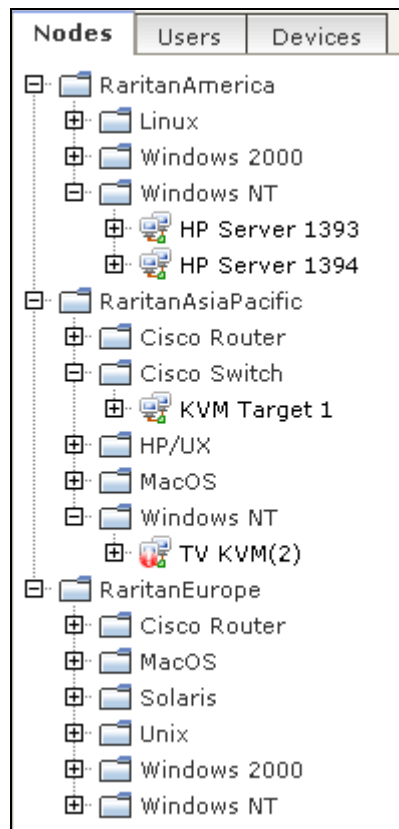


Figure 19 CC-SG Association Example

Association Terminology

Read the following definitions to understand associations:

- **Associations**—are the relationships between categories, elements of a category, and nodes and devices. For example, you want to associate the “Location” category with a device. You should create associations first, or edit them later, before adding devices and ports in CC-SG.
- **Category**—is a variable that contains a set of values called Elements. An example of a Category is Location, which may have elements such as “America,” and “Asia Pacific.” Another example of a Category is “OS Type”, which may have elements such as “Windows” or “Unix” or “Linux”. When you add devices to CC-SG, you associate this information with them.
- **Elements**—are the values of a Category. For example, the “America” Element belongs to the “Location” category.

- **Devices**—are Raritan products such as Dominion KX, Dominion SX, Dominion KSX, IP-Reach, Paragon II System Controller, Paragon II UMT832 with USTIP, and others, that CC-SG manages. These devices control the target systems, or nodes, that are connected to them.
- **Nodes**—are the target systems or servers that CC-SG can access and manage. In CC-SG, you can click a node to access and manage the node via interfaces.

Associations--Defining Categories and Elements

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

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

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

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

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

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

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

CATEGORY	ELEMENT
usergroup1	usergroup1node
usergroup2	usergroup2node
usergroup3	usergroup3node

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

How to Create Associations

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

- **Guided Setup** combines many configuration tasks into an automated interface. Guided Setup is recommended for your initial CC-SG configuration. Once you have completed Guided Setup, you can always edit your configurations individually. Please refer to [Chapter 3: Configuring CC-SG with Guided Setup](#) for additional information.
- **Association Manager** only allows you to work with associations, and does not automate any configuration tasks. Please refer to the [Association Manager](#) section on the following pages for additional information.

Association Manager

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

Add Category

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

Association Manager

Category

Category name: Department

Value type: String

Applicable for: Node

Add Edit Delete

Elements For Category

Engineering

Finance

Human Resources

Publishing

Add Edit Delete

Close

Figure 20 Association Manager Screen

- Click **Add** in the **Category** panel to add a new category. The **Add Category** window appears.

The image shows a Windows-style dialog box titled "Add Category". It has a blue header bar with a close button (X) in the top right corner. Below the title bar, there is a message area with a red "X" icon and the text "Please enter a category name.". Below this, there are three input fields: "Category name:" followed by a text box, "Value type:" followed by a dropdown menu showing "String", and "Applicable for:" followed by a dropdown menu showing "Both". At the bottom right, there are two buttons: "OK" and "Cancel".

Figure 21 Add Category Window

- Type a category name in the **Category Name** field. Maximum length is 31 characters.
- Click the **Value Type** drop-down arrow to select a value type of **String** or **Integer**.
- Click the **Applicable For** drop-down arrow to select the type of device this category applies to: **Device**, **Node**, or **Both**.
- Click **OK** to create the new category or **Cancel** to exit without creating. The new category name appears in the **Category Name** field.

Edit Category

- On the **Associations** menu, click **Association**.
- Click the **Category Name** drop-down arrow and select the category you want to edit.
- Click **Edit** in the **Category** panel of the screen to edit the category. The **Edit Category** window appears.

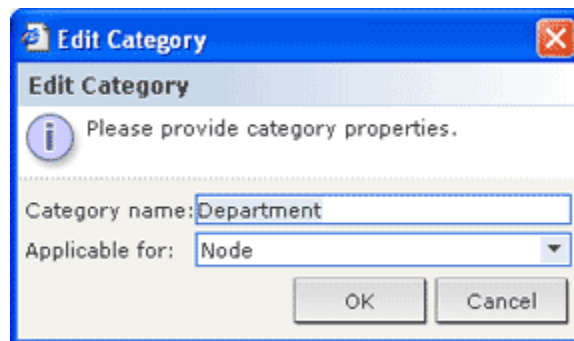
The image shows a Windows-style dialog box titled "Edit Category". It has a blue header bar with a close button (X) in the top right corner. Below the title bar, there is a message area with a blue information icon (i) and the text "Please provide category properties.". Below this, there are two input fields: "Category name:" followed by a text box containing the text "Department", and "Applicable for:" followed by a dropdown menu showing "Node". At the bottom right, there are two buttons: "OK" and "Cancel".

Figure 22 Edit Category Window

- Type the new category name in **Category Name** field.
- Click the **Applicable For** drop-down arrow to change whether this category applies to **Device**, **Node**, or **Both**. Please note that a string value cannot be changed to an integer value, and vice versa. If you must make this type of change, please delete the category, and add a new one.
- Click **OK** to save your changes. The updated category name appears in the **Category Name** field.

Delete Category

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

1. On the **Associations** menu, click **Association**.
2. Click the **Category Name** drop-down arrow and select the category you want to delete.
3. Click **Delete** in the **Category** panel of the screen to delete the category. The **Delete Category** window appears.
4. Click **Yes** to delete the category.

Add Element

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

The screenshot shows the 'Association Manager' window. The 'Category' section has a dropdown for 'Category name' (currently 'Department'), a text field for 'Value type' (currently 'String'), and a text field for 'Applicable for' (currently 'Node'). Below these are 'Add', 'Edit', and 'Delete' buttons. The 'Elements For Category' section has a list box containing 'Engineering', 'Finance', 'Human Resources', and 'Publishing'. Below the list box are 'Add', 'Edit', and 'Delete' buttons. A 'Close' button is at the bottom right.

Figure 23 Association Manager Screen

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

3. Click **Add** in the **Elements For Category** panel to add a new element. The **Add Element** window appears.

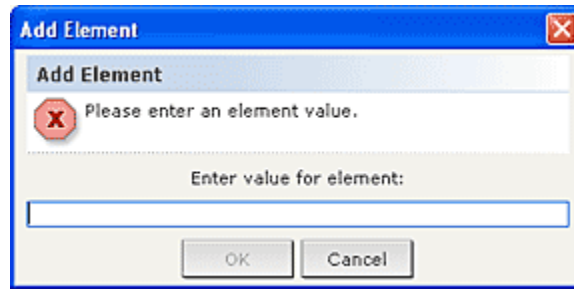


Figure 24 Add Element Window

4. Type the new element name in the **Enter Value for Element** field.
5. Click **OK** to add the element or **Cancel** to exit the window. The new element appears in the **Elements For Category** panel.

Edit Element

1. On the **Associations** menu, click **Association Manager**.
2. Click the **Category Name** drop-down arrow and select the category whose element you want to edit.
3. Select the element to be edited from the **Element For Category** list, and then click **Edit** in the **Elements For Category** panel. The **Edit Element** window appears.

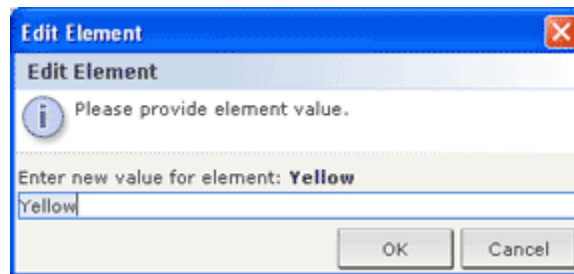


Figure 25 Edit Element Window

4. Type the new name of the element in the **Enter New Value for Element** field.
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 Element

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

1. On the **Associations** menu, click **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 **Element For Category** list, and then click **Delete** in the **Elements For Category** panel. The **Delete Element** window appears.
4. Click **Yes** to delete the element or **No** to close the window. The element name is removed from the **Element For Category** list.

***Note:** Deleting an element removes the element from all device and node category associations, leaving all pre-associated element fields blank.*

This page intentionally left blank.

Chapter 5: Adding KVM and Serial Devices and Device Groups

You must add Raritan KVM and Serial devices to CC-SG before you can use CC-SG to configure and manage them.

If you want to add Raritan PowerStrip Devices that are connected to other Raritan devices to CC-SG, please refer to [Chapter 6: Configuring Power Control](#) for details.

*Note: To configure iLO/RILOE devices, IPMI devices, Dell DRAC devices, IBM RSA devices or other non-Raritan devices, use the **Add Node** menu and add these items as an interface. Please refer to [Chapter 7: Configuring Nodes and Interfaces](#) for additional information.*

The Devices Tab

Click the **Devices** tab to display the Devices tree.

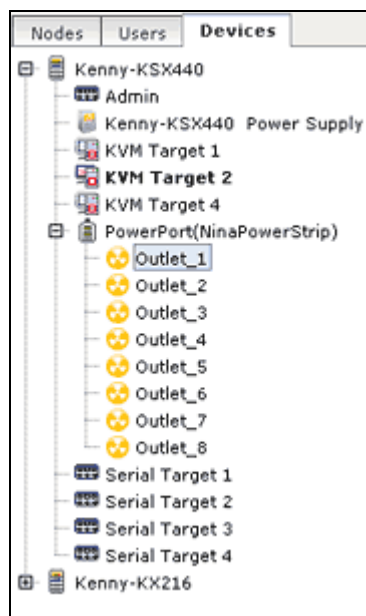


Figure 26 The Devices Tree











The Devices tab displays a set of devices and their configured ports. Ports are nested under the devices they belong to. Devices with configured ports appear in the list with a + symbol next to them. Click the + symbol to expand or hide the list of ports.

Right Click Options in the Device 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.

Device and Port Icons

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

ICON	MEANING
	Device available
	KVM port available or connected
	KVM port inactive
	Serial port available
	Serial port unavailable
	Ghosted port (See Raritan's Paragon II User Guide for details on Ghosting Mode.)
	Device paused
	Device unavailable
	Power strip
	Outlet port

Search for Devices

The Devices tab provides the ability to search for devices within the tree. Searching will only return devices as results and will not include port names. The method of searching can be configured through the **My Profile** screen described later in **Chapter 8: Adding and Managing Users and User Groups**.

To search for a device, at the bottom of the Devices Tree, type a search string in **Search For Device** field, then press **ENTER**. Wildcards are supported in the search string:

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

For example:

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 .

Important! Many of the menu bar commands can be accessed by right-clicking a Device or Port in the Devices tree and selecting a command from the shortcut menu that appears.

Device Profile Screen

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

Figure 27 Devices Tab and Devices Profile

Add a Device

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

If you want to add Raritan PowerStrip Devices that are connected to other Raritan devices to CC-SG, please refer to [Chapter 6: Configuring Power Control](#) for details.

To add a device to CC-SG:

1. On the **Devices** menu, click **Device Manager**, and then click **Add Device**.

Figure 28 Add Device Screen

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

Adding a KVM or Serial Device

3. Type a name for the device in the **Device name** field. Number of characters permitted varies by device. Hold your cursor over the field label to see the number of characters allowed in the name.
4. Type the IP Address or Hostname of the device in the **Device IP or Hostname** field. For hostname rules, refer to **Terminology/Acronyms** in **Chapter 1: Introduction**.
5. Type the TCP communication port used to communicate with the device in the **TCP port number** field. The default port number for most Raritan devices is 5000.
6. Type the name used to log onto this device in the **Username** field. The user must have administrative access.
7. Type the password needed to access this device in the **Password** field. The user must have administrative access.
8. Type the time (in seconds) that should elapse before timeout between the new device and CC-SG in the **Heartbeat timeout (sec)** field.
9. If applicable, check **Allowed** under **Local Access** if you want to allow users to have direct access to this device while it is managed by CC-SG.
10. (Optional) Type a short description of this device in the **Description** field.
11. Check **Configure all ports** if you want to automatically add all ports on this device to the Devices tab, and create a Node for each port on this device in the Nodes tab. Corresponding nodes and ports will be configured with matching names. If checked when the device is added, a new node will be created for each port, and an out-of-band interface will be created for that node.
12. A list of **Categories** and **Elements** can be configured to better describe and organize this device and the nodes connected to it. Please refer to [Chapter 4: Creating Associations](#) for additional information.

To configure **Categories** and **Elements**:

- a. For each **Category** listed, click the **Element** drop-down menu, and then select the element you want to apply to the device from the list. Select the blank item in the **Element** field for each Category you do not want to use.
- b. If you want to assign the Element to the related nodes as well as the device, check the **Apply to Nodes** checkbox.

If you do not see the **Category** or **Element** values you want to use, you can add more through the **Associations** menu. Please refer to **Chapter 4: Creating Associations** for additional information.

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 will alert you and ask if you want to proceed. Click **Yes** to add the device to CC-SG. You can upgrade the device firmware after adding it to CC-SG. Please refer to **Upgrade Devices** later in this chapter.

Adding a PowerStrip Device

The process of adding a PowerStrip Device to CC-SG varies depending on which Raritan device the powerstrip is connected to physically. Please refer to [Chapter 6: Configuring Power Control](#) for details.

Discover Devices

Discover Devices initiates a search for all devices on your network. The search can automatically detect all new and previously existing Raritan devices on your network, including Paragon II System Controller, IP-Reach, Dominion KX, Dominion KX101, Dominion KSX, Dominion SX, and eRIC units. After discovering the devices, you may add them to CC-SG if they are not already managed.

1. On the **Devices** menu, click **Discover Devices**.

Discover Devices

Please provide IP range.

▼ Discover

From IP address: 192.168.32.0 To IP address: 192.168.32.255 Mask: 255.255.255.0

Device types:

- ☒ Dominion KSX
- ☒ Dominion KX
- ☒ Dominion KX101
- ☒ Dominion SX
- ☒ eRIC
- ☒ IP-Reach
- ☒ Paragon II System Controller

☒ Broadcast discovery

☒ Include IPMI Agents

Discover Stop

Figure 29 Discover Devices Screen

2. Type the range of IP addresses where you expect to find the devices in the **From Address** and **To Address** fields. The **To Address** should be larger than the **From Address**. Specify a mask to apply to the range. If a mask is not specified, then a broadcast address of **255.255.255.255** is sent, which broadcasts to all local networks. To discover devices across subnets, you must specify a mask.
3. Check **Broadcast discovery** if searching for devices on the same subnet on which CC-SG resides. Uncheck **Broadcast discovery** to discover devices across different subnets.
4. To search for a particular type of device, select it in the list of **Device types**. By default, all device types are selected. Use **CTRL+click** to select more than one device type.
5. Check **Include IPMI Agents** if you want to find targets that provide IPMI power control.
6. Click **Discover** to start the search. At any time during the discovery, you can click **Stop** to discontinue the discovery process. Discovered devices appear in a list.

IP Address	Device Type	Device Name	Managed	Description
192.168.32.25	Dominion KSX	ISRKSX	No	Dominion KSX model RX440 ver. 3.22.5.3
192.168.32.61	Dominion KSX	Kenny-KSX440	Yes	Dominion KSX model RX440 ver. 3.22.5.3

Add Cancel

Figure 30 Discovered Devices List Window

7. To add one or more discovered devices to CC-SG, select the devices from the list, and then click **Add**. The Add Device screen appears with some of the data already populated. If you selected more than one device to add, you can click **Previous** and **Skip** at the bottom of the screen to navigate through the Add Device screens for the devices you want to add.

Add Device: Dominion KX

Please enter device username.

Device name:
Dominion-KX

Device IP or Hostname:
192.168.32.3

Username:

TCP port number:
5000

Password:

Heartbeat timeout (sec):
600

Firmware
1.4.1.5.11

Description:
Dominion KX model DKX ver. 1.4.1.5.11

☒ Configure all ports

Device Associations

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

Previous OK Apply Skip Cancel

Figure 31 Adding a Discovered Device

8. Type the user name and password (that were created specifically for CC-SG in the device) in the **Username** and **Password** fields to allow CC-SG to authenticate the device when communicating with it in the future. Select the **Categories** and **Elements** you want to apply to the device. If you want a Category and Element to apply to the nodes connected to the device, check the corresponding **Apply to Nodes** checkbox.
9. (Optional) Edit the **Device Name**, **Heartbeat Timeout**, **Local Access** (if available for the device type), **Description**, **Configure all ports**, and **Device Association** fields.
10. When you are done configuring this device, click **Apply** to add this device and open the Add Device screen for the next discovered device. Or, click **OK** to add this device without continuing to the other discovered devices.
11. If the firmware version of a device is not compatible with CC-SG, a message will alert you and ask if you want to proceed. Click **Yes** to add the device to CC-SG, or **No** to cancel the operation. You can upgrade the device firmware after adding the device to CC-SG. Please refer to **Upgrade Devices** later in this chapter for additional information.

Edit Device

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

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

Figure 32 The Device Profile Screen

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 **OK** to save your changes. A **Device Updated Successfully** message confirms that the device has been modified.

Edit PowerStrip Device

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

1. Click the **Devices** tab and select the PowerStrip device you want to edit.
2. Type the new device properties in the appropriate fields on this screen. If necessary, edit the Categories and Elements associated with this device.
3. Click the **Outlet** tab to view all outlets of this PowerStrip.
 - If an outlet is associated with a node, you can click the **Node** hyperlink to open the Node Profile.
 - If an outlet is associated with a node, you can select the outlet, and then click **Power Control** to open the Power Control screen for the associated node.
4. Click **OK** to save your changes. A **Device Updated Successfully** message confirms that the device has been modified.

Delete 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.

1. Click the **Devices** tab and select the device you want to delete.
2. On the **Devices** menu, click **Device Manager**, and then click **Delete Device**.



Figure 33 Delete Device Screen

3. Click **OK** to delete the device. A **Device Deleted Successfully** message confirms that the device has been deleted.

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

Configure Ports

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

Configure a Serial Port

1. Click the **Devices** tab and select a serial device from the Devices tree.
2. On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**.

	Raritan port ID	Port name	Port type	Port status	
<input type="checkbox"/>	Ser_3	Serial Target 4	Serial Port	New	Configure
<input type="checkbox"/>	S0T2	TV KVM	KVM Port	New	Configure

Select All Clear All 1 1/1 Previous Next

Figure 34 Configure Ports Screen

- 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.

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

Configure Serial Port

Please select port properties to add.

Port Properties

Port name: Serial Target 4

Port Status: Up

Availability: Idle

Raritan port ID: Ser_3

Port number: Unknown

Device name: Kenny-KSX440

Device type:

Device IP or Hostname: 192.168.32.61

Node Name: Serial Target 4

Baud rate: 9600

Parity/Data bits: None/8

Parity check: ☐ Enable

Recv/Xmit pace: ☐ Xon/Xoff

H/W flow control: ☐ Enable

Access Application: Auto-Detect

Node Association: n/a

OK Cancel

Figure 35 Configure Serial Ports Screen

- Type a port name in **Port Name** field. For ease of use, name the port after the target that is connected to the port.
- 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.
- 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**.
- Click **OK** to add the port.

Configure a KVM Port

1. Click the **Devices** tab and select a KVM device from the Devices tree.
2. On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**.

Raritan port ID	Port name	Port type	Port status
<input type="checkbox"/> P_HK2e5001_2	Channel 3	KVM Port	Unused
<input type="checkbox"/> P_HK2e5001_6	Channel 7	KVM Port	Unused
<input type="checkbox"/> P_HK2e5001_9	Channel 10	KVM Port	Unused
<input type="checkbox"/> P_HK2e5001_12	Channel 13	KVM Port	Unused
<input type="checkbox"/> P_HK2e5001_13	Channel 14	KVM Port	Unused
<input type="checkbox"/> P_HK2e5001_14	Channel 15	KVM Port	Unused
<input type="checkbox"/> P_HK2e5001_7	TV Channel 8	KVM Port	Unused

Figure 36 Configure Ports Screen

- 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.

Please select port properties to add.

Port Properties

Port name: Channel 14

Raritan port ID: P_HK2e5001_13

Device name: Kenny-KX216

Device IP or Hostname: 192.168.32.63

Node Name: Channel 14

Access Application: Auto-Detect

Port Status: Down

Port number: Unknown

Device type:

Node Association: n/a

Figure 37 Configure KVM Port Screen

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.
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.

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

Edit Ports

You can edit ports to change the name or access application associated with existing configured ports.

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

Port Profile: KVM

Please select port properties to add.

Port Properties

Port name: CC console

Port Status: Down

Availability: ☐

Raritan port ID: P_HK2e5001_10

Port number: Unknown

Device name: Kenny-KX216

Device type: Dominion KX

Access Application: Auto-Detect

Node Association: CC_console

OK Cancel

Figure 38 Ports Profile

- Type a new name for the port in the **Port Name** field, if necessary.
- 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**.
- Click **OK** to save changes to the configured port.

Delete Ports

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

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

1. Click the **Devices** tab and select a device whose ports you want to delete.
2. On the **Devices** menu, click **Port Manager**, and then click **Delete Ports**.

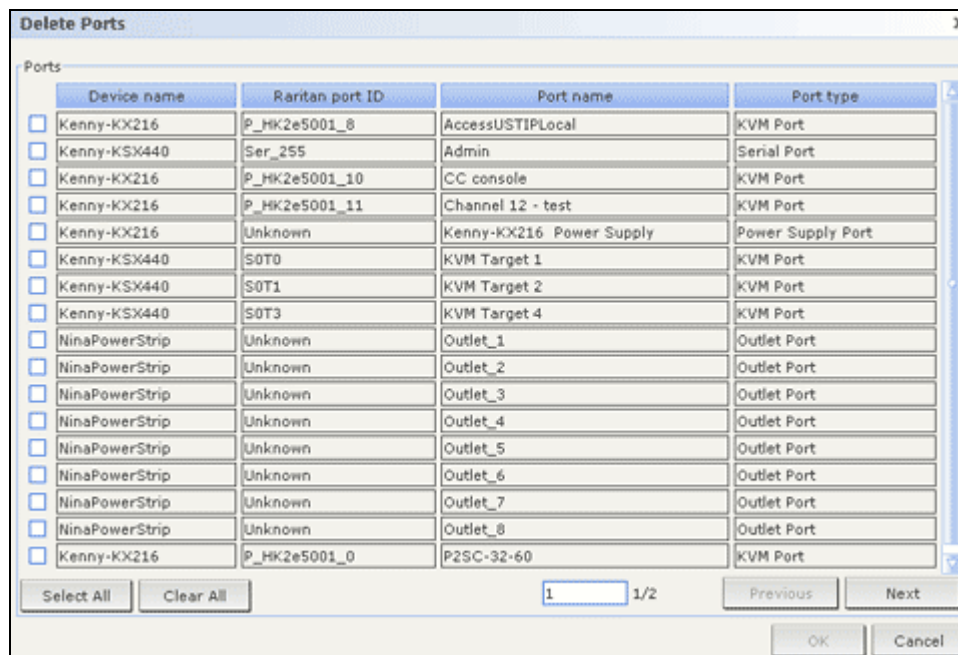


Figure 39 Delete Port Screen

3. Check the ports you wish to delete from the device.
4. Click **OK** to delete the selected port. A **Port Deleted Successfully** window confirms that port has been deleted.

Device Management

Once a device has been added to CC-SG, several management functions besides configuring ports can be performed.

Bulk Copy for Device Categories and Elements

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

1. Click the **Devices** tab and select a device from Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Bulk Copy**.
3. In the **All Devices** list, select the devices to which you are copying the categories and elements of the device in the **Device Name** field.
4. Click > to add a device to the **Selected Devices** list.
5. To remove a device from the **Selected Devices** list, select the device, and then click <.

- Click **OK** to bulk copy. A **Device Copied Successfully** message confirms that device categories and elements have been copied.

Upgrade Device

Upgrade Device allows you to download new versions of device firmware.

- Click the **Devices** tab and select a device from the Devices tree.
- On the **Devices** menu, click **Device Manager**, and then click **Upgrade Device**.

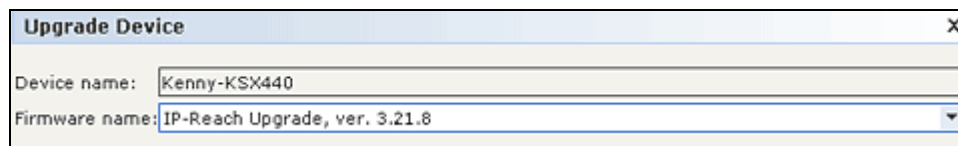


Figure 40 Upgrade Device Screen

- Click the **Firmware Name** drop-down arrow and select the appropriate firmware from the list. Raritan or your reseller will provide this information.
- 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 will alert you and ask if you want to proceed. Please refer to **Chapter 2: Accessing CC-SG** for additional information. Click **Yes** to upgrade the device.
- A **Restart** message appears. Click **Yes** to restart the device.
- A **Device Upgraded Successfully** message confirms that the device has been upgraded.

Backup Device Configuration

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

- Click the **Devices** tab and select the device you want to back up.
- On the **Devices** menu, click **Device Manager**, **Configuration**, then click **Backup**.

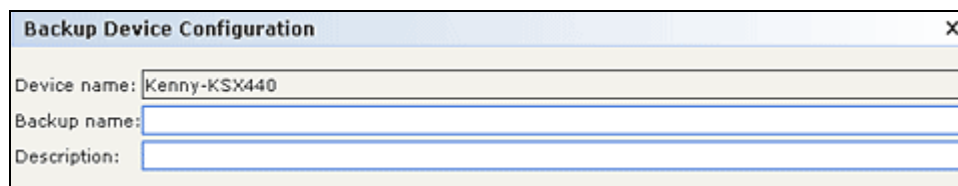


Figure 41 Backup Device Configuration Screen

- Type a name in the **Backup name** field to identify this backup.
- (Optional) Type a short description of the backup in the **Description** field.
- Click **OK** to back up the device configuration. A **Device Configuration Backed Up Successfully** message confirms that device configuration has been backed up.

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

Restore Device Configurations

About Restoring Device Configurations

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

- KX
- KXSX
- KX101
- SX
- IP-Reach

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

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

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

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

1. Click the **Devices** tab and select the device you want to restore to a backup configuration.
2. On the **Devices** menu, click **Device Manager**, **Configuration**, and then click **Restore**.

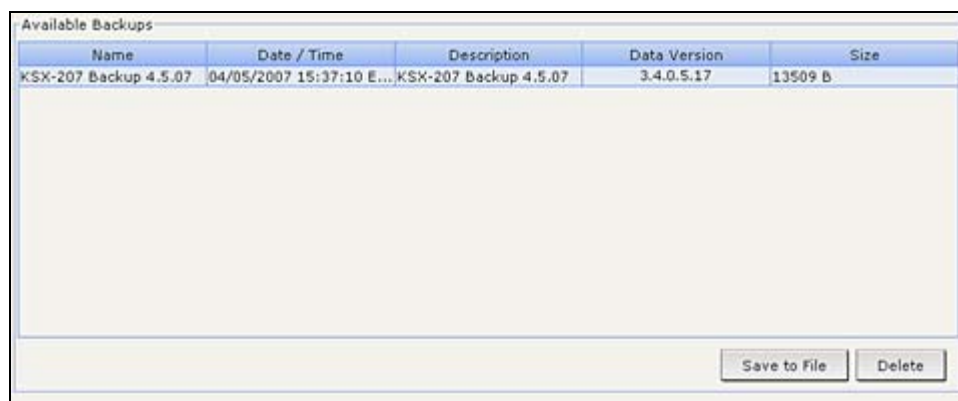


Figure 42 Restore Device Configuration Screen

3. In the **Available Backups** table, select the backup configuration you want to restore to the device.
4. Click **OK**.
5. When the Restart message appears, click **Yes** to restart the device. A **Device Configuration Restored Successfully** message confirms that all data has been restored.

To Restore All Configuration Data Except Network Settings to a KX2 Device

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

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

- On the **Devices** menu, click **Device Manager, Configuration**, and then click **Restore**.

The screenshot shows a dialog box titled "Available Backups". It contains a table with the following data:

Name	Date / Time	Description	Data Version	Size
KX2-53-121-backup	04/05/2007 14:14:09...	Backup of KX2 53-121	2.0	8087 B

Below the table are "Save to File" and "Delete" buttons. Under the "Restore Type" section, the "Protected" radio button is selected. The "Restore Options" section has checkboxes for "Device Settings" and "User and User Group Data", both of which are checked. "OK" and "Cancel" buttons are at the bottom right.

Figure 43 Protected Restore

- In the **Available Backups** table, select the backup configuration you want to restore to the device.
- In the **Restore Type** field, select **Protected**.
- Click **OK**.
- When the Restart message appears, click **Yes** to restart the device. A **Device Configuration Restored Successfully** message confirms that all user and system configuration data has been restored.

To Restore All Configuration Data to a KX2 Device

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

- Click the **Devices** tab and select the device you want to restore to a backup configuration.
- On the **Devices** menu, click **Device Manager, Configuration**, and then click **Restore**.

This screenshot is identical to the one in Figure 43, but the "Full" radio button under the "Restore Type" section is selected instead of "Protected". All other elements, including the table and checkboxes, remain the same.

Figure 44 Full Restore

- In the **Available Backups** table, select the backup configuration you want to restore to the device.
- In the **Restore Type** field, select **Full**.
- Click **OK**.

- When the Restart message appears, click **Yes** to restart the device. A **Device Configuration Restored Successfully** message confirms that all user and system configuration data has been restored.

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

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

- Click the **Devices** tab and select the device you want to restore to a backup configuration.
- On the **Devices** menu, click **Device Manager, Configuration**, and then click **Restore**.

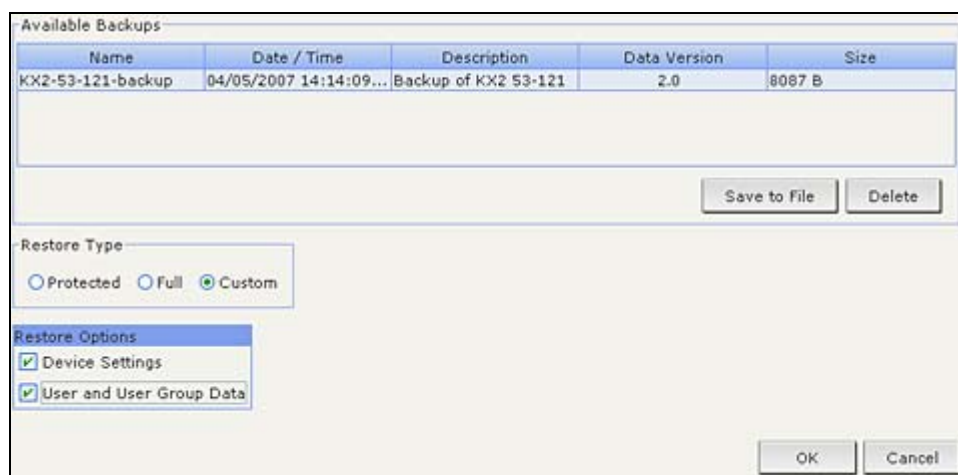


Figure 45 Custom Restore

- In the **Available Backups** table, select the backup configuration you want to restore to the device.
- In the **Restore Type** field, select **Custom**.
- In the **Restore Options** field, select the components you want to restore to the device: Device Settings, User and User Group Data.
- Click **OK**.
- When the Restart message appears, click **Yes** to restart the device. A **Device Configuration Restored Successfully** message confirms that data has been restored.

To Copy Device Configuration

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

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

- Click the **Devices** tab and select the device whose configuration you wish to copy to other devices from the Devices tree.
- On the **Devices** menu, click **Device Manager, Configuration**, and then click **Copy Configuration**.
- 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 **Device Configuration Copied Successfully to** message confirms that the device configuration has been copied.

Restart Device

Use the Restart Device function to restart a device.

1. Click the **Devices** tab and select the device you want to restart.
2. On the **Devices** menu, click **Device Manager**, and then click **Restart Device**.

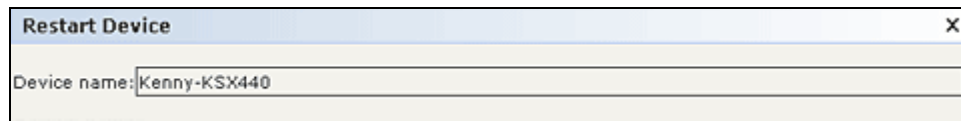
A screenshot of the 'Restart Device' dialog box. It has a title bar with the text 'Restart Device' and a close button (X). Below the title bar, there is a label 'Device name:' followed by a text input field containing the text 'Kenny-KSX440'.

Figure 46 Restart Device Screen

3. Click **OK** to restart the device. A **Device Restart Successfully** message confirms that the device has been restarted.

Ping Device

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

1. Click the **Devices** tab and select the device you want to ping.
2. On the **Devices** menu, click **Device Manager**, and then click **Ping Device**. The **Ping Device** screen appears, showing the result of the ping.

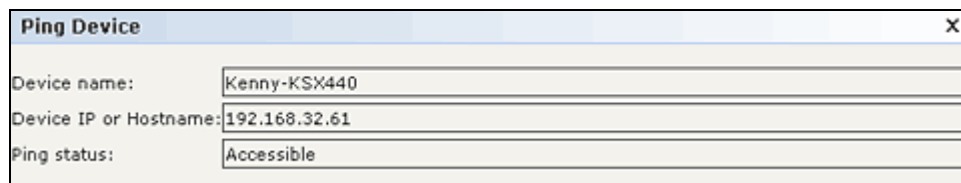
A screenshot of the 'Ping Device' dialog box. It has a title bar with the text 'Ping Device' and a close button (X). Below the title bar, there are three rows of labels and text input fields: 'Device name:' with 'Kenny-KSX440', 'Device IP or Hostname:' with '192.168.32.61', and 'Ping status:' with 'Accessible'.

Figure 47 Ping Device Screen

Pause Management

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

1. Click the **Devices** tab and select the device for which you want to pause CC-SG management.
2. On the **Devices** menu, click **Device Manager**, and then click **Pause Management**. The device's icon in the Device Tree will indicate the device's paused state.

Resume Management

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

1. Click the **Devices** tab and select the paused device from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Resume Management**. The device icon in the Device Tree will indicate the devices active state.

Device Power Manager

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

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

1. In the Devices tree, select a PowerStrip device.
2. On the **Devices** menu, click **Device Power Manager**.
3. The outlets are listed in the **Outlets Status** panel. You may have to scroll to view all outlets.
4. Click the **On** or **Off** radio buttons for each outlet to power ON or power OFF the outlet.
5. Click **Recycle** to restart the device connected to the outlet.

Launch Admin

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

1. Click the **Devices** tab and select the device whose administrator interface you want to launch.
2. On the **Devices** menu, click **Device Manager**, and then click **Launch Admin**. The administrator interface for the selected device will appear.

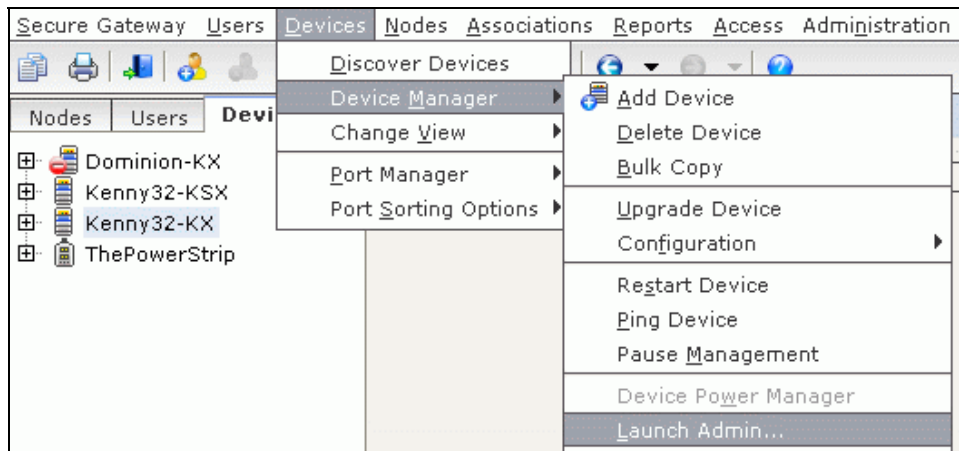


Figure 48 Launch Admin for a KX Device

Topological View

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

1. Click the **Devices** tab and select the device whose topological view you want to see.
2. On the **Devices** menu, click **Device Manager**, and then click **Topological View**. The **Topological View** for the selected device appears.

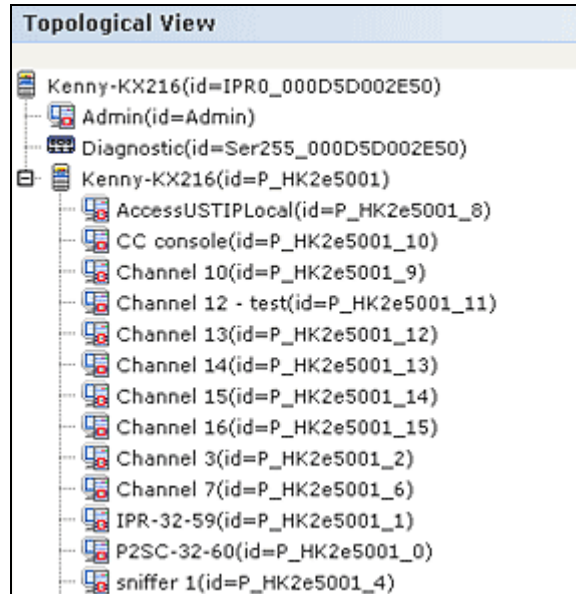


Figure 49 Topological View

3. Navigate the Topological View in the same way you navigate the Devices tree. Click + or – to expand or collapse the view.

*Note: Until you **Close** the **Topological View**, this view will replace the **Device Profile** screen that normally appears when a device is selected.*

Disconnect Users

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

Note: *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.*

1. Click the **Devices** tab and select the device you want to disconnect one or more users from.
2. On the **Devices Menu**, click **Device Manager**, then **Disconnect Users**.

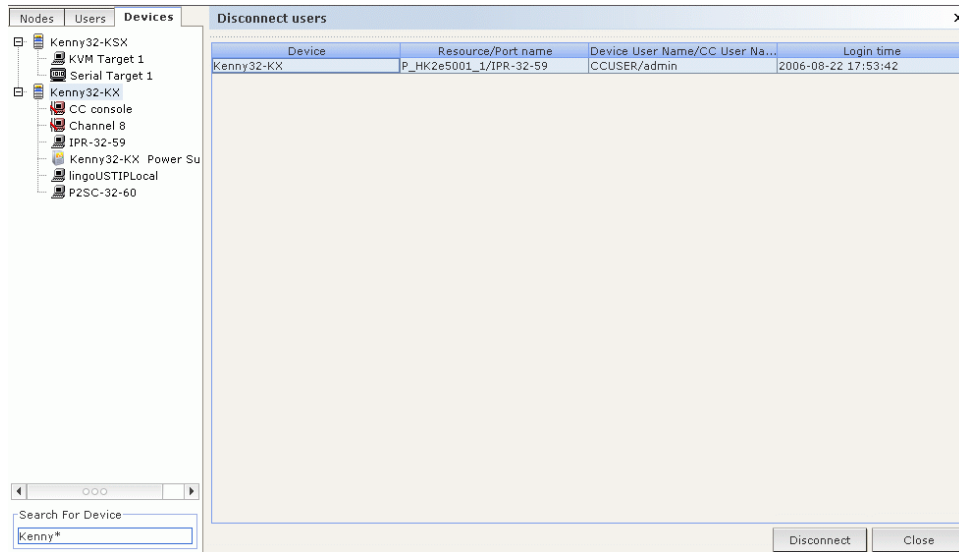


Figure 50 Disconnect Users

3. Select the users whose session you want to disconnect in the **Disconnect users** table.
4. Click **Disconnect** to disconnect them from the device.

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

Viewing Devices

CC-SG offers different options for displaying devices in the Devices tab.

Tree View

Select Tree View to view devices in the Devices tree grouped in the default view. Selecting **Tree View** will also return you to the standard view from a **Custom View**. Please refer to **Custom Views** later in this chapter for additional information.

1. On the **Devices** menu, click **Change View**, and then click **Tree View**. The standard Tree View of the Devices tree appears.

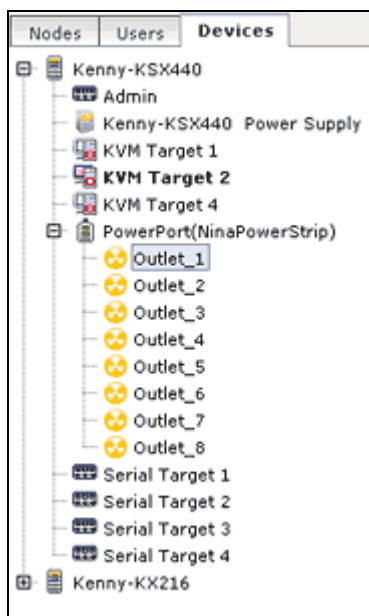


Figure 51 Devices Tree Regular View Screen

Configured ports are nested under their parent devices. To change the way the ports are displayed, click the **Devices** menu, then **Port Sorting Options**. Select **By Port Name** or **By Port Status** to arrange the ports within their devices alphabetically by name or by availability status. Ports arranged by status are sorted alphabetically within their connection status grouping. Devices will also be sorted accordingly.

Custom View

You can customize the Devices tree by organizing devices to appear in a particular format. You might want to view devices by Country, by Time Zone, or by any other option that helps you differentiate between them. Please refer to **Chapter 4: Creating Associations** for additional information on adding Categories to CC-SG.

1. Click the **Devices** tab.

- On the **Devices** menu, click **Change View**, then click **Create Custom View**.

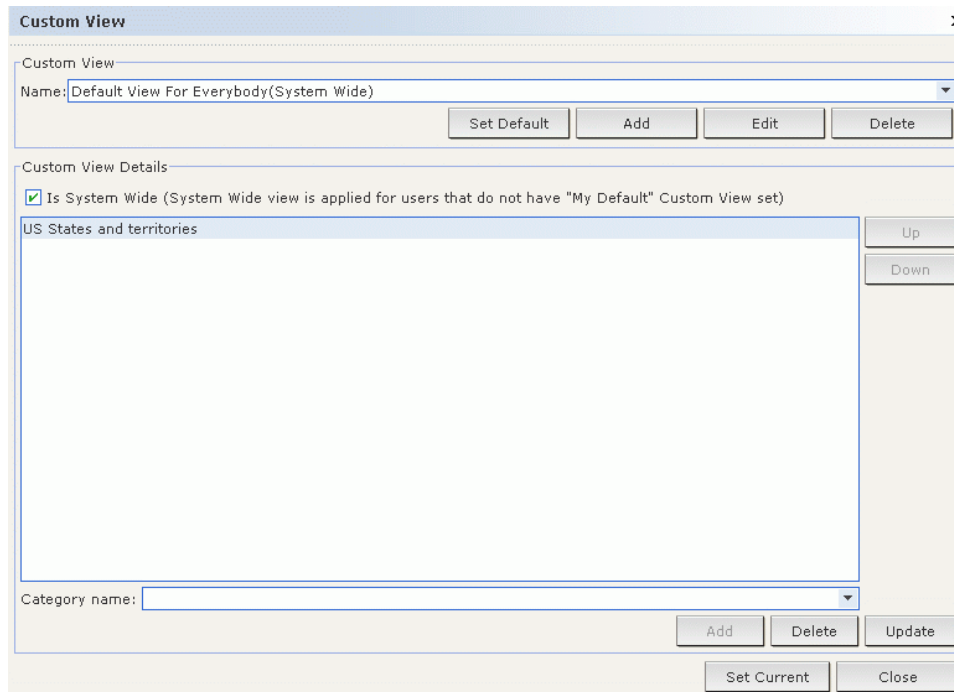


Figure 52 Custom View Screen

- To customize your view, click the **Name** drop-down arrow and select a custom view that has already been saved in the database. Details of the View categories appear in the **Custom View Details** field.
- Click **Set Current** to arrange the Devices tree to reflect the selected custom view.
- Click **Set Default** if you want the selected custom view to be displayed when logging into CC-SG.
- Check **Is System Wide** to make this the default view for all users who are not viewing their own default Custom View.

Selecting a Custom View

To quickly change the current Device Tree view to an already established Custom View:

- Click the **Devices** tab.
- On the **Devices** menu, click **Change View**, and then select the name of the custom view listed under **Create Custom View**. The Device Tree will change to the custom view selected

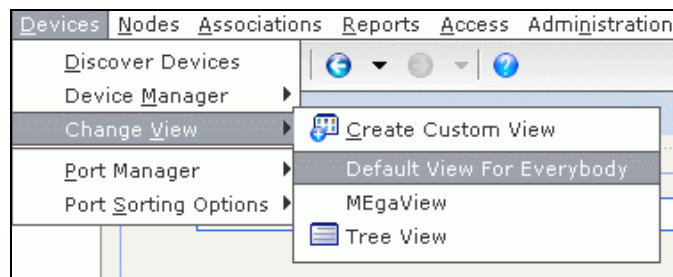


Figure 53 Selecting a Custom View

Add a Custom View

- Click the **Devices** tab.
- On the **Devices** menu, click **Change View**, and then click **Create Custom View**.
- In the **Custom View** panel, click **Add**. An **Add Custom View** window appears.

4. Type a new custom view name, and then click **OK** or click **Cancel** to close the window. The new view name appears in the **Name** field.
5. In the **Custom View Details** panel, click the drop-down arrow at the bottom of the panel. This list contains categories that you can use to filter custom views. Select a detail from the drop-down list, and then click **Add** to add the detail to the **Custom View Details** panel. Select as many details as needed.
6. To re-order the details in the **Custom User Details** panel, select a detail and use the **Up** and **Down** buttons to arrange details in the order you want devices sorted. To remove a detail from the list, select the detail, and then click the **Delete** button in the **Custom User Details** panel.
7. Click **Update** to update the custom view. A **Custom View Updated Successfully** message confirms that the custom view has been updated.
8. Click **Set Current** to arrange the Devices tree to reflect the selected custom view.

Edit a Custom View

1. Click the **Devices** tab.
2. On the **Devices** menu click **Change View**, and then click **Custom View**.
3. Click the **Name** drop-down arrow in the **Custom View** panel and select the custom view to be edited. Click **Edit**. An **Edit Custom View** window appears.
4. Type a new custom view name, and then click **OK** to confirm or **Cancel** to close window.
5. In the **Custom View Details** panel, click the drop-down arrow at the bottom of the panel. This list contains categories that you can use to filter custom views. Select a detail from the drop-down list, and then click **Add** to add the detail to the **Custom View Details** panel. Select as many details as needed.
6. To re-order the details in the **Custom User Details** panel, select a detail and use the **Up** and **Down** buttons to arrange details in the order you want devices sorted. To remove a detail from the list, select the detail, and then click the **Delete** button in the **Custom User Details** panel.
7. Click **Update** to update custom view. A **Custom View Updated Successfully** message confirms that the custom view has been updated.
8. Click **Set Current** to arrange the Devices tree to reflect the selected custom view.

Delete Custom View

1. Click the **Devices** Tab.
2. On the **Devices** menu, click **Change View**, and then click **Create Custom View**.

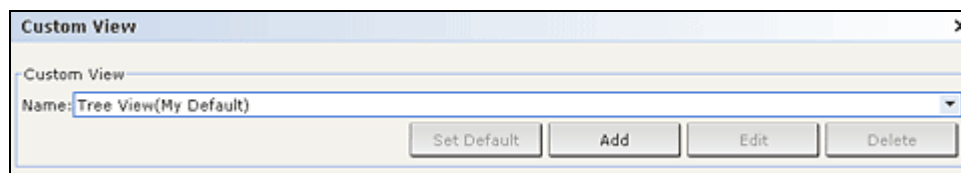


Figure 54 Custom View Screen

3. Click the **Name** drop-down arrow in the **Custom View** panel and select the custom view to be deleted.
4. Click the **Delete** button in the **Custom View** panel. A **Delete Custom View** window appears.
5. Click **Yes** to delete the custom view.

Special Access to Paragon II System Devices

Paragon II System Controller (P2-SC)

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

To access Paragon II System Controller:

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

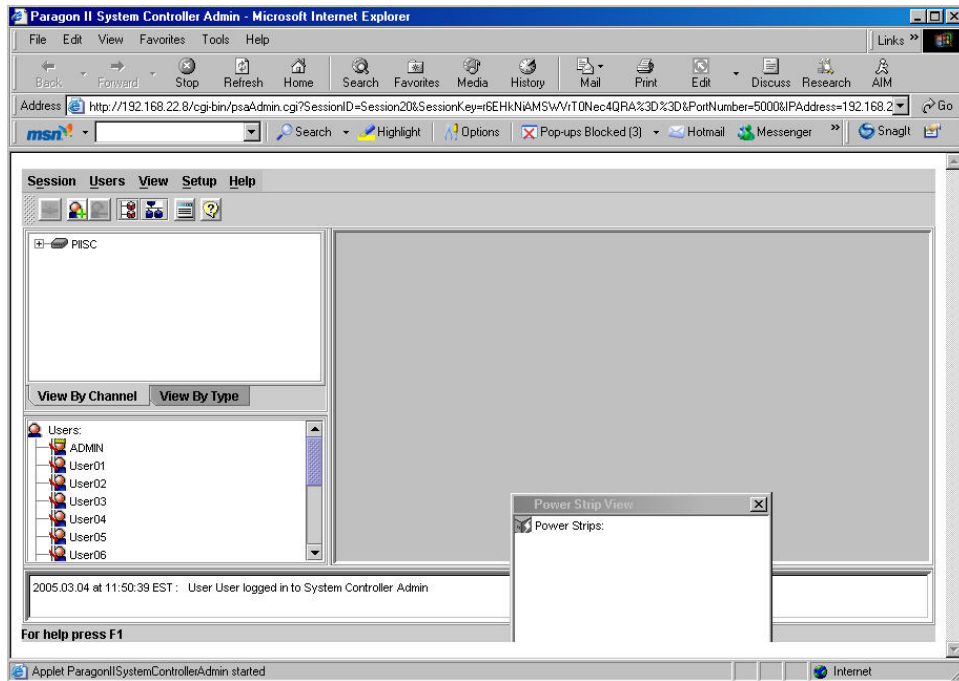


Figure 55 Paragon Manager Application Window

IP-Reach and UST-IP Administration

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

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

To access Remote User Station Administration:

1. Click the **Device** tab, and then select the **Paragon II System Controller**.
2. Right-click the **Paragon II System Controller**, and then click **Remote User Station Admin**. The Remote User Station Admin screen appears, listing all connected IP-Reach and UST-IP units.
3. Click the **Launch Admin** button in the row of the device you want to work with to activate Raritan Remote Console and launch the blue device configuration screen in a new window.

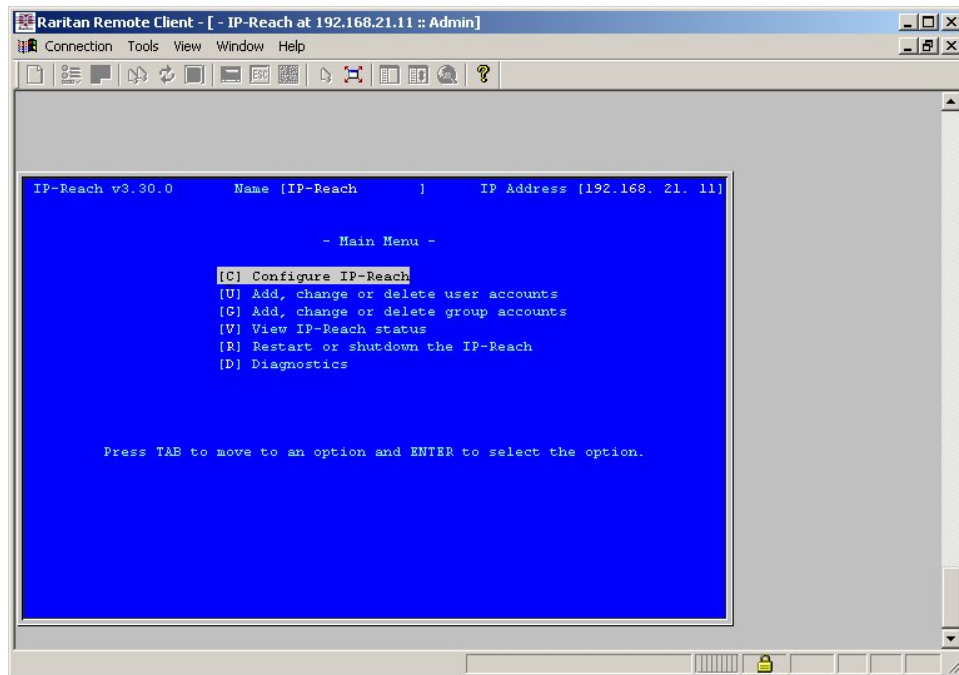


Figure 56 IP-Reach Administration Screen

Device Group Manager

Use the Device Groups Manager screen to add device groups, edit device groups, and remove device groups. When you add a new device group, you can create a full access policy for the group. Please refer to [Chapter 9: Policies](#) for additional information.

Add Device Group

1. On the **Associations** menu, click **Device Groups**. The Device Groups Manager window opens. Existing device groups display in the left panel.

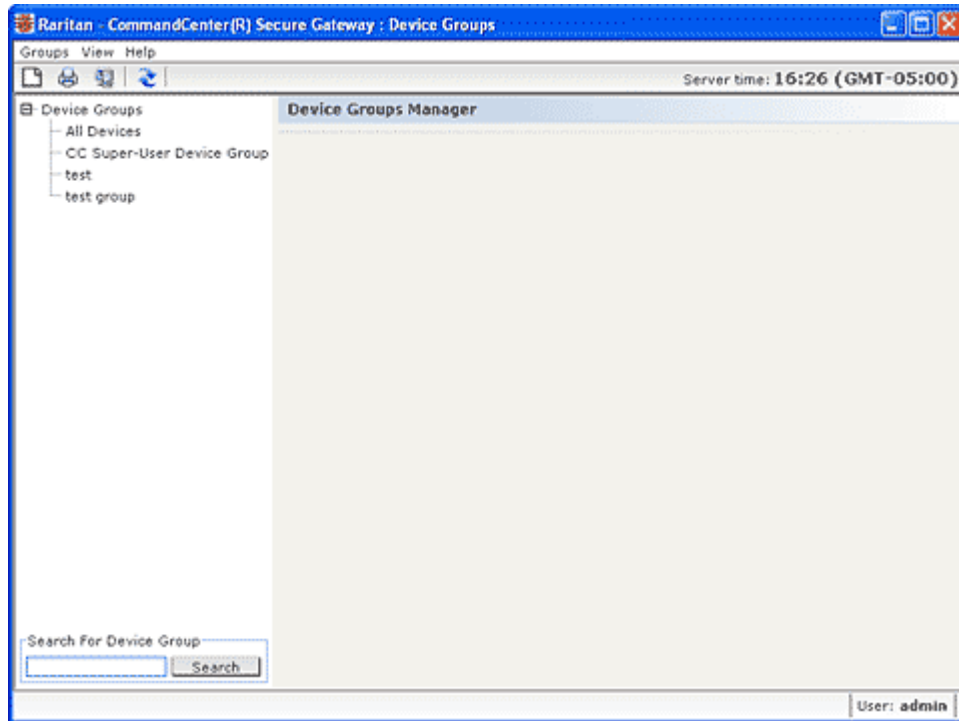


Figure 57 Device Groups Manager

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

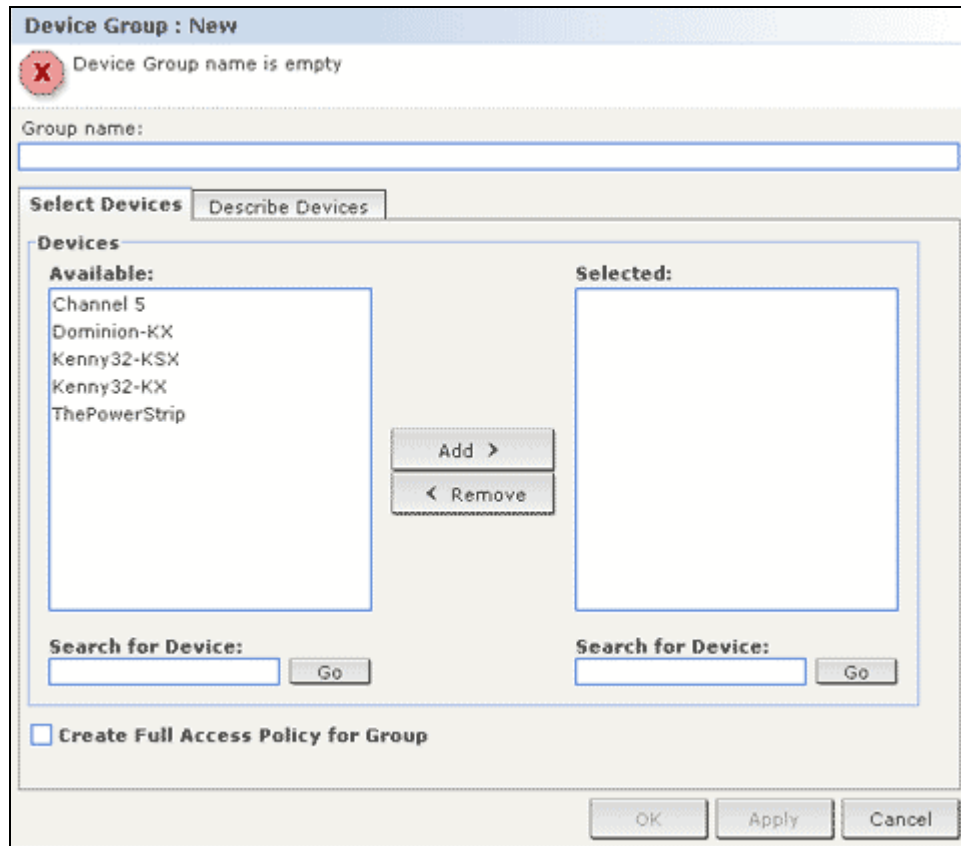


Figure 58 Device Group: New Panel, Select Devices Tab

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

Select Devices

- Click the **Select Devices** tab in the **Device Group: New** panel.
- 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.
 - If you want to remove a device from the group, select the device name in the **Selected** list, and then click **Remove**.
 - You can search for a device in either the **Available** or **Selected** list. Type the search terms in the field below the list, and then click **Go**.

Describe Devices

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


Prefix	Category	Operator	Element	Rule Name
	Device Name			Rule0
	Device Name			Rule1

Short expression:

Normalized expression (Description):

☐ Create Full Access Policy for Group

Figure 59 Describe Devices Tab

- 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** will be 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 display here (for example: if evaluating a “Department” category, “Location” elements will not appear here).
 - **Rule Name**- This is a name assigned to the rule in this row. It is not editable, it is used for writing descriptions in the **Short Expression** field.


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

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

- e. The table of rules only makes available criteria for evaluating nodes. To write a description for the device group, add the rules by **Rule Name** to the **Short Expression** field. If the description only requires a single rule, then simply type that rule's name in the field. If multiple rules are being evaluated, type the rules into the field using a set of logical operators to describe the rules in relation to each other:
 - **&** - the AND operator. A node must satisfy rules on both sides of this operator for the description (or that section of a description) to be evaluated as true.
 - **|** - the OR operator. A device only needs to satisfy one rule on either side of this operator for the description (or that section of a description) to be evaluated as true.
 - **(and)** – grouping operators. This breaks the description into a subsection contained within the parentheses. The section within the parentheses is evaluated first before the rest of the description is compared to the node. Parenthetical groups can be nested inside another parenthetical group.

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

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

- If you want to remove a row from the table, select the row, and then click the Remove Selected Row icon .
 - If you want to see the list of devices whose parameters follow the rules you have defined, click **View Devices**.
- f. 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 will appear in the **Normalized Expression** field.
 - g. Click **View Devices** to see what nodes satisfy this expression. A **Devices in Device Group Results** window will appear 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.
 - h. Check the **Create Full Access Policy for Group** checkbox if you want to create a policy for this device group that allows access to all devices in the group at all times with control permission.
 - i. If you want to add another device group, click **Apply** to save this group, then repeat the steps in this section to add additional device groups. If you have finished adding device groups, click **OK** to save this group and exit the **Device Group: New** panel.

Edit Device Group

1. On the **Associations** menu, click **Device Groups**. The Device Groups Manager window opens.

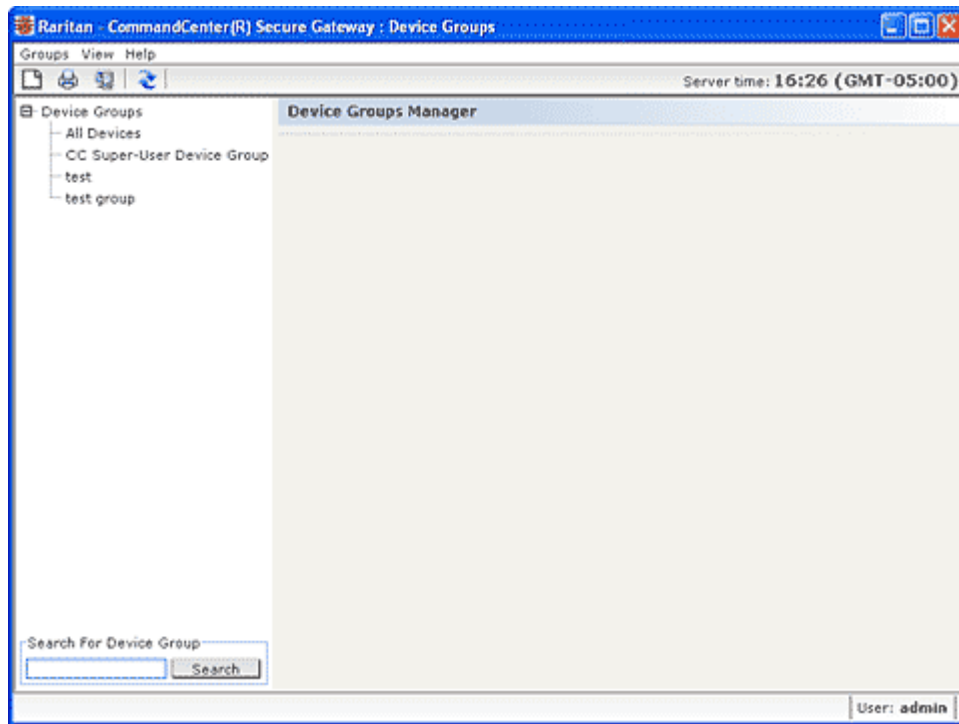


Figure 60 Device Groups Manager Screen

2. Existing device groups display in the left panel.. Select the Device Group whose name you want to edit. The Device Group Details panel appears.
3. If you want to edit the device group name, type a new name for the device group in the **Group Name** field.
4. Edit the device group's included devices using the Select Device or Describe Devices tabs. Please refer to **Add Device Group** in the previous section for additional information.
5. Click **OK** to save your changes.

Delete Device Group

1. On the **Associations** menu, click **Device Groups**. The Device Groups Manager window opens.

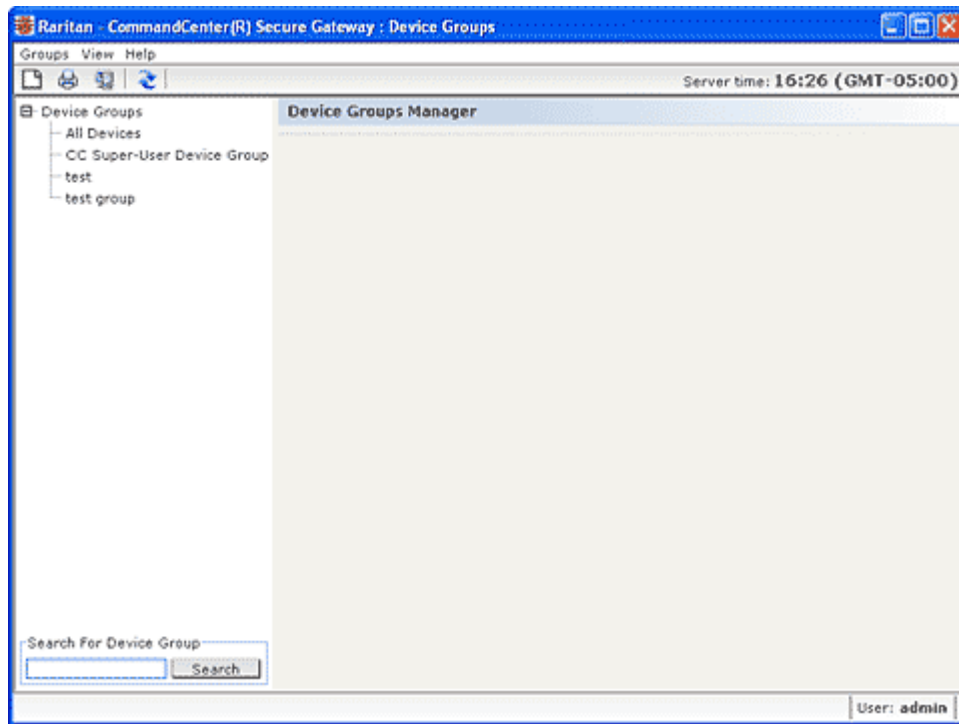


Figure 61 Device Groups Manager Screen

2. Existing device groups display in the left panel. Select the device group you want to delete. The Device Group Details panel appears.
3. On the **Groups** menu, click **Delete**.



Figure 62 Delete Device Group Window

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

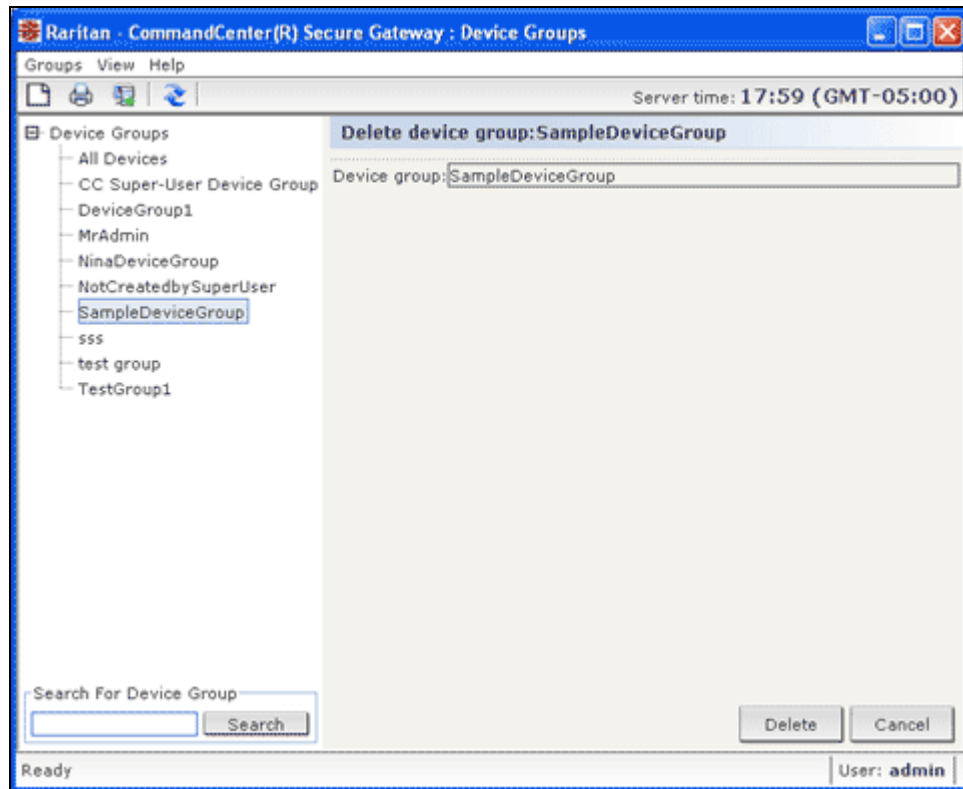


Figure 63 Delete Device Group Panel

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

Chapter 6: Configuring Power Control

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

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

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

Process for Configuring Power Control in CC-SG

- Complete all physical connections between the device, the powerstrip, and the nodes that are powered by the powerstrip. Please refer to the RPC Quick Setup Guide, Dominion PX Quick Setup Guide, and CC-SG Deployment Guide for details on physical connections between PowerStrips, devices, and nodes.
- Add the managing device to CC-SG. The procedure varies for different Raritan devices. Please refer to the section that corresponds to the device to which the PowerStrip is connected:
 - [Configuring PowerStrips Connected to KX, KX2, and P2SC](#)
 - [Configuring PowerStrips Connected to SX 3.0 and KSX](#)
 - [Configuring PowerStrips Connected to SX 3.1](#)
- [Configure outlets](#).
- Associate each outlet with the node that it powers by [adding a Managed PowerStrip interface to the node](#).

Configuring PowerStrips Connected to KX, KX2, and P2SC

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

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

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

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

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

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

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

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

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

Configuring PowerStrips Connected to SX 3.0 and KSX

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

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

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

Add a PowerStrip Connected to an SX 3.0 or KSX device

1. [Add the SX 3.0 or KSX device to CC-SG.](#)
2. On the **Devices** menu, click **Device Manager, Add Device.**
3. Select **PowerStrip** from the **Device type** drop-down menu.

Figure 64 Adding a PowerStrip device

3. 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.
4. Click the **Number of Outlets** drop-down menu and select the number of outlets this PowerStrip contains.
5. Click the **Managing Device** drop-down menu, and then select the SX 3.0 or KSX device that is connected to this power strip.

6. Click the **Managing Port** drop-down menu, and then select the port on the SX 3.0 or KSX device to which this power strip is connected.
7. (Optional) Type a short description of this PowerStrip in the **Description** field
8. (Optional) Check **Configure All Outlets** if you want to automatically add each outlet on this PowerStrip device to the **Devices** tab. If you don't configure all outlets now, you can [configure them later](#).
9. (Optional) For each **Category** listed, click the **Element** drop-down menu, and then select the element you want to apply to the device from the list. Select the blank item in the **Element** field for each Category you do not want to use. Please refer to [Chapter 4: Creating Associations](#) for details.
10. 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.

Delete a PowerStrip Connected to an SX 3.0 or KSX Device

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

1. In the Devices tab, select the PowerStrip you want to delete.
2. On the Devices menu, click Device Manager, Delete Device.
3. Click **OK** to delete the PowerStrip. A **Device Deleted Successfully** message confirms that the PowerStrip has been deleted. The PowerStrip icon is removed from the Devices tab.

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

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

1. In the Devices tab, select the PowerStrip that has been moved from one SX 3.0 or KSX device or port to another.
2. Click the **Managing Device** drop-down menu, and then select the SX 3.0 or KSX device that is connected to this powerstrip.
3. Click the **Managing Port** drop-down menu, and then select the port on the SX 3.0 or KSX device to which this powerstrip is connected.
4. Click **OK**.

Configuring PowerStrips Connected to SX 3.1

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

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

Add a PowerStrip Device Connected to an SX 3.1 Device

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

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

1. [Add the SX 3.1 device to CC-SG](#).
2. CCSG detects the PowerStrip and adds it automatically. The PowerStrip will display in the Devices tab, beneath the SX 3.1 device that it is connected to.

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

1. [Add the SX 3.1 device to CC-SG.](#)
2. [Configure the ports of the SX 3.1 device.](#)
3. In the **Devices** tab, select the SX 3.1 device to which the PowerStrip is connected.
4. Click the + next to the device icon to expand the list of ports.
5. Right-click the SX 3.1 port that the PowerStrip is connected to, and select Add Powerstrip from the pop-up menu.
6. Enter the number of outlets that the PowerStrip contains, and then click **OK**. The PowerStrip

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](#).

Delete a PowerStrip Connected to a SX 3.1 Device

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

1. In the **Devices** tab, select the PowerStrip you want to delete.
2. On the **Devices** menu, click **Device Manager**, **Delete Device**.
3. Click **OK** to delete the PowerStrip. A **Device Deleted Successfully** message confirms that the PowerStrip has been deleted. The PowerStrip icon is removed from the Devices tab.

Configure Outlets on a PowerStrip

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

There are three methods for configuring outlets:

To configure outlets from the PowerStrip profile

1. In the **Devices** tab, click the + next to the device that is connected to the PowerStrip to expand all ports.
2. Select the PowerStrip whose outlets you want to configure.
3. In the Device Profile: PowerStrip screen, select the **Outlets** tab.
4. Select the checkbox for each outlet you want to configure, and then click **OK**.
5. The outlets will display beneath the PowerStrip icon in the **Devices** tab.

To configure outlets from the Configure Ports screen

1. In the **Devices** tab, click the + next to the device that is connected to the PowerStrip to expand all ports.
2. Select the PowerStrip whose outlets you want to configure.
3. On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**.
1. 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.
2. To configure each outlet individually, click the **Configure** button next to the outlet, and then type a name for the outlet in the **Port name** field. Click **OK** to configure the port.

To delete an outlet

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

2. Click the + next to the PowerStrip to expand all outlets.
3. On the **Devices** menu, click **Port Manager, Delete Ports**.
4. Select the checkbox for each outlet you want to delete, and then click **OK** to delete the outlet.

This page intentionally left blank.

Chapter 7: Configuring Nodes and Interfaces

This chapter discusses how to view, configure, and edit nodes and their associated interfaces. Please refer to Raritan's **CommandCenter Secure Gateway User Guide** for additional information on connecting to nodes.

View Nodes

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

Nodes Tree

When you click the Nodes tab, the Nodes tree displays the available nodes. 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**.

Node Profile

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

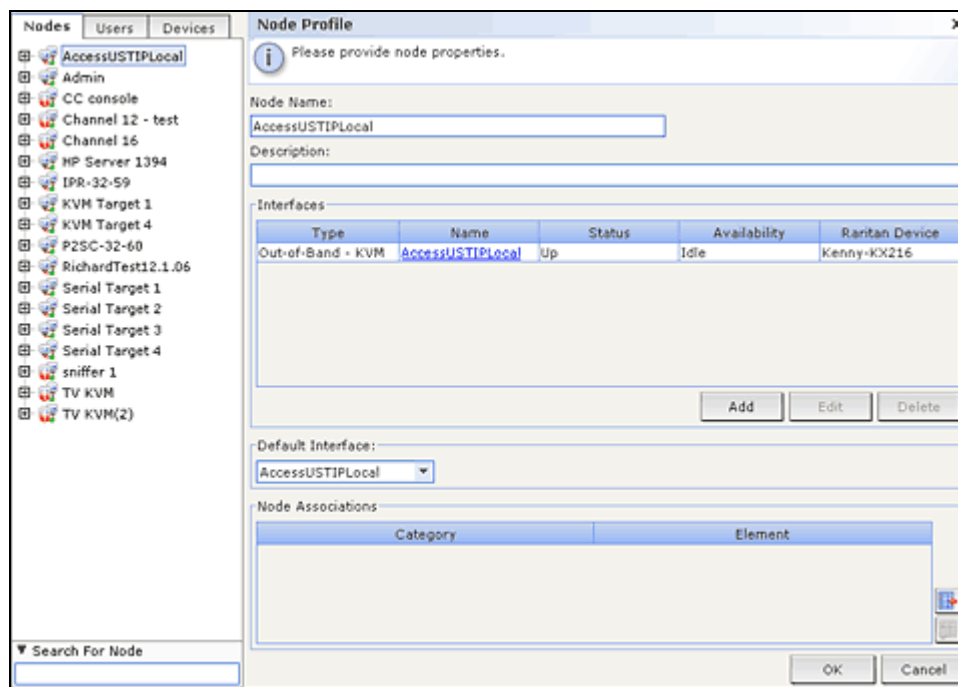


Figure 65 The Nodes Tab and Nodes Profile Screen

Node and Interface Icons

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

ICON	MEANING
	Node available – the node has at least one interface that is up .



Node unavailable – the node has does not have an interface that is **up**.

Nodes and Interfaces Overview

About Nodes

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

You can manually add nodes to CC-SG after you have added the devices to which they are connected. However, nodes can also be created automatically, by checking the **Configure all ports** checkbox on the Add Device screen when you are adding a device. This option allows CC-SG to automatically add all device ports, and add a node and an out-of-band KVM or serial interface for each port. You can always edit these nodes, ports, and interfaces later, as described in this chapter. Please refer to [Chapter 3: Configuring CC-SG with Guided Setup](#) or [Chapter 5: Adding Devices and Device Groups: Add a Device](#), for additional information.

Node Names

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

About Interfaces

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

A single node may have multiple interfaces, but it can only have one out-of-band serial or KVM interface. For example, a PC running Windows Server 2003 may have an out-of-band KVM interface through its keyboard, mouse, and monitor ports, and a power interface to manage the outlet to which it is connected.

Important! Many of the menu bar commands described in this chapter can be accessed by right-clicking a Node and selecting a command from the shortcut menu that appears.

Add Node

To add a new node to CC-SG:

1. Click the **Nodes** tab.
2. On the Nodes menu, click **Add Node**.

Node Profile

Please provide node properties.

Node Name:

Description:

Interfaces

Type	Name	Status	Availability	Raritan Device

Add Edit Delete

Default Interface:

Node Associations

Category	Element
Building	<input type="text"/>
Location	<input type="text"/>
System Type	<input type="text"/>
US States and territories	<input type="text"/>

OK Apply Cancel

Figure 66 Add Node Screen

3. Type a name for the node in the **Node Name** field. All node names in CC-SG must be unique.
4. (Optional) Type a short description for this node under the **Description** field.
5. You must configure at least one interface. Click **Add** in the **Interfaces** area of the Add Node screen to add an interface. Please refer to the [Add an Interface](#) section below for additional information on this procedure.
6. A list of **Categories** and **Elements** can be configured to better describe and organize this node. Please refer to [Chapter 4: Creating Associations](#) for additional information.
 - For each **Category** listed, click the **Element** drop-down menu, and then select the element you want to apply to the node from the list. Select the blank item in the **Element** field for each Category you do not want to use.
 - If you do not see the **Category** or **Element** values you want to use, you can add more through the **Associations** menu. Please refer to [Chapter 4: Creating Associations](#) for additional information.
7. Click **OK** to save the node. The node will be added to the node list.

Add an Interface

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

The **Add Interface Window** appears.

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

In-Band Connections

- **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 afterwards.
- **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).
- **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 afterwards.
- **SSH:** Select this item to create an SSH connection to a node.
- **VNC:** Select this item to create a KVM connection to a node through VNC server software.
- **iLO/RILOE KVM:** Select this item to create a KVM connection to an HP server through an iLO or RILOE interface.

Out-of-Band Connections

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

Power Control Connections

- **DRAC:** Select this item to create a power control connection to a Dell DRAC server.
 - **IPMI:** Select this item to create a power control connection to a node through an IPMI connection.
 - **Managed PowerStrip:** Select this item to create a power control connection to a node powered through a Raritan PowerStrip.
 - **RSA:** Select this item to create a power control connection to an RSA server.
 - **iLO/RILOE:** Select this item to create a power control connection to an HP iLO/RILOE server.
3. A default name will appear in the **Name** field depending on your selection. You can replace this with a name of your choice if you want. This name will appear next to the interface in the Nodes list.

For In-Band connections and DRAC, RSA, and iLO/RILOE power connections:

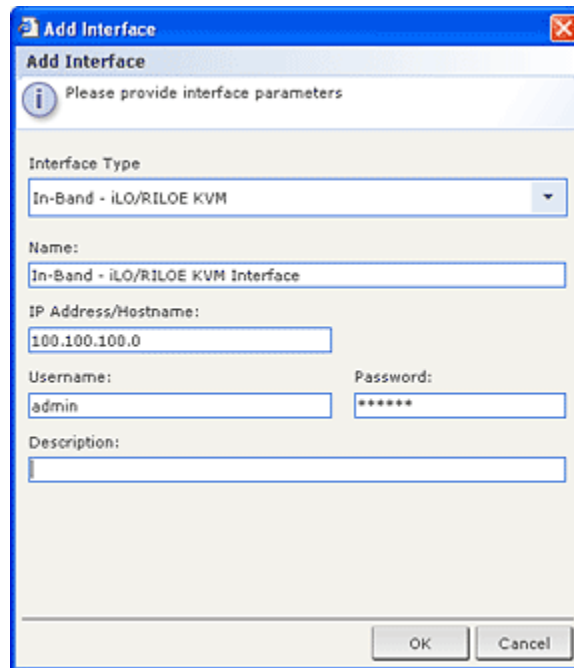


Figure 67 Add Interface—In-Band iLO/RILOE KVM

1. Type the IP Address or Hostname for this interface in the **IP Address/Hostname** field.
2. If necessary, type a TCP Port for this connection in the **TCP Port** field.
3. Type a username for this connection in the **Username** field.
4. If necessary, type a password for this connection in the **Password** field.
5. Click **OK** add the interface to the node. You will be returned to the **Add Node** or **Node Profile** screen.

For Out-of-Band KVM, Out-of-Band Serial connections:

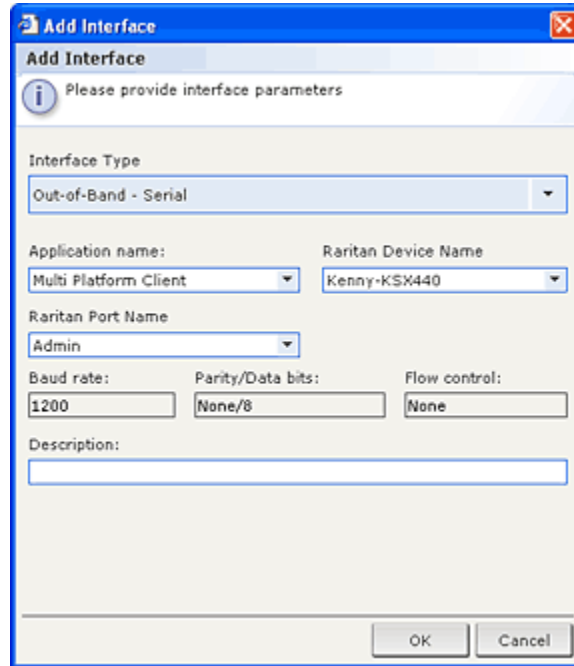
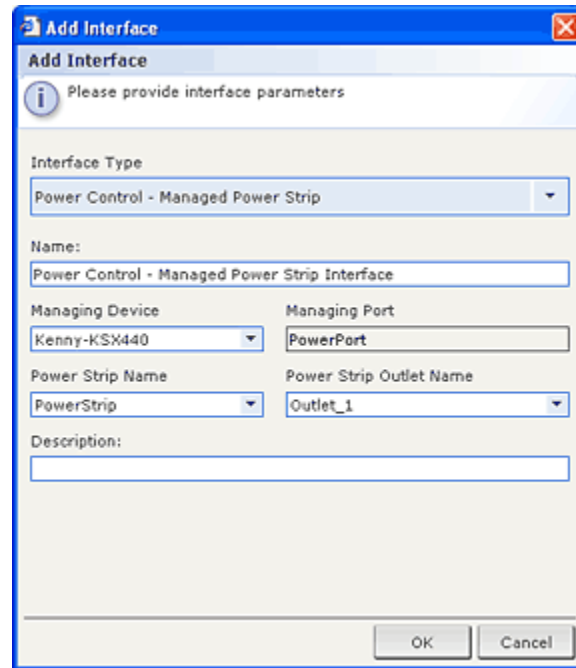


Figure 68 Configuring an Out-of-Band KVM Connection

1. Click the **Application name** drop-down menu and 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. Click the **Raritan Device Name** drop-down menu and select the Raritan device providing access to this node. Note, a device must be added to CC-SG first before appearing in this list.
3. Click the **Raritan Port Name** drop-down menu and select the port on the Raritan device providing access to this node. The port must be configured in CC-SG before it will appear in this list. On serial connections the **Baud Rate**, **Parity** and **Flow Control** values will populate based on the port's configuration.
4. Click **OK** add the interface to the node. You will be returned to the **Add Node** or **Node Profile** screen.

For Managed Power Strip connections:



The screenshot shows a Windows-style dialog box titled "Add Interface". Inside, there is a header bar with the title and a close button. Below the header, there is a message icon and the text "Please provide interface parameters". The main area contains several fields: "Interface Type" is a dropdown menu set to "Power Control - Managed Power Strip"; "Name:" is a text box containing "Power Control - Managed Power Strip Interface"; "Managing Device" is a dropdown menu set to "Kenny-KSX440"; "Managing Port" is a text box containing "PowerPort"; "Power Strip Name" is a dropdown menu set to "PowerStrip"; "Power Strip Outlet Name" is a dropdown menu set to "Outlet_1"; and "Description:" is a large text area. At the bottom right, there are "OK" and "Cancel" buttons.

Figure 69 Configuring a Managed Power Strip Power Control Interface

1. Click the **Managing Device** drop-down menu and select the Raritan device that the Power Strip that provides power to the node is connected to. The device must be added to CC-SG.
2. Click the **Power Strip Name** drop-down menu and select the Power Strip that provides power to the node. The power strip must be configured in CC-SG before it will appear in this list.
3. Click the **Power Strip Outlet Name** and select the name of the outlet the node is plugged into.
4. (Optional) Type a description of this power control interface in the **Description** field.
5. Click **OK** add the interface to the node.

Note: 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.

For IPMI Power Control connections:

Figure 70 Configuring an IPMI Power Control Interface

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. Click the **Authentication** drop-down menu and select an authentication scheme for connecting to this interface.
4. Type a check interval for this interface in the **Check Interval (seconds)** field.
5. Type a username for this interface in the **Username** field.
6. If necessary, type a password for this interface in the **Password** field.
7. Click **OK** add the interface to the node. You will be returned to the **Add Node** or **Node Profile** screen.

Results of Adding an Interface

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

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

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

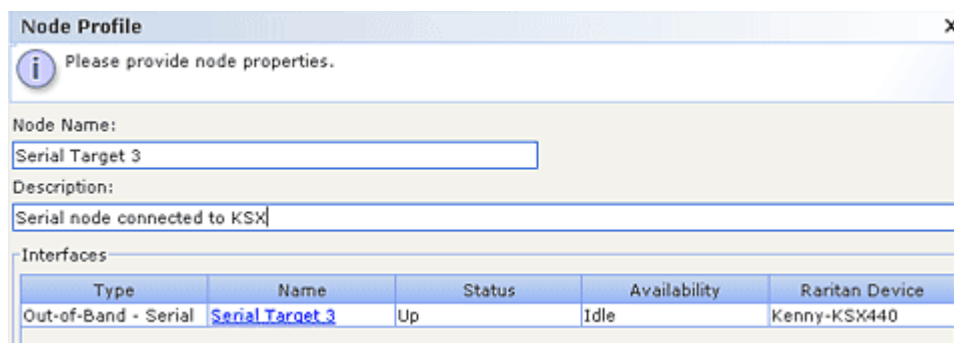
Bulk Copy for Node Categories and Elements

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

1. Click the **Nodes** tab and select a node from Nodes tree.
2. On the **Nodes** menu, click **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.
4. Click > to add a node to the **Selected Nodes** list.
5. To remove a device from the **Selected Nodes** list, select the node, and then click <.
6. Click **OK** to bulk copy. A **Node Copied Successfully** message confirms that node categories and elements have been copied.

Connect to a Node

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



Node Profile

Please provide node properties.

Node Name:
Serial Target 3

Description:
Serial node connected to KSX

Interfaces

Type	Name	Status	Availability	Raritan Device
Out-of-Band - Serial	Serial Target 3	Up	Idle	Kenny-KSX440

Figure 71 Connecting to a Node's Configured Interface

1. Click the **Nodes** tab.
2. Select the node you want to connect to.
3. In the **Interfaces** table, click the name of the interface you want to connect with.

Alternatively:

1. In the Nodes tab, click the + symbol next to the node you want to connect to, expanding the list of interfaces underneath it.
2. Double-click the name of the interface you want to connect with.

Edit an Interface

To edit an interface:

1. Click the **Nodes** tab.
2. Click the node with the interface you want to edit.
3. In the **Interfaces** table, select the row of the interface you want to edit.
4. Click **Edit**.

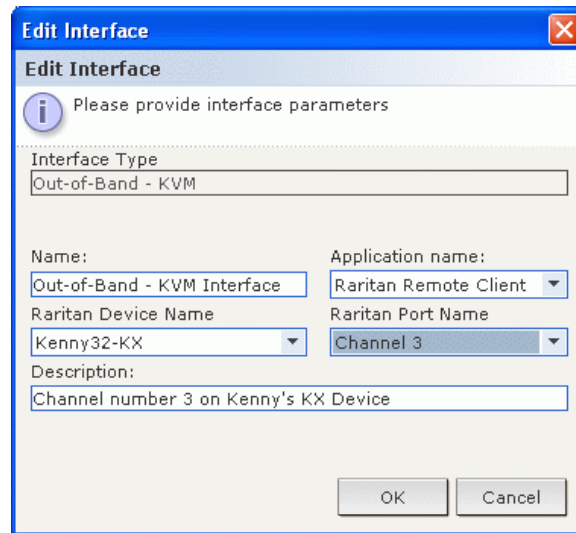


Figure 72 Editing an Interface

5. You cannot change the type of the existing interface. You can change the **Interface Name**, **Description**, and the values of the other fields for this type. Please refer to the **Add Interface** section above for additional information.

Delete an Interface

To delete an interface from a node:

1. Click the **Nodes** tab.
2. Click the node with the interface you want to delete.
3. In the **Interfaces** table, click the row of interface you want to delete.
4. Click **Delete**. You will be prompted to confirm your decision.
5. Click **Yes** to delete the interface.

Ping a Node

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

1. Click the **Nodes** tab, and then select the node you want to ping.
2. On the **Nodes** menu, select **Ping Node**. The ping results appear in the screen.

Edit a Node

Existing nodes appear in the **Nodes** tab and can be edited. To edit a node:

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

Node Profile x

Please provide node properties.

Node Name:
Jay's Engineering Workstation

Description:
Jay's workstation in the lab. Corner desk by the double doors. Fedora Core 3

Interfaces

Type	Name	Status	Availability
Out-of-Band - KVM	Out-of-Band - KVM Interface	Up	Idle

Add Edit Delete

Default Interface
Out-of-Band - KVM Interf...

Node Associations

Category	Element
Department	Engineering
Location	
Market Area	
Memory	1 GB
ServerTypes	
System Type	Linux

OK Cancel

Figure 73 Edit Node Screen

- If you want, type a new name for the node in the **Node Name** field. All node names in CC-SG must be unique.
- (Optional) Type a new short description for this node under the **Description** field.
- Click **Add** in the **Interfaces** area to add a new interface. Please refer to the **Add Interface** section above for additional information on this procedure.
- Select an existing node in the **Interfaces** table, and then click **Edit** or **Delete** to edit or delete that interface from the node. Please refer to the **Edit an Interface** or **Delete an Interface** section above for additional information on this procedure.
- A list of **Categories** and **Elements** can be configured to better describe and organize this node. A category is a way to classify a node and an element is a specific value for that classification. For example, if the node represents a PC belonging to the engineering department, for a category called Department, one could select an element called Engineering.

To configure a **Categories** and **Elements** for the node:

- For each **Category** in the list you want to assign a value to double-click the **Element** field next to it. The field turns into a drop-down menu.
- Click the drop-down menu and select the desired **Element** value. Select **None** if you do not want to use this Category.

If you do not see the **Category** or **Element** values you desire, more can be added through the **Associations** menu. Please refer to **Chapter 4: Creating Associations** for additional information on creating Categories and Elements.

- Click **OK** when you are done configuring the node.

Delete a Node

Deleting a node will remove it from the Nodes List. The node will no longer be available for users to access and it will lose all of its previous interfaces and associations.

To delete a node:

- Click the **Nodes** tab to the left.

2. Right-click the node you want to delete and select **Delete Node**. The **Delete Node** screen appears displaying the name of the selected node.

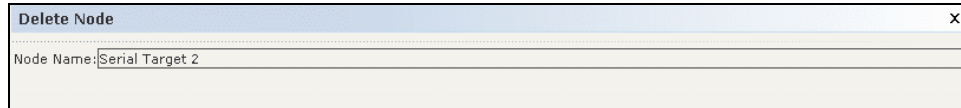


Figure 74 Deleting a Node

3. Click **OK** to delete the node or **Cancel** to exit without deleting.

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 will be able to chat with each other.

To engage in a chat session:

1. Click the **Nodes** tab to the left.
2. Right-click a node you are currently connected to and select **Chat**, then **Start Chat Session** if no session has been created yet. A Chat session will be created.

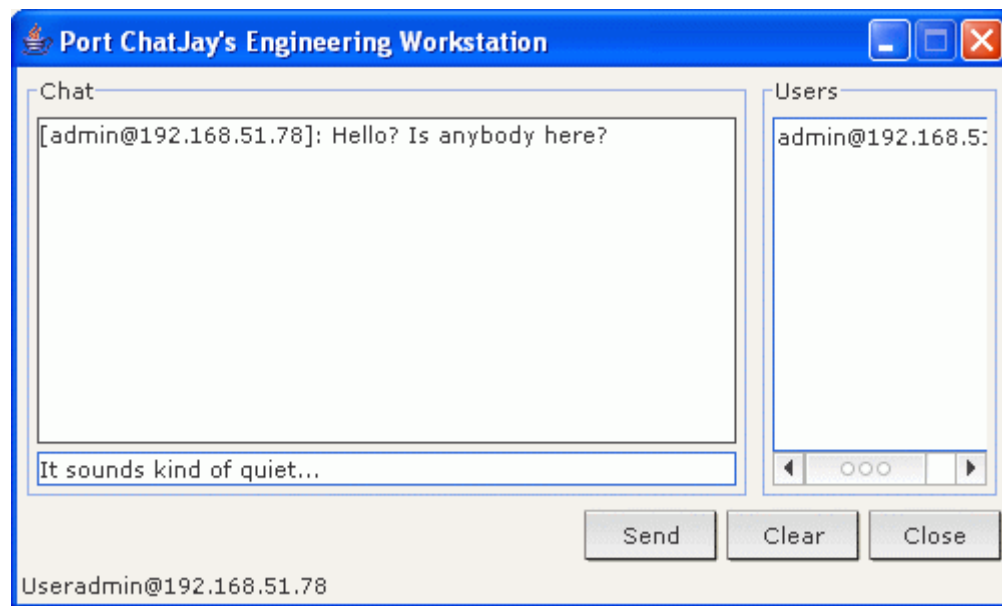


Figure 75 Chat Session for a Node

If a chat session is in progress, Right-click the node, select **Chat**, then **Show Chat Session** to join the chat session.

The chat session window will appear with the message fields on the left and a list of users in the chat session on the right.

3. Type a message in the new message (lower left) field and press the <Enter> key or click **Send**. The message will appear in the chat (upper left) field for all users to see.
4. Click **Clear** to clear any message you have typed in the new message field but have not sent. Clear will not clear the chat field.
5. Click the **Close** to leave or end the chat session.
6. You will be prompted if you want to close the chat session. Click **Yes** to close the chat session for all participants, click **No** to exit the chat session but leave it running for others.

You can also close a chat session for all participants from the nodes tab. Right-click the node with the chat session, select **Chat**, then **End Chat Session**.

Node Groups

Node groups allow administrators to create logical groups of nodes either arbitrarily or based on their Categories and Elements for use in creating access policies. Please refer to **Chapter 9: Policies** for details on creating node groups and applying policies to groups.

The **Node Groups** window is available from the Nodes tab by right-clicking and selecting **Node Groups**.

This page intentionally left blank.

Chapter 8: Adding and Managing Users and User Groups

Users make up the individual users and administrators that connect to CC-SG in order to access nodes and manage devices. **User Groups** are organizations that define a set of privileges for its member users; users by themselves have no privileges. In general, all users must belong to a user group.

CC-SG maintains its own centralized user list and user group list for authentication and authorization, described in this chapter. When using external authentication schemes (for example, RADIUS or Active Directory) users groups and policies still need to be created on CC-SG. Configuring CC-SG to use external authentication is covered in **Chapter 10: Remote Authentication**. Creating policies for access is covered in **Chapter 9: Policies**.

The Users Tree

Click the **Users Tab** to display the Users Tree.

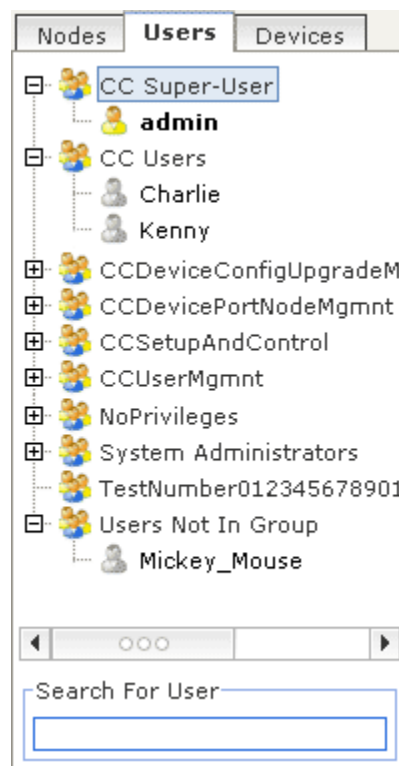


Figure 76 The Users Tree

The Users Tree displays all of the User Groups and Users in CC-SG. Users are nested underneath the User Groups they belong to. User Groups with users assigned to them appear in the list with a + symbol next to them. Click in the symbol will expand or hide their list of member users. Active users, those currently logged in to CC-SG appear in bold.

The Users Tree provides the ability to search for users within the tree. The method of searching can be configured through the **My Profile** screen described later in this chapter.

Special User Groups

CC-SG is configured with three user groups by default: **CC-Super User**, **System Administrators**, and **CC Users**.

CC Super-User Group

The **CC Super-User** group has full administrative and access privileges. Only one user can be a member of this group. The default username is **admin**. You can change the default username. You cannot delete the CC-Super User group. You cannot change the privileges assigned to the CC-Super User group, add members to it, or delete the only user from the group. Strong passwords are always enforced for the member of the CC-Super User group.

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.

Users Not in Group

Users Not In Group has no privileges and users cannot be created in or manually moved to this group. Users are assigned to this group if they are removed from all of their existing User Groups.

Important! Many commands in this chapter cannot be selected unless the appropriate User Group or User is first selected.

Many of the menu bar commands described in this section can be accessed by right-clicking a User Group or User and selecting a command from the shortcut menu that appears.

Add User Groups

Creating user groups first will help you organize users when they are added. When a user group is created, a set of privileges is assigned to the user group. Users that are assigned to that group will inherit those privileges. For example, if you create a group and assign it the **User Management** privilege, all users assigned to the group will be able to see and execute the commands on the **User Manager** menu. Please refer to **Appendix C: User Group Privileges** for additional information on what each privilege means.

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 describe what nodes the user group can access.

To create a new user group:

1. On the **Users** menu, select **User Group Manager**, then **Add User Group**. The **Add User Group** screen appears

Figure 77 Add User Groups Screen

2. Type a name for the user group in the **User Group Name** field. User Group names must be unique.
3. (Optional) Type a short description for the group in the **Description** field.
4. Click the **Privileges** tab.
5. Check the checkbox that corresponds to each privilege you want to assign to the user group.
6. Below the privileges table is the **Node Access** area with privileges for three kinds of node access: **Node Out of Band Access**, **Node In-Band Access**, and **Node Power Control**. Check the checkbox that corresponds to each type of node access you want to assign to the user group.

- Click the **Device/Node Policies** tab. A table of policies appears.

Add User Group

Choose usergroup properties to add.

User Group Name:
Sample Group

Description:

Privileges **Device/Node Policies** Active Directory Associations

Available Policies

Policy	Device Group	Node Group	Permission	Virtual Media	Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Allow No Ports		No Nodes	Control	Deny	00:00:...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Allow Yes Ports	All Devices	Yes Nodes	Control	Deny	00:00:...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add ▼ Delete ▲

Selected Policies

Policy	Device Group	Node Group	Permission	Virtual Media	Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Full Access ...	All Devices	All Nodes	Control	Read-Write	00:00:00 - ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power Policy	All Devices	Power Nodes	Control	Deny	00:00:00 - ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Apply Cancel

Figure 78 The Policies Tab on the Add User Group Screen

The **All Policies** table lists all the policies available on CC-SG. Each policy represents a rule allowing or denying access to a group of nodes. Please refer to **Chapter 9: Policies** for more information on policies and how they are created.

- 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 will allow or deny users access to the node (or devices) controlled by this policy.
- Repeat this step to add additional policies to the user group.
- If you want to simply allow this group to access all available nodes, select the **Full Access Policy** in the **Add Policies** list, 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**.
- When you are done configuring policies for this group, click **Apply** to save this group and create another, or click **OK** to save the user group without creating more. If you click **Apply**, repeat the steps in this section to add user groups.

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 and the **Users not in Group** group.*

To edit a group:

1. Click the **Users** tab to the left.
2. Click the user group in the **Users** tab. The **User Group Profile** appears.
3. (Optional) Type a new name for the user group in the **User Group Name** field.
4. (Optional) Type a new description for the user group in the **Description** field.
5. Click the **Privileges** tab.
6. Check the checkbox that corresponds to each privilege you want to assign to the user group. Uncheck a privilege to remove it from the group.
7. In the **Node Access** area, click the drop-down menu for each kind of interface you want this group to have access through and select **Control**.
8. Click the drop-down menu for each kind of interface you do not want this group to have access through and select **Deny**.
9. Click the **Policies** tab. Two tables of policies will appear.
10. For each policy you want to add to the group, select policy in the **All Policies**, then click **Add** to move the policy to the **Selected Policies** list. Policies in the **Selected Policies** list will allow or deny users access to the node (or devices) controlled by this policy.
11. For each policy you want to remove from the user group, select the policy name in the **Selected Policies** list, and then click **Remove**.
12. When you are done configuring policies for this group, click **OK** to save the changes to the group or **Cancel** to exit without saving.

Delete User Group

Deleting a User Group removes that group from CC-SG. Users in the deleted group will remain in any other groups to which they have been assigned. If the users in the deleted group were not in any other groups, they will be assigned to the Users Not in Group group, which does not have any privileges assigned to it.

To delete a User Group:

1. Click the **Users** tab to the left.
2. Click the user group you want to delete in the **Users** tab.
3. On the **Users** menu, select **User Group Manager**, then **Delete User Group**.

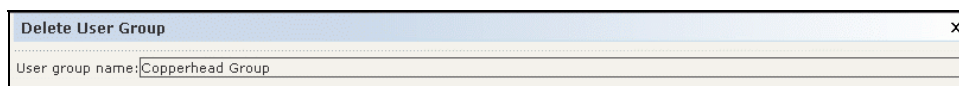


Figure 79 Deleting a User Group

4. Click **OK** to delete the User Group or **Cancel** to exit without deleting the group.
- After clicking OK, a status message will appear to confirm the successful deletion of the group.

Add User

Add users to a group to assign the user access privileges in CC-SG. A User's ability to access nodes or manage devices will depend on what User Group they are added to.

To add a user:

1. Click the **Users** tab to the left.
2. Click the user group you want to add the user to in the **Users** tab (you cannot add a user without selecting a group).
3. On the **Users** menu, select **User Manager**, then **Add User**.

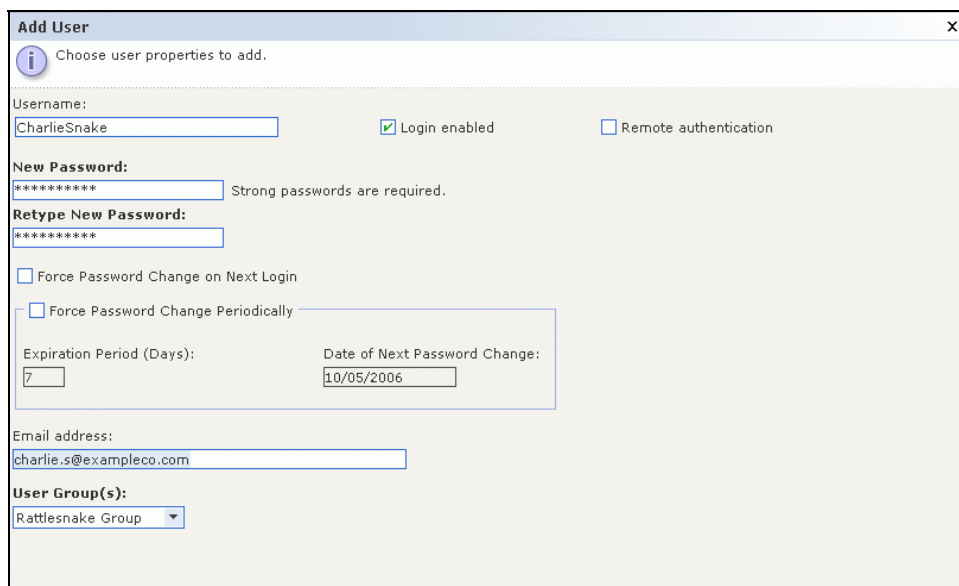


Figure 80 Adding a User

4. In the **Username** field, type the user name of the user you want to add. They will use this name to log in to CC-SG.
5. Check **Login Enabled** if you want the user to be able to log in to CC-SG.

6. Check **Remote Authentication** only if you want the user to be authenticated by an external server, such as TACACS+, RADIUS, LDAP, or AD. If you are using remote authentication, a password is not required and the **New Password** and **Retype New Password** fields will be disabled.
7. In the **New Password** and **Retype New Password** fields, type the password that the user will use to log in to CC-SG.

*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 display messages to assist with the password requirements. Please refer to **Chapter 13: Advanced Administration** for more information on strong passwords.*

8. Check **Force Password Change on Next Login** if you want to force the user to change the assigned password the next time they log in.
9. Check **Force Password Change Periodically** if you want to specify how often the user will be forced to change their password.
 - If checked, in the **Expiration Period (Days)** field, type the number of days that the user will be able to use the same password before being forced to change it.
10. In the **Email address** field, type the user's email address. This will be used to send the user notifications.
11. If you want to change the group you are adding this user to, click the **User Groups** drop-down menu and select a new group.
12. When you are done configuring this user, click **Apply** to add this user and create another one, or click **OK** to add the user without creating more. The users you create will appear in the **Users** tab, nested underneath the user groups to which they belong.

Edit a User

To edit a user:

1. Click the **Users** tab to the left.
2. Click the + symbol next to a User Group with the user you want to edit.
3. Click the user you want to edit. The **User Profile** appears.

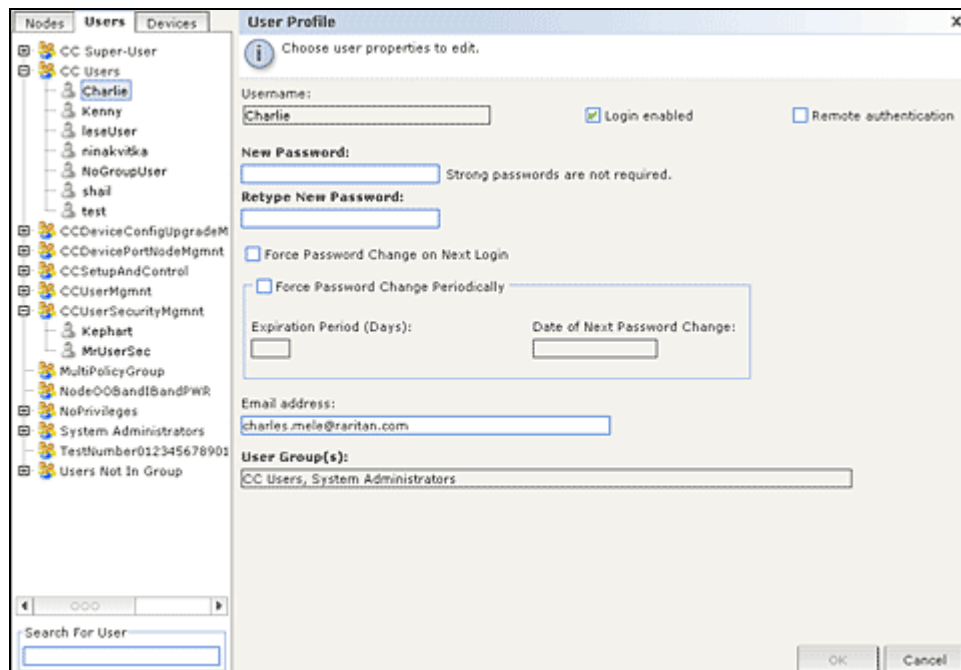


Figure 81 Editing a Selected User

4. Uncheck **Login enabled** if you want to prevent this user from logging in to CC-SG. Check **Login enabled** if you want to allow this user to log into CC-SG.
5. Check **Remote Authentication** only if you want the user to be authenticated by an external server, such as TACACS+, RADIUS, LDAP, or AD. If you are using remote authentication, a password is not required and the **New Password** and **Retype New Password** fields will be disabled.
6. In the **New Password** and **Retype New Password** fields, type a new password to change this user's password.

*Note: If Strong Passwords are enabled the password entered must conform to the established rules. The information bar at the top of the screen will assist with the password requirements. Please refer to **Chapter 13: Advanced Administration** for more information on Strong Passwords.*

7. Check **Force Password Change on Next Login** if you want to force the user to change the assigned password the next time they log in.
8. 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.
9. When you are done editing this user click **OK** to save the changes to the user or **Cancel** to exit without saving.

*Note: You cannot edit a user to change what group they belong to. Please refer to **Add User To Group** below for additional information.*

Delete User

Deleting a user completely removes the user from CC-SG. This is useful for removing accounts that are no longer needed.

To delete a user:

1. Click the **Users** tab to the left.
2. Click the + symbol next to a User Group with the user you want to delete.
3. Click the user you want to delete.
4. On the **Users** menu, select **User Manager**, then **Delete User**.

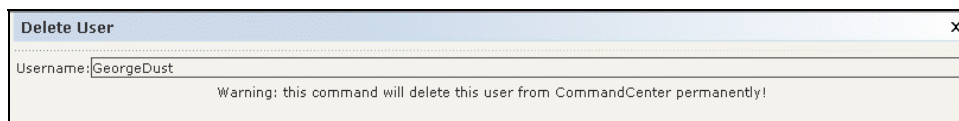


Figure 82 Deleting a User

5. Click **OK** to permanently delete the user from CC-SG, or click **Cancel** to exit without deleting the user.

*Note: This command delete all instances of a user, even if they exist in multiple user groups. Please refer to **Delete User From Group** below if you want to just remove the user from a group.*

Assign Users To Group

Use this command to assign an existing users to a group they currently do not belong to. Users assigned in this way will be added to their new group while still existing in any group they were previously assigned to. To move a user, use this command in conjunction with **Delete User From Group** described below.

To assign a user to a group:

1. Click the **Users** tab to the left.
2. Click the User Group you want to assign users to.
3. On the **Users** menu, select **User Group Manager**, then **Assign Users To Group**.

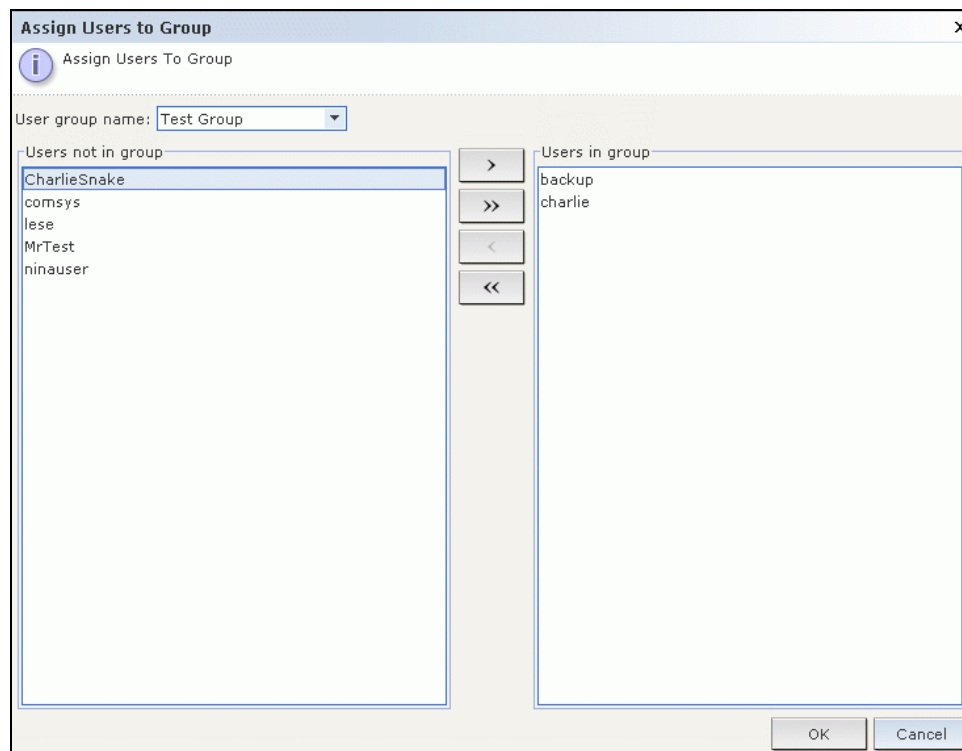


Figure 83 Add Users To Group Screen

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 column, and then click the > button to move them to the **Users in group** list.
5. Click the >> button to move all users not in the group to the **Users in group** list.
6. To remove people from the target group, select the users you want to remove in the **Users in group** list, and then click the < button.
7. Click the << button to remove all users from the **Users in group** list.
8. When all the users have been moved to the appropriate column, click **OK**. The users in the **Users in group** list will be added to the selected User Group.

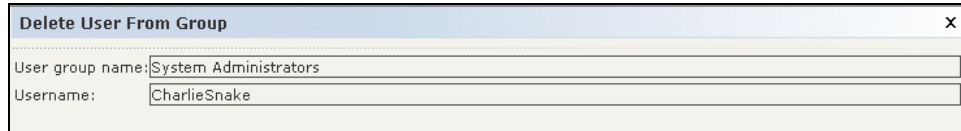
Delete Users From Group

This command removes a selected user from the group they are selected under. This command will not remove the user from any other groups and will not delete the user from CC-SG.

To delete a user from a group:

1. Click the **Users** tab to the left.
2. Click the + symbol next to a User Group you want to remove the user from.
3. Click the user you want to remove.

- On the **Users** menu, click **User Manager**, then **Delete User From Group**. The **Delete User** appears displaying the user and the group they will be removed from.



A dialog box titled "Delete User From Group" with a close button (X) in the top right corner. It contains two text input fields: "User group name:" with the value "System Administrators" and "Username:" with the value "CharlieSnake".

Figure 84 Deleting a User From A Group

- Click **OK** to delete the user from the group or click **Cancel** to exit without removing the user.

*Note: If you delete a user from a group and they do not belong to any other groups, the user will be added to **Users Not In Group** group.*

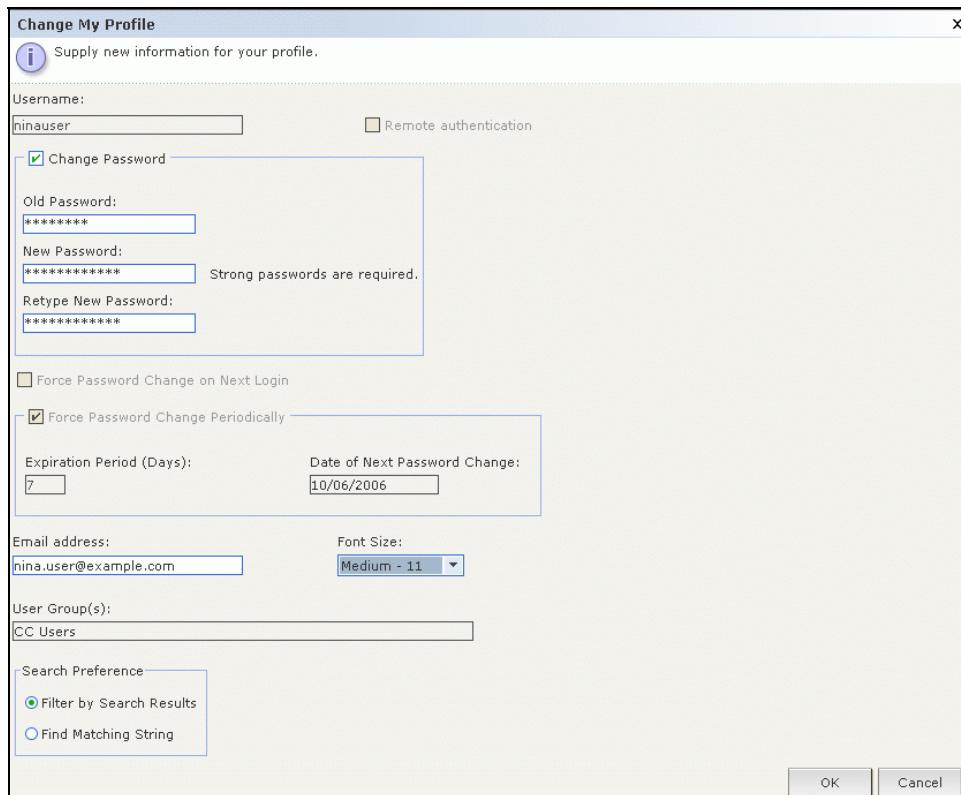
Other User and User Group Functions

My Profile

My Profile allows all users to view details about their account, change some details and customize usability settings. It is the only way for the **admin** account to change the account name.

To edit your profile:

- On the **Secure Gateway** menu, click **My Profile**. The **Change My Profile** screen appears, displaying details about your account.



A dialog box titled "Change My Profile" with a close button (X) in the top right corner. It contains an information icon and the text "Supply new information for your profile." Below this are several fields and checkboxes:

- Username:** A text input field containing "hinauser". To its right is a checkbox labeled "Remote authentication" which is unchecked.
- Change Password:** A checkbox that is checked. Below it are three password input fields: "Old Password:" (containing "*****"), "New Password:" (containing "*****"), and "Retype New Password:" (containing "*****"). To the right of the "New Password:" field is the text "Strong passwords are required."
- Force Password Change on Next Login:** An unchecked checkbox.
- Force Password Change Periodically:** A checked checkbox. Below it are two fields: "Expiration Period (Days):" (containing "7") and "Date of Next Password Change:" (containing "10/06/2006").
- Email address:** A text input field containing "hina.user@example.com". To its right is a "Font Size:" dropdown menu set to "Medium - 11".
- User Group(s):** A text input field containing "CC Users".
- Search Preference:** A section with two radio buttons: "Filter by Search Results" (which is selected) and "Find Matching String".

 At the bottom right are "OK" and "Cancel" buttons.

Figure 85 My Profile Screen

- If you are signed in on the **admin** account, you can type a new name in the **Username** field to change the name of your account.
- Check **Change Password** if you want to change your password.

- a. Type your current password in the **Old Password** field.
- b. Type your new password in the **New Password** field. A notice will appear if Strong Passwords are required.
- c. Type your new password again in the **Retype New Password** field.
4. Type a new address in the **Email address** field to add or change the address CC-SG will use to send you notifications.
5. Click the **Font Size** drop-down menu to adjust the font size the standard CC-SG client displays at.
6. 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**.
7. When you are done editing your profile click **OK** to save the changes or **Cancel** to exit without saving.

Logout Users

This command can be used to log active users out of CC-SG. It can also be used to log out all active users of a User Group.

To log out users:

1. Click the **Users** tab to the left.
2. Click the + symbol next to the User Groups with users you want to log out.
3. Click the user you want to log out. To log out multiple users, hold the **Shift** key, and then click additional users.
4. On the **Users** menu, select **User Manager**, then **Logout User(s)**. The **Logout Users** screen appears with the list of selected users.
5. Click **OK** to log the users out of CC-SG or **Cancel** to exit without logging the users out.

To log out all users of a User Group:

1. Click the **Users** tab to the left.
2. Click the User Group with users you want to log out. To log out multiple groups of users, hold the **Shift** key, and then click additional groups.
3. On the **Users** menu, select **User Group Manager**, then **Logout Users**. The **Logout Users** screen appears with a list of active users from the selected groups.
4. Click **OK** to log the users out of CC-SG or **Cancel** to exit without logging the users out.

Bulk Copy for Users

To save time, **Bulk Copy** can be used to clone one user's privileges and policies to a number of other existing users by moving them to the same User Groups as the selected user. To perform a Bulk Copy:

1. Click the **Users** tab to the left.
2. Click the + symbol next to a User Group with the user you want to copy.
3. Click the user you want to copy.
4. On the **Users** menu, select **User Manager**, then **Bulk Copy**.

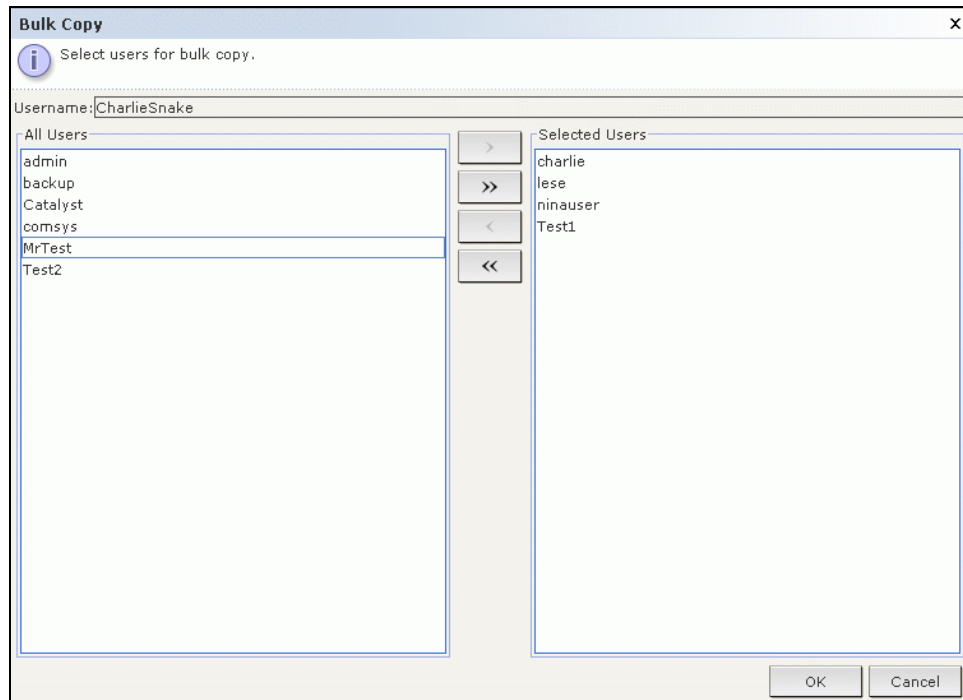


Figure 86 Bulk Copy Screen

5. In the **All Users** list select the users that will be adopting the privileges and policies of the user in the **Username** field.
6. Click the > button to move a user name to the **Selected Users** list.
7. Click the >> button to move all users into the **Selected Users** list.
8. To remove a user from the **Selected Users** list, select the user click the < button.
9. Click the << button to remove all users from the **Users in group** list.
10. Click **OK** to copy user properties. Copied users will be moved from their existing groups to the groups of which the selected user is a member.

Chapter 9: Policies and Node Groups

Controlling Access Using Policies

Configuring policies to provide user access to nodes is optional, but central to making effective use of CC-SG's ability to control access.

If you want to give all users access to all nodes, simply assign the **Full Access Policy** to all user groups. If you want to have more control over user access to nodes you will need to create policies to define rules for access. Like privileges, policies are assigned to user groups to apply those access rules to the users in the group.

If you completed **Guided Setup** (Please refer to **Chapter 3: Configuring CC-SG with Guided Setup**), a number of basic policies may already have been created. Now, you may want to apply these policies to existing user groups. If you have not used **Guided Setup** or created the desired policies you will want to follow the directions below. You will:

- Create Node Groups to organize the nodes you want to create access rules for.
- Create Device Groups if you want to create access rules for Raritan devices providing interfaces to nodes.
- Create a policy for a node or device specifying when access to that node or device can occur.
- Apply the policy to a user group.

Policy Summary

The following diagram is a visual representation of how to implement security with CC-SG:

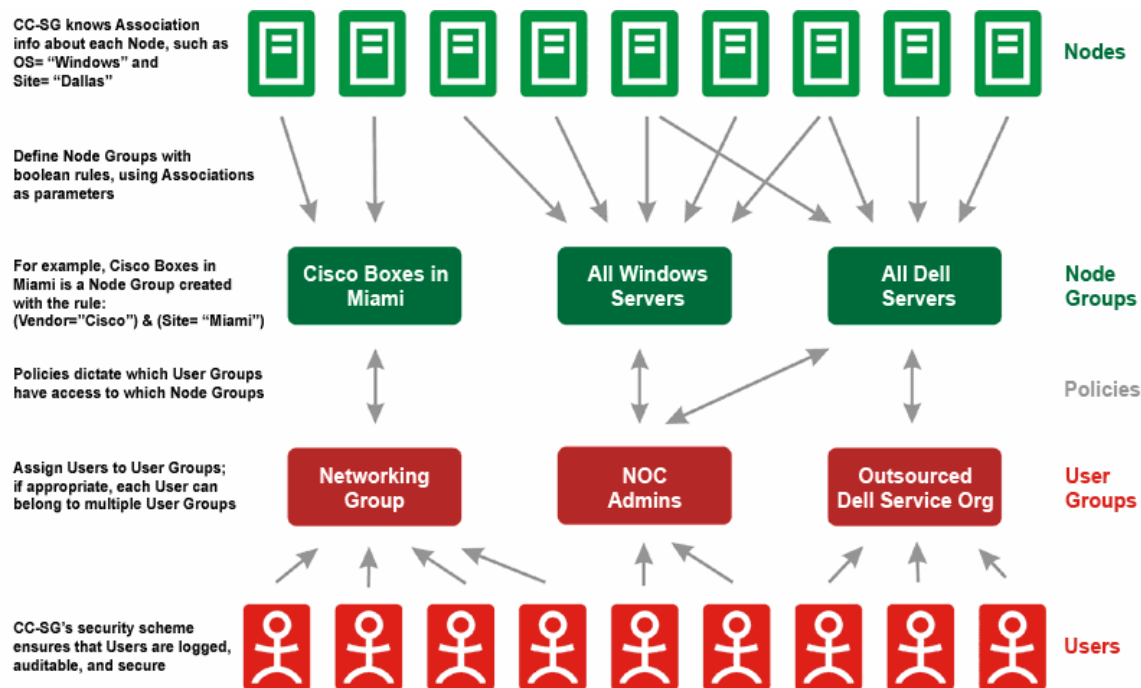


Figure 87 Policy Summary

Node Groups

Node groups are used to organize nodes into a set. This group will then become the basis for a policy either allowing or denying access to this particular set of nodes. Nodes can be grouped arbitrarily or by a set of common attributes.

If you used Guided Setup to create categories and elements for nodes, some means to organize nodes along common attributes have already been created. CC-SG automatically creates default access policies based on these elements. Please refer to **Chapter 4: Associations** for more details on creating categories and elements.

To view existing node groups:

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

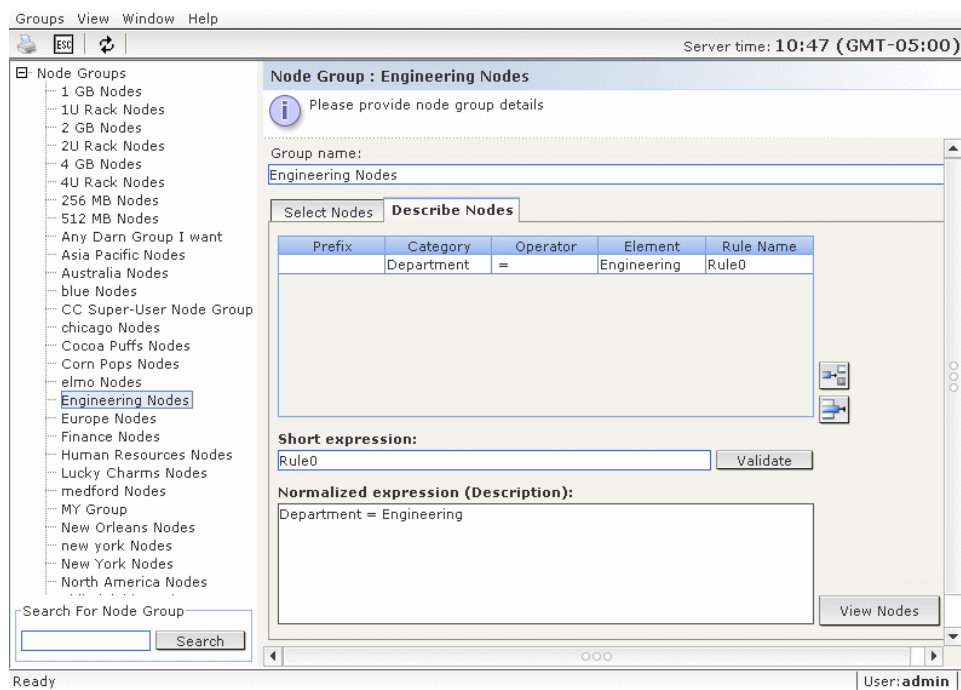


Figure 88 The Node Group Manager

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

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

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

2. To search for a node in the node group list, type a string in the **Search** field at the bottom of the list, and then click **Search**. The method of searching is configured through the **My Profile** screen. Please refer to **Chapter 8: Users and User Groups** for additional information.

3. 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 will appear displaying the nodes and all their attributes.

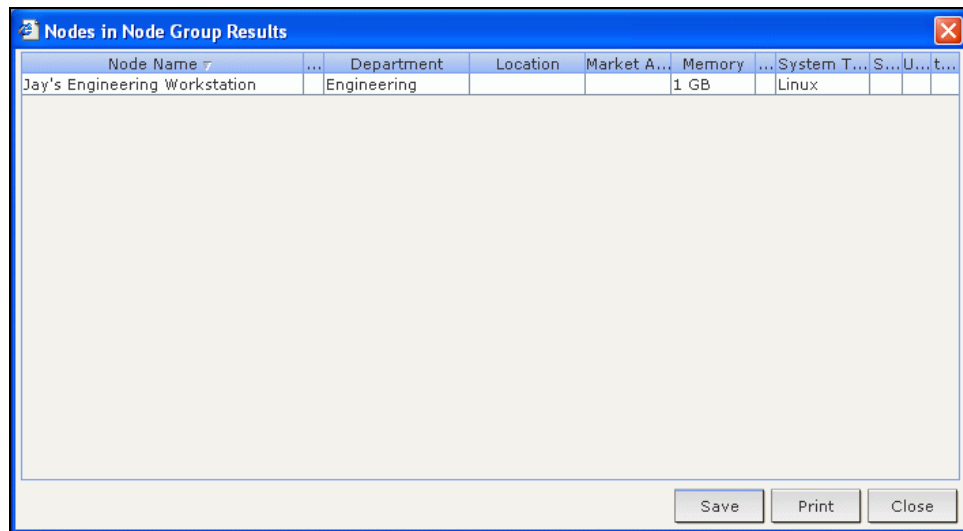


Figure 89 Nodes in a Group Based on Attributes

Add Node Groups

To add a new Node Group:

1. On the **Associations** menu, click **Node Group**. The **Node Groups Manager** window displays.
2. On the **Groups** menu, select **Add**. A template for a node group will appear.
3. In the **Group name** field, type a name for a node group you want to create.

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

Select Nodes

Node Group : New

Please provide node group details

Group name:
Lab Nodes

Select Nodes Describe Nodes

Nodes

Device name:
All

Available:

- Access Local Port Target
- CC-SSH
- IPR-32-59
- P2SC-32-60

Selected:

- Admin
- Jay's Engineering Workstation
- Serial Target 1
- Serial Target 2

Add > < Remove

Search for Node: Go

Search for Node: Go

☒ Create Full Access Policy for Group

Add Cancel

Figure 90 Adding Nodes Using Select Nodes

1. Click the **Select Nodes** tab.
2. Click the **Device Name** drop-down menu and select a device if you want to filter the **Available** list to only display nodes with interfaces from that device.
3. In the **Available** list, select the nodes you want to add to the group, and then click **Add** to move the node into the **Selected** list. Nodes in the **Selected** list will be added to the group.
4. If you want to remove a node from the group, select the node name in the **Selected** list, and then click **Remove**.
5. You can search for a node in either the **Available** or **Selected** list. Type the search terms in the field below the list, and then click **Go**
6. If you want to create a policy that allows access to the nodes in this group at any time, check **Create Full Access Policy For This Group**.
7. When you are done adding nodes to the group, click **Add** to create the node group. The group will be added to the list of Node Groups on the left.

Describe Nodes

Node Group : New

Please provide node group details

Group name:
Complex Group

Select Nodes **Describe Nodes**

Prefix	Category	Operator	Element	Rule Name
	Department	=	Engineering	Rule0
	Location	=	Philadelphia	Rule1
	Memory	=	1 GB	Rule2

Short expression:
{Rule0|Rule1}&Rule2 Validate

Normalized expression (Description):
((Department = Engineering OR Location = Philadelphia) AND Memory = 1 GB) View Nodes

☐ Create Full Access Policy for Group

Add Cancel

Figure 91 Describing a Node Group With Multiple Rules

1. Click the **Select Nodes** tab.
2. Click **Add New Row** to add a row in the table for a new rule. Rules take the form of an expression which can be compared against nodes.
3. Double-click each column in the row to turn the appropriate cell into a drop-down menu, then select the appropriate value for each component:
 - **Prefix** – Leave this blank or select **NOT**. If **NOT** is selected, this rule will filter for values opposite of the rest of the expression.
 - **Category** – Select an attribute that will be evaluated in the rule. All categories you created in the **Association Manager** will be available here. Also included are **Node Name** and **Interface**.
 - **Operator** – Select a comparison operation to be performed between the Category and Element items. Three operators are available: = (is equal to), **LIKE** (used for find the Element in a name) and <> (is not equal to).
 - **Element** – Select a value for the Category attribute to be compared against. Only elements associated with the selected category will display here (for example: if evaluating a “Department” category, “Location” elements will not appear here).
 - **Rule Name**- This is a name assigned to the rule in this row. You cannot edit these values. Use these values for writing descriptions in the **Short Expression** field.

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

4. If you want to add another rule, click **Add New Row** again, and make the necessary configurations. Configuring multiple rules will allow more precise descriptions by providing multiple criteria for evaluating nodes.
5. If you want to remove a rule, highlight the rule in the table, and then click **Remove Row**.
6. The table of rules only 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 simply type that rule's name in the field. If multiple rules are being evaluated, type the rules into the field using a set of logical operators to describe the rules in relation to each other:
 - **&** - the AND operator. A node must satisfy rules on both sides of this operator for the description (or that section of a description) to be evaluated as true.
 - **|** - the OR operator. A 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.

For example: If you simply want to describe nodes that belong to the engineering department, create a rule that says `Department = Engineering`, this will become Rule0. Then simply type Rule0 in the **Short Expression** field.

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

7. 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 will appear in the **Normalized Expression** field.
8. Click **View Nodes** to see what nodes satisfy this expression. A **Nodes in Node Group** window will appear 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.
9. If you know you want to create a policy that allows access to the nodes in this group at any time, check **Create Full Access Policy For This Group**.
10. 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 Node Group

Edit a node group to change the membership or description of the group. To edit a node group:

1. On the **Associations** menu, click **Node Group**. The **Node Groups Manager** window displays.
2. Click the node you want to edit in the Node Group List to the left. The details of that node will appear in the **Node Groups** window.
3. Refer to the instructions in the **Select Nodes** or **Describe Nodes** sections above for details on how to configure the node group.
4. Click **Edit** when you are done editing the Node Group.

Delete Node Group

1. On the **Associations** menu, click **Node Group**. The **Node Groups Manager** window displays.
2. Click the node you want to delete in the Node Group List to the left.
3. On the **Groups** menu, click **Delete**.

Device Groups

Device groups operate in a similar fashion to Node Groups, except that Device Groups are used to organize Raritan devices into sets for management by policies.

Please refer to [Chapter 5: Adding Devices and Device Groups, Device Group Manager](#) for additional information.

Policy Manager

Once your node groups and device groups have been created, they can become the basis for creating a policy—a rule that states whether users can or cannot access the nodes or devices in the group, and what times and days of the week the rule is in effect, and whether users have virtual media permissions to nodes connected to virtual media-enabled devices, such as KX II. Please refer to [Support for Virtual Media](#) for additional information.

Add Policy

To create a policy:

1. On the **Associations** menu, click **Policies**. The **Policy Manager** window displays.

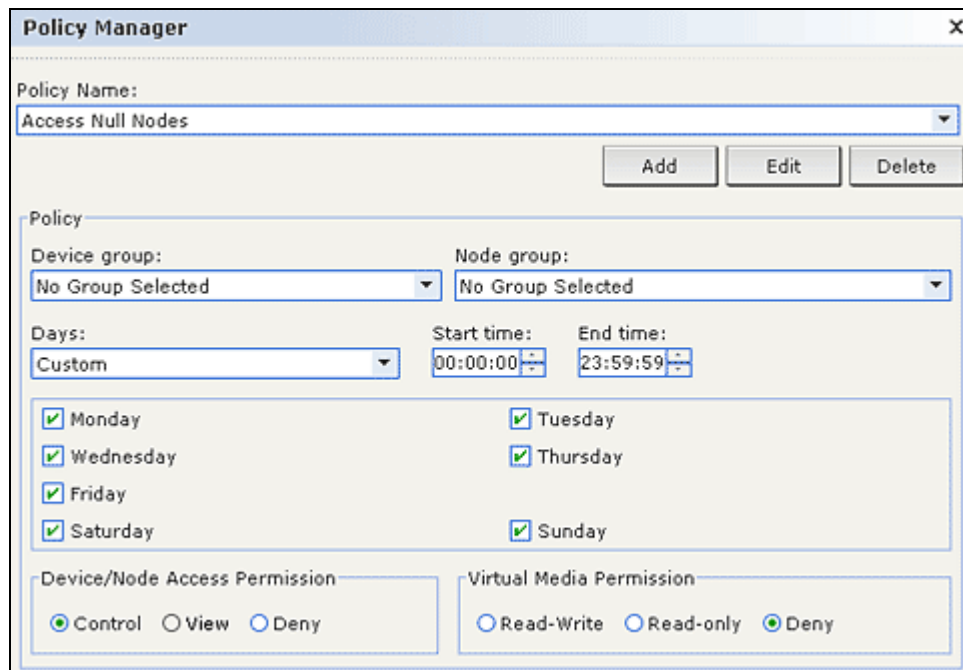


Figure 92 Policy Manager

2. Click **Add**. A dialog window appears requesting a name for the policy.

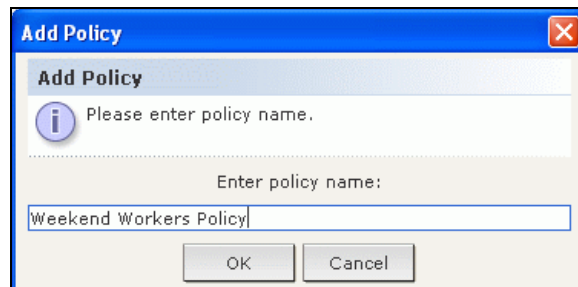


Figure 93 Adding a Policy

3. Type a name for the new policy in the **Enter policy name** field.
4. Click **OK**. The new policy will be added to the **Policy Name** list in the Policy Manager screen.
5. Click the **Device Group** drop-down arrow, and select the Device Group this policy governs access to.
Click the **Node Group** drop-down arrow and select the Node Group this policy governs access to.
If the policy will cover only one type of group, only select a value for that group.
6. 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).
 - a. Select **Custom** to select your own set of days. The individual day checkboxes will become enabled.
 - b. Check the checkbox that corresponds to each day you want this policy to cover.
7. In the **Start Time** field, type the time of day this policy goes into effect. The time must be in 24-Hour format.
8. In the **End Time** field, type the time of day this policy ends. The time must be in 24-Hour format.
9. 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.
10. 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
11. Click **Update** to add the new policy to CC-SG, and then click **Yes** in the confirmation message that appears.

*Note: 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.*

Edit a Policy

When you edit a policy, the changes do not affect users who are currently logged in to CC-SG. The changes will go into effect at the next login. If you need to make sure that your changes go into effect sooner, first enter Maintenance Mode, and then edit policies. When you enter Maintenance Mode, all current users are logged off of CC-SG until you exit Maintenance Mode, when users can login again. Please refer to [Chapter 12: System Maintenance, Maintenance Mode](#) for additional information.

To edit a policy:

1. On the **Associations** menu, click **Policies**. The **Policy Manager** window displays.
2. Click the **Policy Name** drop-down arrow, and then select the policy you want to edit from the list.
3. (Optional) To edit the name of the policy, click **Edit**. An **Edit Policy** window appears. Type a new name for the policy in the field, and then click **OK** to change the name of the policy.

4. Click the **Device Group** drop-down arrow, and select the Device Group this policy governs access to.
Click the **Node Group** drop-down arrow and select the Node Group this policy governs access to.
If the policy will cover only one type of group, only select a value for that type.
5. 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).
 - a. Select **Custom** to select your own set of days. The individual day checkboxes will become enabled.
 - b. Check the checkbox that corresponds to each day you want this policy to cover.
6. In the **Start Time** field, type the time of day this policy goes into effect. The time must be in 24-Hour format.
7. In the **End Time** field, type the time of day this policy ends. The time must be in 24-Hour format.
8. 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
9. Click **Update** to save the changes to the policy, and then click **Yes** in the confirmation message that appears.

Delete a Policy

To delete a policy:

1. On the **Associations** menu, click **Policies**. The **Policy Manager** window displays.
2. Click the **Policy Name** drop-down arrow, and then select the policy you want to delete from the list.
3. Click **Delete**, and then click **Yes** in the confirmation message that appears.

Support for Virtual Media

CC-SG provides remote virtual media support for nodes connected to virtual media-enabled KX II devices. For detailed instructions on accessing virtual media, please refer to the Dominion KX II User Guide. Please refer to [Policy Manager: Add a Policy](#) in this guide for instructions on creating policies to assign virtual media permission to user groups in CC-SG.

What is Virtual Media?

Virtual Media (VM) provides a method in which target servers can access remote media from the client and file servers. Virtual media emulates the function of a mass storage device *without physically being connected* to the target server. Media mounted on the client machine is accessible (i.e., essentially mounted *virtually*) by the target device. The target server then has access to the remote media and can read from and write to that media as if it were physically connected to the server. The media includes internal and USB-mounted CDs and DVD drives, USB mass storage devices, PC hard drive and remote drives, and ISO images (disk images).

Virtual Media provides the ability to perform most tasks remotely including: transferring files, running diagnostics, installing or patching applications, rebooting the target server across the network using a boot file accessed from the client, or even complete installation of the operating system. This expanded KVM control eliminates most trips into the data center, saves time and money, thus making Virtual Media a very powerful feature.

Applying Policies To User Groups

Policies must be assigned to a User Group before they take effect. Once a policy is assigned to a User Group, the members of the group will have their access governed by that policy. Please refer to **Chapter 8: Adding and Managing Users and User Groups** for additional information on assigning policies to a user group.

This page intentionally left blank.

Chapter 10: Configuring Remote Authentication

Authentication and Authorization (AA)

Users of CC-SG can be locally authenticated and authorized on the CC-SG or remotely authenticated using the following supported directory servers:

- Microsoft Active Directory (AD)
- Netscape's Lightweight Directory Access Protocol (LDAP)
- TACACS+
- RADIUS

Any number of remote RADIUS, TACACS+, and LDAP servers can be used for external authentication. For example, you could configure three AD servers, two iPlanet (LDAP) servers, and three RADIUS servers.

Only AD can be used for remote authorization of users.

Flow for Authentication

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

1. The user logs into CC-SG with the appropriate user name and password.
2. CC-SG connects to the external server and sends the user name and password.
3. User name and password are either accepted or rejected and sent back. If authentication is rejected, this results in a failed login attempt.
4. If authentication is successful, authorization is performed. CC-SG checks if the user name entered matches a group that has been created in CC-SG or imported from AD, and grants privileges per the assigned policy.

When remote authentication is disabled, both authentication and authorization are performed locally on CC-SG.

User Accounts

User Accounts must be added to the authentication server for remote authentication. Except when using AD for both authentication and authorization, all remote authentication servers require that users be created on CC-SG. The user's username on both the authentication server and on CC-SG must be the same, although the passwords may be different. The local CC-SG password is used only when remote authentication is disabled. Please refer to **Chapter 8: Adding and Managing Users and User Groups** for additional information on adding users who will be remotely authenticated.

***Note:** If remote authentication is used, users have to contact their Administrators to change their passwords on the remote server. Passwords cannot be changed on CC-SG for remotely authenticated users.*

Distinguished Names for LDAP and AD

Configuration of remotely authenticated users on LDAP or AD servers requires entering user names and searches in Distinguished Name format. The full DN format is described in [RFC2253](#). For the purposes of this document, you need to know how to enter Distinguished Names and in what order each component of the name should be listed.

Specifying a Distinguished Name for AD should follow this structure, but you do not have to specify both **common name** and **organization unit**:

common name (cn), organizational unit (ou), domain component (dc)

Specifying a DN for Netscape LDAP and eDirectory LDAP should follow this structure:

user id (uid), organizational unit (ou), organization (o)

Username

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.

Base DN

You also enter a Distinguished Name (DN) to specify where the search for users begins. Enter a DN in the **Base DN** field to specify an AD container in which the users can be found. For example, entering: **ou=DCAdmins,ou=IT,dc=xyz,dc=com** will search all users in the **DCAdmins** and **IT** organizational units under the **xyz.com** domain.

Specify Modules for Authentication and Authorization

Once you have added all the external servers as modules in CC-SG (see sections below for instructions on adding AD, LDAP, TACACS+, and RADIUS modules), you specify whether you want CC-SG to use each of them for either authentication, authorization, or both.

1. On the **Administration** menu, click **Security**. When the **Security Manager** screen appears, click the **General** tab. All configured external authentication and authorization servers display in the External AA Servers section.
2. For each server, check the **Authentication** checkbox if you want CC-SG to use the server for authentication of users.
3. For each server, check the **Authorization** checkbox if you want CC-SG to use the server for authorization of users. Only AD servers can be used for authorization.
4. Click **Update** to save your changes.

Establish Order of External AA Servers

In the **General** tab, you can set the order in which CC-SG will query the configured external AA servers. If the first checked option is unavailable, CC-SG will try the second, then the third, and so on, until it is successful.

1. On the **Administration** menu, click **Security**. When the **Security Manager** screen appears, click the **General** tab.

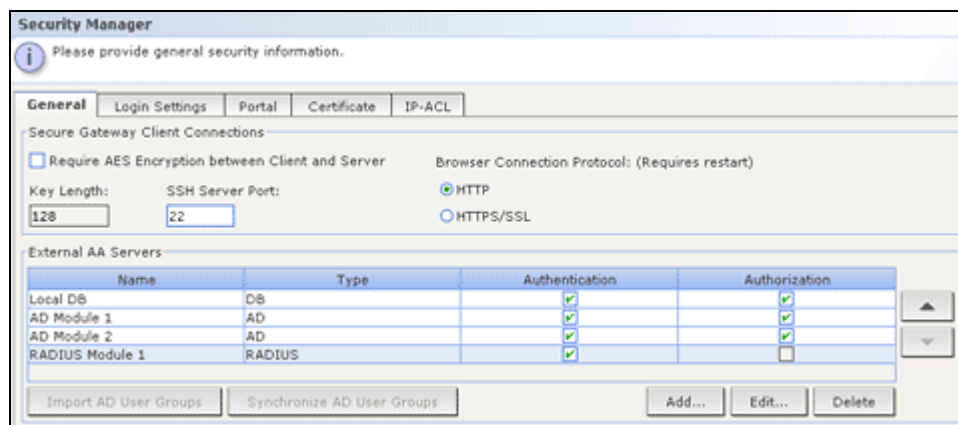


Figure 94 Security Manager General tab

2. The External AA Servers section lists all authentication and authorization options available in CC-SG. Select a name from the list, and then click the up and down arrows to prioritize the sequence of engagement.
3. Click **Update** to save your changes.

AD Configurations

Add AD Module to CC-SG

CC-SG supports authentication and authorization of users imported from an AD domain controller, without requiring that users be defined locally in CC-SG. This allows users to be maintained exclusively on the AD server. Once your AD server is configured as a module in CC-SG, CC-SG can query all domain controllers for a given domain. You can synchronize your AD modules in CC-SG with your AD servers to ensure that CCSG has the most current authorization information on your AD user groups.

Important: Create appropriate AD user groups and assign AD users to them before starting this process. Also, make sure that you have configured the CC-SG DNS and Domain Suffix in Configuration Manager. Please refer to [Chapter 13: Configuration Manager](#) for additional information.

To add an AD module to CC-SG:

1. On the **Administration** menu, click **Security**. The **Security Manager** screen appears, displaying the **General** tab.
2. Click **Add...** to open the Add Module window.

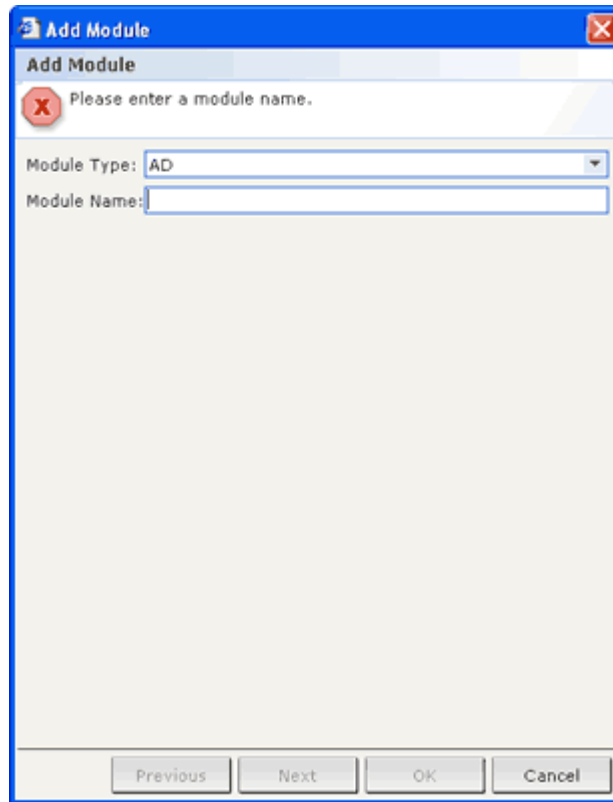
The image shows a Windows-style dialog box titled "Add Module". At the top, there is a red "X" icon and the text "Please enter a module name." Below this, there is a "Module Type:" label followed by a drop-down menu currently showing "AD". Underneath is a "Module Name:" label followed by an empty text input field. At the bottom of the dialog, there are four buttons: "Previous", "Next", "OK", and "Cancel".

Figure 95 Add Module

3. Click the **Module Type** drop-down menu and select AD from the list.
4. 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.
5. Click **Next** to proceed. The **General** tab opens.

AD General Settings

In the **General** tab, you add the information that allows CC-SG to query the AD server.

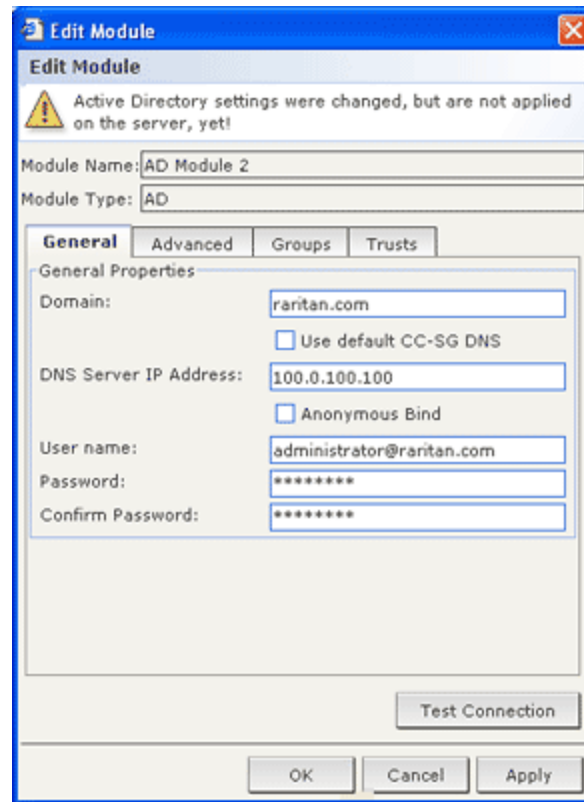


Figure 96 AD General Settings

1. Type the AD domain you want to query in the **Domain** field. For example, if the AD domain is installed in the xyz.com domain, type **xyz.com** in the **Domain** field. CC-SG and the AD server you want to query must be configured either on the same domain or on different domains that trust each other.

Note: CC-SG will query all known domain controllers for the domain specified.

2. Type the IP address of the DNS server in the **DNS Server IP Address** field. Or, check **Use default CC-SG DNS** checkbox to use the DNS configured in the Configuration Manager section of CC-SG. Please refer to [Chapter 13: Configuration Manager](#) for additional information.
3. Check **Anonymous Bind** if you want to connect to the AD server without specifying a username and password. If you use this option, ensure that the AD server allows anonymous queries.

Note: By default, Windows 2003 does NOT allow anonymous queries. Windows 2000 servers do allow certain anonymous operation whose query results are based on the permissions of each object.

4. If you are not using anonymous binding, type the username of the user account you want to use to query the AD server in the **User name** field. Use one of the following formats. The format required will depend on your AD version and configuration:

A user named User Name with a login name UserN in the raritan.com domain could be entered as:

- cn=UserName,cn=users,dc=Raritan,dc=com
- [UserName@raritan.com](#)
- Raritan/UserName

*Note: The user specified must have permission to execute search queries in the AD domain. For example, the user may belong to a group within AD that has **Group scope** set to **Global**, and **Group type** set to **Security**.*

5. Type the password for the user account you want to use to query the AD server in the **Password** and **Confirm Password** fields.
6. Click **Test Connection** to test the connection to the AD server using the given parameters. You should receive a confirmation of a successful connection. If you do not see a confirmation, review the settings carefully for errors and try again.
7. Click **Next** to proceed. The **Advanced** tab opens.

AD Advanced Settings

1. If you want to configure advanced settings, click the **Advanced** tab.

Figure 97 AD Advanced Settings

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 (step 3, below) you may need to change this port. The standard port for secure LDAP connections is **636**.
3. Check **Secure Connection for LDAP** if you want to use a secure channel for the connection. If checked, CC-SG uses LDAP over SSL to connect to AD. This option may not be supported by your AD configuration.
4. Specify a **Base DN** (directory level/entry) under which the authentication search query will be executed. CC-SG can do a recursive search downward from this Base DN.

EXAMPLE	DESCRIPTION
dc=raritan,dc=com	The search query for the user entry will be made over the whole directory

	structure.
cn=Administrators,cn=Users,dc=raritan,dc=com	The search query for the user entry will be performed only in the Administrators sub-directory (entry).

- Type a user's attributes in **Filter** so the search query will be restricted to only those entries that meet this criterion. The default filter is **objectclass=user**, which means that only entries of the type **user** are searched.
- Specify the way in which the search query will be performed for the user entry. If you check **Use Bind**, CC-SG attempts to connect, or **bind**, to AD directly with the username and password supplied in the applet. However, 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.
For example, if you have **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. Only check **Use Bind** when the user logging in from the applet has permissions to perform search queries in the AD server.
- Check **Use Bind After Search** to use the username and password you specified in the **General** tab to connect to the AD server. The entry is searched in the specified Base DN and is found if it meets the specified filtering criterion and if the attribute "samAccountName" is equal to the username entered in the applet. Then, a second connection, or **bind**, is attempted using the username and password supplied in the applet. This second bind assures that the user provided the correct password.
- 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.

- Click the **Groups** tab.

Add Module

Please provide module properties.

Module Name: AD Module 1

Module Type: AD

General Advanced **Groups** Trusts

Directory Search for Groups

Base DN: cn=users,dc=raritan,dc=com

Filter: (objectclass=group)

Test Connection

Previous Next OK Cancel

Figure 98 AD Group Settings

- Specify a **Base DN** (directory level/entry) under which the groups, containing the user to be authorized, will be searched.

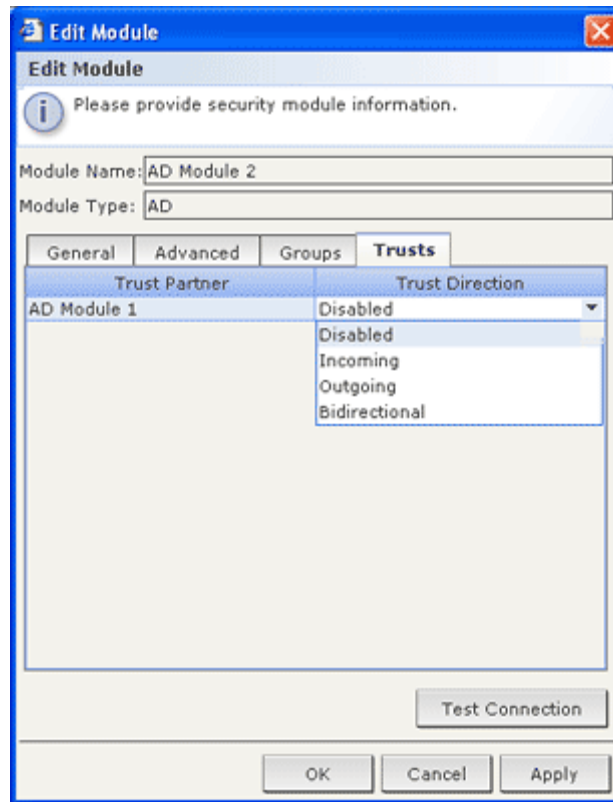
EXAMPLE	DESCRIPTION
dc=raritan,dc=com	The search query for the user in the group will be made over the whole directory structure.
cn=Administrators,cn=Users,dc=raritan,dc=com	The search query for the user in the group will be performed only in the Administrators sub-directory (entry).

- Type a user's attributes in **Filter** so the search query for the user in the group will be restricted to only those entries that meet this criterion. For example, if you specify **cn=Groups,dc=raritan,dc=com** as the Base DN and **(objectclass=group)** as the Filter, then all entries that are in the **Groups** entry and are of type **group** will be returned.
- 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.

- Click the **Trusts** tab. If you have configured more than one AD domain, all other domains are listed in the **Trusts** tab.

*Figure 99 AD Trust Settings*

2. For each domain in the **Trust Partner** column, click the **Trust Direction** drop-down menu, and then select the direction of trust you want to establish between the domains. Trust directions are updated in all AD modules when you make changes to one AD module.
 - **Incoming**: information will be trusted coming in from the domain. In the figure above, AD Module 2 would trust information coming in from AD Module 1
 - **Outgoing**: information will be trusted going to the selected domain. In the figure above, AD Module 1 would trust information coming in from AD Module2.
 - **Bidirectional**: information will be trusted in both directions from each domain.
 - **Disabled**: information will not be exchanged between the domains.
3. Click **Apply** to save your changes, and then click **OK** to save the AD module and exit the window.
4. The new AD module appears in the Security Manager screen, under External AA Servers. Check the **Authentication** checkbox if you want CC-SG to use the AD module for authentication of users. Check the **Authorization** checkbox if you want CC-SG to use the AD module for authorization of users.
5. Click **Update** to save your changes.

Edit AD Modules

Once you have configured AD modules, you can edit them at any time.

1. On the **Administration** menu, click **Security**.
2. Select the AD module you want edit, and then click **Edit**.
3. Click each tab in the Edit Module window to view the configured settings. Make changes as needed. Please refer to the previous sections on [AD General Settings](#), [AD Advanced Settings](#), [AD Group Settings](#), and [AD Trust Settings](#) for additional information.
4. 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.
5. Click **OK** to save your changes. You must synchronize the AD user groups you changed, or you can synchronize all AD modules to synchronize all groups and users in all modules. Please refer to [Synchronize AD User Groups](#) and [Synchronize All AD Modules](#) for additional information.

Import AD User Groups

You must specify Group settings in the AD module before you can import groups from the AD server. Please refer to **AD Group Settings** on page 119. After making a change to imported groups or users, you must synchronize the AD user groups you changed so that the imported groups are mapped to the appropriate groups on AD, and synchronize all AD modules to synchronize all groups and users in all modules. Please refer to [Synchronize AD User Groups](#) and [Synchronize All AD Modules](#) for additional information.

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. Please refer to [Chapter 13: Configuration Manager](#) for additional information.

1. On the **Administration** menu, click **Security**.
2. Select the AD module from which you want to import AD user groups.

- Click **Import 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.

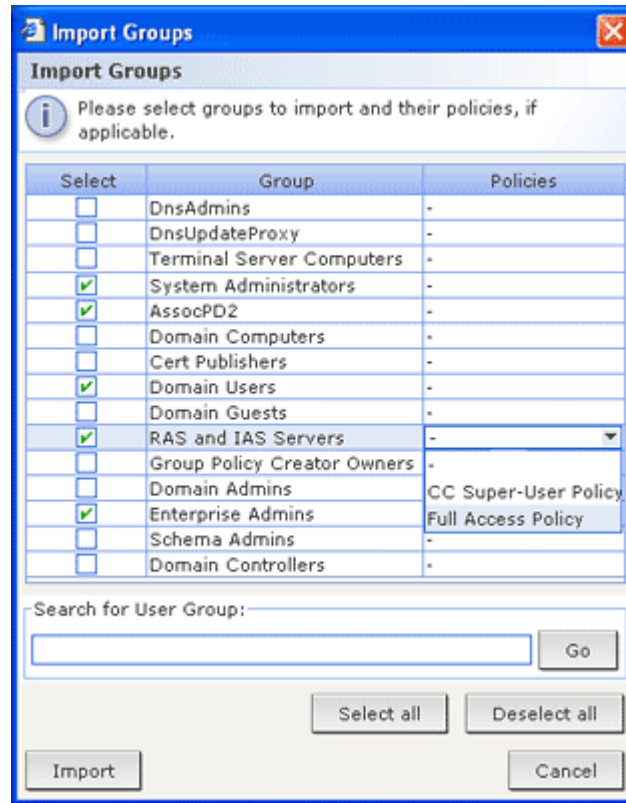


Figure 100 Importing Groups from AD Server

- Check the checkboxes next to the groups you want to import to CC-SG. Click a column header to sort the list of user groups by the information in that column. 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 **Select all** to select all user groups for import. Click **Deselect all** to deselect all selected user groups.
- In the **Policies** column, click the field and then select a CC-SG access policy from the list to assign the policy to the selected group. These policies should already be created, please refer to [Chapter 9: Policies and Node Groups](#) for additional information.
- Click **Import** to import the selected user groups.
- To check that the group was imported properly and to view the privileges of the group just imported, click the **Users** tab, then select the imported group to open the User Group Profile screen. Verify the information in the **Privileges** and **Device/Node Policies** tab. Click the **Active Directory Associations** tab to view information on the AD module associated with the user group.

Synchronize AD User Groups

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—it only maps the group names from AD to CC-SG.

If you have made changes to users or groups in AD, you should [synchronize all AD modules](#) to make sure CC-SG has the latest information. CC-SG synchronizes all AD modules once per day. Please refer to **Set AD Synchronization Time**, below, for additional information.

1. On the **Administration** menu, click **Security**.
2. Select the AD module whose user groups you want to synchronize with the AD server.

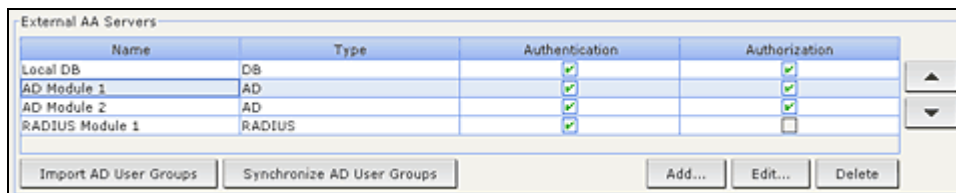


Figure 101 Synchronize AD User Groups

3. Click **Synchronize AD User Groups**.
4. A confirmation message will appear when all imported user groups in the selected module have been successfully synchronized.

Synchronize All AD Modules

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, and refreshes the CC-SG local cache. The CC-SG local cache contains all domain controllers for each domain, all user groups for all modules, and the user information for the known AD users. If user groups have been deleted from the AD modules, CC-SG removes them from its local cache as well. This ensures that CC-SG has the most current AD user group information.

You should synchronize all AD Modules whenever you add or delete a user in AD, or change user permissions in AD.

1. You must enter Maintenance Mode before you can synchronize all AD modules. All users will be logged off CC-SG while it is in Maintenance Mode. On the **System Maintenance** menu, click **Maintenance Mode**, and then click **Enter Maintenance Mode**.
2. In the Enter Maintenance Mode screen, type the message that will display to users who will be logged off CC-SG, and the number of minutes that should elapse before CC-SG enters maintenance mode in the corresponding fields, and then click **OK**.
3. Click **OK** in the confirmation dialog box.
4. A second confirmation message will display when CC-SG enters maintenance mode. Click **OK**.
5. Once CC-SG is in maintenance mode, on the **Administration** menu, click **Security**.
6. Click **Synchronize all AD Modules**.

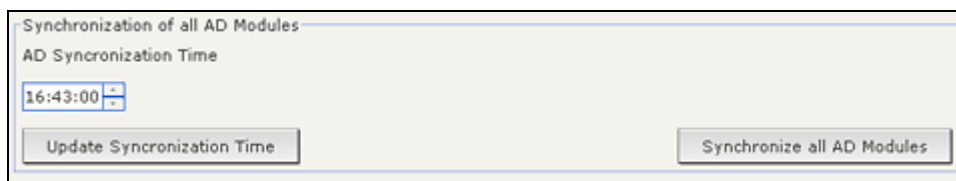


Figure 102 Synchronization of All AD Modules

7. A confirmation message will appear when all AD modules have been successfully synchronized.
8. To exit Maintenance Mode, on the **System Maintenance** menu, click **Maintenance Mode**, and then click **Exit Maintenance Mode**.
9. In the screen that appears, click **OK**. A second confirmation message will display when CC-SG exits maintenance mode. Click **OK**.

Set AD Synchronization Time

By default, CC-SG will synchronize all configured AD modules at 23:30 each day. You can change the time at which this automatic synchronization occurs.

1. On the **Administration** menu, click **Security**.
2. In the **AD 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.

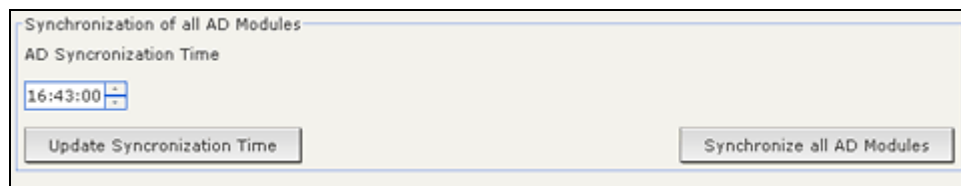


Figure 103 Synchronization of All AD Modules

3. Click **Update Synchronization Time** to save your changes.

AD Configuration—Upgrade from CC-SG 3.0.2

If you have upgraded CC-SG from 3.0.2 to 3.1, you must reconfigure your AD modules before any of your AD users can login to CC-SG. CC-SG 3.1 requires a DNS and Domain Name to be specified for each AD module. This configuration allows CC-SG to query all domain controllers for a given domain.

Important: CC-SG will still be in Maintenance Mode after upgrading to 3.1. Therefore, you must login with the CC Super-User account to perform this action. The default CC Super-User account for systems upgrading from 3.0.2 is ccroot/raritan0.

To reconfigure AD modules:

1. On the **Administration** menu, click **Security**.
2. Select the AD module you want edit, and then click **Edit**.
3. In the **General** tab, type the DNS and Domain Name for the AD module in the corresponding fields. Please refer to [AD General Settings](#) for additional information.
4. 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.
5. Click **OK** to save your changes.
6. If you want to configure Advanced settings, Group settings, or Trust settings, click the corresponding tab to view options. Please refer to the previous sections on [AD Advanced Settings](#), [AD Group Settings](#), and [AD Trust Settings](#) for additional information. Click **OK** to save your changes in these tabs.

7. Repeat these steps to reconfigure all AD modules.
8. Once you have reconfigured all AD modules, you can synchronize your imported AD user groups with the AD servers. Please refer to [Synchronize AD User Groups](#) for additional information.
9. After you have synchronized each modules AD user groups, you should synchronize all AD modules. Please refer to [Synchronize All AD Modules](#) for additional information. Depending on your AD configuration, the synchronization process may take up to 30 seconds per domain controller. If any domain controllers are offline during synchronization, the process may take longer.

Note: Please refer to the following sections to familiarize yourself with how CC-SG 3.1 handles synchronization of AD user groups: [Synchronize All AD Modules](#) and [Set AD Synchronization Time](#). For instructions on generating a report containing information about AD user groups, please refer to [Chapter 11: Generating Reports, AD User Group Report](#).

Add LDAP (Netscape) Module to 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.

1. On the **Administration** menu, click **Security**. The **Security Manager** screen appears, displaying the **General** tab.
2. Click **Add...** to open the Add Module window.

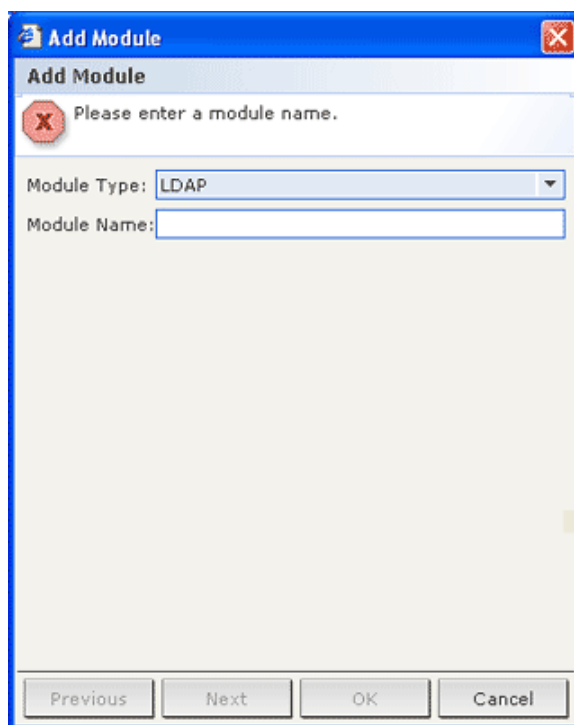


Figure 104 Add LDAP Module

3. Click the **Module Type** drop-down menu and select LDAP from the list.
4. Type a name for the LDAP server in the **Module name** field.
5. Click **Next** to proceed. The **General** tab opens.

LDAP General Settings

1. Click the **General** tab.

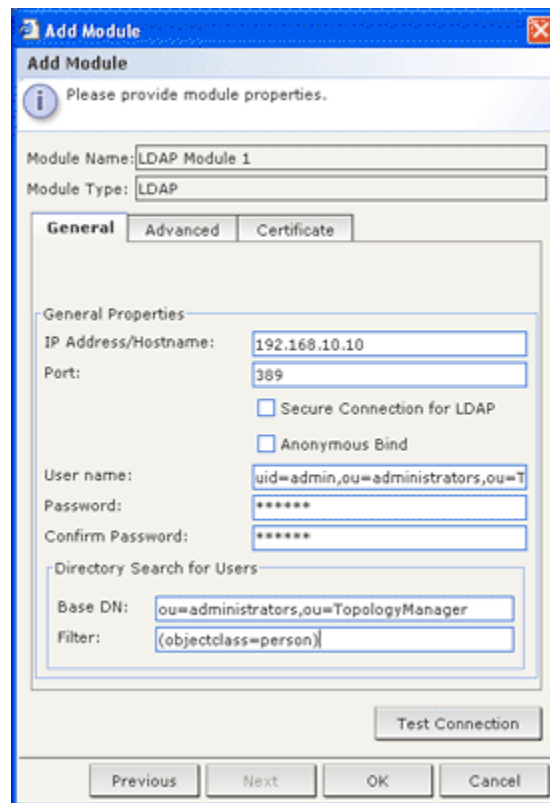


Figure 105 LDAP General Settings

2. Type the IP address or hostname of the LDAP server in the **IP Address/Hostname** field. For hostname rules, please refer to **Terminology/Acronyms** in **Chapter 1: Introduction**.
3. Type the port value in the **Port** field. The default port is 389.
4. Check **Secure Connection for LDAP** if using a secure LDAP server.
5. Check **Anonymous Bind** if your LDAP server allows anonymous queries. You do not need to enter a user name and password with anonymous binding.

***Note:** By default, Windows 2003 does NOT allow anonymous queries. Windows 2000 servers do allow certain anonymous operations, whose query results are based on the permissions of each object.*

6. If you are not using anonymous binding, type a username in the **User name** field. Type a Distinguished Name (DN) to specify the credentials used to query the LDAP server. For DN, enter the common name, organizational unit, and domain. For example, type **uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**. Separate the values with commas but do not use spaces before or after the comma. The value themselves can include spaces, such as **Command Center**.
7. Type the password in the **Password** and **Confirm Password** fields.
8. To specify where the search for users begins, enter a Distinguished Name in **Base DN**. For example, **ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**, searches all organizational units under the domain.
9. To narrow searching to only particular types of objects, type a value in the **Filter** field. For example, **(objectclass=person)** will narrow searching to only person objects.

10. Click **Test Connection** to test the LDAP server using the given parameters. You should receive a confirmation of a successful connection. If not, review the settings carefully for errors and try again.
11. Click **Next** to proceed to the **Advanced** tab to set advanced configuration options for the LDAP server.

LDAP Advanced Settings

1. Click the **Advanced** tab.

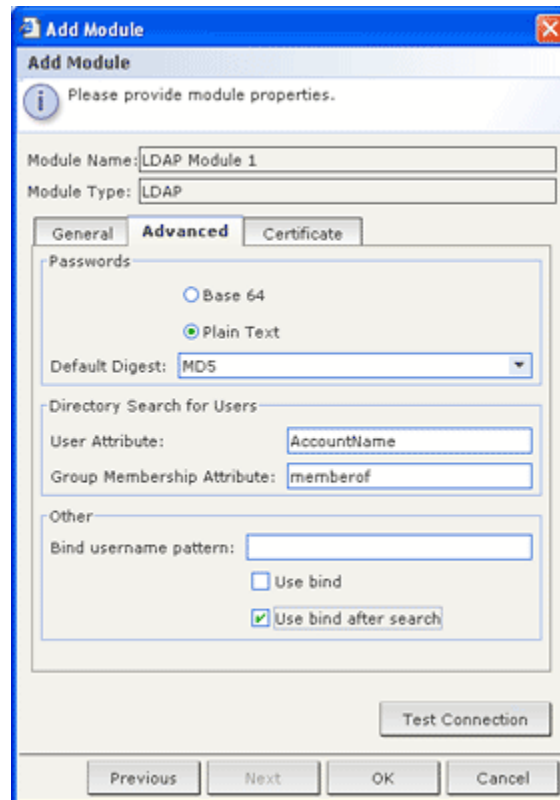
The screenshot shows the 'Add Module' dialog box with the 'Advanced' tab selected. The 'Module Name' is 'LDAP Module 1' and the 'Module Type' is 'LDAP'. Under the 'Passwords' section, 'Base 64' is selected with a radio button, and 'Plain Text' is also selected with a radio button. The 'Default Digest' is set to 'MD5' in a dropdown menu. Under 'Directory Search for Users', the 'User Attribute' is 'AccountName' and the 'Group Membership Attribute' is 'memberof'. Under the 'Other' section, the 'Bind username pattern' is empty, and the 'Use bind' checkbox is unchecked, while the 'Use bind after search' checkbox is checked. At the bottom right is a 'Test Connection' button, and at the bottom are 'Previous', 'Next', 'OK', and 'Cancel' buttons.

Figure 106 LDAP Advanced Settings

2. Click the radio button for **Base 64** if you want the password to be sent to the LDAP server with encryption. Click the radio button for **Plain Text** if you want the password to be sent to the LDAP server as plain text.
3. Click the **Default Digest** drop-down menu and 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.
6. 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.
7. On some LDAP servers, the password cannot be retrieved as part of the LDAP object. Check **Use bind after search** to instruct CC-SG to bind the password to the LDAP object again and send it back to the server for authentication.
8. Click **OK** to save your changes.

9. The new LDAP module appears in the Security Manager screen, under External AA Servers. Check the **Authentication** checkbox if you want CC-SG to use the LDAP module for authentication of users.
10. Click **Update** to save your changes.

Sun One LDAP (iPlanet) Configuration Settings

If using a Sun One LDAP server for remote authentication, use this example for parameter settings:

PARAMETER NAME	SUN ONE LDAP PARAMETERS
IP Address/Hostname	<Directory Server IP Address>
User Name	CN=<Valid user id>
Password	<Password>
BaseDN	O=<Organization>
Filter	(objectclass=person)
Passwords (Advanced Screen)	Plain Text
Password Default Digest (Advanced)	SHA
Use Bind	unchecked
Use Bind After Search	Checked

OpenLDAP (eDirectory) Configuration Settings

If using an OpenLDAP server for remote authentication, use this example:

PARAMETER NAME	OPEN LDAP PARAMETERS
IP Address/Hostname	<Directory Server IP Address>
User Name	CN=<Valid user id>, O=<Organization>
Password	<Password>
User Base	O=accounts, O=<Organization>
User Filter	(objectclass=person)
Passwords (Advanced screen)	Base64
Password Default Digest (Advanced)	Crypt
Use Bind	Unchecked
Use Bind After Search	Checked

Add a TACACS+ Module

CC-SG users who are remotely authenticated by a TACACS+ server need to be created on the TACACS+ server and on CC-SG. The user name on the TACACS+ server and on CC-SG must be the same, although the passwords may be different. Please refer to **Chapter 8: Adding and Managing Users and User Groups** for additional information on adding users who will be remotely authenticated.

1. On the **Administration** menu, click **Security**. The **Security Manager** screen appears, displaying the **General** tab.
2. Click **Add...** to open the Add Module window.

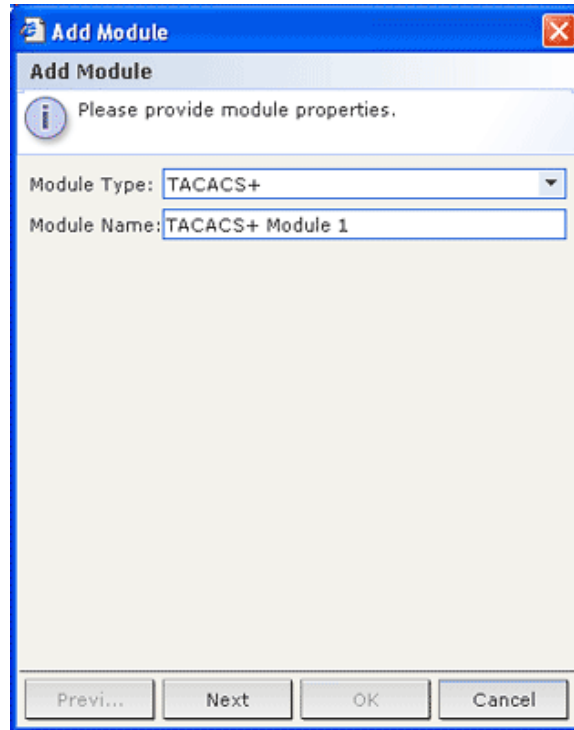
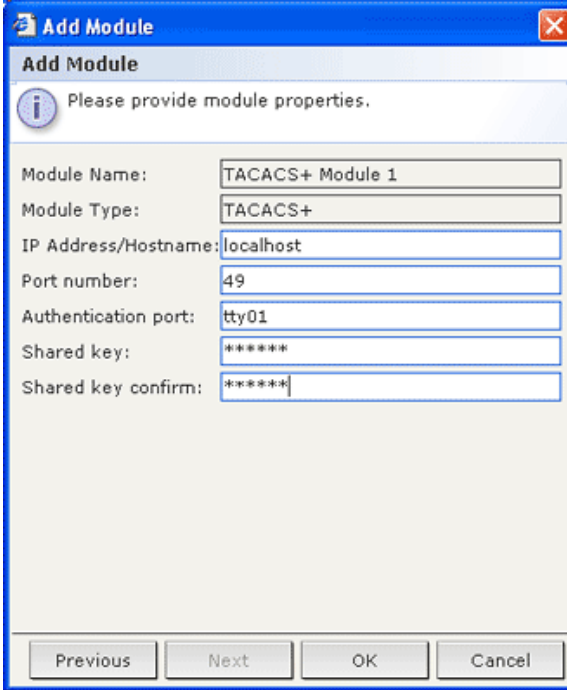


Figure 107 Add TACACS+ Module

3. Click the **Module Type** drop-down menu and select TACACS+ from the list.
4. Type a name for the TACACS+ server in the **Module name** field.
5. Click **Next** to proceed. The **General** tab opens.

TACACS+ General Settings

1. Type the IP address or hostname of the TACACS+ server in the **IP Address/Hostname Name** field. For hostname rules, please refer to Terminology/Acronyms in Chapter 1: Introduction



The screenshot shows a Windows-style dialog box titled "Add Module". Inside, there is a message icon and the text "Please provide module properties." Below this, there are several input fields: "Module Name:" with the value "TACACS+ Module 1", "Module Type:" with the value "TACACS+", "IP Address/Hostname:" with the value "localhost", "Port number:" with the value "49", "Authentication port:" with the value "tty01", "Shared key:" with the value "*****", and "Shared key confirm:" with the value "*****". At the bottom of the dialog, there are four buttons: "Previous", "Next", "OK", and "Cancel".

Figure 108 TACACS+ General Settings

2. Type the port number on which the TACACS+ server is listening in the **Port Number** field. The default port number is **49**.
3. Type the authentication port in the **Authentication Port** field.
4. Type the shared key in the **Shared Key** and **Shared key confirm** fields.
5. Click **OK** to save the changes.
6. The new TACACS+ module appears in the Security Manager screen, under External AA Servers. Check the **Authentication** checkbox if you want CC-SG to use the TACACS+ module for authentication of users.
7. Click **Update** to save your changes.

Add a RADIUS Module

CC-SG users who are remotely authenticated by a RADIUS server need to be created on the RADIUS server and on CC-SG. The user name on the RADIUS server and on CC-SG must be the same, although the passwords may be different. Please refer to **Chapter 8: Adding and Managing Users and User Groups** for additional information on adding users who will be remotely authenticated.

1. On the **Administration** menu, click **Security**. The **Security Manager** screen appears, displaying the **General** tab.
2. Click **Add...** to open the Add Module window.

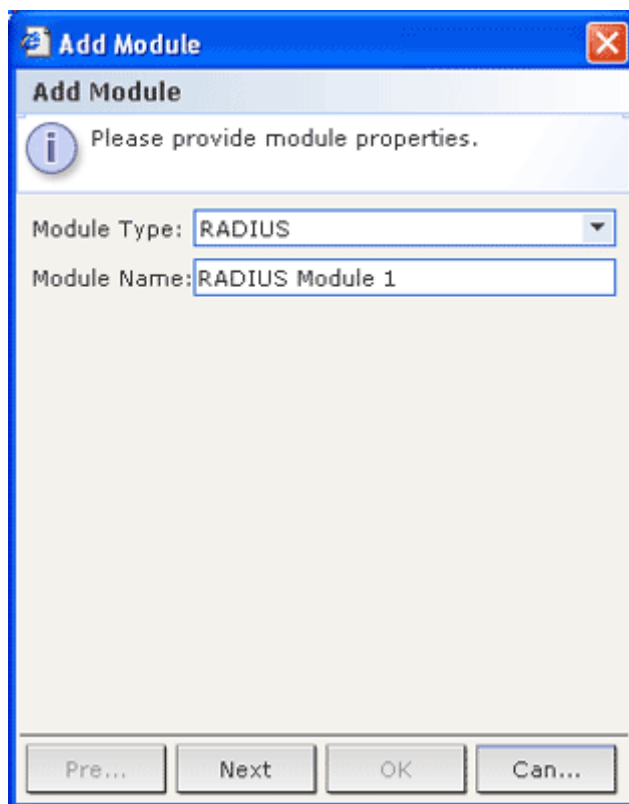
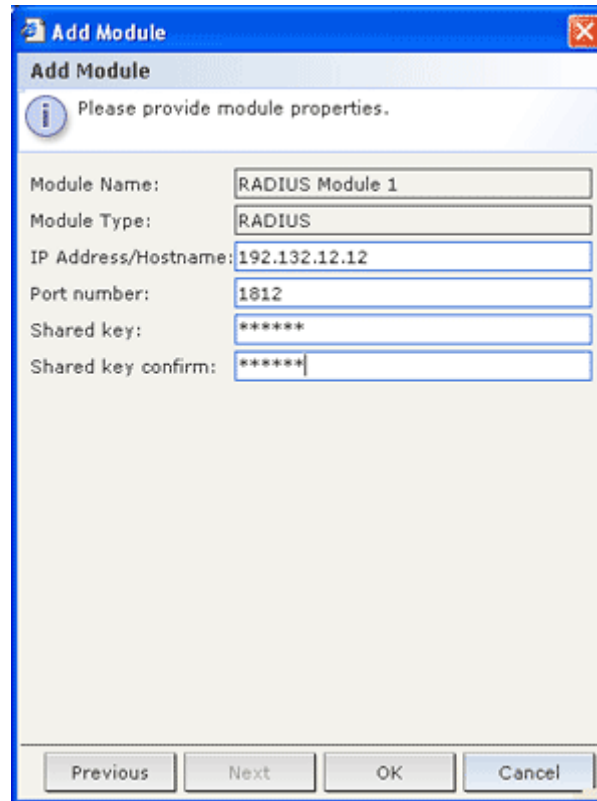


Figure 109 Security Manager Add Module Screen

3. Click the **Module Type** drop-down menu and select RADIUS from the list.
4. Type a name for the RADIUS server in the **Module name** field.
5. Click **Next** to proceed. The **General** tab opens.

RADIUS General Settings

1. Click the **General** tab.



The screenshot shows a Windows-style dialog box titled "Add Module". Inside, there is a message icon and the text "Please provide module properties." Below this, there are several input fields: "Module Name:" with the text "RADIUS Module 1", "Module Type:" with the text "RADIUS", "IP Address/Hostname:" with the text "192.132.12.12", "Port number:" with the text "1812", "Shared key:" with masked text "*****", and "Shared key confirm:" with masked text "*****". At the bottom of the dialog, there are four buttons: "Previous", "Next", "OK", and "Cancel".

Figure 110 Specifying a RADIUS Server

2. Type the IP address or hostname of the RADIUS server in the **IP Address/Hostname** field. For hostname rules, please refer to **Terminology/Acronyms** in **Chapter 1: Introduction**.
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 the changes.
7. The new RADIUS module appears in the Security Manager screen, under External AA Servers. Check the **Authentication** checkbox if you want CC-SG to use the RADIUS module for authentication of users.
8. Click **Update** to save your changes.

Two-Factor Authentication Using RADIUS

By using an RSA RADIUS Server that supports two-factor authentication in conjunction with an RSA Authentication Manager, CC-SG can make use of two-factor authentication schemes with dynamic tokens.

In such an environment, the user logs into CC-SG by first typing their username in the **Username** field. Then the user types their fixed password, followed by the dynamic token value in the **Password** field.

Configuration of the RADIUS server and Authentication manager to enable this is beyond the scope of this document to provide. Configuration of CC-SG is identical to standard RADIUS remote authentication described above. CC-SG should be configured to point at the RADIUS server. Please refer to **Appendix F: Two-Factor Authentication** for additional information.

This page intentionally left blank.

Chapter 11: Generating Reports

Reports can be sorted by clicking on the column headers. 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.

You can resize the column width in all reports. Hold your mouse pointer on the column divider in the header row until the pointer becomes a double-headed arrow. Click and drag the arrow to the left or right to adjust column width.

The sorting value and column width you use becomes the default report view the next time you log in and run CC-SG reports. For all reports, you can double-click a row to view further details of the report.

Note: In all reports, use CTRL+click to deselect a highlighted row.

Audit Trail Report

The **Audit Trail** report displays audit logs and access in CC-SG. It captures actions such as adding, editing, or deleting devices or ports, and other modifications.

CC-SG maintains an Audit Trail of the following events:

- When CC-SG is launched
- When CC-SG is stopped
- When a user logs on CC-SG
- When a user logs off CC-SG
- When a user starts a node connection

1. On the **Reports** menu, click **Audit Trail**.

Figure 111 Audit Trail Screen

2. Set the date range for the report in the **Start Date** and **End Date** fields. Click each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number.
3. You can limit the data that the report will contain by entering additional parameters in the **Message**, **Username**, and **User IP address** fields.
 - If you want to limit the report by the message text associated with an activity, type the text in the **Message** field.
 - If you want to limit the report to a particular user's activities, type the user's username in the **Username** field.
 - If you want to limit the report to a particular IP address's activities, type the user's IP address in the **User IP address** field.

- Click **OK** to run the report. The report is generated, displaying data about activities that occurred during the designated time period that also comply with any additional parameters specified.

No.	Date	User	User IP Address	Message
1	2007.10.24 at 16:32:42 EDT	admin	192.168.50.72	Audit Trail Report generated from Thu Aug 25 ...
2	2007.10.24 at 16:30:01 EDT	admin	192.168.50.72	Audit Trail Report generated from Tue Oct 25 ...
3	2007.10.24 at 16:16:21 EDT	admin	192.168.50.72	User admin with IP address 192.168.50.72 trie...
4	2007.10.24 at 16:00:40 EDT	admin	192.168.50.72	User admin with IP address 192.168.50.72 log...
5	2007.10.24 at 16:00:40 EDT	admin	192.168.50.72	User admin with IP address 192.168.50.72 log...
6	2007.10.24 at 15:33:40 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 lo...
7	2007.10.24 at 15:33:40 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 lo...
8	2007.10.24 at 15:33:40 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 lo...
9	2007.10.24 at 15:33:40 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 lo...
10	2007.10.24 at 15:28:58 EDT	admin	192.168.50.72	ViewStored Reports report generated
11	2007.10.24 at 15:28:38 EDT	admin	192.168.50.72	User admin with IP address 192.168.50.72 trie...
12	2007.10.24 at 15:03:31 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 tri...
13	2007.10.24 at 14:47:11 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 tri...
14	2007.10.24 at 11:43:51 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 lo...
15	2007.10.24 at 11:43:10 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 lo...
16	2007.10.24 at 11:19:10 EDT	admin	192.168.50.72	User admin with IP address 192.168.50.72 log...
17	2007.10.24 at 11:17:29 EDT	admin	192.168.50.72	Tasks retrieved by filter.
18	2007.10.24 at 11:13:47 EDT	admin	192.168.50.176	User admin with IP address 192.168.50.176 tri...
19	2007.10.24 at 11:11:46 EDT	admin	192.168.50.176	Accessed Devices Report generated
20	2007.10.24 at 11:11:46 EDT	admin	192.168.50.176	Error Log Report generated from Wed Oct 24 ...
21	2007.10.24 at 11:11:25 EDT	admin	192.168.50.176	Audit Trail Report generated from Wed Oct 24 ...
22	2007.10.24 at 11:10:45 EDT	admin	192.168.50.176	Accessed Devices Report generated
23	2007.10.24 at 11:08:03 EDT	admin	192.168.50.176	Accessed Devices Report generated

Figure 112 Audit Trail Report

- Click **Next** or **Previous** to navigate through the pages of the report.
- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Clear** to clear the log files used in the report.
- Click **Close** to close the report.

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.

- On the **Reports** menu, click **Error Log**.

Figure 113 Error Log Screen

- Set the date range for the report in the **Start Date** and **End Date** fields. Click each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number.
- You can limit the data that the report will contain by entering additional parameters in the **Message**, **Username**, and **User IP address** fields.
 - If you want to limit the report by the message text associated with an activity, type the text in the **Message** field.
 - If you want to limit the report to a particular user's activities, type the user's username in the **Username** field.

- If you want to limit the report to a particular IP address's activities, type the user's IP address in the **User IP address** field.
4. Click **OK** to run the report. The report is generated, displaying data about activities that occurred during the designated time period that also comply with any additional parameters specified.

No.	Date	User	User IP Address	Message
1	2006.10.18 at 16:07:50...		192.168.51.86	User admin with IP address 192.168.51.86 tried to ...
2	2006.10.18 at 15:36:28...		24.84.14.92	User comsys with IP address 24.84.14.92 tried to l...
3	2006.10.18 at 15:35:48...		24.84.14.92	User comsys with IP address 24.84.14.92 tried to l...
4	2006.10.18 at 12:18:24...		192.168.50.176	User admin with IP address 192.168.50.176 tried t...
5	2006.10.17 at 19:15:25...		24.84.14.92	User Comsys with IP address 24.84.14.92 tried to l...
6	2006.10.17 at 14:07:46...		192.168.58.52	User admin with IP address 192.168.58.52 tried to ...
7	2006.10.17 at 14:07:26...		192.168.58.52	User admin with IP address 192.168.58.52 tried to ...
8	2006.10.17 at 09:38:10...		192.168.50.62	User admin with IP address 192.168.50.62 tried to ...
9	2006.10.17 at 09:36:50...		192.168.50.90	User admin with IP address 192.168.50.90 tried to ...
10	2006.10.17 at 09:36:30...		192.168.50.90	User admin with IP address 192.168.50.90 tried to ...
11	2006.10.17 at 09:28:30...		192.168.51.21	User admin with IP address 192.168.51.21 tried to ...
12	2006.10.17 at 09:28:10...		192.168.51.21	User admin with IP address 192.168.51.21 tried to ...
13	2006.10.16 at 16:34:51...		192.168.50.176	User charlie with IP address 192.168.50.176 tried t...
14	2006.10.16 at 16:34:51...		192.168.50.176	User charlie with IP address 192.168.50.176 tried...
15	2006.10.16 at 16:06:45...		192.168.51.91	User admin with IP address 192.168.51.91 tried to ...
16	2006.10.16 at 16:06:45...		192.168.51.91	User admin with IP address 192.168.51.91 tried to ...
17	2006.10.16 at 16:06:25...		192.168.51.91	User admin with IP address 192.168.51.91 tried to ...
18	2006.10.16 at 13:25:00...		71.224.200.69	User Comsys with IP address 71.224.200.69 tried t...
19	2006.10.16 at 13:24:40...		71.224.200.69	User Comsys with IP address 71.224.200.69 tried t...
20	2006.10.16 at 06:28:03...		219.134.26.39	User remoteaccess with IP address 219.134.26.39 t...
21	2006.10.16 at 06:26:03...		219.134.26.39	User Comsys with IP address 219.134.26.39 tried t...
22	2006.10.16 at 06:25:43...		219.134.26.39	User Comsys with IP address 219.134.26.39 tried t...
23	2006.10.16 at 06:25:43...		219.134.26.39	User Comsys with IP address 219.134.26.39 tried t...

Figure 114 Error Log Report

- Click **Next** or **Previous** to navigate through the pages of the report.
- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Clear** to clear the log files used in the report.
- Click **Close** to close the report.

Access Report

Run the Access report to view information about accessed devices and ports, when they were accessed, and the user who accessed them.

1. On the **Reports** menu, click **Accessed Report**.

Figure 115 Access Report Screen

2. Set the date range for the report in the **Start Date** and **End Date** fields. Click each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number.

3. You can limit the data that the report will contain by entering additional parameters in the **Message**, **Device name**, **Port name**, **Username**, and **User IP address** fields.
 - If you want to limit the report by the message text associated with an activity, type the text in the **Message** field.
 - If you want to limit the report to a particular device, type the device name in the **Device name** field.
 - If you want to limit the report to a particular port, type the port name in the **Port name** field.
 - If you want to limit the report to a particular user's activities, type the user's username in the **Username** field.
 - If you want to limit the report to a particular IP address's activities, type the user's IP address in the **User IP address** field.
4. Click **OK** to run the report. The report is generated, displaying data about access that occurred during the designated time period that also complies with any additional parameters specified.

Access Report						
No.	Date	Device	Port	User	User IP Address	Message
9	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	Kephart	192.168.51.38	Connection expired
10	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	admin	192.168.50.176	Connection expired
11	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	admin	192.168.50.176	Connection expired
12	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	Kephart	192.168.51.38	Connection expired
13	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	Kephart	192.168.51.38	Connection expired
17	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	Kephart	192.168.51.38	Connection expired
18	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	Kephart	192.168.51.38	Connection expired
19	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	Charlie	192.168.50.176	Connection expired
20	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	Charlie	192.168.50.176	Connection expired
21	2007.10.20 at 1...	Kenny32-KX	AccessUSTIPLocal	admin	192.168.50.62	Connection expired
25	2007.10.20 at 0...	Kenny32-KX	IPR-32-59	admin	192.168.50.90	Connection expired
26	2007.10.19 at 2...	Kenny32-KX		admin	192.168.50.90	Connection expired
27	2007.10.19 at 2...	Kenny32-KX		admin	192.168.50.90	Connection expired
29	2007.10.19 at 2...	Kenny32-KX	lingoUSTIPLocal	admin	192.168.50.90	Connection expired
46	2006.10.17 at 1...	Kenny32-KX	lingoUSTIPLocal	Charlie	192.168.50.176	Connection expired
47	2006.10.17 at 1...	Kenny32-KX	lingoUSTIPLocal	Charlie	192.168.50.176	Connection expired
50	2006.10.17 at 1...	Kenny32-KX	lingoUSTIPLocal	admin	192.168.51.91	Connection expired
51	2006.10.17 at 1...	Kenny32-KX	lingoUSTIPLocal	Charlie	192.168.50.176	Connection expired
53	2006.10.17 at 1...	Kenny32-KX	lingoUSTIPLocal	Charlie	192.168.50.176	Connection expired
54	2006.10.17 at 1...	Kenny32-KX	lingoUSTIPLocal	Charlie	192.168.50.176	Connection expired
63	2006.10.14 at 0...	Kenny32-KX	P2SC-32-60	comsys	66.133.247.6	Connection expired
65	2006.10.11 at 1...	Kenny32-KX	P2SC-32-60	admin	192.168.51.134	Connection expired
67	2006.10.10 at 1...	Kenny32-KX	P2SC-32-60	admin	192.168.58.37	Connection expired

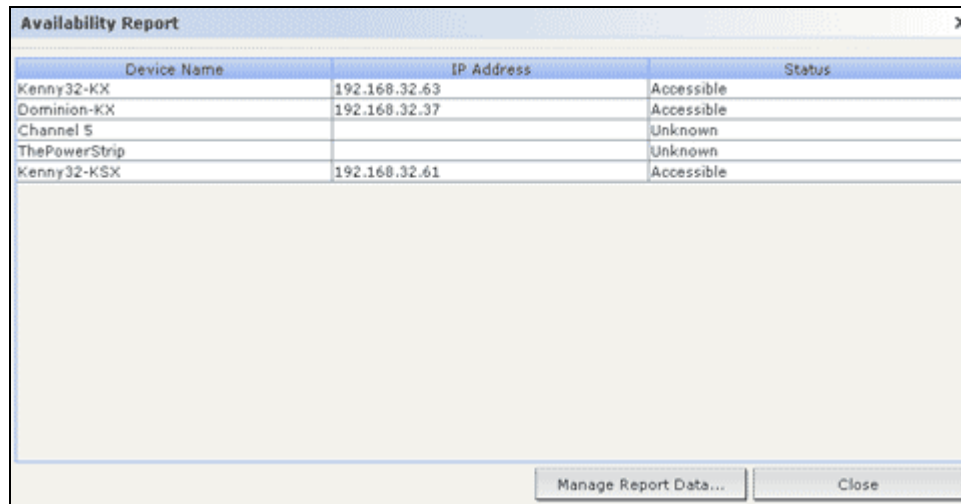
Figure 116 Access Report

- Click **Next** or **Previous** to navigate through the pages of the report.
- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Clear** to clear the log files used in the report.
- Click **Close** to close the report.

Availability Report

The Availability Report displays the status of all connections, showing devices by name and IP address. This report gives you the full accessibility picture for all devices on your system, and supplies information that could be useful for troubleshooting.

1. On the **Reports** menu, click **Availability Report**. The **Availability Report** is generated.



The screenshot shows a window titled "Availability Report" with a close button (X) in the top right corner. Inside the window is a table with three columns: "Device Name", "IP Address", and "Status". The table contains five rows of data. Below the table is a large empty rectangular area. At the bottom right of the window are two buttons: "Manage Report Data..." and "Close".

Device Name	IP Address	Status
Kenny32-KX	192.168.32.63	Accessible
Dominion-KX	192.168.32.37	Accessible
Channel 5		Unknown
ThePowerStrip		Unknown
Kenny32-KSX	192.168.32.61	Accessible

Figure 117 Availability Report

- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.

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.

1. On the **Reports** menu, click **Users**, and then click **Active Users**. The **Active Users** report is generated.

User Name	Access Time	Register Time	Remote Ad...	Remote ...	Server Node	Login Type	Cl...
shail	2007.10.24 at 18:09:25 EDT	2007.10.24 at 18:09:25 EDT	192.168.50...	192.168....	192.168.32....	Html Client	
shail	2007.10.24 at 18:10:29 EDT	2007.10.24 at 18:10:29 EDT	192.168.50...	192.168....	192.168.32....	Html Client	
shail	2007.10.24 at 18:16:47 EDT	2007.10.24 at 18:16:47 EDT	192.168.50...	192.168....	192.168.32....	Html Client	
shail	2007.10.24 at 18:19:34 EDT	2007.10.24 at 18:19:34 EDT	192.168.50...	192.168....	192.168.32....	Html Client	
shail	2007.10.24 at 18:20:47 EDT	2007.10.24 at 18:20:47 EDT	192.168.50...	192.168....	192.168.32....	Html Client	
admin	2007.10.24 at 16:16:10 EDT	2007.10.24 at 16:16:10 EDT	192.168.50...	192.168....	192.168.32....	CC Client	
admin	2007.10.24 at 18:08:02 EDT	2007.10.24 at 18:08:02 EDT	192.168.50...	192.168....	192.168.32....	CC Client	

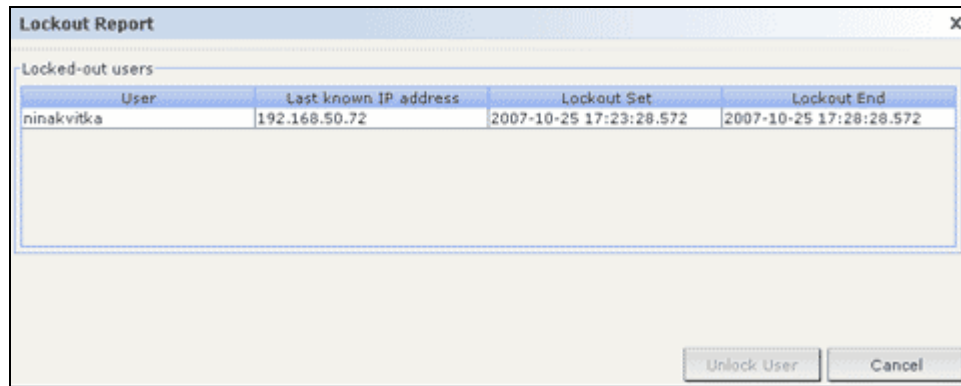
Figure 118 Active Users Report

- To disconnect a user from an active session in CC-SG, select the user name you want to disconnect, and then click **Logout**.
- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.

Locked Out Users Report

The Locked Out Users report displays users who are currently locked out of CC-SG because they made too many unsuccessful login attempts. You can unlock users from this report. Please refer to [Chapter 13: Advanced Administration, Lockout Settings](#) for additional information on lockout settings.

1. On the **Reports** menu, click **Users**, and then click **Locked Out Users**.



The screenshot shows a window titled "Lockout Report" with a close button (X) in the top right corner. Below the title bar, there is a section labeled "Locked-out users" containing a table. The table has four columns: "User", "Last known IP address", "Lockout Set", and "Lockout End". There is one row of data with the following values: "ninakvitka", "192.168.50.72", "2007-10-25 17:23:28.572", and "2007-10-25 17:28:28.572". Below the table, there are two buttons: "Unlock User" and "Cancel".

User	Last known IP address	Lockout Set	Lockout End
ninakvitka	192.168.50.72	2007-10-25 17:23:28.572	2007-10-25 17:28:28.572

Figure 119 Locked Out Users Report

- To unlock a user who has been locked out of CC-SG, select the user name you want to unlock, and then click **Unlock User**. An
- Click **Cancel** to close the report.

User Data Report

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

1. On the **Reports** menu, click **Users**, and then click **User Data**. The All Users' Data report is generated.

User Name	Phone	Enabled	Password Ex...	Groups	Privileges	Email	User Type
shail		true	7	CC Users	Node Out-of-...	shail.laronne...	local
ninakvitka		true		System Adm...	CC Setup An...	nina.kvitka@...	local
Mickey_Mouse		true				mickey@disn...	remote
Hetalp		true		System Adm...	CC Setup An...	hetal.patel@r...	local
IeseUser		true		CC Users	Node Out-of-...	elizabeth.elli...	local
Kephart		true		CCUserSecu...	User Securit...	craig.kephar...	local
Charlie		true		System Adm...	CC Setup An...	charles.mele...	local
comsys		true		System Adm...	CC Setup An...		local
Mikey		true		System Adm...	CC Setup An...		local
testx		true					remote
UserDevCon...		true		CCDeviceCe...	Device Confi...		local
MrUserMgmnt		true		CCUserMgmnt	User Manage...		local
UserSetupCo...		true		CCSetupAnd...	CC Setup An...		local
DrNo		true		NoPrivileges			local
MrUserSec		true		CCUserSecu...	User Securit...		local
test		true		System Adm...	CC Setup An...		local
test1		true		System Adm...	CC Setup An...		local
test12		true		System Adm...	CC Setup An...		local
NoGroupUser		true		CC Users	Node Out-of-...		local
admin		true	100	CC Super-User	CC Setup An...		local
MrNoGroup		true					local
Kenny		true		System Adm...	CC Setup An...		local

Manage Report Data... Close

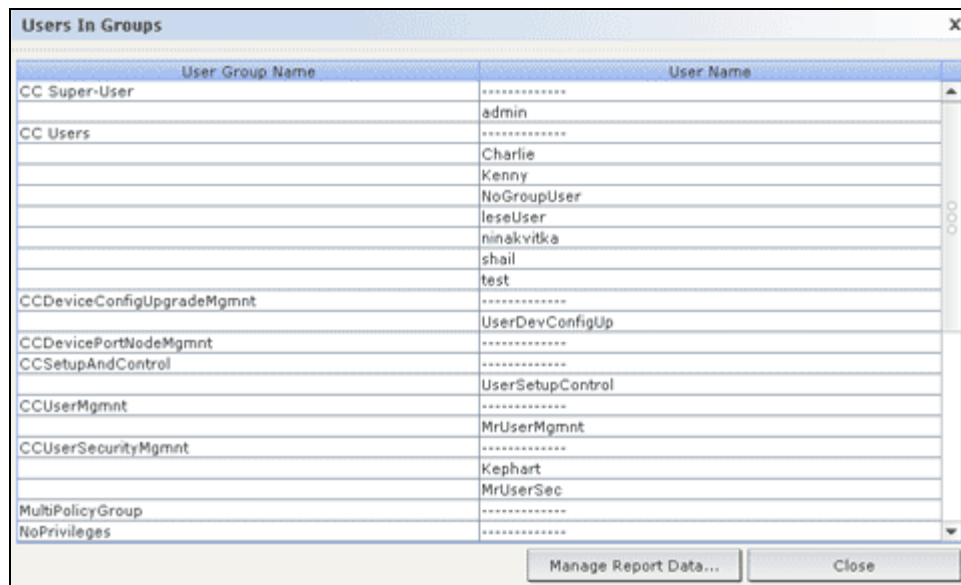
Figure 120 All Users' Data Report

- The **User Name** field displays the user names of all CC-SG users.
- The **Phone** field displays the user's dial back telephone number, which is only applicable for users of CC-SG G1 systems that include a modem.
- The **Enabled** field displays **true** if the user is able to log in to CC-SG, or **false** if the user is not able to log in to CC-SG, based on whether the **Login Enabled** checkbox is checked in the User Profile. Please refer to [Chapter 8: Adding and Managing Users and User Groups, Add User](#) for additional information.
- The **Password Expiration** field displays the number of days that the user can use the same password before being forced to change it. Please refer to [Chapter 8: Adding and Managing Users and User Groups, Add User](#) for additional information.
- The **Groups** field displays the user groups that the user belongs to.
- The **Privileges** field displays the CC-SG privileges assigned to the user. Please refer to [Appendix C: User Group Privileges](#) for additional information.
- 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.
- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.

Users in Groups Report

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

1. On the **Reports** menu, click **Users**, and then click **Users In Groups**. The **Users In Groups** report is generated.



User Group Name	User Name
CC Super-User	admin
CC Users	Charlie
	Kenny
	NoGroupUser
	IeseUser
	ninakvitka
	shail
	test
CCDeviceConfigUpgradeMgmnt	UserDevConfigUp
CCDevicePortNodeMgmnt	
CCSetupAndControl	UserSetupControl
CCUserMgmnt	MrUserMgmnt
CCUserSecurityMgmnt	Kephart
	MrUserSec
MultiPolicyGroup	
NoPrivileges	

Figure 121 Users In Groups Report

- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.

Group Data Report

The Group Data report displays user group, node group, and device group information. View user groups by name and description, view node groups by name, and view device groups by name, all in one screen.

1. On the **Reports** menu, click **Users**, and then click **Group Data**. The **Groups** report is generated.

User Group Name	Group Description	Privileges	Policies
CC Super-User	Do Not Delete	CC Setup And Control, De...	
CC Users	Command Center Users	Node Out-of-band Access, ...	Full Access Policy
CCDeviceConfigUpgradeM...		Device Configuration And ...	
CCDevicePortNodeMgmnt		Device, Port and Node Ma...	
CCSetupAndControl		CC Setup And Control	

Node Group Name	Full Rule String
All Nodes	Node Name LIKE %
MrAdmin	
Server Room North	
Server Room South	
engineering Nodes	Department = engineering

Device Group Name	Full Rule String
All Devices	Device Name LIKE %
CC Super-User Device Group	Device Name LIKE %
DeviceGroup1	
MrAdmin	
NinaDeviceGroup	

Figure 122 Groups Report

- Click **Manage Report Data...** to save or print the report section. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.
- Click the ... button next to a row to display either the policies associated with the user group, the list of nodes that satisfy the node group rule, or the list of devices that satisfy the device group rule.

AD User Group Report

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

1. On the **Reports** menu, click **Users**, and then click **AD Users Group Report**.
2. The **AD Server** list includes all AD servers that have been configured on CC-SG for both authentication and authorization. Check the checkbox that corresponds to each AD server you want CC-SG to include in the report.
3. In the **AD User Groups** section, the **Available** list includes all user groups that were imported into CC-SG from the AD servers you checked in the **AD Server** list. Select the user groups you want to include in the report, and then click **Add** to move the user groups to the **Selected** list.

- Click **Apply**. The AD User Group report is generated.

Figure 123 AD User Group Report

- Click **Manage Report Data...** to save or print the report section. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.

Asset Management Report

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

- On the **Reports** menu, click **Devices**, and then click **Asset Management Report**. The **Asset Management** report is generated for all devices.
- If you want to filter the report data by device type, click the **Device** type drop-down arrow, select a device type from the list, and then click **Apply**. The report is generated again with the selected filter applied.

Figure 124 Asset Management Report

- Devices whose versions do not comply with the Compatibility Matrix will display in red text in the **Device Name** field.
- Click **Manage Report Data...** to save or print the report section. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all

records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.

- Click **Refresh** to generate a new report. The report may take several minutes to generate, based on the size of your system configuration.
- Click **Close** to close 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 also filter the report to include only data about nodes that correspond to a specified node group, interface type, device type, or device.

1. On the **Reports** menu, click **Nodes**, and then click **Node Asset Report**. The Node Asset Report screen displays.

Figure 125 Node Asset Report Screen

2. Click the radio button that corresponds to the filtering criteria you want to apply to the report, **All Nodes**, **Node Group**, **Device Group**, or **Devices**.
 - If you selected **Node Group**, **Interface Type** or **Device Group**, click the corresponding drop-down arrow, and then select a parameter from the list.
 - If you selected **Devices**, select the devices in the **Available** list whose node assets you want to include in the report, and then click **Add** to move them to the **Selected** list.

- Click **Apply** to generate the report. The Node Asset Report generates.

Node Asset Report

Filter

☒ All Nodes ☐ Devices

☐ Node Group:

☐ Interface Type:

☐ Device Group:

Available:

- Channel 5
- Kenny32-KSX
- Kenny32-KX
- ThePowerStrip

Selected:

Node Name	Interface Name	Interface Type	Node Group	Device Name	Device Type
HP ML370 Server	In-Band - VNC Int...	In-Band - VNC	test node group, ...	N/A	N/A
HP ML370 Server	In-Band - SSH Int...	In-Band - SSH	test node group, ...	N/A	N/A
HP ML370 Server	In-Band - iLO/RIL...	In-Band - iLO/RIL...	test node group, ...	N/A	N/A
HP ML370 Server	Power Control - iL...	Power Control - iL...	test node group, ...	N/A	N/A
HP ML370 Server	Out-of-Band - KV...	Out-of-Band - KVM	test node group, ...	Kenny32-KSX	Dominion KSX
Cisco 2600	Out-of-Band - KV...	Out-of-Band - KVM	test node group, ...	Dominion-KX	Dominion KX
LINUX	Linux OOB - KVM ...	Out-of-Band - KVM	All Nodes	Dominion-KX	Dominion KX
in-band same add...	Power Control - iL...	Power Control - iL...	MrAdmin, All Nodes	N/A	N/A
in-band same add...	In-Band - iLO/RIL...	In-Band - iLO/RIL...	MrAdmin, All Nodes	N/A	N/A
CC-SG	In-Band - SSH Int...	In-Band - SSH	MrAdmin, All Nodes	N/A	N/A
WIN	Power Control - M...	Power Control - M...	Server Room Sou...	Channel 5	PowerStrip

Figure 126 Node Asset Report

- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.

Active Nodes Report

The Active Nodes report includes the name and type of each active interface, the current user, a timestamp, and the user IP address for each node with an active connection. You can view the active nodes list and disconnect nodes from this report.

- On the **Reports** menu, click **Nodes**, and then click **Active Nodes**. The Active Nodes report generates if there are currently active nodes.

Active Nodes Report

User Name	Node	Device	Date/Time Opened	User IP Address	Interface	Type
admin	KVM Target 1	Kenny32-KSX	Tue Nov 07 10:19:07 ...	192.168.50.151	Out-of-Band - KVM Interface	Out-of-Band - KVM

Figure 127 Active Nodes Report

- To disconnect a node from a current session, select the node you want to disconnect, and then click **Disconnect**.
- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records.

Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.

- Click **Close** to close the report.

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.

1. On the **Reports** menu, click **Nodes**, and then click **Node Creation**. The Node Creation screen displays.

Figure 128 Node Creation Report Screen

2. Set the date range for the report in the **Start Date** and **End Date** fields. Click each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number.
3. Check the **Potential Duplicates Only** checkbox to limit the report to only those nodes that have been flagged as potential duplicates.
4. Click **Apply**. The Node Creation report is generated.

Node	Date/Time of Creation	Created By	Result
LINUX	2006.10.18 at 11:32:04 EDT	admin	SUCCESS
SunUltra	2006.10.18 at 11:32:04 EDT	admin	SUCCESS
Cisco 2600	2006.10.18 at 11:32:04 EDT	admin	SUCCESS
WIN .	2006.10.18 at 11:32:04 EDT	admin	SUCCESS
KVM Target 1	2006.10.13 at 09:32:54 EDT	comsys	SUCCESS
CC-SG	2006.10.11 at 18:46:03 EDT	admin	SUCCESS
Hetal's Server	2006.10.11 at 15:11:05 EDT	admin	SUCCESS
IBM Server	2006.10.11 at 13:07:54 EDT	admin	SUCCESS
HP ML370 Server	2006.10.11 at 12:31:20 EDT	admin	SUCCESS
unknown Kuolin interface	2006.10.10 at 17:22:40 EDT	admin	SUCCESS
iLO Card on an HP Server	2006.10.10 at 17:15:00 EDT	admin	SUCCESS
Serial Target 1	2006.10.10 at 14:24:58 EDT	admin	SUCCESS
IPR-32-59	2006.10.10 at 09:37:22 EDT	admin	SUCCESS
lingoUSTIPLocal	2006.10.10 at 09:37:21 EDT	admin	SUCCESS
P2SC-32-60	2006.10.10 at 09:37:21 EDT	admin	SUCCESS

Figure 129 Node Creation Report

- The Result field displays **Success**, **Failed**, or **Potential Duplicate** to describe the outcome of the node creation attempt
- Click **Manage Report Data...** to save or print the report section. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.

Query Port Report

The Query Port Report displays all ports according to port status.

1. On the **Reports** menu, click **Ports**, and then click **Query Port**.

Figure 130 Query Port Screen

2. In the **Select port status** section, check the checkboxes that correspond to the port statuses you want to include in the report. Checking more than one checkbox and clicking **Apply** will display ports with all statuses that are selected.

PORT STATUS	DEFINITION
All	All port statuses.
New	Port is available (physical connection to target server is in place), but the port has not been configured.
Unused	Port is unavailable (physical connection to target server is not in place) and the port has not been configured.
Available	Port has been configured and connection to port is possible.
Unavailable	Connection to port is not possible since the device is down and unavailable.
Busy	A user is connected to this port.

3. Check the **Show Ghosted Ports** checkbox in conjunction with one or more port statuses to display ports that have the selected port status in addition to being ghosted. A ghosted port can occur when a CIM or target server is removed from a Paragon system or powered off (manually or accidentally). Refer to Raritan's **Paragon II User Manual** for additional information.

- Click **Apply** to generate the report.

Query Port

Filter

Select port status:

☒ All ☒ Available ☒ Busy ☒ New ☒ Unavailable ☒ Unused

☐ Show Ghosted Ports **Apply**

Ports

Device Name	Port Name	Port Type	Port Status
Dominion-KX	LINUX	KVM Port	Unavailable
Dominion-KX	SunUltra	KVM Port	Unavailable
Dominion-KX	Unnamed	KVM Port	Unavailable
Dominion-KX	WIN .	KVM Port	Unavailable
Dominion-KX	Dominion-KX Power Supply	Power Supply Port	Unavailable
Kenny32-KSX	KVM Target 1	KVM Port	Available
Kenny32-KSX	KVM Target 2	KVM Port	New
Kenny32-KSX	KVM Target 3	KVM Port	New
Kenny32-KSX	KVM Target 4	KVM Port	New
Kenny32-KSX	Kenny32-KSX Power Supply	Power Supply Port	New
Kenny32-KSX	Admin	Serial Port	New
Kenny32-KSX	PowerPort	Serial Port	New
Kenny32-KSX	Serial Target 1	Serial Port	Busy
Kenny32-KSX	Serial Target 2	Serial Port	Available
Kenny32-KSX	Serial Target 3	Serial Port	New

2 2/4 **Close**

Figure 131 Query Port Report

- Click the arrow icons at the bottom right of the report to navigate through multiple page reports.
- Click **Configure** next to a New or Unused port in the report to configure it.
- Click **Close** to close the report.

Active Ports Report

The Active Ports report displays out-of-band ports that are currently in use. You can view the active ports list and disconnect ports from this report.

- On the **Reports** menu, click **Ports**, and then click **Active Ports**. The **Active Ports** report is generated.

Active Ports

Active Sessions

User	Device	Port	Allowed	Opened	User IP Address	Connection Type
admin	Kenny32-KSX	Serial Target 1	Tue Nov 07 18:1...	Tue Nov 07 18:...	192.168.50.151	Out-Of-Band

Manage Report Data... **Disconnect** **Close**

Figure 132 Active Ports Report

- To disconnect a port from a current session, select the port you want to disconnect, and then click **Disconnect**.
- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.
- Click **Close** to close the report.

Scheduled Reports

Scheduled Reports displays reports that were scheduled in the Task Manager. All Scheduled Reports can be viewed in HTML format. Please refer to **Chapter 13: Advanced Administration** for additional information.

1. On the **Reports** menu, click **Scheduled Reports**.
2. Click **Get Reports** to view the entire list of all scheduled reports that were created by all owners. By default, all reports that were scheduled from one hour ago until the current time are displayed.
3. To filter the reports displayed, you can select a particular **Report Type**, such as Active Ports Report, or **Report Owner**, or change the start and end dates in the **Reports generated between** fields by clicking each component of the default date (month, day, year, hour, minute, second) to select it, and then click the up and down arrows to reach the desired number. You can enter a **Report Name** to filter on the name—enter a phrase or partial phrase of the name; matches are case in-sensitive and wildcards are not allowed.
4. Click **Get Reports** to view the filtered list.
5. To view an individual report, highlight the report in the list, and then click **Show Report**.
6. Click **Close** to close the report.

CC-NOC Synchronization Report

The CC-NOC Synchronization report lists all targets, along with their IP addresses, that the CC-SG subscribes to and that are monitored by a CC-NOC given a particular discovery date. Any new targets that are discovered in the configured range are displayed here as well. Please refer to **Add a CC-NOC** in **Chapter 13: Advanced Administration** for details. You can also purge targets from the CC-SG database from this report.

1. On the **Reports** menu, click **CC-NOC Synchronization**.

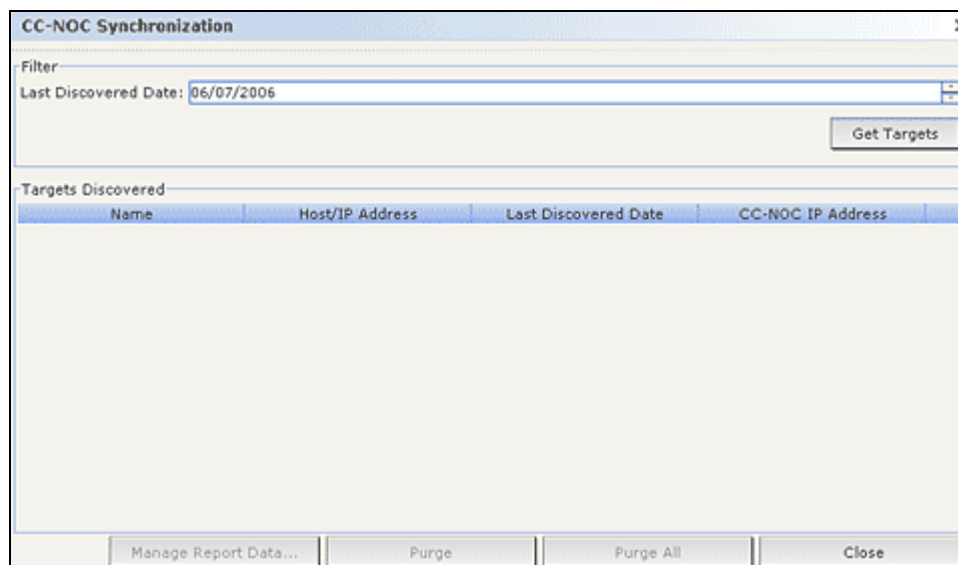


Figure 133 CC-NOC Synchronization Report

2. Select a **Last Discovered Date**, and then click **Get Targets**. The targets that were discovered on or earlier than the **Last Discovered Date** are displayed under **Targets Discovered**.
 - If you want to purge a target from the CC-SG database, select the target you want to purge, and then click **Purge**.
 - If you want to purge the entire list of targets from the CC-SG database, click **Purge All**.
 - Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed in the current report page to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed in the current report page or **Print All** to print all records.

Chapter 12: System Maintenance

About Maintenance Mode

Maintenance mode restricts access to CC-SG so that an administrator can perform various operations without disruption. Operations can be performed from the GUI or from an SSH command line interface via clients, such as Putty or OpenSSH Client. Please refer to **Chapter 13: Advanced Administration, SSH Access** for additional information.

Current users, except the administrator who is initiating Maintenance Mode, are alerted and logged out after the configurable time period expires. While in Maintenance Mode, other administrators are allowed to log into CC-SG, but non-administrators are prevented from logging in. An SNMP trap is generated each time CC-SG enters or exits Maintenance Mode.

Note: Maintenance Mode is only available on standalone CC-SG units and not in a cluster configuration. Upgrade CC-SG is disabled until you enter Maintenance Mode.

Scheduled Tasks and Maintenance Mode

Scheduled tasks cannot execute while CC-SG is in Maintenance Mode. Please refer [Chapter 13: Advanced Administration, Task Manager](#) for additional information on scheduled tasks. When CC-SG exits Maintenance Mode, scheduled tasks will be executed as soon as possible.

Entering Maintenance Mode

To enter Maintenance Mode:

1. On the **System Maintenance** menu, click **Maintenance Mode**, and then click **Enter Maintenance Mode**.

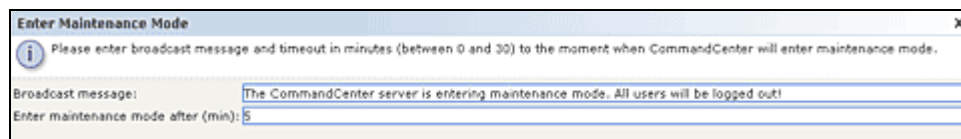


Figure 134 Enter Maintenance Mode

2. Type a **Broadcast message** or accept the default that is provided. This message will display to all logged in users to warn them that they will be logged off once CC-SG enters maintenance mode.
3. Enter a time (in minutes) in the **Enter maintenance mode after (min)** field. This is the amount of time CC-SG will wait before entering maintenance mode. The time can be between **0** and **30** minutes, a time of **0** means that Maintenance Mode is starting immediately.
4. Click **OK**.

Exiting Maintenance Mode

To exit Maintenance Mode:

1. On the **System Maintenance** menu, click **Maintenance Mode**.
2. Click **Exit Maintenance Mode**.
3. Click **OK** to exit Maintenance Mode.

A message will display indicated CC-SG has exited Maintenance Mode. All users will now be able to access CC-SG normally.

Backup CC-SG

Best practice is to enter Maintenance Mode before backing up CC-SG.

1. On the **System Maintenance** menu, click **Backup**.

Figure 135 Backup CommandCenter Screen

2. Type a name for this backup in the **Backup Name** field.
3. (Optional) Type a short description for the backup in the **Description** field.
4. Select a **Backup Type**.
 - **Custom** – Allows you to specify which components to add to the backup by checking them in the **Backup Options** area below. Check each of the following to include them in the backup.
 - **Data** – CC-SG configuration, Device and Node configuration and User Data. (Standard)
 - **Logs** – Error logs and event reports stored on CC-SG
 - **CC-SG firmware files** – Stored firmware files used for updating the CC-SG server itself.
 - **Device firmware files** – Stored firmware files used for updating Raritan devices managed by CC-SG.
 - **Application files** – Stored applications used by CC-SG to connect users to nodes.
 - **Full** – Creates a backup of all **Data**, **Logs**, firmware and **Application Files** stored on CC-SG. This produces the largest sized backup files.
 - **Standard** – Only creates a back up of critical **Data** on CC-SG. This backup includes CC-SG configuration information, Device and Node configurations and User configurations. This produces the smallest sized backup file.
5. (Optional) If you want to save a copy of this backup file to an external server, check **Backup to Remote Location**.
 - a. Select a **Protocol** used to connect to the remote server, either **FTP** or **SFTP**
 - b. Type the IP address or hostname of the server in the **Hostname** field.

- c. 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.
 - d. Type a username for the remote server in the **Username** field.
 - e. Type a password for the remote server in the **Password** field.
 - f. 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.
6. Click **OK**.

A success message will appear to confirm CC-SG backup. 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.

Restore CC-SG

1. On the **System Maintenance** menu, click **Restore**. The **Restore CommandCenter** screen appears with a table of back up sessions available to CC-SG. The table also lists the type of backup, the date of the backup, the description, what CC-SG version it was made from and the size of the backup file.

Name	Type	Date	Description	Data Version	Size
weekly backup	Custom	Mon Oct 16 12:54:22 E...	backup of critical infor...	3.1.0.2.2	215kB
weekly backup	Custom	Thu Oct 18 19:20:09 E...	backup of critical infor...	3.1.0.2.2	246kB

Figure 136 Restore CommandCenter Screen

2. If you want to restore from a backup stored off of the CC-SG system, you will first need to upload it to make it available. Click **Upload**. An open dialog screen appears. You can retrieve the file from anywhere on your client's network.
 - a. Browse for the backup file, and select it in the dialog window.
 - b. Click **Open** to upload this file to CC-SG.
 - c. When complete, the back-up file will appear in the **Available Backups** table.
3. Select the backup you wish to restore from the **Available Backups** table.
4. If applicable, select what kind of restore you wish to perform from this backup:
 - **Standard** – Only restores critical **Data** to CC-SG. This includes CC-SG configuration information, Device and Node configurations and User configurations.
 - **Full** – Restores all **Data**, **Logs**, firmware and **Application Files** stored in the backup file. This requires that a full backup was made for the file.

- **Custom** – Allows you to specify which components of the backup to restore to CC-SG by checking them in the **Restore Options** area below. Check each of the following to include them in the restore:
 - a. **Data** – CC-SG configuration, Device and Node configuration and User Data.
 - b. **Logs** – Error logs and event reports stored on CC-SG
 - c. **CC firmware files** – Stored firmware files used for updating the CC-SG server itself.
 - d. **Device firmware files** – Stored firmware files used for updating Raritan devices managed by CC-SG.
 - e. **Application files** – Stored applications used by CC-SG to connect users to nodes.
- 5. Type the number of minutes, from 0-60, that CC-SG will wait before performing the restore operation in the **Restore after** field. This allows users time to complete their work and log off.
- 6. In the **Broadcast Message** field, type a message to notify other CC-SG users that a restore will occur.
- 7. Click **Restore**.

After clicking **Restore**, CC-SG will wait for the time specified in the **Restore after** field before restoring its configuration from the selected backup. When the restore occurs, all other users will be logged off.

Saving and Deleting Backup Files

You can also save and delete backups stored on the CC-SG system from the **Restore CommandCenter** screen. Saving backups allows you to maintain a copy of the backup file on another PC, while deleting backups that are no longer needed can save space on the CC-SG.

To Save a backup

1. From the **Available Backups** table, select the backup you want to save to your PC.
2. Click **Save to File**. A Save dialog appears.

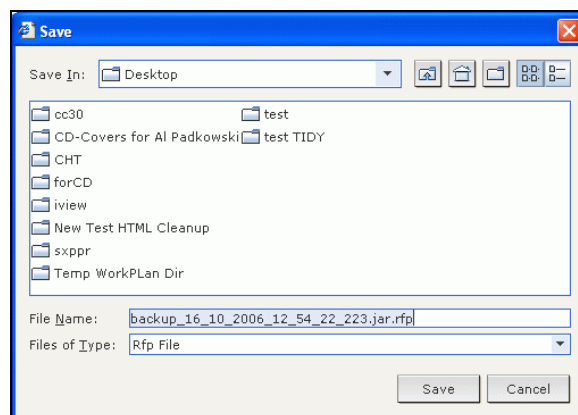


Figure 137 Saving a Backup File

3. Specify a location to save your CC-SG backup file, then click **Save**. The backup file will be copied to you client PC.

To Delete a backup

1. From the **Available Backups** table, select the backup you want to delete.
2. Click **Delete**. A confirmation dialog appears.
3. Click **OK** to delete the backup from the CC-SG system or **Cancel** to exit without deleting. Once deleted, the file backup file will be removed from the CC-SG.

***Note:** Saving and restoring can be used to move a backup from one CC-SG unit to another. Saving and deleting can be used to maintain a secure archive of CC-SG backups without storing the full archive on the system.*

Reset CC-SG

Use the Reset CommandCenter command to purge CC-SG database data. This will not reset system configuration data, such as the IP address of CC-SG. The following actions will be taken: reset CC-SG database, reset SNMP configuration, reset to default firmware, load default firmware into CC-SG database, and reset the Diagnostic Console to default values.

1. On the **System Maintenance** menu, click **Reset**.

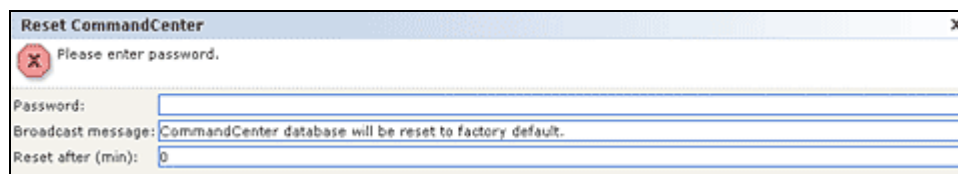


Figure 138 Reset CC-SG Screen

2. Type your CC-SG **password**.
3. Either accept the current **Broadcast message** or edit to create one of your own.
4. Type the number of minutes, from 0-60, that CC-SG will wait before performing the reset operation in **Reset after (min)**. Default is 0, which will reset the CC-SG unit immediately.
5. Click **OK** to reset your CC-SG unit. A success message will appear to confirm the reset.

Important: Using the Reset command will purge the database of CC-SG. All Devices, Nodes, Ports, and Users will be removed. Authentication is also reset to the Local DB. You should back up CC-SG before using Reset.

Restart CC-SG

The restart command is used to restart the CC-SG software. Restarting CC-SG will log all active users out of CC-SG.

***Note:** Restart will not cycle power to the CC-SG. To perform a full reboot you will need to access the Diagnostic Console or the power switch on the unit itself.*

1. On the **System Maintenance** menu, click **Restart**.

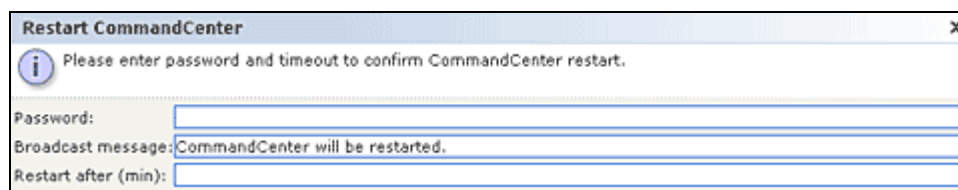


Figure 139 Restart Screen

2. Type your password in the **Password** field.
3. Accept the default message or type a warning 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 or tell them why you are restarting the system). All users will be disconnected when you restart CC-SG.
4. Type the number of minutes, from 0-60, that CC-SG will wait before it restarts in the **Restart after (min)** field.
5. Click **OK** to restart CC-SG or **Cancel** to exit the screen without restarting. Once you restart CC-SG, your Broadcast Message appears.
6. Click **OK** to restart CC-SG. CC-SG will restart, and be ready for use.

Upgrade CC-SG

The upgrade command is used to upgrade CC-SG's firmware to a newer version. To upgrade CC-SG, you should first have the latest firmware file saved to your client PC. Firmware files can be found in the Support section of the Raritan Website here:

http://www.raritan.com/support/sup_upgrades.aspx

It is recommended that you first back up CC-SG before upgrading.

***Note:** If you are operating a CC-SG cluster, you must remove the cluster first and upgrade each node separately.*

1. On the **System Maintenance** menu, click **Maintenance Mode**, then **Enter Maintenance Mode** to place CC-SG in Maintenance Mode. You will not be able to upgrade CC-SG without performing this action. Please refer to the **Maintenance Mode** section of this chapter for additional information.
2. Once CC-SG is in maintenance mode, on the **System Maintenance** menu, click **Upgrade**.

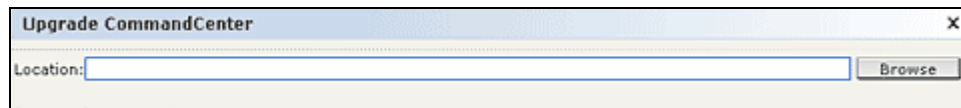


Figure 140 Upgrade CC-SG Screen

3. Click **Browse**, navigate to and select the CC-SG firmware file, and then click **Open**.
4. Click **OK** to upload the firmware file to CC-SG.
5. After the firmware file is uploaded to CC-SG, you will receive a success message. This indicates that CC-SG has received the file and has begun the upgrade process. All users will be disconnected from CC-SG at this time. Click **OK** to exit CC-SG and allow it to restart.
6. You must wait approximately 8 minutes while CC-SG restarts. Close your browser window, and then clear your browser cache.
7. After 8 minutes, open a new browser window and launch CC-SG. On the **Help** menu, click **About Raritan Secure Gateway**. In the window that appears, 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.
8. CC-SG will still be in **Maintenance Mode**, which means that most users cannot login. To exit Maintenance Mode, on the **System Maintenance** menu, click **Maintenance Mode**, and then click **Exit Maintenance Mode**. Click **OK**.

Shut Down CC-SG

These are the recommended methods for Administrators to shut down CC-SG. Shutting down CC-SG shuts down the CC-SG software, but it does not power off the CC-SG unit.

1. On the **System Maintenance** menu, click **Shutdown CommandCenter**.

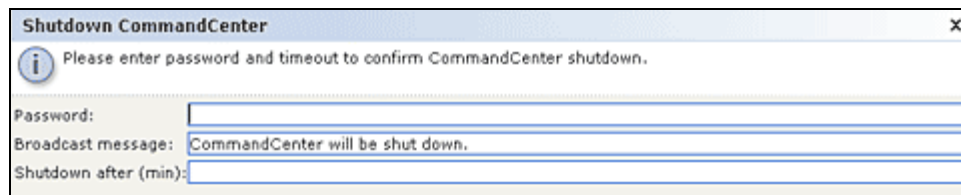


Figure 141 Shutdown CC-SG Screen

2. Type your password in the **Password** field.
3. Accept the default message or type a message to display to any users currently online in the **Broadcast message** field (for example, you might give users a brief time period to finish their tasks in CC-SG and tell them when they can expect the system to be functional again). All users will be disconnected when you shutdown CC-SG.
4. Type the number of minutes, from 0-60, that should pass before CC-SG shuts down in the **Shutdown after (min)** field.
5. Click **OK** to shut down CC-SG or **Cancel** to exit the screen without shutting down. Once you shut down, the CC-SG login window appears.

Note: After CC-SG shuts down, all users are logged out and redirected to the login screen. Users cannot log back in until you restart CC-SG as described in the next section.

Restarting CC-SG after Shutdown

After shutting down CC-SG, use one of these two methods to restart the unit:

1. Use the Diagnostic Console. Please refer to **Diagnostic Console** in **Chapter 13: Advanced Administration** for additional information.
2. Recycle the power to your CC-SG unit.

End CC-SG Session

Log Out

To exit CC-SG at the end of a session, or to refresh the database in case you or another user have made changes while you were logged in, log off from CC-SG entirely, then log in again.

1. On the **Secure Gateway** menu, click **Logout**. The **Logout** window appears.
2. Click **Yes** to log out of CC-SG or **No** to close the window. Once you log out, the CC-SG login window appears.
3. Log on to CC-SG again, or click **Exit** to shut down CC-SG completely.

Exit CC-SG

If at any time you want to exit CC-SG, you can exit.

1. On the **Secure Gateway** menu, click **Exit**. The **Exit** window appears.
2. Click **Yes** to exit CC-SG or **No** to close the **Exit** window and continue working.

This page intentionally left blank.

Chapter 13: Advanced Administration

Guided Setup

Guided Setup steps an administrator through some of the most common tasks on CC-SG: creating associations, setting up Raritan devices, creating user groups and creating users. For information on running **Guided Setup**, please refer to **Chapter 3: Configuring CC-SG With Guided Setup**.

Message of the Day Setup

The Message of the Day feature allows Secure Gateway administrators to provide a message viewable by all users when they login. In order to configure the message of the day, administrators must have the **CC Setup and Control** privilege.

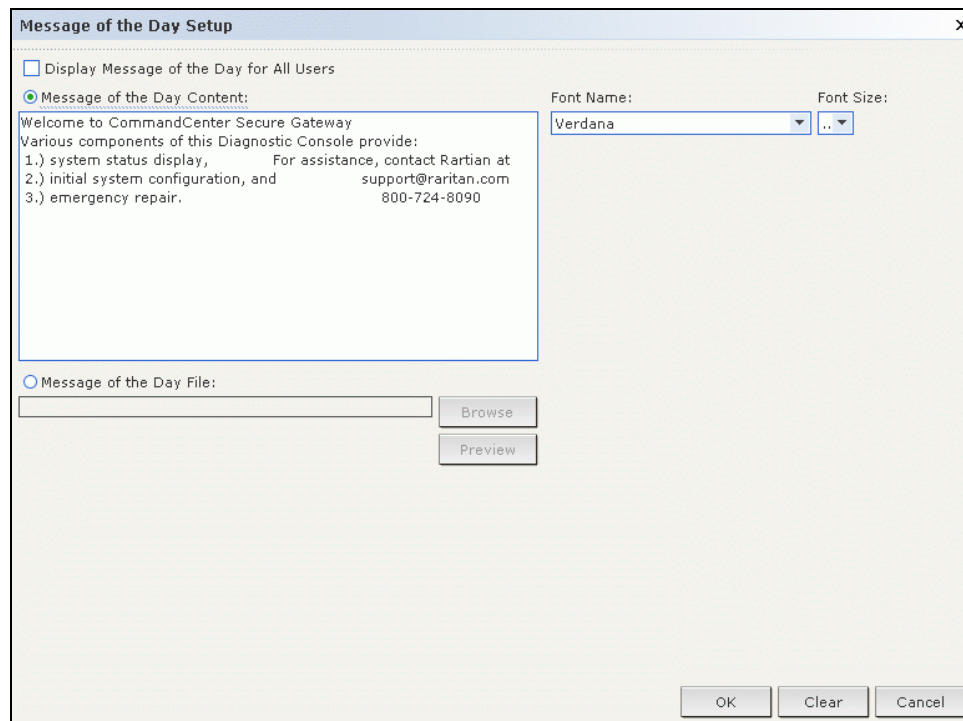


Figure 142 Configuring the Message of the Day

1. On the **Administration** menu, click **Message of the Day Setup**.
2. (Optional) Check **Display Message of the Day for All Users** if you want the message to be displayed to all users after they log in.
3. Select **Message of the Day Content** if you want to type a message in CC-SG, or select **Message of the Day File** if you want to load the message from an existing file.

If you select **Message of the Day Content**:

- a. Type a message in the dialog box provided.
- b. Click the **Font Name** drop-down menu and select a font to display the message in.
- c. Click the **Font Size** drop-down menu and select a font size to display the message in.

If you select **Message of the Day File**:

- a. Click **Browse** to browse for the message file.
- b. Select the file in the dialog window that opens, and then click **Open**.
- c. Click **Preview** to review the contents of the file.

4. Click **OK** to save your settings to CC-SG.

Application Manager

The Application Manager provides an interface for administrators to add access applications to CC-SG and set the default application for accessing nodes on Raritan devices.

1. On the **Administration** menu, click **Applications**.

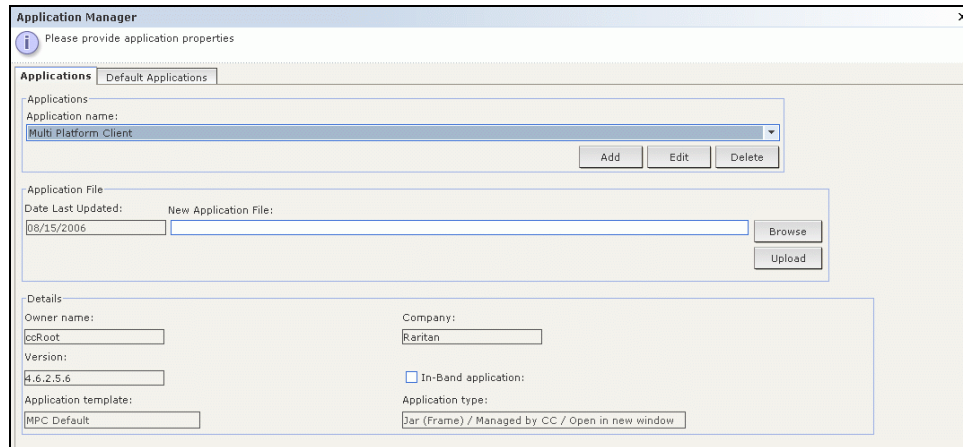


Figure 143 Applications Tab of the Application Manager

Adding and Deleting Applications

Click the **Applications** tab of the Application Manager to add or delete an application.

Adding an Application:

1. Click **Add** in the **Applications** section of the Applications tab. The **Add Applications** dialog window appears.

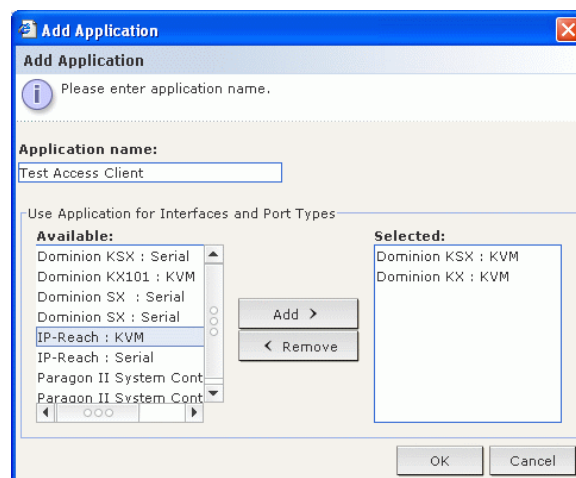


Figure 144 Adding an Application

2. Type a name for the application in the **Application Name** field.
3. Select the Raritan devices the application will function with from the **Available** list, and then click **Add** to add them to the **Selected** list. After the application is added, the devices in the **Selected** list will be able to select this application for access. If a device provides both KVM and serial access the device is listed twice, once for each method.
4. To remove devices from use with the application, select the device in the **Selected** list, and then click **Remove**.

5. Click **OK** when the necessary devices have been selected to work with the application. An Open dialog window will appear.
6. In the Open dialog window, browse for the location of your application file (usually a .jar or .cab file), select the file, and then click **Open**.

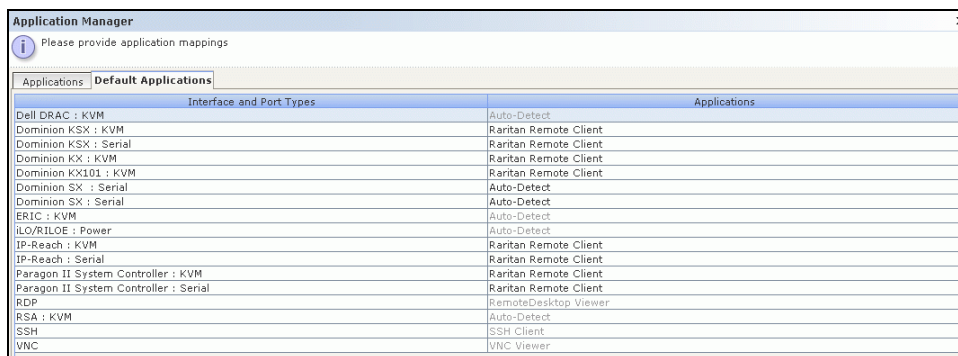
The selected application will then be loaded on to CC-SG.

Deleting an Application:

1. Select an application from the **Application Name** drop-down menu in the **Applications** section of the Applications tab. Details about the selected application will appear in the **Details** area of the tab.
2. Click **Delete** to delete the selected application. A confirmation dialog will appear.
3. Click **Yes** to confirm or **No** to cancel without deleting the application.

Default Applications

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.



Interface and Port Types	Applications
Dell DRAC : KVM	Auto-Detect
Dominion KSX : KVM	Raritan Remote Client
Dominion KSX : Serial	Raritan Remote Client
Dominion KX : KVM	Raritan Remote Client
Dominion KX101 : KVM	Raritan Remote Client
Dominion SX : Serial	Auto-Detect
ERIC : KVM	Auto-Detect
ILO/BILOE : Power	Auto-Detect
IP-Reach : KVM	Raritan Remote Client
IP-Reach : Serial	Raritan Remote Client
Paragon II System Controller : KVM	Raritan Remote Client
Paragon II System Controller : Serial	Raritan Remote Client
RDP	RemoteDesktop Viewer
RSA : KVM	Auto-Detect
SSH	SSH Client
VNC	VNC Viewer

Figure 145 A List of Default Applications

To edit the default application of an Interface or Port Type:

1. Select the row for an Interface or Port Type.
2. Double-click the **Application** listed on that row. The value becomes a drop-down menu. Note that grayed-out values are not editable.
3. On the drop-down menu, select a default application to use when connecting to highlighted Interface or Port Type. If you select **Auto-Detect**, CC-SG will auto-detect the application based on the client browser.
4. After all default applications have been configured, click **Update** to save your selection to CC-SG.

Firmware Manager

CC-SG stores firmware for Raritan devices in order to update the devices under its control. The firmware manager is used to upload and delete device firmware files to and from CC-SG.

Upload Firmware

This command allows you to upload different versions of firmware to your system. When new firmware versions become available, they are posted on the Raritan website.

1. On the **Administration** menu, click **Firmware**.

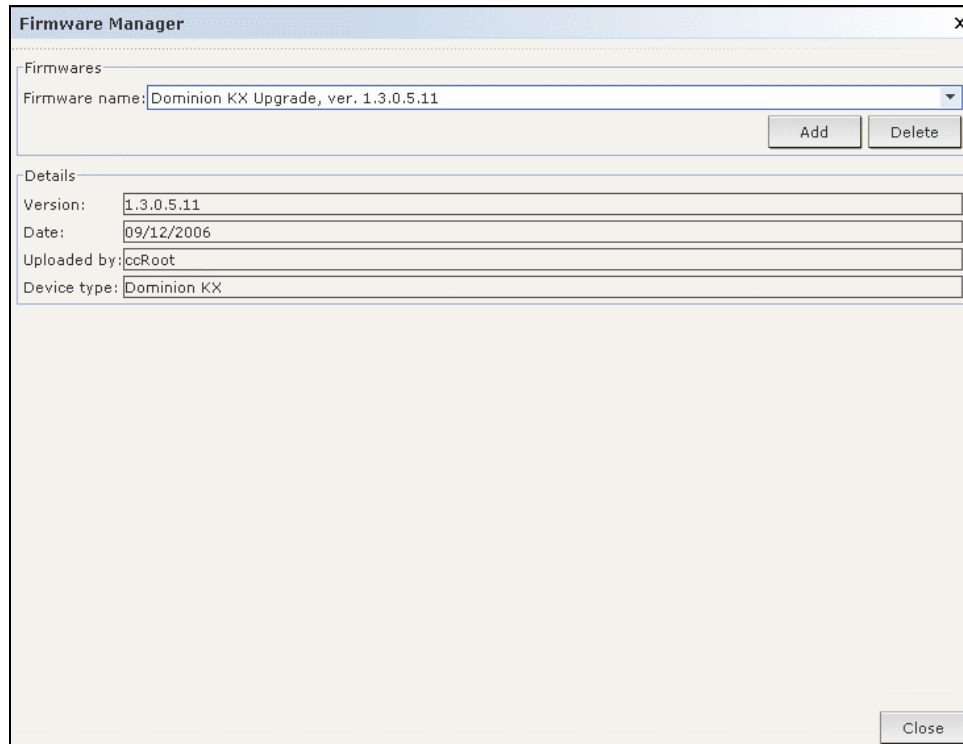


Figure 146 Firmware Manager Screen

2. Click **Add** to add a new firmware file. A search window appears.

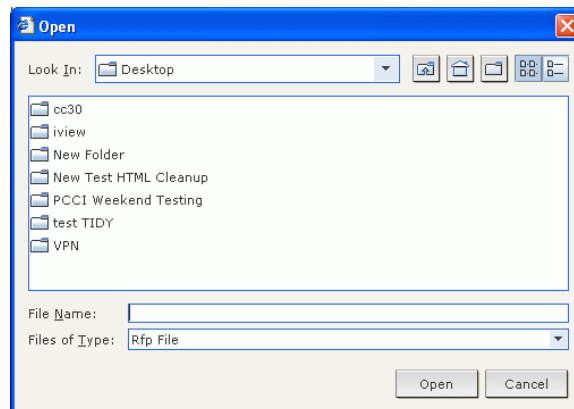


Figure 147 Firmware Search Window

3. Click the **Look In** drop-down arrow and navigate to locate the firmware file in your system. When you find the firmware, select it, and then click **Open**. Once added, the firmware name will appear in the **Firmware Name** field of the Firmware Manager.

Delete Firmware

1. On the **Administration** menu, click **Firmware**.
2. Click the **Firmware Name** drop-down arrow and select the firmware to be deleted.
3. Click **Delete**. The **Delete Firmware** window appears.
4. Click **Yes** to delete the firmware or **No** to close the window.

Configuration Manager

The Configuration Manager contains many of the CC-SG core settings:

- Network Setup
- Logs
- Inactivity Timer
- Time/Date
- Connection Mode
- Device Settings
- SNMP Configuration.

About Network Setup

CC-SG offers two modes for network setup:

- [Primary/Backup mode](#)
- [Active/Active mode](#)

CC-SG also allows either Static or DHCP-assigned IP addresses. Please refer to [Recommended DHCP Configurations for CC-SG](#) for best practices on using DHCP with your CC-SG.

About CC-SG LAN Ports

A CC-SG provides two main LAN ports: Primary LAN and Secondary LAN. Primary/Backup and Active/Active modes require you to connect the CC-SG LAN ports in different ways.

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

G1 LAN Ports

MODEL	PRIMARY LAN NAME	PRIMARY LAN LOCATION	SECONDARY LAN NAME	SECONDARY LAN LOCATION
G1	LAN0	Right LAN port	LAN1	Left LAN port

V1 LAN Ports

MODEL	PRIMARY LAN NAME	PRIMARY LAN LOCATION	SECONDARY LAN NAME	SECONDARY LAN LOCATION
V1	LAN1	Left LAN port	LAN2	Right LAN port

E1 LAN Ports

MODEL	PRIMARY LAN NAME	PRIMARY LAN LOCATION	SECONDARY LAN NAME	SECONDARY LAN LOCATION
E1	Not labeled.	Top LAN port in set of 2 ports in center of unit back panel	Not labeled.	Bottom LAN port in set of 2 ports in center of unit back panel

What is Primary/Backup mode?

Primary/Backup mode allows you to use two CC-SG LAN ports to implement network failover and redundancy. In this mode, only one LAN port is active at a time.

Please refer to [About CC-SG LAN Ports](#) for the locations of the Primary LAN and Secondary LAN ports on each CC-SG model.

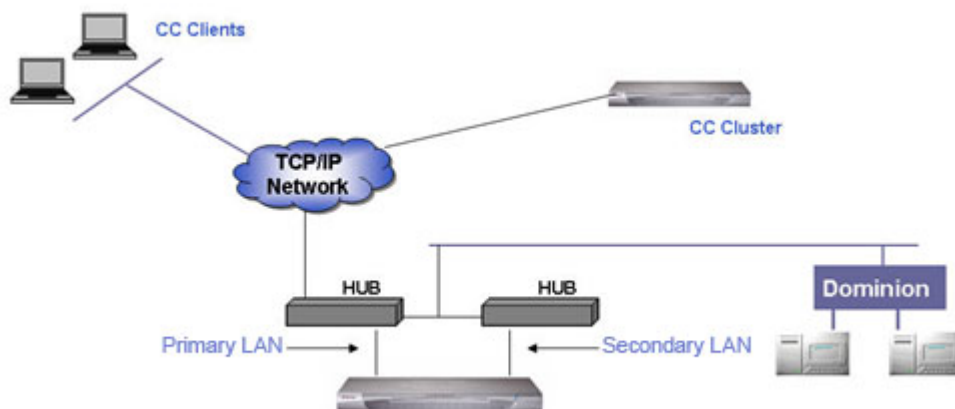


Figure 148 Primary/Backup Network

If the Primary LAN is connected and receiving a Link Integrity signal, CC-SG uses this LAN port for all communications. If the Primary LAN loses Link Integrity, and Secondary LAN is connected, CC-SG will failover its assigned IP address to the Secondary LAN. The Secondary LAN will be used until the Primary LAN returns to service. When the Primary LAN is back in service, CC-SG automatically reverts to using the Primary LAN.

As long as one LAN connection is viable, a client should not notice any disruption in service during a failure.

Setup for Primary/Backup mode

When implementing Primary/Backup mode for your CC-SG network:

- Both CC-SG LAN ports must be attached to the same LAN sub-network.
- (Optional) You can attach each LAN port to a different switch or hub on the same subnetwork for reliability.

To configure Primary/Backup mode in CC-SG

1. On the **Administration** menu, click **Configuration**.
2. Click the **Network Setup** tab.

Figure 149 Network Setup Panel—Primary/Backup

3. Select **Primary/Backup mode**.
4. Type the CC-SG hostname in the Host name field. Please refer to Chapter 1 [Terminology/Acronyms](#) for hostname rules. When you click **Update Configuration** to save the configuration, the **Host name** field will be updated to reflect the Fully-Qualified Domain Name (FQDN) if a DNS and domain suffix have been configured.
5. Click the **Configuration** drop-down arrow and select either **DHCP** or **Static**.

DHCP:

- If you choose DHCP, the Primary DNS, Secondary DNS, Domain Suffix, IP address, Subnet mask, and Default gateway fields will be automatically populated (if your DHCP server is configured to provide this information) once you save this network setup and restart CC-SG.
- With the information the DHCP server provides, CC-SG registers itself dynamically with the DNS server if it accepts dynamic updates.
- Please refer to [Recommended DHCP Configurations for CC-SG](#) for details.

Static:

If you choose **Static**, type Primary DNS, Secondary DNS, Domain Suffix, IP address, Subnet mask, and Default gateway in the appropriate fields.

6. Click the **Adapter Speed** drop-down arrow and select a line speed from the list. Make sure your selection agrees with your switch's adapter port setting.
7. If you selected **Auto** in the **Adapter Speed** field, the **Adapter Mode** field is disabled, with **Full Duplex** selected automatically. If you specified an Adapter Speed other than Auto, click the **Adapter Mode** drop-down arrow and select a duplex mode from the list.
8. Click **Update Configuration** to save the network setup.
9. 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.
 - Click **Cancel** to return to the Network Setup panel without saving your changes. You must click **Update Configuration**, then click **Restart Now** or **Restart Later** to save your changes.

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

What is Active/Active mode?

Active/Active mode allows you to use CC-SG to manage devices and nodes that are on two separate networks. In this mode, CC-SG manages traffic between the two separate IP domains. Active/Active mode does not offer failover. If either LAN connection fails, users won't have access.

Please refer to [About CC-SG LAN Ports](#) 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.

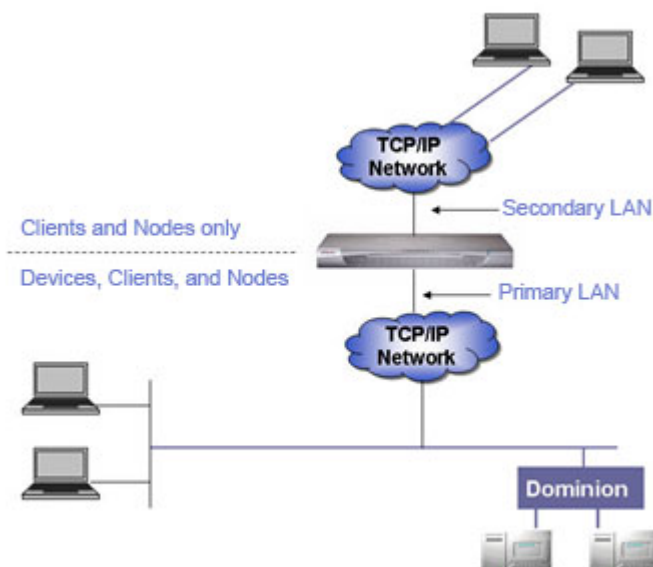


Figure 150 Active/Active Network

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. Please refer to Editing Static Routes on page 216 for details.

To configure Active/Active mode in CC-SG

1. On the **Administration** menu, click **Configuration**.
2. Click the **Network Setup** tab.

Network Setup		Logs	Inactivity Timer	Time/Date	Connection Mode	Device settings	SNMP
Host name: CommandCenter.localdomain							
Primary DNS: 192.168.50.114				Secondary DNS: 192.168.53.80			
Domain Suffix: localdomain							
<input type="radio"/> Primary/Backup mode				<input checked="" type="radio"/> Active/Active mode			
Configuration: Static		Configuration: Static		Configuration: Static		Configuration: Static	
IP address: 192.168.33.103		IP address: 192.168.20.21		IP address: 192.168.20.21		IP address: 192.168.20.21	
Subnet mask: 255.255.255.0		Subnet mask: 255.255.255.0		Subnet mask: 255.255.255.0		Subnet mask: 255.255.255.0	
Default gateway: 192.168.33.126		Default gateway:		Default gateway:		Default gateway:	
Adapter speed: Auto		Adapter speed: Auto		Adapter speed: Auto		Adapter speed: Auto	
Adapter mode: Full Duplex		Adapter mode: Full Duplex		Adapter mode: Full Duplex		Adapter mode: Full Duplex	

Figure 151 Network Setup Panel—Active/Active

3. Select **Active/Active mode**.
4. Type the CC-SG hostname in the Host name field. Please refer to Chapter 1 [Terminology/Acronyms](#) 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: Click the **Configuration** drop-down arrow and select either **DHCP** or **Static**.

DHCP:

- If you choose DHCP, the Primary DNS, Secondary DNS, Domain Suffix, IP address, Subnet mask, and Default gateway fields will be automatically populated (if your DHCP server is configured to provide this information) once you save this network setup and restart CC-SG.
- With the information the DHCP server provides, CC-SG registers itself dynamically with the DNS server if it accepts dynamic updates.
- Please refer to [Recommended DHCP Configurations for CC-SG](#) for details.

Static:

- If you choose **Static**, type Primary DNS, Secondary DNS, Domain Suffix, IP address, and Subnet mask in the appropriate fields.
 - Specify only one **Default gateway**, not both.
6. Click the **Adapter Speed** drop-down arrow and select a line speed from the list. Make sure your selection agrees with your switch's adapter port setting.
 7. If you selected **Auto** in the **Adapter Speed** field, the **Adapter Mode** field is disabled, with **Full Duplex** selected automatically. If you specified an Adapter Speed other than Auto, click the **Adapter Mode** drop-down arrow and select a duplex mode from the list.
 8. Click **Update Configuration** to save the network setup. CC-SG will restart.

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.

Log Configuration

From the **Logs** tab you can configure CC-SG to report to external logging servers. You can configure what level of messages is reported in each of the logs.

Configuring Logging Activity:

1. On the **Administration** menu, click **Configuration**.
2. Click the **Logs** tab.

The screenshot shows the 'Configuration Manager' window with the 'Logs' tab selected. The window has a title bar with 'Configuration Manager' and a close button. Below the title bar is a message icon and the text 'Please provide log configuration.'. The main area has several tabs: 'Network Setup', 'Logs' (selected), 'Inactivity Timer', 'Time/Date', 'Connection Mode', 'Device settings', and 'SNMP'. The 'Logs' tab is divided into sections. The 'Syslog' section has two sub-sections: 'Primary Server' and 'Secondary Server'. Under 'Primary Server', there is a 'Server address' field with the value '192.168.99.101' and a 'Level To forward' dropdown menu set to 'INFO'. Under 'Secondary Server', there is a 'Server address' field and a 'Level To forward' dropdown menu set to 'OFF'. The 'CommandCenter Log' section has a 'Level To forward' dropdown menu set to 'DEBUG'. At the bottom right of the window are two buttons: 'Purge' and 'Update Configuration'.

Figure 152 Configuration Manager Logs Screen

3. To assign an external log server for CC-SG to use, type the IP address into 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. When you are done configuring logs, click **Update Configuration** to save the settings to CC-SG.

Purging CC-SG's Internal Log:

The **Logs** tab can also be used to clear CC-SG's log of events. This command only clears CC-SG's log of events, it will not purge events recorded by external logging servers.

1. On the **Administration** menu, click **Configuration**.
2. Click the **Logs** tab.
3. Click **Purge** at the bottom of the screen. A dialog window will appear asking for confirmation.
4. Click **Yes** to clear CC-SG's log of events.

Note: The Audit Trail and Error Log reports are based off of CC-SG's internal log. If you purge CC-SG's internal log, these two reports will also purge their data.

Inactivity Timer Configuration

Use this screen to configure how long a session can remain active before being logged out.

1. On the **Administration** menu, click **Configuration**.
2. Click the **Inactivity Timer** tab.

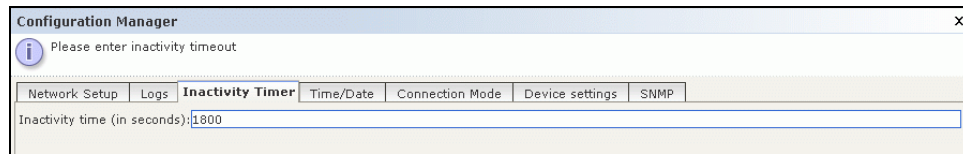


Figure 153 Inactivity Timer Tab

3. Type the desired time limit for inactivity (in seconds) in the **Inactivity Time** field.
4. Click **Update Configuration** to save the settings to CC-SG.

Time/Date Configuration

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 [Chapter 13: Advanced Administration, Task Manager](#) for additional information. The time set on the client 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.

1. On the **Administration** menu, click **Configuration** to open the **Configuration Manager** screen.
2. Click the **Time/Date** tab.

Figure 154 Configuration Manager Time/Date Screen

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

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

3. Click **Update Configuration** to apply the time and date changes to CC-SG.
4. Click **Refresh** to reload the new server time in the **Current Time** field.
5. On the **Maintenance** menu, click **Restart** to restart CC-SG.

Note: Changing the time zone is disabled in a cluster configuration.

Modem Configuration

Use this screen to access a CC-SG G1 from a client machine over a dial-up connection. This method of accessing CC-SG can be used in emergency situations.

Note: A modem is not available and cannot be configured on the V1 or E1 platforms.

Configure CC-SG

1. On the **Administration** menu, click **Configuration**. When the Configuration Manager screen appears, click the **Modem** tab.

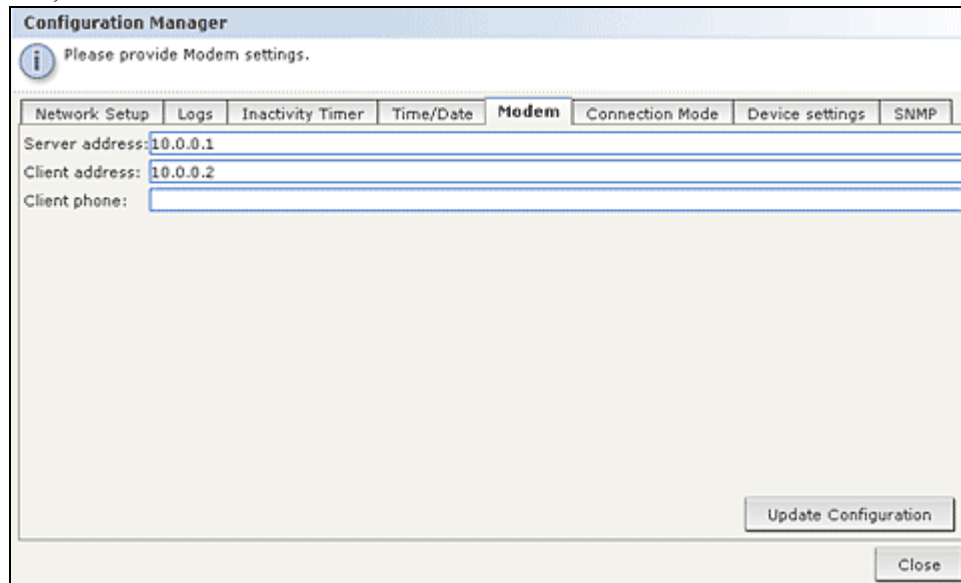


Figure 155 Configuration Manager Modem Screen

2. Type the IP address of the CC-SG in the **Server Address** field.
3. Type the IP address of the client that will dial into CC-SG in the **Client Address** field.
4. If you are using call-back dialing, type the call-back number that CC-SG dials to connect to the client in the **Client Phone** field.
5. Click **Update Configuration** to save the modem information.

Configure the Modem on Client PC

Connect a phone line to the CC-SG G1, which has a built-in modem. Optionally, remove the LAN cables.

On the client that will be dialing in, connect a modem to the client machine, for example, a Windows XP machine. Connect a phone line to the client modem. Restart the client machine and the connected modem is discovered as new hardware. Install the modem on the client as follows, which assumes a Windows XP client machine:

1. Select **Control Panel** → **Phone and Modem Options**.

2. Click the **Modems** tab.

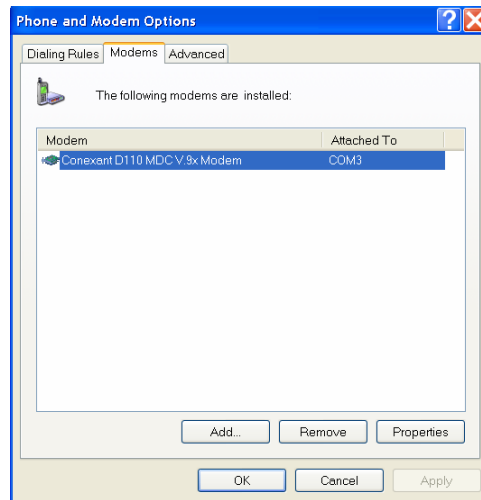


Figure 156 Modems Tab

3. Click **Properties**.
4. Click the **Advanced** tab.

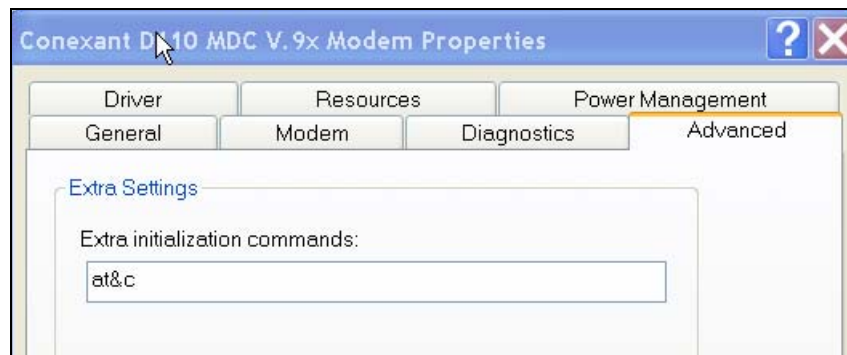


Figure 157 Extra Initialization Commands

5. Type an initialization command in **Extra initialization commands** that will be used by your modem to set the “Carrier detection” flag. For example, type **at&c** for a SoftK56 Data Fax modem. This is necessary to tell Windows not to close the started Modem connection process when the modem connection is closed from the other (dialed-in) side. Click **OK** to save the settings.

Configure the Dial-Up Connection

The following procedure illustrates creating an inbound dial-up connection to CC-SG from a Windows XP client machine:

1. On the **start** menu, click **My Network Places**.
2. Right-click in the window and select **Properties**.

- Under **Network Tasks** in the **Network Connections** window, click **Create a new connection**.

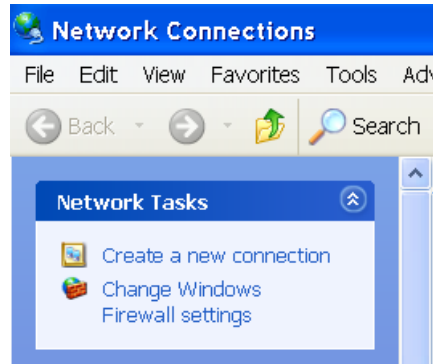


Figure 158 Create a New Connection

- Click **Next**, **Connect to the network at my workplace, Dial-up connection**.
- Type a name for CC-SG, for example **CommandCenter**.

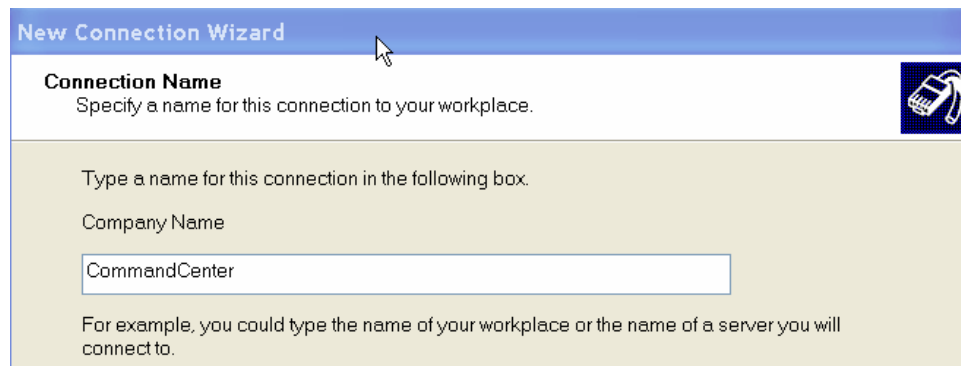


Figure 159 Connection Name

- Type the phone number used to connect to CC-SG, and then click **Next**. This is NOT the dial-back number that was configured as the **Client phone** under the **Modem** tab in **Configuration Manager** on CC-SG.

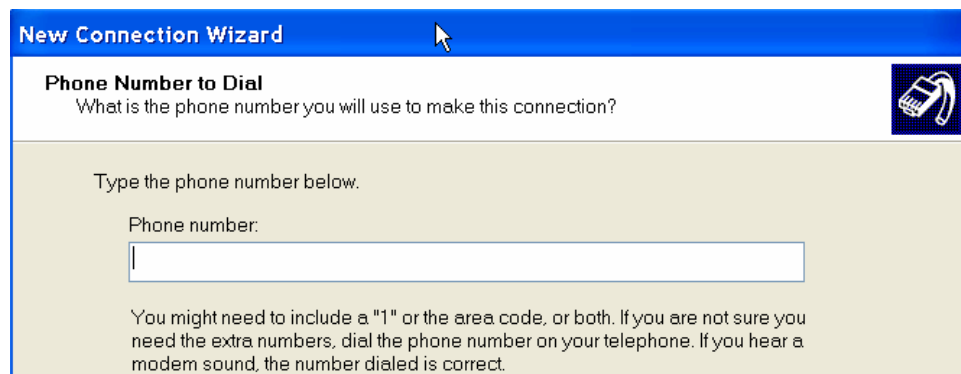


Figure 160 Phone Number to Dial

- A smart card is not necessary to dial into CC-SG. If you are not using one, click **Do not use my smart card** for this connection, and then click **Next**.
- In the next screen, typically click **My use only** in the next screen to make the connection available only to yourself.
- Click **Finish** in the last screen to save the connection settings.

Configure the Call-back Connection

If the CC-SG uses a call-back connection, you need to use a script file that is described below. To supply the script file for call-back:

1. On the **Start** menu, click **My Network Places**.
2. Click **view network connections** under **Network Tasks**.
3. Right-click the **CommandCenter** connection, and then click **Properties**.
4. Click the **Security** tab.

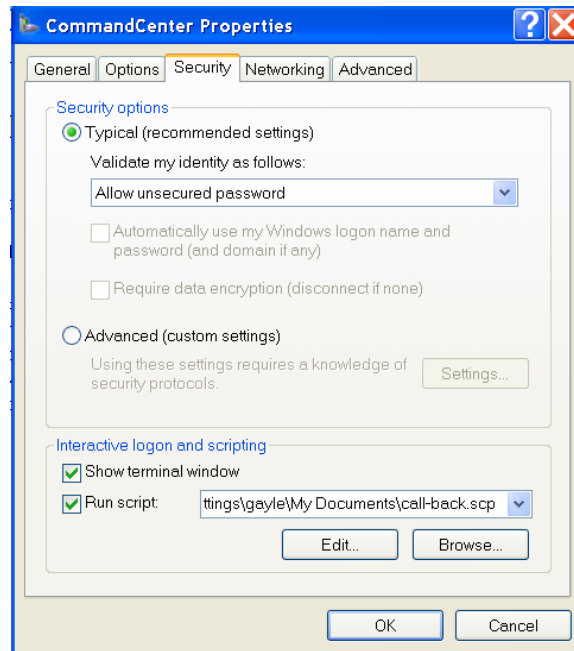


Figure 161 Specify Dial-up Script

5. Click the **Show terminal window**.
6. Click **Run script**, and then click **Browse** to enter the dial-up script, for example, **call-back.scp**.
7. Click **OK**.

Call-back Script File Example:

```
proc main
delay 1
waitfor "ogin:"
transmit "ccclient^M"
waitfor "client:"
transmit "dest^M"
waitfor "callback."
transmit "ATH^M"
waitfor "RING"
transmit "ATA^M"
waitfor "CONNECT"
waitfor "ogin:"
transmit "ccclient^M"
endproc
```

Connect to CC-SG with Modem

To connect to CC-SG:

1. On the **start** menu, click **My Network Places**.
2. Click **view network connections** under **Network Tasks**.
3. Double-click the **CommandCenter** connection.

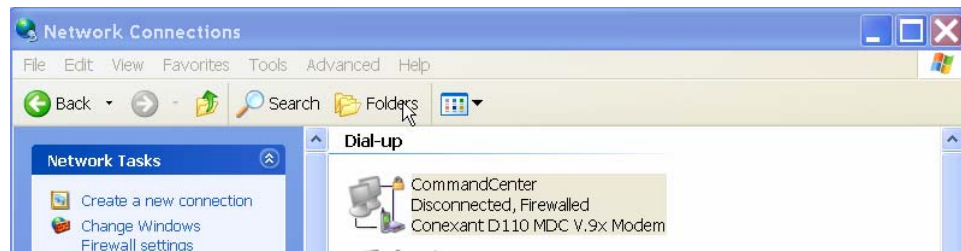


Figure 162 Connecting to CC-SG

4. Type a username of **ccclient** and password of **cbupass**.



Figure 163 Entering username and password

5. If not filled in already, enter the phone number used to connect to CC-SG. This is NOT the dial-back number.
6. Click **Dial**. If using call-back, the modem will dial CC-SG and then CC-SG will dial your client PC.

7. If **Show terminal window** was checked as described in section **Configure the Call-back Connection** earlier in this chapter, then a window similar to the one below will be displayed:

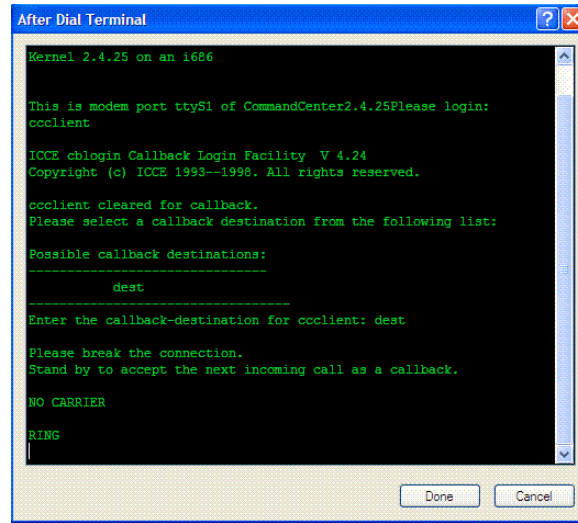


Figure 164 After Dial Terminal

8. Wait 1 or 2 minutes and in a supported browser, enter the IP address of CC-SG that was configured as the **Server address** under the **Modem** tab in **Configuration Manager** on CC-SG and login to CC-SG.

Connection Modes: Direct and Proxy

About Connection Modes

CC-SG offers three connection modes: Direct, Proxy, and Both, which is a combination of Direct and Proxy.

Direct mode allows you to connect to a node or port directly, without passing data through CC-SG. Direct mode generally provides faster connections.

Proxy mode allows you to connect to a node or port by passing all data through CC-SG. Proxy mode increases the load on your CC-SG server, which may cause slower connections. However, proxy mode is recommended if you are more concerned about the security of the connection. You only need to keep the CC-SG TCP ports (80, 443, and 2400) open in your firewall.

Both mode allows you to configure CC-SG to use a combination of Direct mode and Proxy mode. In Both mode, Proxy mode is the default, but you can configure CC-SG to use Direct mode when connections are made using client IP addresses in specified ranges.

To Configure Direct Mode for All Client Connections

1. On the **Administration** menu, click **Configuration**.
2. Click the **Connection Mode** tab.

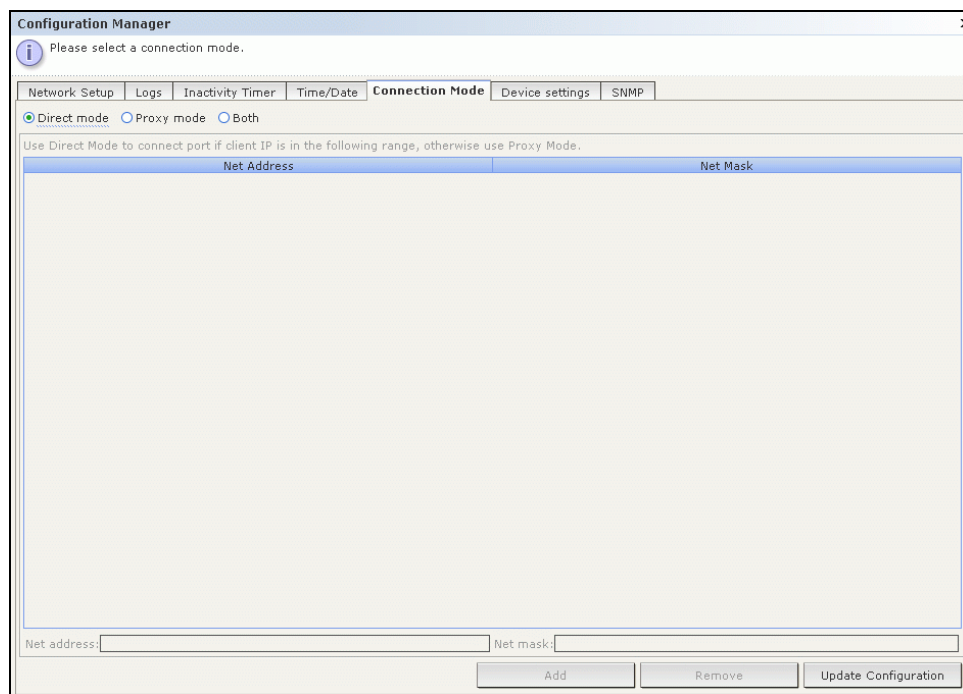


Figure 165 Connection Modes

3. Click the **Direct mode** radio button.
4. Click **Update Configuration**.

To Configure Proxy Mode for All Client Connections

1. On the **Administration** menu, click **Configuration**.
2. Click the **Connection Mode** tab.
3. Click the **Proxy mode** radio button.
4. Click **Update Configuration**.

To Configure a Combination of Direct Mode and Proxy Mode

When you configure CC-SG to use a combination of Direct mode and Proxy mode, Proxy mode will be the default connection mode, and Direct mode will be used for the client IP addresses you specify.

1. On the **Administration** menu, click **Configuration**.
2. Click the **Connection Mode** tab.

The screenshot shows the 'Configuration Manager' window with the 'Connection Mode' tab selected. The window has a title bar with a close button. Below the title bar is a message: 'Please select a connection mode.' The 'Connection Mode' tab is active, showing three radio buttons: 'Direct mode' (selected), 'Proxy mode', and 'Both'. Below the radio buttons is a text area with the instruction: 'Use Direct Mode to connect port if client IP is in the following range, otherwise use Proxy Mode.' The text area contains a table with two columns: 'Net Address' and 'Net Mask'. The table is currently empty. At the bottom of the window, there are input fields for 'Net address:' and 'Net mask:', followed by 'Add', 'Remove', and 'Update Configuration' buttons.

Figure 166 Configuration Manager Connection Screen – Direct Mode

3. Click the **Both** radio button.
4. In the **Net Address** and **Net Mask** fields, specify the client IP address range that should connect to nodes and ports via Direct mode, and then click **Add**.
5. Click **Update Configuration**.

Device Settings

1. On the **Administration** menu, click **Configuration**.
2. Click the **Device Settings** tab.

Device Type	Default Port
Dominion KX	5000
IPMI Server	623
Dominion KSX	5000
IP-Reach	5000
Dominion KX101	5000
Dominion SX	5000
Paragon II System Controller	5000

Heartbeat (sec): 600

Update Configuration

Figure 167 Configuration Settings Device Settings Screen

3. To update device Default Port, select a Device Type in the table and double-click the Default Port value. Type the new Default Port value and press the **Enter** key.
4. To update device timeout duration, double-click the Heartbeat (sec) value at the bottom of the screen. Type new timeout duration for this device.
5. Click **Update Configuration** to save the new device values. A success message will appear to confirm the update of all associated device settings.

SNMP

Simple Network Management Protocol allows CC-SG to push SNMP traps (event notifications) to an existing SNMP manager on the network. Only a CC-SG Administrator trained in handling an SNMP infrastructure should configure CC-SG to work with SNMP.

CC-SG also supports SNMP GET/SET operations with third-party enterprise Management 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. Refer to RFC 1213 for details. These identifiers provide contact, administrative, and location information regarding the managed node.

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. Please refer to **Appendix D: SNMP Traps**. This custom MIB file can be found on the CD included with your CC-SG unit and also under **Firmware Upgrades** on <http://www.raritan.com/support>.

Configuring SNMP in CC-SG

1. On the **Administration** menu, click **Configuration**.
2. Click the **SNMP** tab.

Configuration Manager

Please, provide SNMP configuration settings

Network Setup | Logs | Inactivity Timer | Time/Date | Connection Mode | Device settings | **SNMP**

Agent Configuration

Version: 2
 IP Address: 192.168.32.58 System Desc: Raritan Computer; CommandCenter Secure Gateway; Version 3.1.0.1.7; CC-SG-V1 HW
 Port: 161 System Contact:
 Read-Only Community: public System Name:
 Read-Write Community: private System Location:

Update Agent Configuration

Traps Configuration

☐ Enable SNMP Traps

Trap Sources

☒ System Log ☒ Application Log

Selected	Name	Description
<input checked="" type="checkbox"/>	ccDeviceUpgrade	CC SecureGateway has upgraded the firmware o...
<input checked="" type="checkbox"/>	ccImageUpgradeResults	CC Secure Gateway Image Upgrade results
<input checked="" type="checkbox"/>	ccImageUpgradeStarted	CC Secure Gateway Image Upgrade started
<input checked="" type="checkbox"/>	ccIncompatibleDeviceFirmware	CC Secure Gateway detected device with incomp...
<input checked="" type="checkbox"/>	ccLeafNodeAvailable	CC Secure Gateway detected leaf node reachable

Select All Clear All

Trap Destinations

Host	Port	Version	Community
Trap Destination Host:	Port: 162	Version: v1	Community:

Add Remove

Update Trap Configuration

Figure 168 Configuration Settings Device Settings Screen

- 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.
- Click **Update Agent Configuration** to save the SNMP agent identifier information.
- Under **Traps Configuration**, check the box marked **Enable SNMP Traps** to enable sending SNMP traps from CC-SG to a SNMP host.
- Check the checkboxes before the traps you want CC-SG to push to your SNMP hosts: Under **Trap Sources**, there is a list of SNMP traps grouped into two different categories: **System Log** traps, which include notifications for the status of the CC unit itself, such as a hard disk failure, and **Application Log** traps for notifications generated by events in the CC application, such as modifications to a user account. To enable traps by type, check the boxes marked **System Log** and **Application Log**. Individual traps can be enabled or disabled by checking their corresponding checkboxes Use **Select All** and **Clear All** to enable all traps or clear all checkboxes. Refer to the MIB files for the list of SNMP traps that are provided. Please refer to **MIB Files** for additional information.
- Type the **Trap Destination Host** IP address and **Port** number used by SNMP hosts in the **Trap Destinations** panel. Default port is **162**.
- Type the **Community** string and **Version** (**v1** or **v2**) used by SNMP hosts in the **Trap Destinations** panel.
- Click **Add** to add this destination host to the list of configured hosts. To remove a host from the list, select the host, and then click **Remove**. There is no limit to the number of managers that can be set in this list.
- When SNMP traps and their destinations are configured, click **Update Trap Configuration**.

Cluster Configuration

A CC-SG cluster uses two CC-SG nodes, one Primary node and one Secondary node, for backup security in case of Primary CC-SG node failure. Both nodes share common data for active users

and active connections, and all status data is replicated between the two nodes. The primary and secondary nodes in a cluster must be running the same version of software, on the same version of hardware (G1, V1, or E1). Unless defined by the user, CC-SG will assign a default name to each cluster node.

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 CC-SG unit will recognize that the Primary node is not responding and will respond to requests initiated by the Secondary node.

***Note:** In a cluster configuration, only the Primary CC-SG communicates with CC-NOC. Whenever a CC-SG becomes primary, it sends its IP address, in addition to the IP address of the Secondary CC-SG, 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.

Important: It is recommended to backup your configuration on both nodes before setting up a cluster configuration.

*Note: A CC-SG must be running its network ports in **Primary/Backup** mode in order to be used for clustering. Clustering will not work with an Active/Active configuration. Please refer to [About Network Setup](#) in this chapter for additional information.*

Set Primary CC-SG Node

1. On the **Administration** menu, click **Cluster Configuration**.

- 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**.

Cluster Configuration

This CommandCenter is not a member of any cluster. To create a cluster with this CommandCenter as the primary node click the Create Cluster button. To create a cluster with another CommandCenter as the primary node click the Discover CommandCenters button, select a CommandCenter to be the primary node (one that is not already part of another cluster), and then click the Create Cluster button.

Cluster Name	Node Address	Node State	CommandCenter version
	192.168.32.58	Standalone	3.1.0.2.6
cluster192.168.32.56	192.168.32.56	Primary	3.0.2.5.6
	192.168.32.34	Standalone	3.0.2.5.6
	192.168.32.123	Standalone	3.0.0.2.15
	192.168.32.85	Standalone	2.21.5.1
	192.168.32.155	Standalone	3.1.0.2.5

Cluster Management

CommandCenter address:

Cluster Name:

Backup username: Password:

Figure 169 Cluster Configuration Screen

- Type a name for this cluster in **Cluster Name**. If you do not provide a name now, a default name will be provided, such as **cluster192.168.51.124**, when the cluster is created.
- Click **Create Cluster**.
- Click **Yes** when prompted if you want to continue. The CC-SG you are currently using will become the Primary node and a default name will be provided unless you previously entered a name in the Cluster Name field.

Cluster Configuration

This CommandCenter is a member of cluster: NinaTestCluster. To create a new cluster click the Discover CommandCenters button, select a CommandCenter to be the primary node (one that is not already part of another cluster), and then click the Create Cluster button.

Cluster Name	Node Address	Node State	CommandCenter version
NinaTestCluster	192.168.32.58	Primary	3.1.0.2.6
cluster192.168.32.56	192.168.32.56	Primary	3.0.2.5.6
	192.168.32.34	Standalone	3.0.2.5.6
	192.168.32.123	Standalone	3.0.0.2.15
	192.168.32.85	Standalone	2.21.5.1
	192.168.32.155	Standalone	3.1.0.2.5

Cluster Management

CommandCenter address:

Cluster Name:

Backup username: Password:

Figure 170 Cluster Configuration – Primary Node Set

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**.

***Note:** Adding a backup CC-SG from a different subnet or network may avoid issues affecting a single network or physical location.*

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 will appear. Click **Yes** to assign Secondary status to the selected node, or click **No** to cancel.

Important! Once you begin the Join process, do not perform any other functions in CC-SG until the Join process has completed as indicated in step 6, below.

6. After you click **Yes**, CC-SG will restart the newly selected Secondary node. This process can take several minutes. When restart is complete, a confirmation message appears on your screen.
7. On the **Administration** menu, click **Cluster Configuration** to view the updated Cluster Configuration table.

***Note:** 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.*

Remove Secondary CC-SG Node

1. To remove Secondary Node status from a CC-SG unit and reassign it to a different unit in your configuration, select the Secondary CC-SG Node in the Cluster Configuration table, and then click **Remove “Backup” Node**.
2. When the confirmation message appears, click **Yes** to remove Secondary Node status, or click **No** to cancel.

***Note:** Clicking **Remove “Backup” Node** removes the designation of Secondary Node. It does not delete the Secondary CC-SG unit from your configuration.*

Remove Primary CC-SG Node

1. To remove Primary Node status from a CC-SG unit and reassign it to another unit in your configuration, select the Primary CC-SG Node in the Cluster Configuration table, and then click **Remove Cluster**.
2. When the confirmation message appears, click **Yes** to remove Primary Node status, or click **No** to cancel.

Note: Clicking **Remove Cluster** does not delete the Primary CC-SG unit from your configuration; it simply removes the designation of Primary Node. **Remove Cluster** is only available when no backup nodes exist.

Recover a Failed CC-SG Node

When a node fails and failover occurs, the failed node will recover in **Waiting** status.

1. Select the Waiting node in the Cluster Configuration table.
2. Add it as a backup node by clicking **Join “Waiting” Node**.
3. A confirmation message will appear. Click **Yes** to assign Secondary status to the selected node, or click **No** to cancel. If you click **Yes**, you will need to wait for the secondary node to restart just as with **Join “Backup” Node**.

Note: Once a node is in **Waiting** status it can be started in **Standalone** mode or **Backup** mode.

Set Advanced Settings

To configure advanced settings of a cluster configuration:

1. Select the Primary node just created.
2. Click **Advanced**. The **Advanced Settings** window appears.

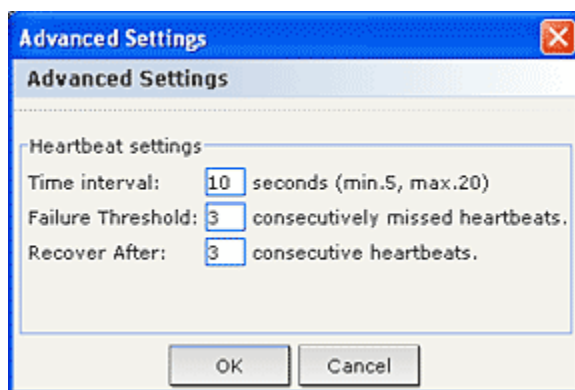


Figure 171 Cluster Configuration Advanced Settings

3. For **Time Interval**, enter how often CC-SG should check its connection with the other node.

Note: Setting a low Time Interval will increase the network traffic generated by heartbeat checks. Also, clusters with nodes located far apart from each other may want to set higher intervals.

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 the settings.

Note: Changing the time zone is disabled in a cluster configuration.

Configure Security

The Security Manager is used to manage how CC-SG provides access to users. Within Security Manager you can configure authentication methods, SSL access, AES Encryption, strong password rules, lockout rules, the login portal, certificates, and access control lists.

Remote Authentication

Please refer to **Chapter 10: Configuring Remote Authentication** for detailed instructions on configuring remote authentication servers.

About CC-SG and AES Encryption

You can configure CC-SG to require AES 128 encryption between your client and the CC-SG server. When AES encryption is required, all users must access CC-SG using an AES-enabled client. If AES encryption is required, and you try to access CC-SG with a non-AES browser, you will not be able to connect to CC-SG.

Check Your Browser for AES Encryption

If you do not know if your browser uses AES, check with the browser manufacturer.

You may also want to try navigating to the following web site using the browser whose encryption method you want to check: <https://www.fortify.net/sslcheck.html>. This web site will detect your browser's encryption method and display a report. Raritan is not affiliated with this web site.

Requiring 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. On the **Administration** menu, click **Security**.
2. In the **General** tab, check the **Requires AES Encryption between Client and Server** check box.
3. 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.
4. The **Key Length** field displays 128. 128-bit encryption will be required between your client and the CC-SG server.
5. The **Browser Connection Protocol** field displays HTTPS/SSL selected.
6. Click **Update** to save your change.

Configuring Browser Connection Protocol: HTTP or HTTPS/SSL

In Security Manager, you can configure CC-SG to use either regular HTTP connections from clients, or to require HTTPS/SSL connections. You must restart CC-SG for changes to this setting to take effect.

1. On the **Administration** menu, click **Security**.
2. In the **General** tab, click the **HTTP** or **HTTPS/SSL** radio button to select the Browser Connection Protocol you want clients to use when connecting to CC-SG.

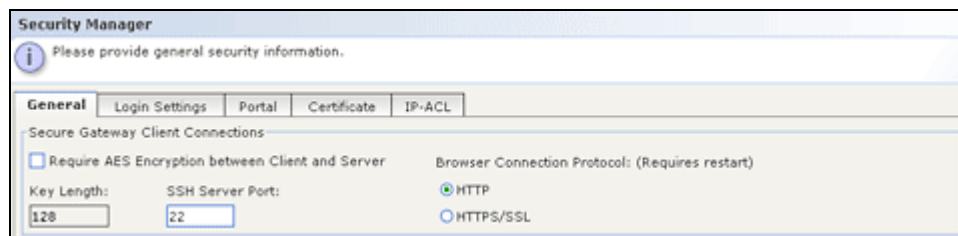


Figure 172 Secure Client Connections

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

Setting the Port Number for SSH Access to CC-SG

In Security Manager, you can set the port number you want to use for SSH access to CC-SG. Please refer to **SSH Access to CC-SG**, later in this chapter, for additional information.

1. On the **Administration** menu, click **Security**.
2. In the **General** tab, type the port number for accessing CC-SG via SSH in the **SSH Server Port** field.
3. Click **Update** to save your change.

Login Settings

The **Login Settings** lets you configure the **Strong Password Settings** and **Lockout Settings**.

1. On the **Administration** menu, click **Security**.
2. Click the **Login Settings** tab.

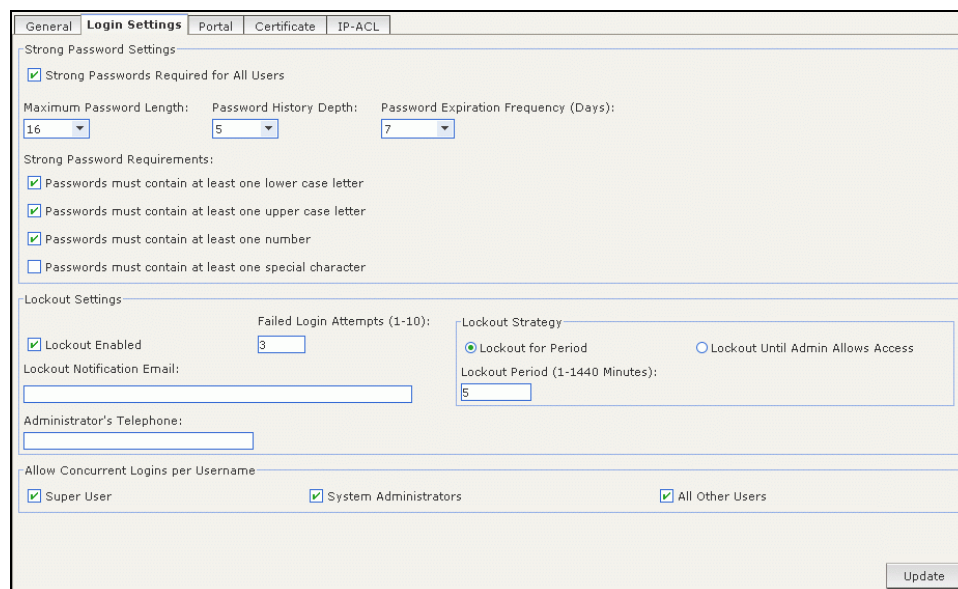


Figure 173 Login Settings

Strong Password Settings

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. In order to use strong passwords, administrators must first check **Strong Passwords Required For All Users**.

***Note:** A strong password that includes all strong password requirements is always required for the CC Super-User.*

Once enabled, administrators can edit the fields in the Strong Password Settings area to customize their password rules. At minimum, all strong passwords must be configured with the following criteria:

- **Minimum Password Length** – All passwords must contain a minimum number of characters. Click the drop down menu and select the minimum length of passwords.
- **Password History Depth** – Click the drop down menu and select how many previous passwords are kept in the history. While in the history, users will not be able to reuse a password when asked to choose a new one. For example, if **Password History** is set to 5, users cannot reuse any of their last 5 passwords.
- **Password Expiration Frequency** – All passwords must expire after a set number of days. Click the drop down menu and select the number of days passwords remain valid. After a password expires, users will be asked to choose a new password the next time they log in.

In addition, any four contiguous characters in the user name and the password cannot match.

Under **Strong Password Requirements**, the administrator can configure password rules to require a number of extra items:

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

When you are done configuring strong password rules, click **Update** to save the settings. All selected rules are cumulative, that is all passwords must meet every criteria that the administrator configures. After configuring strong password rules, all future passwords must meet these criteria and all existing users will need to 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 itself.

Raritan suggests using the **Message of the Day** feature to provide advanced notice to users when the strong password rules will be changing and what the new criteria are.

Lockout Settings

Administrators can lock out CC-SG, CC-NOC users, and SSH users after a specified number of failed login attempts. This feature applies to users who are authenticated and authorized locally by CC-SG and does not apply to users who are remotely authenticated by external servers. Please refer to Chapter 10: Configuring Remote Authentication for additional information. Failed login attempts due to insufficient user licenses also do not apply.

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 configure user Lockout:

1. Check **Lockout Enabled**.
2. The default number of failed login attempts before a user is locked out is **3**. You can change this value by entering a number from **1** to **10**.
3. Choose a Lockout Strategy:
 - a. If you choose **Lockout for Period**, specify the period of time, in minutes, the user will be locked out before they can login again. The default number is **5** minutes, but you can specify anywhere from **1** minute up to **1440** minutes (24 hours). After the time expires, the user can login again. At any time during the lockout period, an administrator can override this value and allow the user to log back into CC-SG.
 - b. If you choose **Lockout Until Admin Allows Access**, users are locked out until an administrator allows them to log back in. To unlock a user, please refer to **Chapter 11: Generating Reports** for additional information.
4. Type an email address in **Lockout notification email** so notification is sent to the address informing the recipient that lockout has occurred. If the field is blank, notification is not sent.
5. Type a phone number in **Administrator's Phone** if the administrator needs to be contacted.
6. Click **Update** to save configuration settings.

Allow Concurrent Logins per Username

These settings permit more than one concurrent session on CC-SG with the same Username.

1. Check **Super User** if you want to allow more than one simultaneous connection to CC-SG under the **admin** account.
2. Check **System Administrators** if you want to allow concurrent logins with accounts under the **System Administrators** user group.
3. Check **Other Users** if you want to allow concurrent logins with all other accounts.

Portal

Portal settings allow administrators to configure a logo and an access agreement to greet users when they access a client. To access the Portal settings:

1. On the **Administration** menu, click **Security**.
2. Click the **Portal** tab.

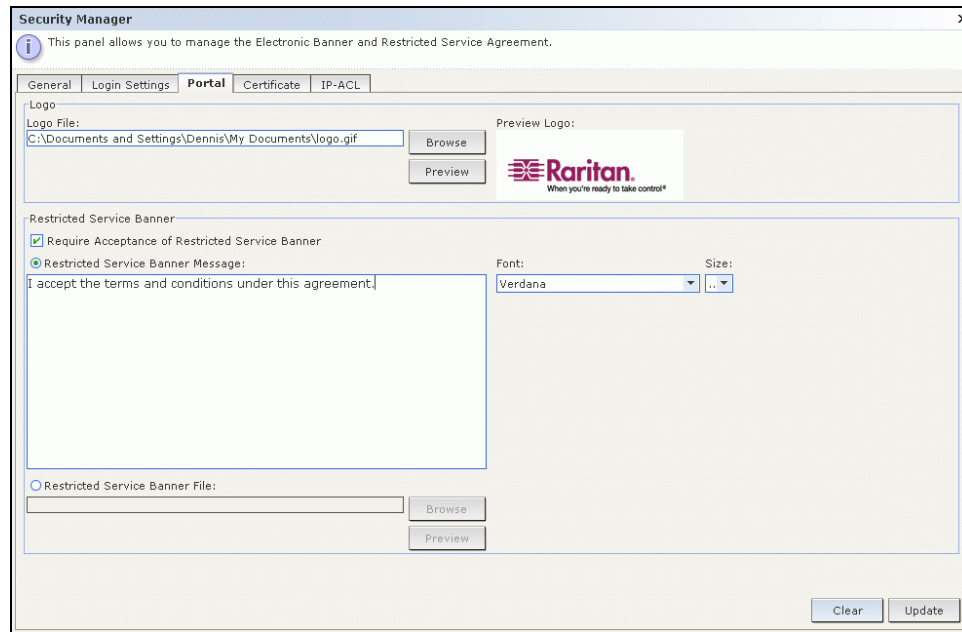


Figure 174 Portal Settings

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 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. If desired, click **Preview** to preview the logo. The selected graphic file will appear to the right.
4. Click **Update** to save your Logo changes to CC-SG.

Restricted Service Agreement

A message can be configured to appear to the left of the login fields on the login screen. This is intended for use as a Restricted Service Agreement, or a statement users agree to upon accessing the CC-SG. A user's acceptance of the Restricted Service Agreement is noted in the log files and the audit trail report.

1. Check **Require Acceptance of Restricted Service Agreement** to require users to check an agreement box on the login screen before they are allowed to enter their login information.
2. Select **Restricted Service Agreement Message** if you want to enter the banner text directly.
 - a. Type an agreement message in the text field provided. The maximum length of the text message is 10,000 characters.
 - b. Click the **Font** drop-down menu and select a font to display the message in.
 - c. Click the **Size** drop-down menu and select a font size to display the message in.

Select **Restricted Service Agreement Message File** if you want to load a message from a text (.TXT) file.

- a. Click **Browse**. A dialog window appears.
 - b. 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.
 - c. Click **Preview** if you want to preview the text contained in the file. It will appear in the banner message field above.
3. Click **Update** to save your Restricted Service Banner changes to CC-SG.

After your Logo and Restricted Service Agreement settings have been updated, they will appear on the login screen the next time a user accesses a client.

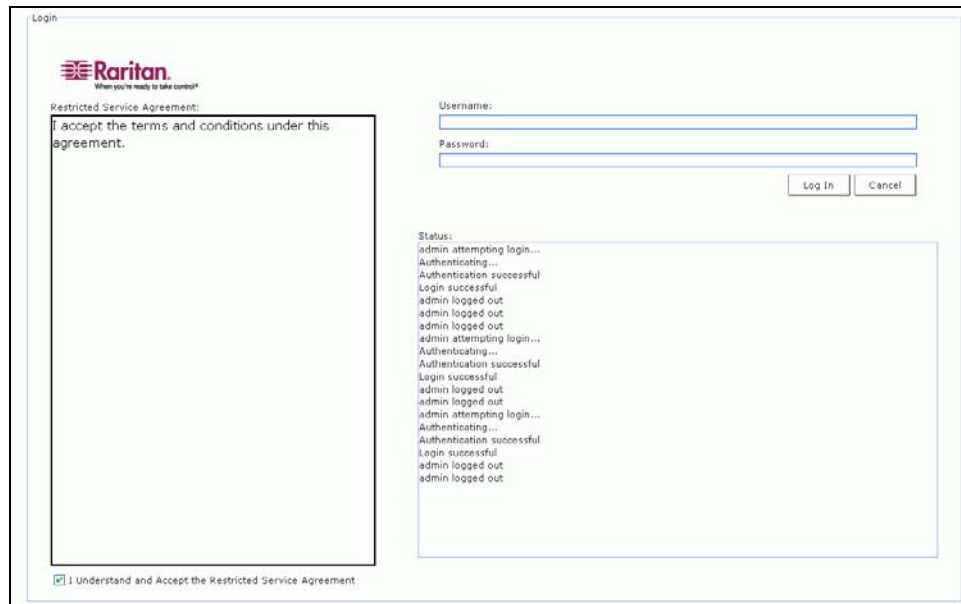


Figure 175 Login Portal With Restricted Service Agreement

Certificate

Options in this window can be used to generate a certificate signing request (also CSR or certification request). A CSR is a message sent from an applicant to a certificate authority to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant.

*Note: The button at the bottom of the screen will change from **Export** to **Import** to **Generate**, depending on which certificate option is selected.*

1. On the **Administration** menu, click **Security**.

2. Click the **Certificate** tab.

Security Manager

This panel allows you to manage certificate.

General Login Settings Portal **Certificate** IP-ACL

☒ Export current certificate and private key
☐ Import pasted certificate and private key
☐ Generate certificate signing request
☐ Generate self signed certificate

Certificate

Private Key

CA file: Browse Password:

Clear All Export

Figure 176 Security Manager Certificate Screen

Export Current Certificate and Private Key

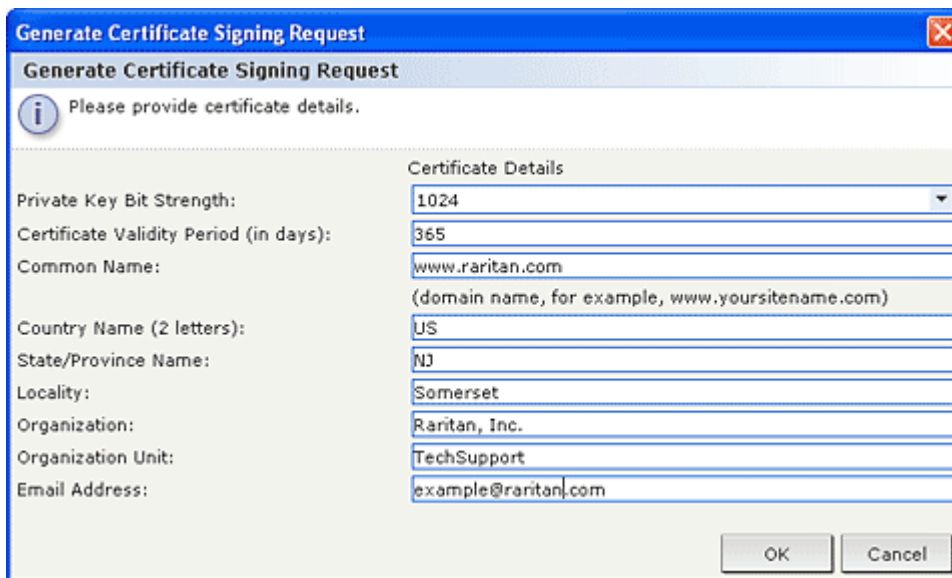
Click **Export current certificate and private key**. The certificate appears in the **Certificate** panel and the private key appears in **Private Key** panel. Copy the text of the **Certificate** and **Private Key** and submit it by clicking **Export**.

Generate Certificate Signing Request

The following explains how to generate a CSR and a private key on CC-SG. 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. The signed certificate, root certificate, and private key will then be imported.

1. Click **Generate Certificate Signing Request**, and then click **Generate**. The **Generate Certificate Signing Request** window appears.

2. Type the requested data for the CSR into the fields.



Generate Certificate Signing Request

Please provide certificate details.

Certificate Details	
Private Key Bit Strength:	1024
Certificate Validity Period (in days):	365
Common Name:	www.raritan.com (domain name, for example, www.yoursitename.com)
Country Name (2 letters):	US
State/Province Name:	NJ
Locality:	Somerset
Organization:	Raritan, Inc.
Organization Unit:	TechSupport
Email Address:	example@raritan.com

OK Cancel

Figure 177 Generate Certificate Signing Request Screen

3. Click **OK** to generate the CSR or **Cancel** to exit the window. The CSR and Private Key appear in the corresponding fields of the **Certificate** screen.



Certificate Request

-----BEGIN CERTIFICATE REQUEST-----
MIIB2jCCAUMCAQAwZkxCZAJBgNVBAYTAIVTMQswCQYDVQQIEWJOSjERMA8GA1UE
BxMIU29tZXJzZXQxFjAUBgNVBAoTDVJhcm10YW4sIEluYy4xFDASBgNVBA5TC1Rl
Y2htdXBwb3J0MRgwFgYDVQQDEW93d3cucmFyaXRhbi5jb20xIjAgBgkqhkiG9w0B
CQEWEZV4YW1wbGVAcnFyaXRhbi5jb20wZDQYJkoZIhvcNAQEBBQADgY0AMIGJ
AoGBAORmo8IsI+9tUnEnL0ADQIRHjIYQLQD+j3ffcVAgZeHsgsClqBE7OhkZJcfV
5sQFEcyx+eGDF4UmfzOhCpdFnCm5gh0yvHN9IVJqDdmVpTriVNGBD3UY3OrSC42y
H3397cEbqS4Z0sFAcuMLYhVRXWWhxo64L9NrVDiDfPqSLdKlAgMBAAAGgADANBgkq
hkiG9w0BAQFQAQOBgQBBQEew/vC7ufBBrvnHLzEY1YM+zRiv7/NVHLYOYwuaY9HrP
A1q1Oh0rRMiSS1n0i14M33Gib/T0a05XiG0vVtKSR1tT9ubdtv7S0tvaFd65/

Private Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,203FBFB0ACA6CAC5

qFen02cyR+cp1x+X6NzIFD22wKsBlaVJZnaejTDBVbo3c832VzcGjjerHnE5VbQA
JGlskWeqjrt+rorEGXtoqZsbucj0HGEwPUMZ8PdmiE8LxNdqZh0/nkaAxpB/i/
aGRksXnI1xZnhxdkEk8UQsKq0Hn576bqLp3kuIQnGQhapAPtnbzDLxiUURQn0ETN
z3yo+GsWF0v+fsQ8J3W6/ymNAXZ280FCpsjZos+vLBcsBb89icqilhqnoqc7m8Mp
Ti/IzW1VKfElkLVMwCiEFJZUtdlmmO1V4ELLwcNV2DYMrFLbeaVus12DnHCHH6Fg
m37a73+5LvLb0h0CM2v7uMdieV3nlt1Ga011G+1L90rYdlud01vdxTC8ni6XCa

Figure 178 Certificate Request Generated

4. Using an ASCII editor such as Notepad, copy and paste the CSR into a file and save it with a **.cer** extension.
5. Using an ASCII editor, for example, Notepad, copy and paste the Private Key into a file and save it as a text file.
6. Submit the CSR file (**.cer**) saved in Step 4. to the Certificate Server to obtain a signed certificate from the Server.
7. 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.
8. Once you receive the signed certificate from the Certificate Server, click **Import pasted certificate and private key**.

9. Copy and paste the signed certificate into the Certificate Request field. Paste the Private Key that was saved previously into the Private Key field.
10. Click **Browse** next to **CA file:** and select the root certificate file that was saved in Step 6.
11. Type **raritan** in the **Password** field if the CSR was generated by CC-SG. If a different application generated the CSR, use the password for that application.

Note: If the imported certificate is signed by a root and subroot CA (certificate authority), using only a root or subroot certificate will fail. To resolve this, copy and paste both root and subroot certificate into one file and then import it.

Generate Self Signed Certificate Request

Click the **Generate Self Signed Certificate** option button, and then click **Generate**. The **Generate Self Signed Certificate** window appears. Type the data needed for the self-signed Certificate into the fields. Click **OK** to generate the certificate or **Cancel** to exit the window. The Certificate and Private Key will appear encrypted in the corresponding fields of the **Certificate** screen.

Generate Certificate Signing Request	
Please provide certificate details.	
Private Key Bit Strength:	1024
Certificate Validity Period (in days):	365
Common Name:	www.raritan.com (domain name, for example, www.yoursitename.com)
Country Name (2 letters):	US
State/Province Name:	NJ
Locality:	Somerset
Organization:	Raritan, Inc.
Organization Unit:	TechSupport
Email Address:	example@raritan.com
<div>OK Cancel</div>	

Figure 179 Generate Self Signed Certificate Window

IP-ACL

This feature restricts access to CC-SG based on IP addresses. Specify an IP-access control list (IP-ACL) by entering an IP address range, the group to which it applies, and an Allow/Deny privilege.

1. On the **Administration** menu, click **Security**.

2. Click the **IP-ACL** tab.

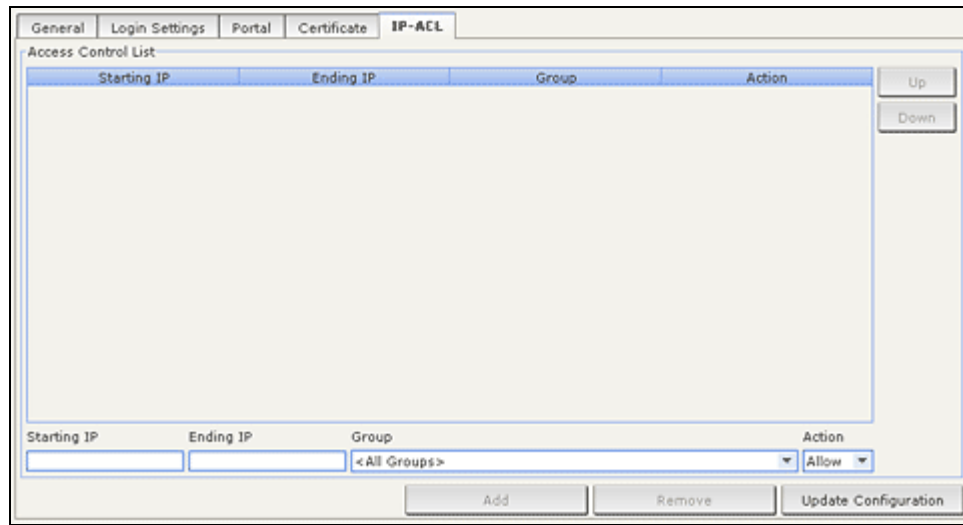


Figure 180 Security Manager IP-ACL Screen

3. To change the order of the line items in the **Access Control List**, select the line item, and then click **Up** or **Down**. Connecting users will be allowed or denied according to the first rule that applies (from top to bottom).
4. To add a new item to the list, specify a range to apply the rule to by typing the starting IP value in the **Starting IP** field, and the ending IP value in the **Ending IP** field.
5. Click the **Group** drop-down arrow to select a group to apply the rule to.
6. Click the **Action** drop-down arrow and choose to **Allow** or **Deny** the group access to the IP range.
7. Click **Add** to add the new rule to the **Access Control List**.
8. To remove any line item, select it, and then click **Remove**.
9. Click **Update Configuration** to update your system with the new access control rules.

Notification Manager

Use Notification Manager to configure an external SMTP server so notifications can be sent from CC-SG. Notifications are used to email reports that have been scheduled, email reports if users are locked out, and to email status of failed or successful scheduled tasks. Please refer to [Task Manager](#), later in this chapter for additional information. 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.

To configure an external SMTP server:

1. On the **Administration** menu, click **Notifications**.

Figure 181 Notification Manager

2. Check the **Enable SMTP Notification** checkbox.
3. Type the SMTP host in the **SMTP host** field. For hostname rules, please refer to **Terminology/Acronyms** in **Chapter 1: Introduction**.
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
- Power Management (Power On/Off/Recycle Outlet ports)
- Purge Logs
- Restart Device (does not apply to device groups)
- Restore Device Configuration (does not apply to device groups)
- Upgrade Device Firmware (individual device or device group). Note that the firmware should be made available before scheduling this task.
- Generate all reports (HTML or CSV format)

Scheduling Sequential Tasks

You may want to schedule tasks sequentially to confirm that expected behavior occurred. For example, you may want to schedule an Upgrade Device Firmware task for a given device group, and then schedule an Asset Management Report task immediately after it to confirm that the correct versions of firmware were upgraded.

Email Notifications for Tasks

Upon completion of a task, an email message can be sent to a specified recipient. You can specify where and how the email is sent, such as if it is sent securely via SSL, in the Notification Manager. Please refer to [Notification Manager](#), earlier in this chapter, for additional information.

Scheduled Reports

Reports that are scheduled are sent via email to the recipients that you specify.

All reports that have a **Finished** status are stored on CC-SG for 30 days. You can view the finished reports in HTML format by selecting **Scheduled Reports** on the **Reports** menu. Please refer to [Chapter 11: Generating Reports, Scheduled Reports](#) for additional information.

Schedule a New Task

To schedule a new task:

1. On the **Administration** menu, click **Tasks**. The Task Manager screen appears

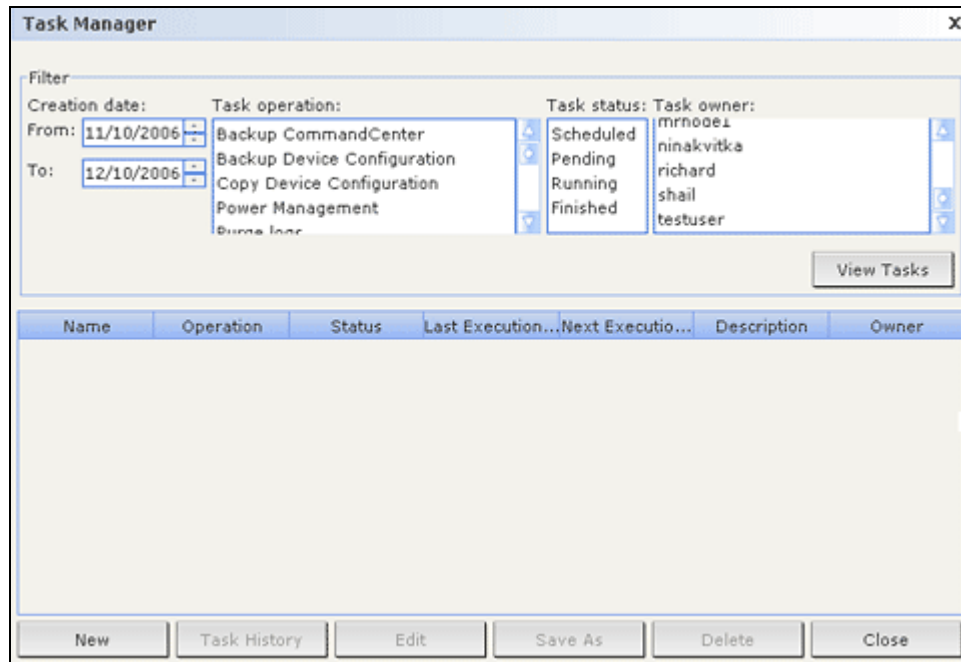


Figure 182 Task Manager

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 to be scheduled, such as **Upgrade Device Firmware**, from the list. Note that the fields requiring data will vary according to the task selected. Please refer to the following sections for details on each task:
 - [Backup CC-SG](#)
 - [Backup Device Configuration](#)
 - [Copy Device Configuration](#)
 - Group Power Control: Please refer to the CC-SG User Guide.
 - Power Management: Please refer to the CC-SG User Guide.
 - [Purge Logs](#)
 - [Restart Device](#)
 - [Restore Device Configuration](#) (does not apply to device groups)
 - [Upgrade Device Firmware](#) (individual device or device group). Note that the firmware should be made available before scheduling this task.
 - [Generate all reports](#)
6. Click the **Recurrence** tab.
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.
 - **Once**: Use the up and down arrows to select the **Start time** at which the task should begin.

- **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.
 - **Daily:** Click the radio button next to **Every day** if you want the task to repeat 7 days per week. Click the radio button next to **Every weekday** if you want the task to repeat each day from Monday through Friday.
 - **Weekly:** Use the up and down arrows to select how many weeks should elapse between task executions, then check the checkbox next to each day on which the task should recur each week that it runs.
 - **Monthly:** Type the date on which the task should execute in the **Days** field, and then check the checkbox next to each month in which the task should recur on the specified date.
 - **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. You can 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. Please refer to [Chapter 8: Adding and Managing Users and User Groups](#) for additional information. To add another email address, click **Add**, type the email address in the window that appears, and then click **OK**. By default, email is sent if the task is successful. To notify recipients of failed tasks, check the **On Failure** checkbox.
13. Click **OK** to save the task.

View a Task, Details of a Task, and Task History

To view a task:

1. On the **Administration** menu, click **Tasks**.
 2. To search for tasks, use the up and down buttons to select the date range you want to search. You can filter the list further by selecting one or more (**CTRL+click**) tasks, status, or owner from each list. Click **View Tasks** to view the list of tasks.
- To delete a task, select the task, and then click **Delete**.

Note: You cannot delete a task that is currently running.

- To view the history of a task, select the task, and then click **Task History**.
- To view details of a task, double-click a task.
- To change a scheduled task, select the task, and then click **Edit** to open the Edit Task window. Change the task specification as needed, and then click **Update**. Please refer to **Create a New Task**, earlier in this chapter, for tab descriptions.
- To create a new task based on a previously configured task, select the task you want to copy, and then click **Save As** to open the Save As Task window. The tabs are populated with the information from the previously configured task. Change the task specifications as needed, and then click **Update**. Please refer to [Schedule a New Task](#) for tab descriptions.

***Note:** If a task is changed or updated, its prior history no longer applies and the “Last Execution Date” will be blank.*

CommandCenter NOC

Adding a CommandCenter NOC (CC-NOC) to your setup will expand your target management capabilities by providing monitoring, reporting, and alert services for your serial and KVM target systems. Please refer to Raritan’s CommandCenter NOC documentation for additional information on installing and operating your CC-NOC appliance.

Important: In the following procedure, passcodes are generated. You must provide these 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.

Add a CC-NOC

***Note:** To create a valid connection, the time settings on both the CC-NOC and CC-SG should be synchronized. The best method of achieving this synchronization is to use a common NTP (Network Time Protocol) server. For this reason, the CC-NOC and CC-SG are required to be configured to use an NTP server.*

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. For additional information on CC-NOC 5.1, please refer to www.raritan.com/support. Click **Product Documentation**, and then click **CommandCenter NOC**.

Figure 183 Add CC-NOC Configuration Screen

4. Type a descriptive name for the CC-NOC in the **Name** field. Maximum length is 50 alphanumeric characters.
5. Type the IP address or hostname of the CC-NOC in the **CC-NOC IP/Hostname** field. This is a required field. For hostname rules, please refer to **Terminology/Acronyms** in **Chapter 1: Introduction**.
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. This IP range represents the range of addresses CC-SG is interested in and instructs CC-NOC to send events for these devices to CC-SG. This range is related to the discovery range that is configured in the CC-NOC. Please refer to Raritan's **CommandCenter NOC Administrator Guide** for details. Type a range, keeping the following rules in mind:

IP ADDRESS RANGE	DESCRIPTION
If CC-SG range entered here is a <i>subset</i> 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 <i>partial</i> 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 <i>superset</i> 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 <i>overlap</i> the range configured in CC-NOC...	... then , CC-NOC will not return any target device information at all.

To stop CC-NOC from monitoring a device, it can be *unmanaged*. Please refer to the **CommandCenter NOC Administrator Guide** for additional information.

Note: Use the CC-NOC Synchronization Report to view targets that the CC-SG is subscribing to. The report also displays any new targets that have been discovered by CC-NOC. Please refer to Chapter 11: Generating Reports, CC-NOC Synchronization Report for additional information.

7. 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.
8. For **Heartbeat Interval**, 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. Normally, this does not have to be changed.
9. For **Failed Heartbeat Attempts**, 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. Normally, this does not have to be changed.
10. Click **Next**.
11. Either copy and paste the passcodes into CC-NOC fields if you are the CC-NOC administrator, or submit the two passcodes to the CC-NOC administrator. As documented in the **CommandCenter NOC Administrator Guide**, the CC-NOC administrator will then enter the passcodes in CC-NOC, which initiates an exchange of security certificates.

Important: To increase security, you must enter the passcodes in CC-NOC within five minutes after they are generated on CC-SG. This will minimize the window of opportunity for intruders to breach the system with a brute-force attack. Avoid transmitting the passcodes over email or other electronic means to avoid a possible interception by automated systems. A phone call or exchange of written codes between trusted parties is better protection against automated interception.

12. Once the certificate exchange process is complete, a secure channel has been established between CC-NOC and CC-SG. The CC-NOC data will be copied to CC-SG. Click **OK** to complete the process. If the process does not complete within **5** minutes, it times out and data is not saved in CC-SG and any stored certificates are deleted. Retry the procedure again—go to Step 1. in **Add a CC-NOC** on page 201.

Note: CommandCenter NOC can only be added to standalone or primary node CC-SG servers.

Edit a CC-NOC

1. On the **Access** menu, click **CC-NOC Configuration**.
2. Highlight a CC-NOC in the list, and then click **Edit**.
3. Change the configuration as needed. Please refer to the previous section, **Add a CC-NOC**, for additional information fields.

Launch CC-NOC

To launch CC-NOC from CC-SG:

1. On the **Access** menu, click **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

To remove and unregister a CC-NOC in CC-SG, do the following.

1. On the **Access** menu, click **CC-NOC Configuration**.
2. Select the CC-NOC you want to delete from CC-SG, and then click **Delete**. You are prompted to confirm the deletion.
3. Click **Yes** to delete the CC-NOC. A **CC-NOC Deleted Successfully** message confirms that CC-NOC has been deleted.

SSH Access to CC-SG

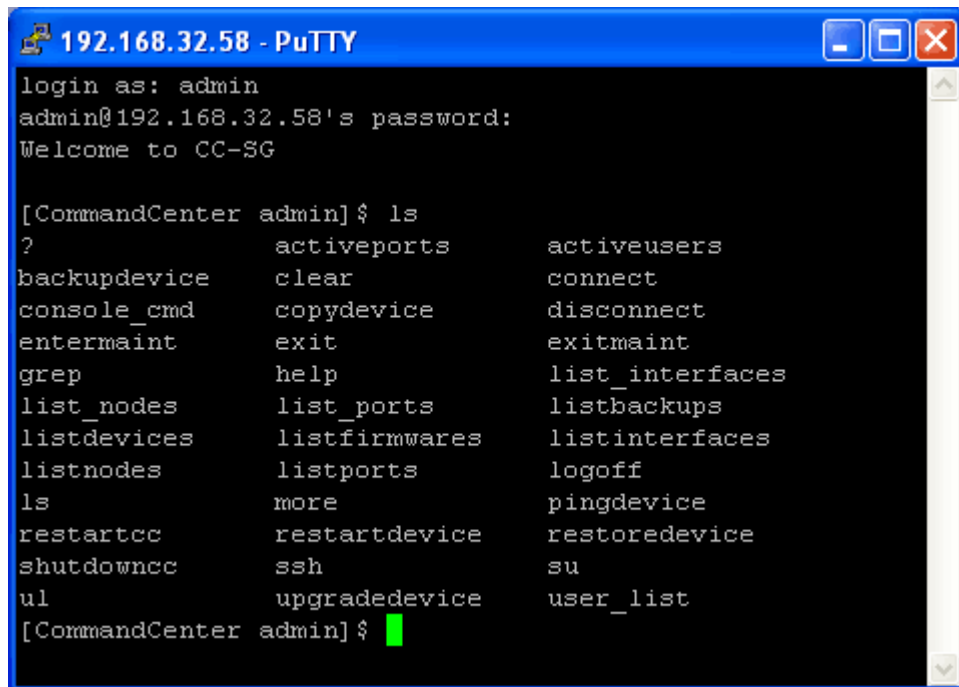
Use Secure Shell (SSH) clients, such as Putty or OpenSSH Client, to access a command line interface to SSH (v2) server on CC-SG. Only a subset of CC-SG commands is provided via SSH to administer devices and CC-SG itself.

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 logout a CC Super-User SSH user, but are able to log out all other SSH client users, including System Administrators.

To access CC-SG via SSH:

1. Launch an SSH client, such as Putty.
2. Specify the IP address of the CC-SG and specify **22** for the port, and open the connection. You can configure the port for SSH access in Security Manager. Please refer to Security Manager earlier in this chapter for additional information.
3. When prompted, log in with your CC-SG username and password.
4. A shell prompt appears. Type **ls** to display all commands available. You can type **?** or **help** to display descriptions and format for typing all commands.



```
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]$
```

Figure 184 CC-SG Commands via SSH

SSH Commands

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

COMMAND DESCRIPTION
activeports List active ports.
activeusers List active users.
backup device <[-host <host>] [-id <device_id>]> backup_name [description] Backup device configuration.
clear Clear screen.
connect [-d <device_name>] [-e <escape_char>] <[-i <interface_id>] [-n <port_name>] [port_id]> Establish a connection to a serial port. If <port_name> or <device_name> contains spaces it should be surrounded by quotes.
copydevice <[-b <backup_id>] [source_device_host]> target_device_host Copy device configuration
disconnect <[-u <username>] [-p <port_id>] [-id <connection_id>]> Close port connection.
entermaint minutes [message] Place CC-SG in maintenance mode.
exitmaint Remove CommandCenter from maintenance mode.
grep search_term Search text from piped output stream.
help View help screen.
listbackups <[-id <device_id>] [host]> List available device configuration backups.
listdevices List available devices.
listfirmwares [[-id <device_id>] [host]] List firmware versions available for upgrade.
listinterfaces [-id <node_id>] List all interfaces.
listnodes List all nodes.
listports [[-id <device_id>] [host]] List all ports.
logout [-u <username>] message Logout user
ls List commands

<code>more [-p <page_size>]</code>
Make paging
<code>pingdevice <[-id <device_id>] [host]></code>
Ping device
<code>restartcc minutes [message]</code>
Restart CC-SG
<code>restartdevice <[-id <device_id>] [host]></code>
Restart device
<code>restoredevice <[-host <host>] [-id <device_id>] > [backup_id]</code>
Restore device configuration
<code>shutdowncc minutes [message]</code>
Shutdown CC-SG.
<code>ssh [-e <escape_char>] <[-id <device_id>] [host]></code>
Open SSH connection to an SX device
<code>su [-u <user_name>]</code>
Change a user.
<code>upgradedevice <[-id <device_id>] [host]></code>
Upgrade device firmware
<code>exit</code>
Exit SSH session.

Typing the command followed by the `-h` switch displays help for that command, such as `listfirmwares -h`.

Command Tips

The following describes several nuances of the SSH commands:

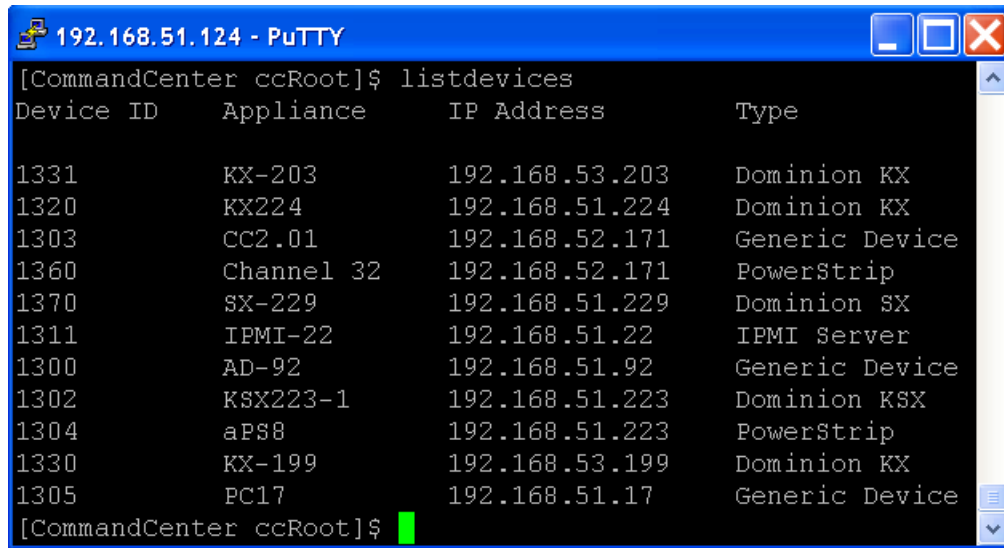
- For commands that pass an IP address, such as `upgradedevice`, you can substitute the hostname for an IP address. For hostname rules, please refer to Terminology/Acronyms in **Chapter 1: Introduction**.
- The `copydevice` and `restartdevice` commands apply only to some Raritan devices, for example, Dominion SX. IPMI servers, generic devices are not supported by these commands.

Create an SSH Connection to an SX Device

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

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

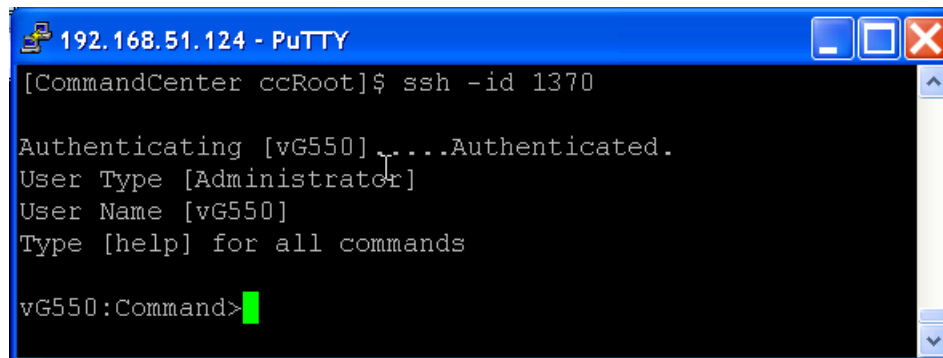
1. Type `listdevices` to ensure the SX has been added to CC-SG.



```
[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]$
```

Figure 185 Listing Devices on CC-SG

2. Connect to the SX device by typing `ssh -id <device id>`. For example, using the figure above as an example, you can connect to SX-229 by typing `ssh -id 1370`.



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

Figure 186 Access SX Device via SSH

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]$

```

Figure 187 Listinterfaces in SSH

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]$
[CommandCenter admin]$ connect -i 100
Connecting to port ...

```

Figure 188 Connecting to a Node via a Serial Out-of-Band Interface

3. Once connected to the node, type the default Escape keys of '~' followed by a dot '.' At the prompt that displays, you can enter specific commands or aliases as described below:

COMMAND	ALIAS	DESCRIPTION
quit	q	Terminates connection and returns to SSH prompt.
get_write	gw	Gets Write Access. Allows SSH user to execute commands at target server while browser user can only observe proceedings.
get_history	gh	Gets History. Displays the last few commands and results at target server.
send_break	sb	Sends Break. Breaks the loop in target server initiated by browser user.
help	?,h	Prints help screen.

Exit a Session

To exit the entire SSH connection to CC-SG, type `exit`.

Diagnostic Console

The Diagnostic Console is a standard, non-graphical interface that provides local access to CC-SG. It can be accessed from a serial or KVM port, or from Secure Shell (SSH) clients, such as PuTTY or OpenSSH Client.

Two logins are provided—one is **status**, which gives access to the Status Console, and the other is **admin**, which gives access to the Administrator Console. All login usernames and passwords are case-sensitive.

About Status Console

In the default configuration, the Status Console does not require a password. Typing **status** at the **login** prompt displays the current system information. You can use the Status Console to ascertain the health of CC-SG, the various services CC-SG uses, and the attached network.

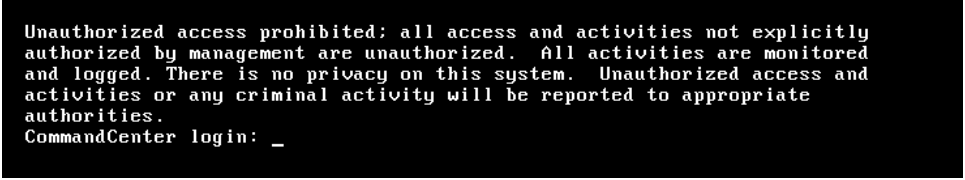
About Administrator Console

The default username/password for the Administrator Console is **admin/raritan**. The admin account allows you to set some initial parameters, provide initial networking configuration, debug log files, and perform some limited diagnostics and restarting CC-SG. The Diagnostic Console **admin** account is separate and distinct from the CC Super User **admin** account and password used in the CC-SG administrator's Director Client and the html-based Access Client. The same or different passwords may be used for both accounts. Changing one of these passwords does not affect the other.

***Note:** If accessing Diagnostic Console via SSH, the Status Console and the Administrator Console inherit the appearance settings that are configured in your SSH client and keyboard bindings, which may not agree in all aspects with this documentation.*

Accessing Diagnostic Console via VGA/Keyboard/Mouse Port

1. Attach a VGA monitor plus PS2 keyboard and mouse to the rear of the CC-SG unit.
2. Press RETURN to display a login prompt on the screen.



```
Unauthorized access prohibited: all access and activities not explicitly
authorized by management are unauthorized. All activities are monitored
and logged. There is no privacy on this system. Unauthorized access and
activities or any criminal activity will be reported to appropriate
authorities.
CommandCenter login: _
```

Figure 189 Login to Diagnostic Console

Accessing Diagnostic Console via SSH

1. Launch a SSH client, such as PuTTY, on a client PC that has network connectivity to the CC-SG.
2. Specify the IP address, or IP hostname (if CC-SG has been registered with a DNS server) of the CC-SG, and specify 23 for the port.
3. Click the button that allows you to connect. A window opens, prompting you for a login.

Accessing Status Console

A password is not required to access the Status Console, but password usage can be enforced.

1. 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>|
+-----+

```

Figure 190 Status Console

- This screen dynamically displays information about the health of the system and whether CC-SG and its sub-components are working.
- The time in the upper-right corner of the screen is the last time at which the CC-SG data was polled.
- Information on this screen updates approximately every 5 seconds.
- Type **CTRL-L** to clear the current screen and reload with updated information. You can update the screen a maximum of once per second.
- Pressing **CTRL-Q** or **CTRL-C** to exit the screen.
- The Status Console does not accept any other inputs or screen navigation. All other inputs are ignored.

The following table describes the statuses for CC-SG and the CC-SG database:

STATUS	DESCRIPTION
CC-SG Status: Up	CC-SG is available.
CC-SG Status: Down	CC-SG may be in the process of rebooting. If the Down status is continual, try restarting CC-SG.
CC-SG Status: Restarting	CC-SG is in the process of restarting.
DB Status: Responding	CC-SG's database is available.
DB Status: Down	CC-SG may be in the process of rebooting.

Accessing Administrator Console

***Note:** All information displayed in the Administrator Console is static. If the configuration changes through the CC-SG GUI or the Diagnostic Console, you must re-login to Administrator Console after the changes have taken effect to view them in Administrator Console*

1. At the login prompt, type **admin**.
2. Type the CC-SG password. The default password is **raritan**. On first login, this password expires, and you must choose a new one. Type this password and when prompted, type a new password. Please refer to **Diagnostic Console Passwords (Admin)** for information on setting password strength.
3. The main Administrator Console screen appears.

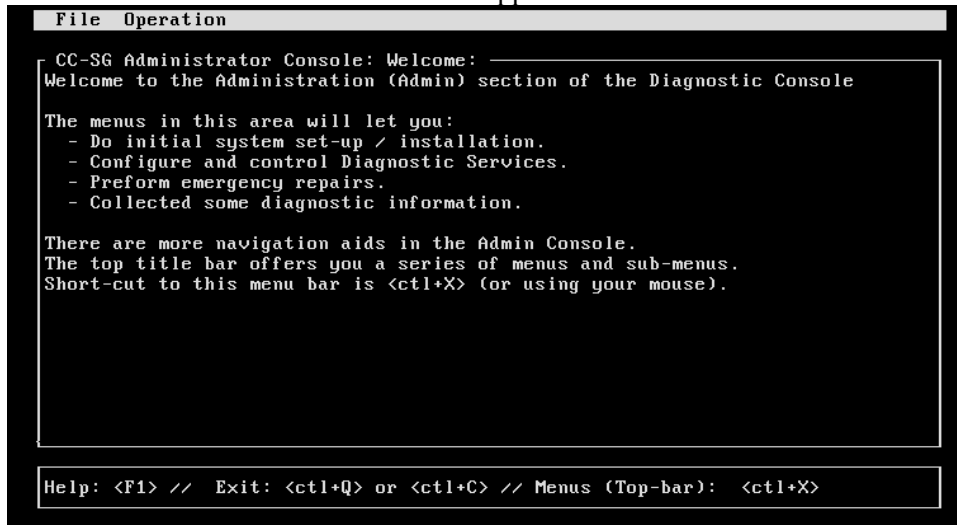


Figure 191 Administrator Console

Navigating Administrator Console

The following table provides the various navigation means within the Diagnostic Console menus. For some sessions, the mouse may also be used to navigate. However, the mouse may not work in all SSH clients or on the KVM console.

PRESS	To
CTRL+C or CTRL+Q	To exit Diagnostic Console.
CTRL+L	Clear screen and redraw the information (but the information itself is not updated nor refreshed).
TAB	Move to next available option.
SPACE	Select current option.
ENTER	Select current option.
ARROW	Move to different fields within an option.

Editing Diagnostic Console Configuration

The Diagnostic Console can be accessed via the serial port (COM1), VGA/Keyboard/Mouse (KVM) port, or from Secure Shell (SSH) clients. For each port type, you can configure whether or not **status** or **admin** logins are allowed, and whether field support can also access Diagnostic Console from the port. For SSH clients, you can also configure which port number should be used, as long as no other CC-SG service is using the desired port.

To edit Diagnostic Console configuration:

1. On the **Operation** menu, click **Diagnostic Console Config**.
2. Determine how you want the Diagnostic Console configured and accessible. There are three Diagnostic Console Access mechanisms: Serial Port (COM1), KVM Console, SSH (IP network). The Diagnostic Console offers three services: Status Display, Admin Console, Raritan Field Support. This screen allows the selection of which services are available via the various access mechanisms.
3. Type the port number you want to set for SSH access to Diagnostic Console in the **Port** field. The default port is **23**.

Important: Be careful not to completely lockout all Admin or Field Support access.

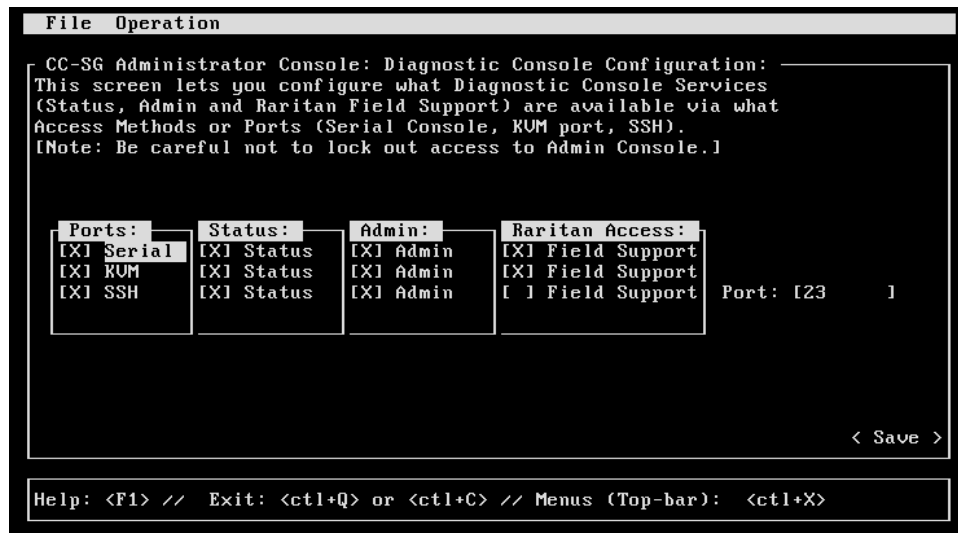


Figure 192 Edit Diagnostic Console Configuration

4. Click **Save**.

Editing Network Interfaces Configuration (Network Interfaces)

In Network Interface Configuration, you can perform initial setup tasks, such as setting the hostname and IP address of the CC-SG.

1. Click **Operation**, **Network Interfaces**, and then click **Network Interface Config**.

- If the network interfaces have already been configured, you will see a **Warning** message stating that you should use the CC-SG GUI (administrator's Director Client) to configure the interfaces. If you want to continue, click **YES**.

```

File  Operation

CC-SG Administrator Console: Network Interface Configuration:
Hostname: [CommandCenter.localdomain]
Domain Suffix: [localdomain]
Primary DNS: [ ] Secondary DNS: [ ]

Mode: <o> Primary/Backup
      <> Active/Active

Configuration: <> DHCP      Configuration: <> DHCP
               <o> STATIC    <o> STATIC

IP Address: [192.168.0.192] IP Address: [ ]
Netmask: [255.255.255.0] Netmask: [ ]
Gateway: [ ] Gateway: [ ]
Adapter Speed: <o> AUTO      Adapter Speed: <o> AUTO
Adapter Duplex: <o> FULL      Adapter Duplex: <o> FULL

< Save >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>

```

Figure 193 Editing Network Interfaces

- Type your hostname in the **Host Name** field. After you save, this field will be updated to reflect the Fully-Qualified Domain Name (FQDN), if known. For hostname rules, please refer to **Terminology/Acronyms** in **Chapter 1: Introduction**.
- In the **Mode** field, select either **Primary/Backup Mode** or **Active/Active Mode**. Please refer to **About Network** earlier in this chapter for details.
- In the **Configuration Field**, select either **DHCP** or **Static**.
 - If you choose DHCP and your DHCP server has been configured appropriately, the DNS information, the domain suffix, IP address, default gateway and subnet mask will be automatically populated once you save, and you exit and re-enter Admin Console.
 - If you choose **Static**, type an **IP Address** (required), **Netmask** (required), **Default Gateway** (optional), **Primary DNS** (optional) and **Secondary DNS** (optional), and Domain Name in **Domain Suffix** (optional).
 - Even if DHCP is being used to determine the IP configuration for an interface, a properly formatted **IP address** and **Netmask** must be provided.
- 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 $\downarrow\uparrow$ keys are used to navigate to them. Press the SPACEBAR key to select the option displayed.
- If you did not select **AUTO** for **Adapter Speed**, click **Adapter Duplex** and use the $\downarrow\uparrow$ 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**.
- Repeat these steps for the second network interface if you selected **Active/Active Mode**.
- Select **Save**. CC-SG will restart, logging off all CC-SG GUI users and terminating their sessions. A **Warning** screen will be presented informing of the impending network reconfiguration and associated CC-SG GUI user impact. Select **<YES>** to proceed.
- System progress can be monitored in a Diagnostic Console Status Screen. On the KVM port, another terminal session can be selected by typing **<ALT>+<F2>** and logging in as **status**. You may return to the original terminal session by typing **<ALT>+<F1>**. There are six available terminal sessions on **<F1>** through **<F6>**.

Ping an IP Address (Network Interfaces)

Use ping to check that the connection between CC-SG computer and a particular IP address is working correctly.

Note: Some sites explicitly block ping requests. Verify that the target and intervening network allow pings before assuming that there is a problem.

1. Click **Operation, Network Interfaces**, and then click **Ping**.
2. Enter the IP address or hostname (if DNS is appropriately configured on the CC-SG) of the target you want to check in the **Ping Target** field.
3. (Optional) Select:

OPTION	DESCRIPTION
Show other received ICMP packets	Verbose output, which lists other received ICMP packets in addition to ECHO_RESPONSE packets. Rarely seen.
No DNS Resolution	Does not resolve addresses to host names.
Record Route	Records route. Sets the IP record route option, which will store the route of the packet inside the IP header.
Use Broadcast Address	Allows pinging a broadcast message.
Adaptive Timing	Adaptive ping. Interpacket interval adapts to round-trip time, so that effectively not more than one unanswered probes present in the network. Minimal interval is 200 msec.

4. (Optional) Type values for how many seconds the ping command will execute, how many ping requests are sent, and the size for the ping packets (default is 56, which translates into 64 ICMP data bytes when combined with 8 bytes of ICMP header data). If left blank, defaults will be used.
5. Click **Ping** in the bottom right-hand corner of the window. 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, there is a breakdown somewhere between your computer and the domain. In this case, the next step is to perform a traceroute – see the next section.
6. Press **CTRL+C** to terminate the ping session. The system prompts with a “Return?” before returning to the Diagnostic Console (so that any output can be viewed and analyzed as appropriate).

Note: Pressing **CTRL+Q** displays a statistics summary for the session so far and continues to ping the destination.

Using Traceroute (Network Interfaces)

Traceroute is often used for network troubleshooting. By showing a list of routers traversed, it allows you to identify the path taken from your computer to reach a particular destination on the network. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes. This can help identify routing problems or firewalls that may be blocking access to a site.

To perform a traceroute on an IP address or hostname:

1. Click **Operation, Network Interfaces**, then **Traceroute**.
2. Enter the IP address or hostname of the target you wish to check in the **Traceroute Target** field.

3. (Optional) Select:

OPTION	DESCRIPTION
Verbose	Verbose output, which lists received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs.
No DNS Resolution	Does not resolve addresses to host names.
Use ICMP (vs. normal UDP)	Use ICMP ECHO instead of UDP datagrams.

- (Optional) Type values for how many hops the traceroute command will use in outgoing probe packets (default is 30), the UDP destination port to use in probes (default is 33434), and the size for the traceroute packets. If left blank, defaults will be used.
- Click **Traceroute** in the bottom right-hand corner of the window.
- Press **CTRL+C** or **CTRL+Q** to terminate the traceroute session. A **Return?** prompt appears; press **ENTER** to return to the Traceroute menu. The **Return?** prompt also appears when Traceroute terminates due to “destination reached” or “hop count exceeded” events occur.

Editing Static Routes (Network Interfaces)

In Static Routes, you can view the current IP routing table and modify, add, or delete routes. Careful use and placement of static routes may actually improve the performance of your network, allowing you to conserve bandwidth for important business applications and may be useful for Active/Active network settings where each interface is attached to a separate IP domain—see section About Network in Chapter 13: Advanced Administration for additional information. Click with the mouse or use the **TAB**, arrow keys to navigate and press the **Enter** key to select a value.

To view or change static routes:

- Click **Operation**, **Network Interfaces**, and then click **Static Routes**.
- The current IP routing table is displayed. You can add a host or network route, or delete a route. The **Refresh** button updates the routing information in the above table.

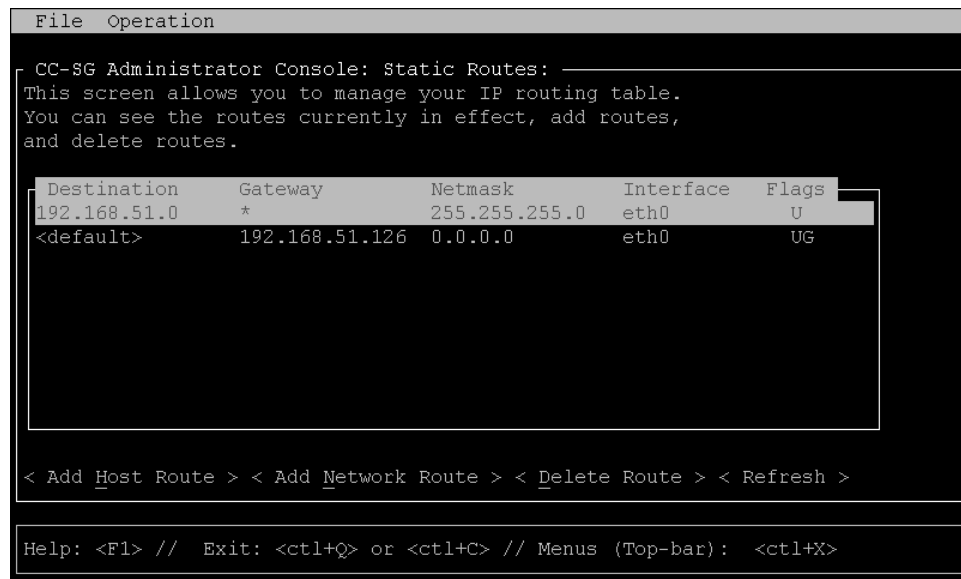


Figure 194 Editing Static Routes

Viewing Log Files (Admin)

You can view one or more log files simultaneously via LogViewer, which allows browsing through several files at once, to examine system activity.

To view log files:

1. Click **Operation, Admin**, then **System Logfile Viewer**.
2. The Logviewer screen is divided into 4 main areas (see screen below):
 - 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 (details below).
 - Export / View selector.
3. Click with the mouse or use the arrow keys to navigate and press the **SPACEBAR** key to select a log file, marking it with an **X**. You can view more than one log file at a time.

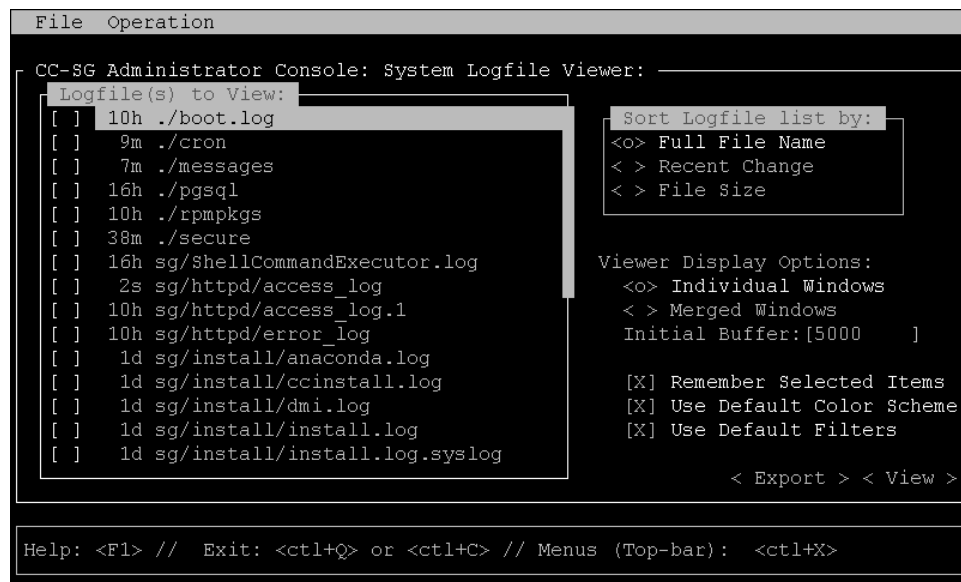


Figure 195 Selecting Log Files to View

The Logfile list is only updated when the associated list becomes active (e.g., user enters the logfile list area) or when a new Sort by option is selected. File names are either preceded by a timestamp indicating how recently the logfile has received new data or the file size of the logfile. Timestamps are s → seconds, m → minutes, h → hours and d → days. File sizes are B → Bytes, K → Kilo (1000) Bytes, M → Mega (1,000,000) Bytes and G → Gigabytes. When the Sort By options is either Full Name or Recent Change, timestamps are used, and file sizes are used for File Sizes.

The “Sort Logfile list by:” window is a set of radio-button (e.g., mutually exclusive) and controls the order of how logfiles are displayed in the “Logfile to View” window.

OPTION	DESCRIPTION
Individual Windows	Display the selected logs in separate sub-windows.
Merged Windows	Merge the selected logs into one display window.
Initial Buffer	Sets initial buffer or history size. 5000 is default. This system is configured to buffer all the new information that comes along.
Remember Selected Items	If this box is checked, the current logfile selections (if any) will be remembered. Otherwise, selection is reset each time a new Logfile list is generated. This is useful if you want to step thorough files.
Use Default Color Scheme	If this box is checked, some of the logfiles will be viewed with a standard color scheme. Note: multitail commands can be used to change the color scheme once the logfile(s) are being viewed.
Use Default Filters	If this box is checked, some of the logfiles will have automatic filters applied.
Export	This option packages up all the selected logfiles and makes them available via Web access so that they can be retrieved and forwarded to Raritan Technical Support. Access to the contents of this package is not available to customer. Exported logfiles will be available for up to 10 days, and then the system will automatically delete them.
View	View the selected log(s).

When **View** is selected with Individual Windows, the LogViewer displays:

```

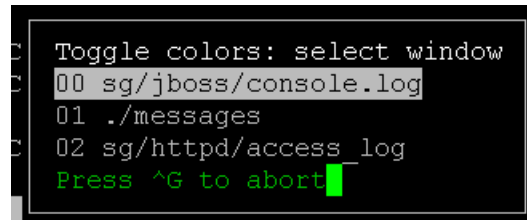
15:30:54,366 INFO [ChannelSocket] JK: ajp13 listening on /0.0.0.0:8009
15:30:54,378 INFO [JkMain] Jk running ID=0 time=0/26 config=null
15:30:54,480 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-9443
15:30:54,756 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-0.0.0.0-8080
15:30:54,801 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

```

Figure 196 Selecting Log Files to View

- While viewing log files, type **q**, **CTRL-Q** or **CTRL+C** to return to the previous screen.

- If desired, 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 if you have chosen to view several.

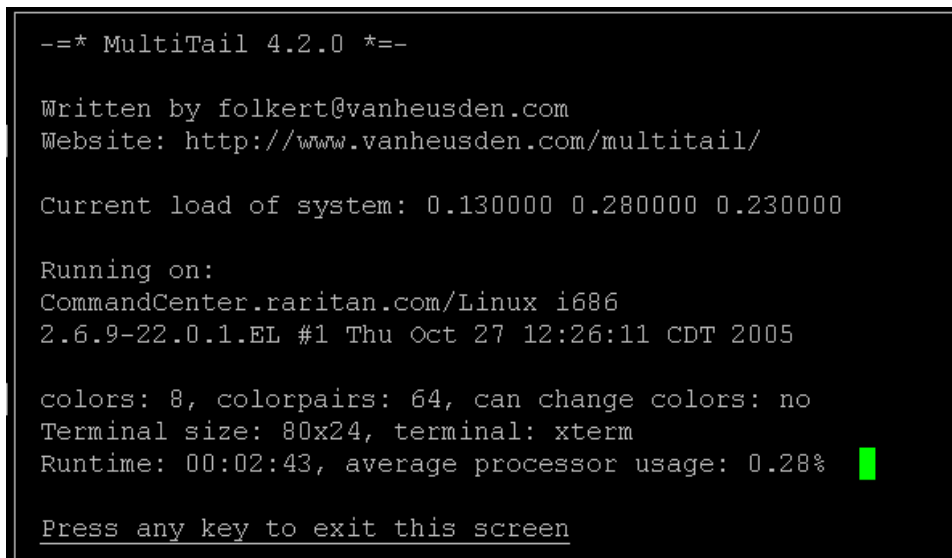


```
Toggle colors: select window
00 sg/jboss/console.log
01 ./messages
02 sg/httpd/access_log
Press ^G to abort
```

Figure 197 Changing Colors in Log Files

- 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.



```
--* MultiTail 4.2.0 *--

Written by folkert@vanheusden.com
Website: http://www.vanheusden.com/multitail/

Current load of system: 0.130000 0.280000 0.230000

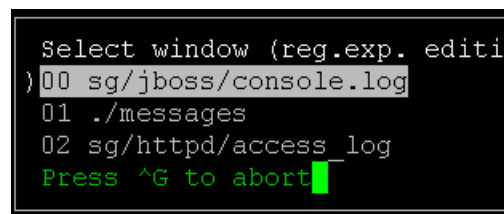
Running on:
CommandCenter.raritan.com/Linux i686
2.6.9-22.0.1.EL #1 Thu Oct 27 12:26:11 CDT 2005

colors: 8, colorpairs: 64, can change colors: no
Terminal size: 80x24, terminal: xterm
Runtime: 00:02:43, average processor usage: 0.28%

Press any key to exit this screen
```

Figure 198 Displaying Information

- If desired, you can filter the log file with a regular expression. 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
```

Figure 199 Adding Expressions in Log Files

8. Type **a** to add a regular expression. For example, if you want 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

01] . 46:02
Edit regular expression:
WARN

Usage of regexp? (match, v do not match
Color, Bell, bell + colorize, execute)

02] s 46:02

```

Figure 200 Specifying a Regular Expression for a Log File

9. Select **F1** to get help on all LogViewer options. Pressing **CTRL+C** and **CTRL+Q** terminates this LogViewer session.

Restarting CC-SG (Admin)

You can restart CC-SG, which will log off all current CC-SG users and terminate their sessions to remote target servers.

Important: It is HIGHLY recommended to restart CC-SG in the CC-SG GUI instead, unless it is absolutely necessary to restart it here. Please refer to **Restart CC-SG in Chapter 12: System Maintenance** for additional information. Restarting CC-SG in Diagnostic Console will NOT notify CC-SG GUI users that it is being restarted.

To restart CC-SG:

1. Click **Operation**, **Admin**, and then click **CC-SG Restart**.
2. Either click **Restart CC-SG Application** or press **ENTER**. Confirm the restart in the next screen to proceed.

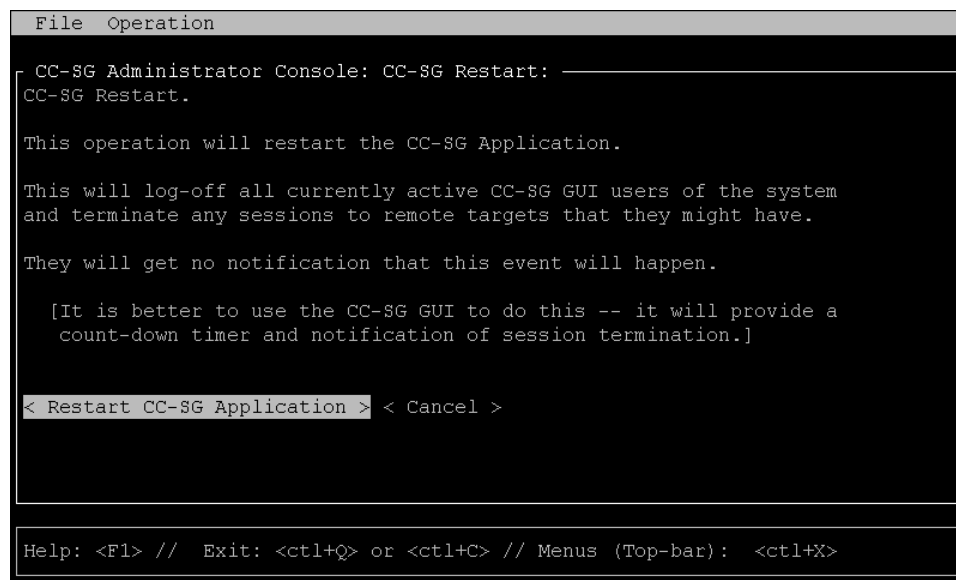


Figure 201 Restarting CC-SG in Diagnostic Console

Rebooting CC-SG (Admin)

This option will reboot the entire CC-SG, which simulates a power cycle. Users will not receive a notification. CC-SG, SSH, and Diagnostic Console users (including this session) will be logged off. Any connections to remote target servers will also be terminated.

To reboot CC-SG,

1. Click **Operation**, **Admin**, and then click **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.

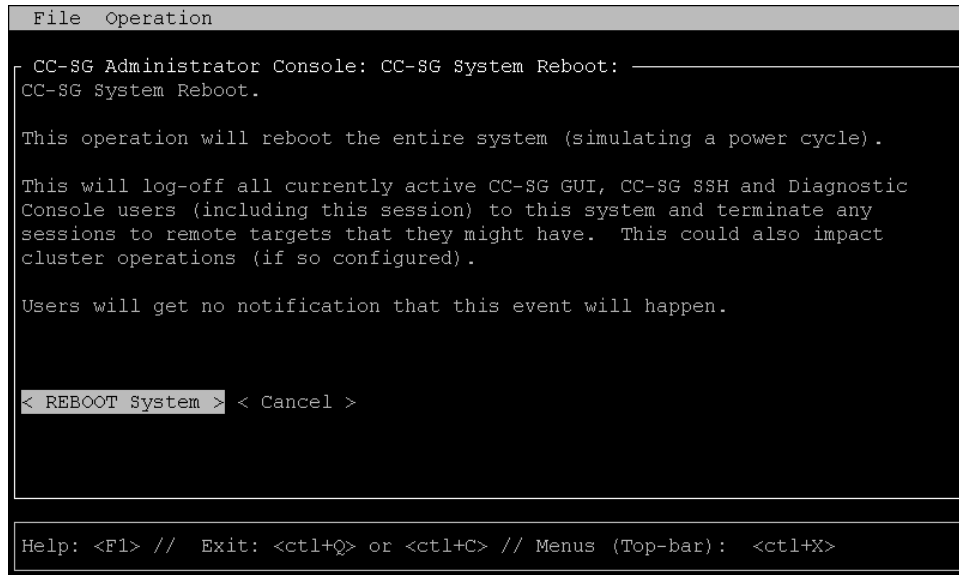


Figure 202 Rebooting CC-SG in Diagnostic Console

Powering Off the CC-SG System (Admin)

This option will power down the entire CC-SG. Users will not receive a notification. CC-SG, SSH, and Diagnostic Console users (including this session) will be logged off. Any connections to remote target servers will also be terminated. The only way to power the CC-SG unit back on is to press the power button on the front panel of the unit.

To power off the CC-SG:

1. Click **Operation**, **Admin**, and then click **CC-SG System Power OFF**.
2. Either click **Power OFF the CC-SG** or press **ENTER** to remove AC power from the CC-SG. Confirm the power down operation in the next screen to proceed.

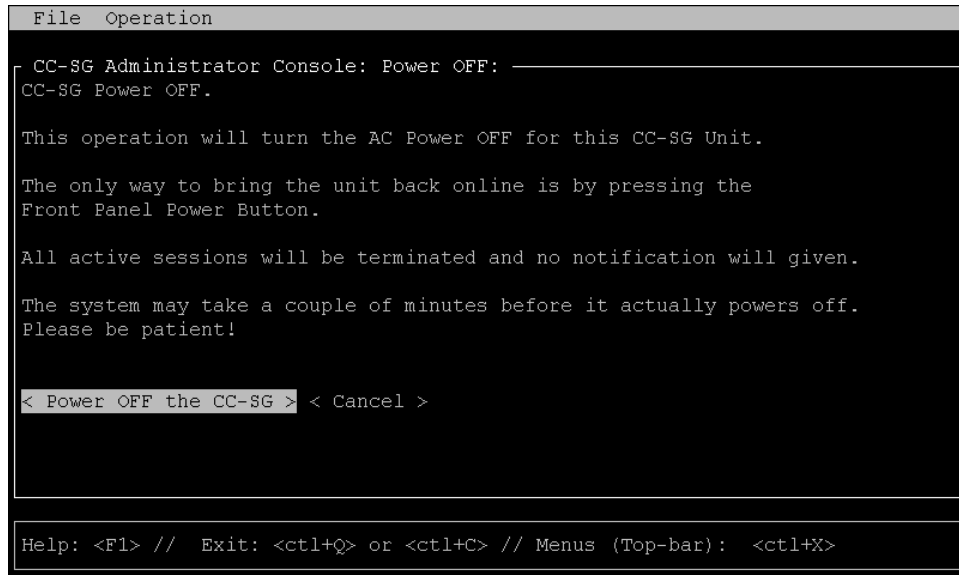


Figure 203 Power Down CC-SG in Diagnostic Console

Resetting CC-SG GUI Admin Password (Admin)

This option will reset the password for the admin account CC-SG GUI user to the documented factory default value.

Note: This is not the password for the Diagnostic Console admin user. Please refer to *DiagCon Passwords* below for information about changing this account's password.

To reset the CC-SG GUI admin password:

1. Click **Operation**, **Admin**, and then click **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.

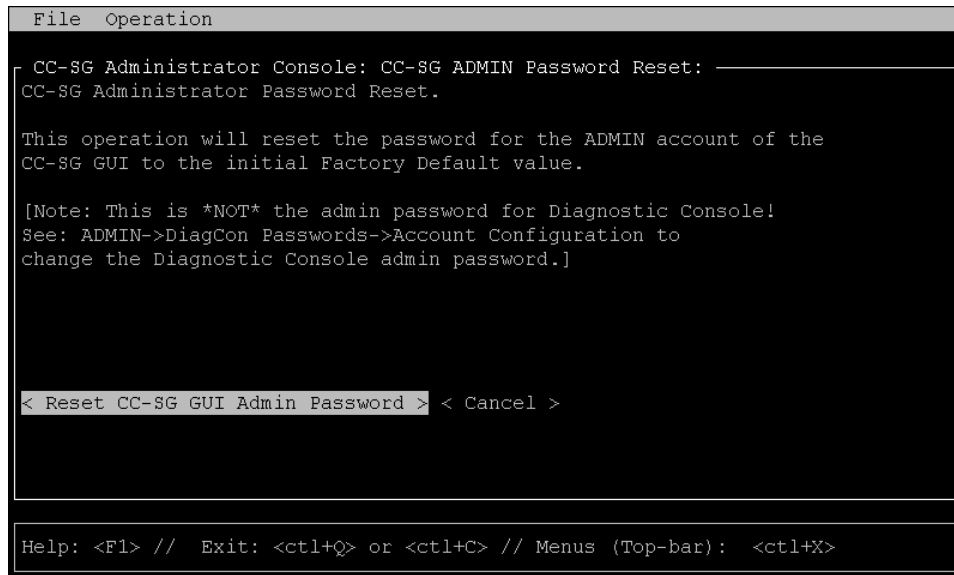


Figure 204 Admin Password Reset for CC-SG GUI in Diagnostic Console

Resetting CC-SG Factory Configuration (Admin)

This option will reset all or parts of the CC-SG system back to their factory default values. All active CC-SG users will be logged off without notification, and SNMP processing will stop. It is highly recommended that CC-SG be placed in **Maintenance Mode** prior to initiating this operation. If possible, reset CC-SG from within the administrator's Director Client, rather than from the Diagnostic Console. The Director Client Reset option can perform all functions listed here, except for resetting Network values.

1. On the **Operation** menu, click **Admin**, and then click **Factory Reset**. The following screen with seven **Reset Options** appears.

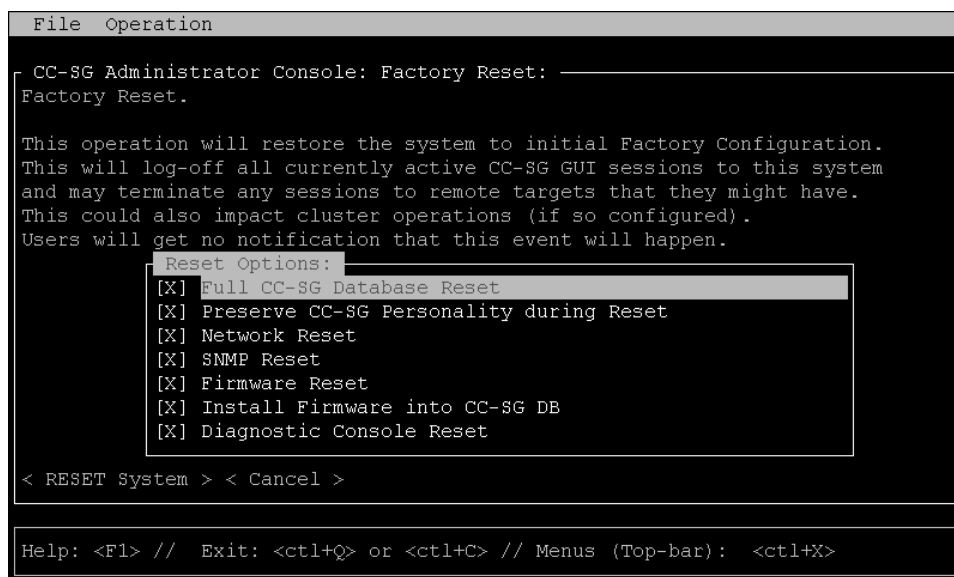


Figure 205 Reset CC-SG Factory Configuration

OPTION	DESCRIPTION
Full CC-SG Database Reset	Selecting this option completes removes the existing CC-SG Database and builds a new version from scratch loading it with all the Factory Default values.
Preserve CC-SG Personality during Reset	<p>This option is only valid and effective if the previous option is also selected. As the CC-SG Database is rebuilt (in the previous option), the following values are migrated to the new version of the database (if they can be read and are available; otherwise default values will be used). An attempt to keep the following information is made. Default value in brackets.</p> <ul style="list-style-type: none"> ▪ Secure Communication [unsecured] between PC Clients and CC-SG ▪ Strong Password Check [off] select if strong password enforcement is enabled. ▪ Direct vs. Proxy Connections [Direct] selects if PC clients use direct or proxy connections to Out-of-Band nodes ▪ Inactivity Timer [1800] the time before idle sessions log out ▪ Modem Setting [10.0.0.1/10.0.0.2/<none>] the setting for the modem Server IP Address, Client IP Address, and callback phone number.
Network Reset	<p>This option sets the networking 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>Resets SNMP configuration to Factory Defaults</p> <ul style="list-style-type: none"> ▪ Port: 161 ▪ Read-only Community: public ▪ Read-write Community: private ▪ System Contact, Name, Location: <empty> ▪ SNMP Trap Configuration ▪ SNMP Trap Destinations
Firmware Reset	Removes uploaded Firmware files and restores the default versions into filesystem repository. Does not change the CC-SG DB.
Install Firmware into CC-SG DB	Loads Firmware files found in the filesystem-based repository into the CC-SG DB.
Diagnostic Console Reset	Restores Diagnostic Console to Factory Configuration, Account Settings and Defaults

Diagnostic Console Passwords (Admin)

This option provides the ability to configure the strength of passwords (status and admin) and allows you to configure password attributes, such as, the setting maximum number of days that must lapse before you need to change the password, which should be done via the Account Configuration menu. The operation in these menus only applies to Diagnostic Console accounts (status and admin) and passwords – it has no effect on the regular CC-SG GUI accounts or passwords.

Password Configuration

1. Click **Operation, Admin, DiagCon Passwords**, and then click **Password Configuration**.
2. In the Password History Depth field, type the number of passwords that will be remembered. The default setting is **5**.

```

File  Operation

CC-SG Administrator Console: Password Settings:
Use this screen to update how all subsequent Diagnostic Console (only!)
password operations will work.  You can set the type of passwords (regular,
strong or random) that the system will let the user use on any subsequent
password change operation.  Also, the number of passwords henceforth that
the system will remember and not let the user duplicate or reuse.

Password Configuration:

Password History Depth: [5 ]

Password Type & Parameters:
<O> Regular
< > Random  Size:[20 ] Retries:[10 ]
< > Strong  Retries:[3  ] DiffOK:[4  ] MinLEN:[9  ]
           Digits: [-1 ] Upper: [-1 ] Lower: [-1 ] Other:[-1 ]

                                     < Update >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> //  Menus (Top-bar):  <ctl+X>

```

Figure 206 Configuring Password Settings

3. Select either **Regular**, **Random**, or **Strong** for the **admin** and **status** (if enabled) passwords.

PASSWORD SETTING	DESCRIPTION
Regular	These are standard. Passwords must be longer than 4 characters with few restrictions. This is the system default password configuration.
Random	Provides randomly generated passwords. Configure the maximum password size in bits (minimum is 14, maximum is 70, default is 20) and number of retries (default is 10), which is the number of times you will be asked if you want to accept the new password. You can either accept (by typing in the new password twice) or reject the random password. You cannot select your own password.
Strong	Enforce strong passwords. Retries is the number of times you are prompted before an error message is issued. DiffOK is how many characters can be the same in the new password relative to the old. MinLEN is the minimum length of characters required in the password. Specify how many Digits, Upper-case letters, Lower-case letters, and Other (special) characters are required in the password. Positive numbers indicate the maximum amount of “credit” of this character class can be accrued towards the “simplicity” count. Negative numbers implies that the password MUST have at least that many characters from this given class. Thus, numbers of -1 means that every password must have at least one digit in it.

Account Configuration

By default, the **status** account does not require a password, but you can configure it to require one. Other aspects of the **admin** password can be configured and the Field Support accounts can be enabled or disabled.

- To configure accounts, click **Operation**, **Admin**, **DiagCon Passwords**, and then click **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	< > Disabled
	< > Enabled	< > Enabled	< > Enabled
	< > 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>

Figure 207 Configuring Accounts

This screen is split into three main areas:

- The top displays read-only information about the accounts on the system.
 - The middle section displays the various parameters related and pertinent to each ID, along with a set of buttons, to allow the parameters to be updated or new passwords provided for the accounts.
 - The final area restores the password configuration to Factory Defaults (or how the system was initially shipped).
3. If you want to require a password for the **Status** account, select **Enabled** underneath it.
 4. For the **Admin** and **Status** accounts, you can configure:

SETTING	DESCRIPTION
User \ User Name	(Read-only). This is the current user name or ID for this account.
Last Changed	(Read-only). This is the date of the last password change for this account.
Expire	(Read-only). Tells the day that this account must change its password.
Mode	A configurable option if the account is disabled (no login allowed), or enabled (authentication token required), or access is allowed and no password is required. (Do not lock out both the Admin and FS1 accounts at the same time, or you cannot use Diagnostic Console.)
Min Days	The minimum number of days after a password has been changed before it can be changed again. Default is 0 .
Max Days	The maximum number of days the password will stay in affect. Default is 99999 .
Warning	The number of days that warning messages are issued before the password expires.
Max # of Logins	The maximum number of concurrent logins the account will allow. Negative numbers indicate no restrictions (-1 is the default for status login). 0 means no one can log in. A positive number defines the number of concurrent users who can be logged in (2 is the default for admin login).
UPDATE	Saves any changes that have been made for this ID.
New Password	Enter a new password for the account.

Displaying Disk Status (Utilities)

This option displays status of CC-SG disks, such as size of disks, if they are active and up, state of the RAID-1, and amount of space currently used by various file systems.

To display disk status of the CC-SG:

1. Click **Operation**, **Utilities**, and then click **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>

```

Figure 208 Displaying Disk Status of CC-SG in Diagnostic Console

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]).

Displaying Top Display (Utilities)

This option displays the list of processes and their attributes that are currently running on CC-SG, as well as overall system health.

1. To display the processes running on the CC-SG, click **Operation**, **Utilities**, and then click **Top Display**.
2. View the total running, sleeping, total number, and processes that have stopped.

```

top - 20:19:27 up 1 day, 23:33,  6 users,  load average: 0.55, 0.27, 0.20
Tasks: 117 total,  1 running, 116 sleeping,  0 stopped,  0 zombie
Cpu(s):  5.6% us,  8.6% sy,  0.0% ni, 85.7% id,  0.0% wa,  0.0% hi,  0.0% si
Mem:   2076088k total, 1351804k used,  724284k free,  245720k buffers
Swap:  2031608k total,    0k used,  2031608k free,  795588k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
20271 sg        16   0  275m  26m  11m  S   1.7   1.3   0:14.09  jsvc
4990 root      23   0  5452 3460 1780  S   0.3   0.2   4:30.55  status-poller.p
12634 admin    16   0  2584  960  748  R   0.3   0.0   0:00.01  top
   1 root      16   0  2280  544  468  S   0.0   0.0   0:00.79  init
   2 root      34  19    0    0    0  S   0.0   0.0   0:00.24  ksoftirqd/0
   3 root       5 -10    0    0    0  S   0.0   0.0   0:00.68  events/0
   4 root       5 -10    0    0    0  S   0.0   0.0   0:00.00  khelper
   5 root      15 -10    0    0    0  S   0.0   0.0   0:00.00  kacpid
  25 root       5 -10    0    0    0  S   0.0   0.0   0:00.00  kblockd/0
  35 root      15   0    0    0    0  S   0.0   0.0   0:00.12  pdflush
  36 root      15   0    0    0    0  S   0.0   0.0   0:01.13  pdflush
  38 root      13 -10    0    0    0  S   0.0   0.0   0:00.00  aio/0
  26 root      15   0    0    0    0  S   0.0   0.0   0:00.00  khubd
  37 root      15   0    0    0    0  S   0.0   0.0   0:00.02  kswapd0
 111 root      25   0    0    0    0  S   0.0   0.0   0:00.00  kseriod
 181 root       5 -10    0    0    0  S   0.0   0.0   0:00.00  ata/0
 183 root      22   0    0    0    0  S   0.0   0.0   0:00.00  scsi_eh_0

```

Figure 209 Displaying CC-SG Processes in Diagnostic Console

3. Type **h** to bring up an extensive help screen for the top command. The standard **F1** help key is not operational here. To return to the Admin Console, type **CTL+Q** or **CTL+C**.

Displaying NTP (Network Time Protocol) Status (Utilities)

This option displays the status of the NTP time daemon if it is configured and running on CC-SG.

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

1. Click **Operation, Utilities**, and then click **NTP Status Display**.
2. The NTP Daemon can only be configured in the CC-SG administrator's Director Client. If NTP is not enabled and configured properly, the following will be displayed:

```

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>

```

Figure 210 NTP not configured in CC-SG GUI

3. If NTP is properly configured and running on the CC-SG, a display similar to this should be generated:

```

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>

```

Figure 211 NTP running on the CC-SG GUI

4. Selecting **Refresh** will update the information on this page.

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.



Figure 212 Serial Admin Port on G1



Figure 213 Serial Admin Port on E1

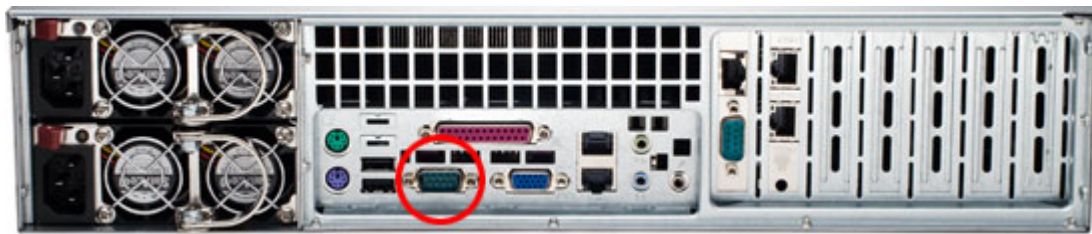


Figure 214 Serial Admin Port on E1

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.

This page intentionally left blank.

Appendix A: Specifications (G1, V1, and E1)

G1 Platform

General Specifications

Form Factor	1U
Dimensions (DxWxH)	22.1" x 17.32" x 1.75" 563mm x 440mm x 44mm
Weight	24.07lb (10.92kg)
Power	Redundant, hot-swappable power supplies, auto-sensing 110/220 V – 2.0A
Mean Time Between Failure (MTBF)	38,269 hours
KVM Admin Port	(DB15 + PS2 Keyboard/Mouse)
Serial Admin Port	DB9
Console Port	N/A

Hardware Specifications

Processor	Intel® Pentium® III 1 GHz
Memory	512 MB
Network Interfaces	(2) 10/100 Ethernet (RJ45)
Hard Disk & Controller	(2) 40-GB IDE @7200 rpm, RAID 1
CD-ROM Drive	CD-ROM 40x Read Only

Environmental Requirements

OPERATING	
Humidity	20% - 85% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (est.)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A
NON-OPERATING	
Temperature	0 - 30 deg C; 32 – 104 deg F
Humidity	10% - 90% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (est.)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

V1 Platform

General Specifications

Form Factor	1U
Dimensions (DxWxH)	24.21" x 19.09" x 1.75" 615mm x 485mm x 44mm
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

Hardware Specifications

Processor	AMD Opteron 146
Memory	2 GB
Network Interfaces	(2) 10/100/1000 Ethernet (RJ45)
Hard Disk & Controller	(2) 80-GB SATA @ 7200 rpm, RAID 1
CD-ROM Drive	DVD-ROM

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, 0.38mm, 1 minutes per cycle; 30 minutes for each axis(X,Y,Z)
Shock	N/A
NON-OPERATING	
Temperature	-40° - +60° (-40° - 140°)
Humidity	5% - 95% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (Estimated)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X,Y,Z)
Shock	N/A

E1 Platform

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 degree 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

Hardware Specifications

Processor	(2) AMD Opteron 250 2.4G 1MB processors
Memory	4 GB
Network Interfaces	Intel PRO/1000 PT Dual Port Server Adapter
Hard Disk & Controller	(2) WD740ADFD SATA 74GB 10K RPM 16MB cache
CD-ROM Drive	DVD-ROM

Environmental Requirements

OPERATING	
Humidity	5-90%, non-condensing
Altitude	Sea level to 7,000 feet
Vibration	10 Hz to 500 Hz sweep at 0.5 g constant acceleration for one hour on each of the perpendicular axes X, Y, and Z
Shock	5 g for 11 ms with a ½ sine wave for each of the perpendicular axes X, Y, and Z
NON-OPERATING	
Temperature	-40-70 degree 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 $\frac{1}{2}$ sine wave for each of the perpendicular axes X, Y, and Z
--------------	----------------------------------------------------------------------------------------------

Appendix B: CC-SG and Network Configuration

Introduction

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

As depicted in the diagram below, a typical CC-SG deployment may have none, some, or all of the features, for example, a firewall or a Virtual Private Network (VPN). The tables that follow disclose the protocols and ports that are needed by CC-SG and its associated components, which are essential to understand especially if firewalls or VPNs are present in your network and access and security policies are to be enforced by the network.

Executive Summary

In the sections below, a very complete and thorough analysis of the communications and port usage by CC-SG and its associated components is provided. For those customers who just want to know what ports to open on a firewall to allow access to CC-SG and the targets that it controls, the following ports should be opened:

Port Number	Protocol	Purpose
80	TCP	HTTP Access to CC-SG
443	TCP	HTTPS (SSL) Access to CC-SG
8080	TCP	CC-SG <-> PC Client
2400	TCP	Node Access (Proxy Mode & In-Band Access)
5000 ¹	TCP	Node Access (Direct Mode)
51000 ¹	TCP	SX Target Access (Direct Mode)

This list can be further trimmed:

- Port 80 can be dropped if all access to the CC-SG is via HTTPS addresses.
- Ports 5000 and 51000 can be dropped if CC-SG Proxy mode is used for any connections from the firewall(s).

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

In the sections below, the details about these access methods and ports are provided along with configuration controls and options.

¹ 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.

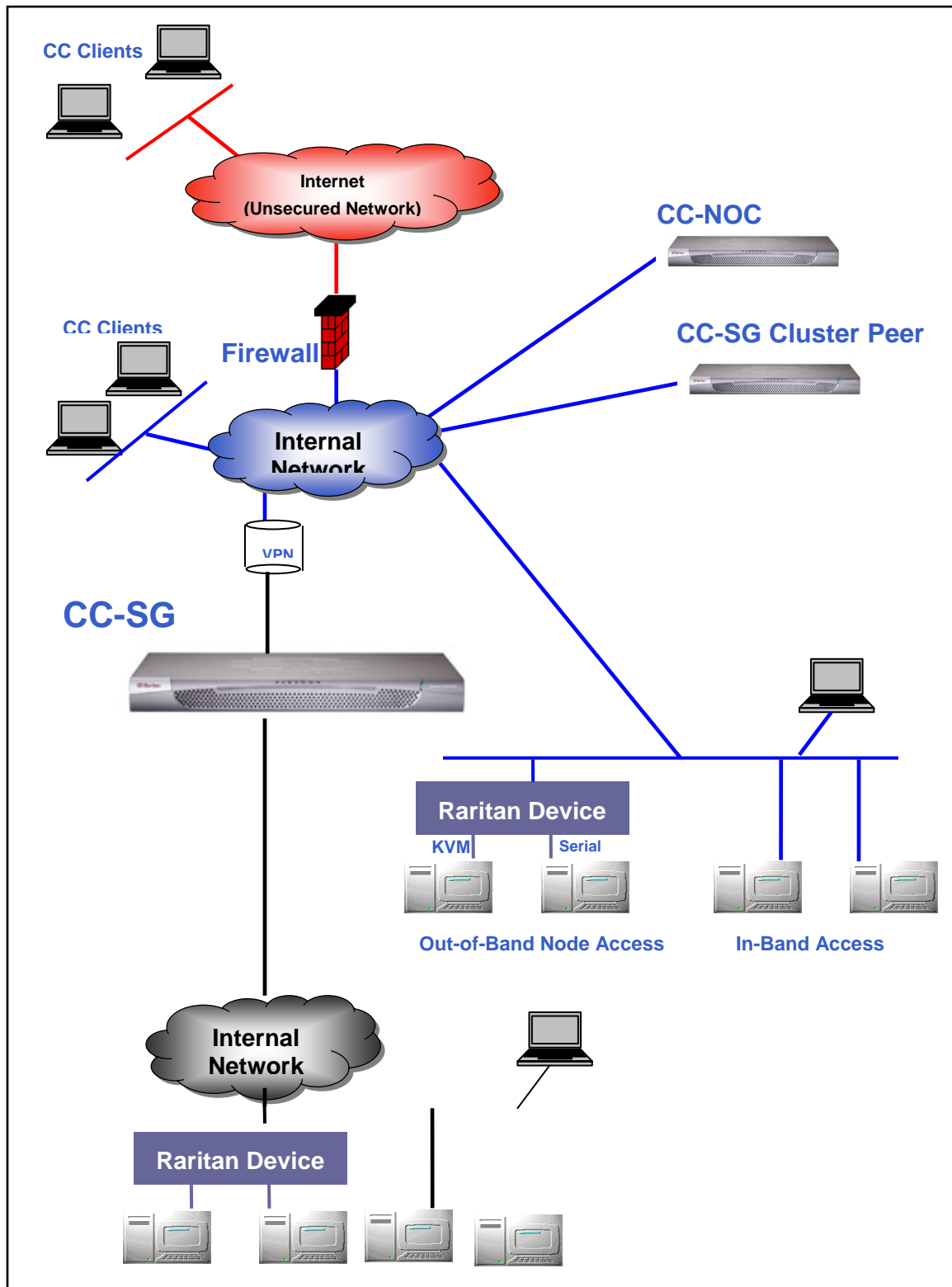


Figure 215 CC-SG Deployment Elements

CC-SG Communication Channels

The communication channels are partitioned as follows:

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

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

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

CC-SG and Raritan Devices

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

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

CC-SG Clustering

When the optional CC-SG clustering feature is used (that is, two CC-SG units are inter-connected and function as one unit), the following ports must be available for the inter-connecting sub-networks. {If the optional clustering feature is not used, none of these ports need to be made available in the network.}

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

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

Access to Infrastructure Services

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

Communication Direction	Port Number	Protocol	Configurable?
DHCP Server → CC-SG	68	UDP	no
CC-SG → DHCP Server	67	UDP	no
NTP Time Server ↔ CC-SG	123	UDP	no
CC-SG → DNS	53	UDP	no

PC Clients to CC-SG

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

- Web / Java Applet CC-SG GUI interface
- CC-SG Command Line Interface via SSH
- CC-SG Diagnostic Console

Web access via the CC-SG GUI is the primary means for users and administrators to connect to CC-SG. The other two modes, CLI and Diagnostic Console, are less frequently used. These modes require the following networking configuration:

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

PC Clients to Nodes

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

Another facet of PC client to target communication is whether:

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

Communication Direction	Port Number	Protocol	Configurable?
Client → CC-SG via Proxy → Target	2400 (on CC-SG)	TCP	no
Client → Raritan Target (Direct Mode)	5000 (on device)	TCP	yes
Client → Dominion SX → (Direct Mode)	51000	TCP	yes

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

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

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

CC-SG & SNMP

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

Communication Direction	Port Number	Protocol	Configurable?
SNMP Manager → CC-SG	161	UDP	yes
CC-SG → SNMP Manager	162	UDP	yes

CC-SG & CC-NOC

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

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

CC-SG Internal Ports

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

1088, 1098, 2222, 4444, 4445, 8009, 8083 and 8093

In addition to these ports, CC-SG may have a couple of TCP and UDP ports in the 32xxx (or higher) range open. 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 possibly Port Address Translation (PAT), then Proxy mode should be used for all connections that use this firewall. Moreover, the firewall must be configured for external connections to Ports 80(non-SSL)/443(SSL)², 8080 and 2400 to be forwarded to CC-SG (since the PC Client will initiate sessions on these ports).

All In-Band Access (IBA) connections use the CC-SG as the Proxy connection and no additional configuration is required. Out-of-Band Access (OBA) connections using the firewall must be configured on the **Setup → Configuration Manager → Connection Mode** menu to use Proxy mode. This way, CC-SG will connect to the various targets (either IBA or OBA) on behalf of the PC Client requests. However, the CC-SG will terminate the PC Client to Target TCP/IP connection that comes through the firewall.

² It is not recommended to run non-SSL traffic through a firewall.

Security and Open Port Scans

As part of the CC-SG Quality Assurance process, several open port scanners are applied to the product and Raritan makes certain that its product is not vulnerable to these known attacks. All the open or filtered/blocked ports are listed in the above sections. Some of the more common exposures are:

Issue ID ³	Synopsis	Comment
CVE-1999-0517 CVE-1999-0186 CVE-1999-0254 CVE-1999-0516	snmp (161/UDP) - the community name of the remote SNMP server can be guessed.	Default CC-SG SNMP community name is “public”. Users are encouraged to change this to the site-specific value (Setup → Configuration Manager → SNMP menu). Please refer to the CC-SG Administrator Guide for more additional information.
CVE-2000-0843	The remote telnet server shut the connection abruptly when given a long username followed by a password.	Traditionally, port 23 is used for telnet services. However, CC-SG uses this port for SSH V2 Diagnostic Console sessions. Users may change the port and/or completely disable Diagnostic Console from using the SSH Access method. Please refer to the CC-SG Administrator Guide for more additional information.
CVE-2004-0230	The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections.	The underlying TCP/IP protocol stack used by CC-SG has not been shown to be susceptible to this exposure.
CVE-2004-0079 CVE-2004-0081 CVE-2004-0112	The remote host is using a version of OpenSSL which is older than 0.9.6m or 0.9.7d.	The following patches have been applied to OpenSSL, therefore removing this exposure: <ul style="list-style-type: none"> • RHSA-2004:120 • RHSA-2005:830. • RHSA-2003:101-01

³ CVEs can be found on <http://cve.mitre.org>.

This page intentionally left blank.

Appendix C: User Group Privileges

MENU > SUB-MENU	MENU ITEM	REQUIRED PRIVILEGE	DESCRIPTION
Secure Gateway	This menu is available for all users.		
	My Profile	None*	
	Message of the Day	None*	
	Print	None*	
	Logout	None*	
	Exit	None*	
Users	This menu and the User tree are available only for users with the User Management privilege.		
> User Manager	> Add User	User Management	
	(Editing users)	User Management	Via User Profile
	> Delete User	User Management	
	> Delete User from Group	User Management	
	> Logout User(s)	User Management	
	> Bulk Copy	User Management	
> User Group Manager	> Add User Group	User Management	
	(Editing user groups)	User Management	Via User Group Profile
	> Delete User Group	User Management	
	> Assign Users to Group	User Management	
	> Logout Users	User Management	
Devices	This menu and the Devices tree is available only for users with any one of the following privileges: Device, Port and Node Management Device Configuration and Upgrade Management		
	Discover Devices	Device, Port and Node Management	
> Device Manager	> Add Device	Device, Port and Node Management	
	(Editing devices)	Device, Port and Node Management	Via Device Profile
	> Delete Device	Device, Port and Node Management	

MENU > SUB-MENU	MENU ITEM	REQUIRED PRIVILEGE	DESCRIPTION
	> 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	
	> Launch Admin	Device, Port and Node Management or Device Configuration and	

MENU > SUB-MENU	MENU ITEM	REQUIRED PRIVILEGE	DESCRIPTION
		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	> By Port Name	Device, Port and	

MENU > SUB-MENU	MENU ITEM	REQUIRED PRIVILEGE	DESCRIPTION
Options		Node Management or Device Configuration and Upgrade Management	
	> By Port Status	Device, Port and Node Management or Device Configuration and Upgrade Management	
Nodes	This menu and the Nodes tree is available only for users with any one of the following privileges: Device, Port and Node Management Node In-Band Access Node Out-of-Band Access Node Power Control		
	Add Node	Device, Port and Node Management	
	(Editing Nodes)	Device, Port and Node Management	Via the Node Profile
	Delete Node	Device, Port and Node Management	
	<interfaceName>	In-Band Access or Out-of-Band Access	
	Disconnect	In-Band Access or Out-of-Band Access	
	Power Control	Power Control	
	Group Power Control	Power Control	
> Node Sorting Options	> By Node Name	Any of the following: Device, Port and Node Management or In-Band Access or Out-of-Band Access or Power Control	

MENU > SUB-MENU	MENU ITEM	REQUIRED PRIVILEGE	DESCRIPTION
	> By Node Status	Any of the following: Device, Port and Node Management or Node In-Band Access or Node Out-of-Band Access or Node Power Control	
> Chat	> Start Chat	Node In-Band Access or Node Out-of-Band Access or Node Power Control	
	> Show Chat Session	Node In-Band Access or Node Out-of-Band Access or Node Power Control	
	> 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	

MENU > SUB-MENU	MENU ITEM	REQUIRED PRIVILEGE	DESCRIPTION
		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.
	> 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	Only available to users in the System Administrators group	
	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	
	> User Data	To view all user data: User Management To view your own user data: None	
	> Users in Groups	User Management	
	> Group Data	User Security Management	
	> AD Users Group Report	CC Setup and Control or User Management	

MENU > SUB-MENU	MENU ITEM	REQUIRED PRIVILEGE	DESCRIPTION
> Devices	Asset Management	Device, Port and Node Management	
> Nodes	> Node Asset Report	Device, Port and Node Management	
	> Active Nodes	Device, Port and Node Management	
	> Node Creation	Device, Port and Node Management	
> Ports	> Query Port	Device, Port and Node Management	
	> Active Ports	Device, Port and Node Management	
	Scheduled Reports	CC Setup and Control	
	CC-NOC Synchronization	CC Setup and Control	
Access			
	CC-NOC Configuration	CC Setup and Control	
Administration	This menu is available only for users with one of the following privilege(s): CC Setup and Control Combination of Device, Port and Node Management, User Management, and User Security Management		
	Guided Setup	All of the following: Device, Port and Node Management, User Management, and User Security Management	
	Message of the Day Setup	CC Setup and Control	
	Applications	CC Setup and Control	
	Firmware	CC Setup and Control	
	Configuration	CC Setup and Control	
	Security	CC Setup and Control	

MENU > SUB-MENU	MENU ITEM	REQUIRED PRIVILEGE	DESCRIPTION
	Notifications	CC Setup and Control	
	Tasks	CC Setup and Control	
	Compatibility Matrix	Device Configuration and Upgrade Management	
System Maintenance			
	Backup	CC Setup and Control	
	Restore	CC Setup and Control	
	Reset	CC Setup and Control	
	Restart	CC Setup and Control	
	Upgrade	CC Setup and Control	
	Shutdown	CC Setup and Control	
> Maintenance Mode	> Enter Maintenance Mode	CC Setup and Control	
	> Exit Maintenance Mode	CC Setup and Control	
View		None*	
Window		None*	
Help		None*	

*None means that no particular privilege is required. Any user who has access to CC-SG will be able to view and access these menus and commands.

Appendix D: SNMP Traps

CC-SG provides the following 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
ccDiagnosticConsoleLogout	User has logged out of the CC-SG Diagnostic Console
ccNOCAvailable	CC-SG has detected that CC-NOC is available
ccNOCUnavailable	CC-SG has detected that CC-NOC is unavailable
ccUserGroupAdded	A new user group has been added to CC-SG
ccUserGroupDeleted	CC-SG user group has been deleted

ccUserGroupModified	CC-SG user group has been modified
ccSuperuserNameChanged	CC-SG Superuser password has changed
ccSuperuserPasswordChanged	CC-SG Superuser password has changed
ccLoginBannerChanged	CC-SG login banner has changed
ccMOTDChanged	CC-SG Message of the Day (MOTD) has changed

Appendix E: Troubleshooting

- To launch CC-SG from your web browser, it requires a Java plug-in. If your machine has an incorrect version, CC-SG will guide you through the installation steps. If your machine does not have a Java plug-in, CC-SG cannot automatically launch. In this case, you must uninstall or disable your old Java version and provide serial port connectivity to CC-SG to ensure proper operation.
- If the CC-SG applet does not load, check your web browser settings.
 - In Internet Explorer: Ensure Java (Sun) is enabled.
 - Open Java Plug-in in Control Panel, and adjust the settings for your browser.
- If you have problems adding devices, ensure the devices have the correct firmware versions.
- If the network interface cable is disconnected between the device and CC-SG, wait for the configured heartbeat minutes, and then plug the network interface cable back in. During the configured heartbeat period, the device operates in standalone mode and can be accessed through RRC, MPC, or RC.
- If you receive an error message that states your client version is different from the server version and that behavior may be unpredictable, you should restart and empty the cache of your browser.

Client Browser Requirements

For a complete list of supported browsers and platforms, please refer to the **Compatibility Matrix** on <http://www.raritan.com/support>. On the **Support** page, click **Firmware Upgrades**, and then click **CommandCenter Secure Gateway**.

This page intentionally left blank.

Appendix F: Two-Factor Authentication

As part of CC-SG RADIUS based remote authentication, CC-SG can be configured to point to a RSA RADIUS Server which 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.

Supported Environments

The following RSA 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.

Setup Requirements

Proper configuration of an RSA RADIUS Server and RSA Authentication manager is beyond the scope of this guide. Please consult the RSA documentation for additional information.

Note, however, that the following procedures must be completed:

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.

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.

This page intentionally left blank.

Appendix G: FAQs

QUESTION	ANSWER
General	
What is CC-SG?	CC-SG is a network management device for aggregating and integrating multiple servers and network equipment typically deployed in a datacenter and which are connected to a Raritan IP-enabled product.
Why would I need CC-SG?	As you deploy more and more datacenter servers and devices, their management becomes exponentially complex. CC-SG allows a systems administrator or manager to access and manage all servers, equipment, and users from a single device.
What is CommandCenter NOC?	CommandCenter NOC is a network monitoring device for auditing and monitoring the status of servers, equipment and Raritan devices that CC-SG provides access to.
Which Raritan products does CC-SG support?	CC-SG supports all Dominion products - Raritan's KVM over IP products - Dominion KX and KX II - Raritan's Secure Console Server products - Dominion SX - Raritan's Remote office management products - Dominion KSX CC-SG also supports Paragon II when used with the optional IP user stations.
How does CC-SG integrate with other Raritan Products?	CC-SG uses a unique and proprietary search and discovery technology that identifies and connects to selected Raritan devices with a known network address. Once CC-SG is connected and configured, the devices connected to CC-SG are transparent, and operation and administration is extremely simple.
Is PDA access possible?	Yes, as long as the PDA has a Java-enabled browser and supports 128-bit (or lower strength for some geographies) SSL encryption. Call Raritan Tech Support for further information. No testing has been done in this area.
Is the status of CC-SG limited by the status of the devices which it proxies?	No. Because CC-SG software resides on a dedicated server, even if a device being proxied by the CC-SG is turned off, you will still be able to access CC-SG.
Can I upgrade to newer versions of CC-SG software as they become available?	Yes. Contact your authorized Raritan sales representative or Raritan, Inc. directly.
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

QUESTION	ANSWER
	sure that they are not checked.
What do I do if I am unable to add a console/serial port to CC-SG?	Assuming the console/serial device is a Dominion, ensure that the following conditions are met: - The Dominion unit is active. - The Dominion unit has not reached the maximum number of configured user accounts.
Which version of Java will Raritan's CC-SG be supporting?	For server and client side minimum Java requirements, please refer to the Compatibility Matrix on http://www.raritan.com/support . Click Firmware Upgrades and then CommandCenter Secure Gateway .
An administrator added a new node to the CC-SG database and assigned it to me, how can I see it in my Nodes tree?	To update the tree and see the newly assigned node, click the Refresh shortcut button on the toolbar. Remember that refreshing CC-SG will close all of your current console sessions.
How will the Windows desktop be supported in the future?	Accessing CC-SG from outside the firewall can be achieved by configuring the right ports on the firewall. The following ports are standard ports: 80: for HTTP access via web browser 443: for HTTPS access via web browser 8080: for CC-SG server operations 2400: for Proxy mode connections 5001: for IPR/DKSX/DKX/ P2-SC event notification If there is firewall between two cluster nodes, the following ports should be opened for cluster to be worked properly: 8732: for cluster nodes heartbeat 5432: for cluster nodes DB replication
What are some design guidelines for large-scale systems? Any constraints or assumptions?	Raritan provides two models for server scalability: the datacenter model and the network model. The datacenter model uses Paragon to scale to thousands of systems in a single datacenter. This is the most effective and cost-efficient way to scale a single location. It also supports the network model with IP-Reach and the IP User Station (UST-IP). The network model scales through use of the TCP/IP network and aggregates access through CC-SG, so users don't have to know IP addresses or the topology of access devices. It also provides the convenience of single sign-on.
Authentication	
How many user accounts can be created for CC-SG?	Check your licensing restrictions. There is no specified limit to the number of user accounts that can be created for CC-SG, but the number is not limitless. The size of the database, the performance of the processor, and the amount of memory on the hosting server will determine how many user accounts can actually be created.
Can I assign specific node	Yes, if you have Administrator permissions. Administrators

QUESTION	ANSWER
access to a specific user?	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, etc.	CC-SG permits local authentication as well remote authentication. Remote authentication servers supported include: AD, TACACS+, RADIUS, and LDAP.
Security	
Sometimes when I try to log on, I receive a message that states my “login is incorrect” even though I am sure I am entering the correct username and password. Why is this?	There is a session-specific ID that is sent out each time you begin to log on to CC-SG. This ID has a time-out feature, so if you do not log on to the unit before the time-out occurs, the session ID becomes invalid. Performing a Shift-Reload refreshes the page from CC-SG. Or, you may close the current browser, open a new browser, and log on again. This provides an additional security feature so that no one can recall information stored in the web cache to access the unit.
How is a password secure?	Passwords are encrypted using MD5 encryption, which is a one-way hash. This provides additional security to prevent unauthorized users from accessing the password list.
Sometimes I receive a “No longer logged in” message when I click any menu in CC-SG, after leaving my workstation idle for a period of time. Why?	CC-SG times each user session. If no activity happens for a pre-defined period of time, CC-SG logs the user out. The length of the time period is pre-set to 60 minutes, but it can be reconfigured. It is recommended that users exit CC-SG when they finish a session.
As Raritan has root access to server, this may potentially cause issue with government bodies. Can customers also have root access or can Raritan provide a method of auditability / accountability?	No party will have root access to server once the unit is shipped out of Raritan, Inc.
Is SSL encryption internal as well as external (not just WAN, but LAN, too)?	Both. The session is encrypted regardless of source, LAN or WAN.
Does CC-SG support CRL List, that is, LDAP list of invalid certificates?	No.
Does CC-SG support Client Certificate Request?	No.

Accounting	
The event times in the Audit Trail report seem incorrect. Why?	Log event times are logged according to the time settings of the client computer. You can adjust the computer's time and date settings.
Can audit/logging abilities track down who switched on or off a power plug?	Direct power switch-off is not logged, but power control through CC-SG can be logged to audit logs.
Performance	
As a CC-SG Administrator, I added over 500 nodes and assigned all of them to me. Now it takes a long time to log on to CC-SG.	When you, as Administrator, have many nodes assigned to you, CC-SG downloads all information for all nodes during the logging process, which slows the process considerably. It is recommended that Administrator accounts used primarily to manage CC-SG configuration/settings do not have many nodes assigned to them.
What is the bandwidth usage per client?	<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	
Is it possible to put a given server in more than one group?	<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>
What impact to other usage that would be blocked through the active usage of the console port, for example, some UNIX variants not allowing admin over network interfaces?	<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>
How do you recommend the issue of CIMs being moved / swapped at the physical level with changes to the logical database?	Each CIM includes a serial number and target system name. Our systems assume that a CIM remains connected to its named target when its connection is moved between switches. This movement is automatically reflected in the system configuration and is propagated to CC-SG. If, instead, the CIM is moved to another server, an administrator must rename it.

Interoperability	
How does CC-SG integrate with Blade Chassis products?	CC-SG can support any device with a KVM or serial interface as a transparent pass-through.
To what level is CC-SG able to integrate with 3rd party KVM tools, down to 3rd party KVM port level or simply box level?	3 rd party KVM switch integration is typically done through keyboard macros when the 3 rd party KVM vendors do not publicize the communications protocols for the 3 rd party KVM switches. Depending on the capability of the 3 rd party KVM switches, the tightness of integration will vary.
How would I mitigate the restriction of four simultaneous paths through any IP-Reach box, including the roadmap for the potential 8-path box?	Currently, the best possible implementation is to aggregate IP-Reach boxes with CC-SG. In the future, Raritan plans to increase simultaneous access paths per box. These plans have yet to complete development as other projects have taken priority, but we welcome comments about the market demand and use cases of an 8-path solution.
Authorization	
Can authorization be achieved via RADIUS/TACACS/LDAP?	LDAP and TACACS are used for remote authentication only, not authorization.
User Experience	
Regarding console management via network port or local serial port (for example, COM2): What happens to the logging, does CC-SG capture local management or is this lost?	Logging on to CC-SG through the CC-SG console itself is the same as gaining the root privilege of the operating system (Linux) upon with CC-SG is running. Syslog will record such event, but what the user types at the CC-SG console itself will be lost.

This page intentionally left blank.

Appendix H: Keyboard Shortcuts

The following keyboard shortcuts can be used in the Director Client.

OPERATION	KEYBOARD SHORTCUT
Refresh	F5
Print panel	Ctrl + P
Help	F1
Insert row in Associations table	Ctrl + I

North American Headquarters

Raritan

400 Cottontail Lane
Somerset, NJ 08873
U.S.A.
Tel. (732) 764-8886
or (800) 724-8090
Fax (732) 764-8887
Email: sales@raritan.com
Website: Raritan.com

Raritan NC

4901 Waters Edge Dr.
Suite 101
Raleigh, NC 27606
Tel. (919) 277-0642
Email: sales.nc@raritan.com
Website: Raritan.com

Raritan Canada

4 Robert Speck Pkwy, Suite 1500
Mississauga, ON L4Z 1S1 Canada
Tel. (905) 949-3650
Fax (905) 949-3651
Email: sales.canada@raritan.com
Website: Raritan.ca

European Headquarters

Raritan Netherlands

Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. (31) 10-284-4040
Fax (31) 10-284-4049
Email: sales.europe@raritan.com
Website: Raritan.info

Raritan Germany

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

Raritan France

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

Raritan U.K.

36 Great St. Helen's
London EC3A 6AP, United Kingdom
Tel. (44) 20-7614-7700
Fax (44) 20-7614-7701
Email: sales.uk@raritan.com
Website: Raritan.co.uk

Raritan Italy

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

Japanese Headquarters

Raritan Japan

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

Raritan Osaka

1-15-8 Nishihonmachi, Nishi-ku
Osaka 550-0005, Japan
Tel. (81) (6) 4391-7752
Fax (81) (6) 4391-7761
Email: sales@raritan.co.jp
Website: Raritan.co.jp

Asia Pacific Headquarters

Raritan Taiwan

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

Raritan Shanghai

Rm 17E Cross Region Plaza
No. 899 Lingling Road
Shanghai, China 200030
Tel. (86) 21 5425-2499
Fax (86) 21 5425-3992
Email: sales.china@raritan.com
Website: Raritan.com.cn

Raritan Beijing

Unit 1310, Air China Plaza
No.36 XiaoYun Road
Chaoyang District
Beijing 100027, China
Tel. (86) 10 8447-5706
Fax (86) 10 8447-5700
Email: sales.china@raritan.com
Website: Raritan.com.cn

Raritan Guangzhou

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

Raritan Korea

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

Raritan Australia

Level 2, 448 St Kilda Road,
Melbourne, VIC 3004, Australia
Tel. (61) 3 9866-6887
Fax (61) 3 9866-7706
Email: sales.au@raritan.com
Website: Raritan.co.au

Raritan India

210 2nd Floor Orchid Square Sushant Lok 1,
Block B, Gurgaon 122 002 Haryana India
Tel. (91) 124 510 7881
Fax (91) 124 510 7880
Email: sales.india@raritan.com
Website: Raritan.co.in

Raritan OEM Division

Peppercon AG, Raritan OEM Division
Scheringerstrasse 1
08056 Zwickau Germany
Tel. (49) 375-27-13-49-0
Email: info@peppercon.com
Website: www.peppercon.de