

CommandCenter® Secure Gateway Release 3.2.1

**This is to announce the General Availability
of CommandCenter® Secure Gateway
Firmware Release 3.2.1
as of date:
January 31, 2008**

Release Note Contents

Introduction	2
Applicability	2
Updates in This Release	2
Major Fixes in This Release	3
Security and Compliance Information.....	4
Additional Release Documentation	4
Release Package Details	4
General Upgrade Instructions.....	4
Important Notices	5
Limitations and Restrictions.....	5
Troubleshooting.....	5
Raritan Support Contacts:.....	6

Introduction

These Release Notes contain important information regarding the release of this product. We strongly recommend you read the entire document and the related documentation available for this product.

Applicability

CommandCenter ® Secure Gateway hardware Models CC-SG-G1, CC-SG-V1, and CC-SG E1

Updates in This Release

For customers upgrading their CC-SG 3.2.0 to this release updates include:

- **Dominion KSX II Compatibility** – The new KSX II device is now supported for discovery, management, and centralized KVM and Serial access as well as control of remotely managed power strips connected to this new device. You can launch KVM and serial console connections from the CC-SG graphical user interface. Direct CLI access to serial targets connected to a managed KSX II is also available.
- **Dominion KX II-101 Compatibility** – The new KX II-101 device is now supported for discovery, management, and centralized KVM access as well as control of remotely managed power strips connected to this new device. You can launch KVM console connections from the CC-SG graphical user interface.

Customers upgrading their CC-SG 3.1.1 or 3.1.0 to this release may also be interested in the following recent updates:

- **iLO2 Support** – a new interface has been added to nodes and provides a single sign on to iLO2 console and power command capability directly from CC-SG. [E6756]
- **Web Browser Interface** – the new interface can be added to nodes to provide access to devices and applications supporting integrated web server functionality. Some applications include IP access to Dominion PX management interface and access to embedded service processors like HP iLO, Dell RAC, and IBM RSA.
- **Improved Upgrade Device Firmware Task** – a new scheduled task has been added to the Task Manager that allows multiple devices of the same product type to be upgraded concurrently.
- **Group Restart Task** – a new scheduled task has been added to the Task Manager that allows multiple devices to be restarted simultaneously. [E4519]
- **Upgrade Status Report** – a new report found in the Scheduled Reports area provides real-time device upgrade task information.
- **Node and Device Group-based Custom Views** – In addition to support of custom views creation using predefined Categories and Elements, now users can define views based on Node Groups.
- **Power Status Messages window** – power control operation status is now reflected in real time on a pop up window. Status messages indicate power control command sent,

succeeded, or fail on a single interface and power control operation complete status for a group of power interfaces.

- **IPMI 2.0 Support** –cards incorporated into servers can now be discovered and added as power control interfaces to nodes. [E9057]
- **64 Character User Group Names** – name length increased from 32 to 64 characters. [E10509]

For those customers upgrading to this release from a release older than CC-SG 3.1.0, we strongly recommend that you review the ‘What’s new in this release’ presentation designed for customers upgrading from release 3.0 or earlier. The presentation is available on the www.raritan.com/support website to understand how these changes improve user and administrator experience with CC-SG.

Major Fixes in This Release

1. Possible slow response for all CC-SG users or browser lockup for users with CC-SG administrative privileges due to a running parallel firmware upgrade task is now resolved [E12253, E12180]
2. Access Report can now be run as a daily task in Task Manager [E9886]
3. Active Directory™ remote authentication issue where users intermittently received "You are not a member of any group" message and are not logged in to CC-SG is now fixed. [E12162]
4. Virtual Media Permission not available for KXII targets through CC-SG for users not assigned with Full access Policy is now resolved. [E12010]
5. After a new device is added manually (not through Discover Device function), the add device screen is still available to enter another new device. The default heartbeat time is set to 600 not 0 seconds. [E4353]
6. When client is accessing CC-SG with no JRE installed or a JRE version older than 1.4.2_15a page would be displayed linking customer to a JRE download site. [E8976]
7. When adding a new node, node name of up to 64 characters can now be entered. [E9367]
8. Automatic sign on to DRAC4 console is now available with passwords including special characters like '!'. [E10523]
9. Power cycle command to an iLO power interface does no longer require a user to be logged in to the iLO card. [E9582]
10. A backup file store on a remote FTP location can now be restored to CC-SG. [E10419]
11. The sign “ can now be entered using RDP interface. [E10326]
12. When adding a PCS20 managed power strip connected to Dominion SX 3.1.0 to CC-SG 3.1.1 device power manager outlet list only shows partial number of outlets. When the power strip is added to CC-SG 3.2, all power outlets show. [E9162]
13. When issuing power cycle command to a group of outlets on managed power strips connected to Dominion SX firmware version 2.5.7 or 3.1.0, command time interval of 10 seconds is no longer added. The cycle command is issued at the same time to all power interfaces. [E10234]

14. When CC-SG user from System Administrators group adds Dominion SX, configures port and adds power strip, the port automatically change itself to a power strip and becomes available. [E10074]

Security and Compliance Information

Refer to the CC-SG Admin Guide ‘Appendix B: CC-SG and Network Configuration’ for specific settings and for updated Security and Open Port Scan report.

Additional Release Documentation

The following document can be found on <http://www.raritan.com/support/firmwareupgrades>

- **Compatibility Matrix** – summary of supported firmware and hardware versions of Dominion Series, IP-Reach, and Paragon devices and supported client applications of those devices; supported firmware versions of third party devices (e.g. HP iLO/RiLOE); and supported client platforms, including browser versions and JRE versions.

Additional documents can be found on <http://www.raritan.com/support/productdocumentation>

- **Deployment Guide** – guide to deployment and configuration of devices.
- **Administrators Guide** – an administrator guide to features and functionality.
- **User Guide** – a user guide to features and functionality.
- **Quick Setup Guide** – a reference to quick setup instructions. CC-SG E1, V1, and G1 each has its own version of the Quick Setup Guide.

Release Package Details

The upgrade includes the following files:

- Firmware file: scc321_upgrade_p17_rpm_rfp.zip

This upgrade is only available upon direct request from Raritan.

General Upgrade Instructions

To upgrade to this release you must be running CC-SG firmware version 3.2.0, 3.1.1, or 3.1.0. Note that this upgrade process would make updates to the CC-SG database. Therefore, the database must also be included with your CC-SG 3.2.0, 3.1.1, or 3.1.0 prior to upgrade and may be modified as part of the upgrade process. We recommend you backup CC-SG prior and after the upgrade process. Refer to detailed instructions for upgrading CC-SG to this release in the Admin Guide.

CC-SG cannot be upgraded in a cluster mode. If using a cluster, first take the CC-SG out of a cluster mode and only then proceed with upgrading each individual CC-SG appliance.

Install the Thick Client directly from the CC-SG by typing <CC-SG IP Address>/install into a web browser Address field. For complete information about how to install, use, and check for CC-SG security settings refer to CC-SG documentation.

Important Notices

1. CC-SG will reboot as part of the upgrade process. **DO NOT** stop the process, reboot the unit manually, power off or power cycle the unit during the upgrade. [E10010]
2. Scheduled Upgrade Device and Accessed Devices Report tasks created prior to a CC-SG upgrade from releases 3.1.1 and 3.1.0 will be deleted if they are pending execution. If a scheduled Upgrade Device or Accessed Devices Report task is completed prior to the CC-SG 3.2.1 upgrade, the task will appear after the upgrade as a completed task. [E10507]
3. When upgrading a Dominion SX with a connected remotely managed power strip to firmware release SX 3.1.0, power association may take time to reestablish. You may need to wait up to 15 minutes after upgrade of all SX devices in completed before power associations reappear in CC-SG. [E9779]
4. For optimal operation, disable the pop-up blocker in your browser.
5. When device is under "Pause Management," the ports on that device cannot be deleted.

Limitations and Restrictions

1. For Dominion KX2 if using CC-SG in Proxy mode change the default in the Default Application tab in Application manager to Virtual KVM Client. [E7146]
2. User closing the browser window of the HTML client is not logged out. In order to logout of the HTML client, user must select the logout button available in multiple locations in the client. [E8489].
3. While trying to configure a KSX device in CC-SG when the encryption mode in the KSX is set to 'No Encryption' the following error message "CSC:Csc Protocol error: Fatal Error: Line=1: Premature end of file." is displayed. The KSX cannot be configured. KSX needs to be setup in encryption mode when under CC-SG management. [E10846]
4. In the Audit Trail and Error Log reports the Print button prints a screen shot instead of a report contents. Suggested workaround is to save the report to a file and print the information from that file. [E11229]
5. Maximum Password Length, Password history depth, and Password Expiration Frequency for CC Super-User are changed if these values are changed from all users from the default values provided in the Login Settings in the Security Manager. [E12937, E12938]

Troubleshooting

- If the CC-SG applet does not load, check the web browser settings.
 - If you are using Internet Explorer, on the **Tools** menu, click **Internet Options**, click on the **Advanced** tab, and check if **Java (Sun)** is enabled.
 - Open the Java Plug-in from the Control Panel, click on the **Browser** tab, and enable the setting for your browser.
 - Check your browser's popup blocker

Raritan Support Contacts:

➤ *U.S./Canada/Latin America*

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

➤ *Beijing*

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

➤ *Japan*

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

➤ *Europe*

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

➤ *Korea*

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

➤ *France*

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

➤ *Melbourne, Australia*

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

➤ *Germany*

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

➤ *Shanghai*

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

➤ *GuangZhou*

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

➤ *Taiwan*

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

➤ *India*

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

➤ *United Kingdom*

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

© Copyright 2008 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. Copyright 2008 Raritan, Inc. All rights reserved.