Raritan. When you're ready to take control.™ Release Notes

CommandCenter® Secure Gateway Release 3.1.1

This is to announce the General Availability of CommandCenter® Secure Gateway

Firmware Release 3.1.1

as of date: May 14, 2007

Document last modified: July 5, 2007

Release Note Contents

==

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

- **Support for Dominion KX II–** the new devices can be added, configured, and managed through CC-SG.
- **Support for Raritan Dominion PX** – the new power strip can be connected to Dominion or Paragon devices and accessed for power control commands through CC-SG.
- **Virtual Media –** virtual media configuration is now available for KX II devices. Access and setup for virtual media capabilities require D2CIM-VUSB CIM and is controlled using CC-SG policies.
- **AES Encryption –** now can be enabled between client and CC-SG, between CC-SG and KX II, and between KX II client applications (e.g., MPC, VKC, KX II Manager) and target servers.
- **Selective Restore for DKX II –** restore of KX II backup include the ability to selectively choose components of the backup. CC-SG supports KX II restore selection options.
- **Bulk Copy for Categories/Elements –** Categories/Elements can now be applied across a selected group of nodes or devices.

Following are new features introduced in previous release 3.1.0 (available to customers using release 3.1.1):

- **Access Client** – Users can now access CC-SG using HTML UI Access client by entering the CC-SG DNS or IP address into a web browser address filed. The Access Client is simplifying user access to nodes. For administrator's management Java client is available at CC-SG_IP_Address/admin or by launching CC-SG from the Thick Client (Standalone Client).
- **Nodes and Interfaces** – Release 3.1.0 introduces the concept of nodes. The Port tab part of the tree view in earlier releases is replaced with the new Node tab. Access, power management, and other privileges are now provided on a node and not port basis. Each node contains one or more interfaces, where an interface is defined of a method to access or power manage a target. Interfaces may include Out of Band KVM, Out of Band Serial, Managed Power Strip Outlet, In-band application (e.g., RDP), In-band access (e.g., iLO virtual KVM access), or In-band power (e.g., iLO power management).
- **Privileges** – new privileges are introduced to address a need for granular level of permission required. Specifically, node access policies are defined in three mutually

exclusive categories: Node Out-of-Band Access, Node In band Access, and Node Power Control. User groups can be created with different combinations of these privileges.

- **Embedded Card Access** –support for Dell DRAC 4 and IBM RSA II embedded cards.
- **Predefined User Groups** –three user groups are predefined in this release: CC Users, System Administrators, and CC Super-User. Privileges for these three groups are preset.
- **Strong Password** – Ability to enforce strong password requirement for local authentication. Strong password incorporates a selectable set of options including:
    a. Minimum and maximum character set
    b. One or more of a variety of character sets
    c. System defined expiration date
    d. Password history depth
- **Customizable Banners and Message of the Day** – Login page provides customizable electronic notifications, corporate graphical logos, and post login messages of the day.
- **Active Directory Group Search Enhancements** – Recursive searches for AD Groups and Nested AD groups.
- **LDAP Authentication over SSL** – provided that the LDAP server is configured for SSL support, CC-SG can now provide an SSL secure session.
- **Automated Remote Backup** – CommandCenter Secure Gateway provides an automated file transfer mechanism that allows an administrator to schedule recurring or ad-hoc back ups of the CC-SG to a remote location. The completed task is followed by a configurable successful/unsuccessful task notification via email.
- **Guided Setup** –Simplified creation of groups, associations, and privileges.
- **Mouse over operations** – Provides node level information
- **New Raritan Serial Client (RSC)** - New application for Dominion SX devices
- **Enhancement to Dominion SX CLI commands –** reflecting node and interface list, connect, and disconnect commands
- **Enhancements to Search functions** – selectable ‘wild card’ or string match search format
- **Graceful Shutdown command –** the graceful shutdown command is available through the IPMI, DRAC4, and RSAII interfaces.
- **Custom views** – System-wide custom views can be created by administrators and shared with users.
- **AD User Group Report** – new report

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. When SSL is set on CC-SG, “HTTPS://CCSG_IP_Address” has to be explicitly used in the web browser address field. CC-SG only redirects the web browser correctly for SSL settings when DNS is configured. [E4965]
2. User with no power control privileges can still see the power control options available to them in the HTML Access Client even though they cannot execute power commands. [E4621]
3. OutOfMemory error message indicating out of memory issue. [E8187]

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.
- **Admin Guide –** an Administrators 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 have its own version of the Quick Setup Guide.

Release Package Details

The file provided for this upgrade includes the following components:

- Firmware file: scc311_upgrade_p18_rpm_rfp.zip
- Readme file: CC-SGv3.1.1_Upgrade_Readme.txt

This upgrade is available for download on the www.raritan.com/support/firmwaredownloads website.

General Upgrade Instructions

In order to upgrade to this release you must be running CC-SG firmware version 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 prior to upgrade and would be modified as part of the upgrade process. We recommend you backup CC-SG prior and after the upgrade process.

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.

When upgrading to CC-SG 3.1.1 the AES encryption between client and CC-SG option will be unchecked even if previously selected. If no further action is taken AES encryption is optional and can be used if the client application supports AES. To require AES encryption between CC-SG and the client, go to Administration > Security panel and click on the "Requires AES Encryption Between Client and Server" checkbox.

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.

Limitations and Restrictions

1. When using JRE 1.5.0 and accessing the RSC 1.0.0 application help from the menu, no topics appear in the help screen. In order to avoid this upgrade to any later JRE version. [E7033]
2. When using JRE 1.6.0._01 and attempting a connection to RDP, DRAC, or iLO/RiLOE interfaces or when accessing CC-SG through Internet Explorer a Java exception error is provided and connection fails. Workaround: change JRE to any later or earlier supported JRE version. For supported JRE versions review the updated CC-SG 3.1.1 Compatibility Matrix on the Raritan support website. [E8424, E8427, E8844]
3. If using CC-SG in Proxy mode change the default in the Default Application tab in Application manager to Virtual KVM Client. [E7146]
4. 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].
5. Modifications to font in RSC application display-settings are reflected in CC-SG tooltip. [E8651]
6. Categories and Elements can be created and assigned within the user interface as well as assigned via new bulk copy feature of CC-SG 3.1.1. However, the CSV file Import Category function is not available. [E3087]
7. When upgrading to CC-SG 3.1.0, nodes are not created for outlet ports. However, if an outlet was previously associated to a KVM or Serial port, a power control interface is added to the node that is created for the KVM/Serial port. Categories and Elements previously associated to the KVM/Serial port would now be assigned to the node. [E3715]
8. When SSL is set to off and CC-SG is configured for Proxy mode, RRC can not connect to serial ports. Use RC or RRC to connect to serial ports. [E2903]
9. After a new device is added manually (not through Discover Device function), the add device screen is still available to enter another new device. However, the default heartbeat time of 600 seconds no longer appear. [E4353]
10. Element names are case sensitive when input, but not when selected. Do not add two Elements using different case, as only the first one entered can be used. [ST11180]
11. If the configure ports command is running on the primary CC-SG in a cluster when a power failure occurs, these ports cannot be configured or deleted using the backup node. [ST10711]

12. During switchovers in cluster mode, a direct mode connection between a CC client and the SX will remain intact while a similar connect using IP-Reach will be disconnected. The SX connection will not appear in the Active Ports or Disconnect Users reports on the backup node. [ST10725]
13. If using the G1 hardware platform, on the Network Setup tab do not select 10Mbps/Full Duplex mode. Instead select 10Mbps/Half Duplex, 100Mbps or Auto-Detect.
14. When using Firefox browser along with Windows operating system, any opening pop up window in CC-SG, such as Add a new device group, or configure CC-NOC may cause all previous opened Firefox windows to freeze. [E1321].

Important Notices

1. When upgrading from CC-SG 3.0.2 all Active Directory modules must be reconfigured in the Administration > Security panel: domain name and DNS values are now required for each Active Directory module. Until these values are configured, no remotely authenticated user will be able to login to CC-SG. This message does not apply to customers not using Active Directory for remote authentication.
2. After upgrade from CC-SG 3.0.2 user groups are by default provided with Node Out-of Band Access and Node In-band Access privileges. Node Power Control privilege is not granted by default. In order to provide power control privileges to a user group, edit the User Group Profile by checking the Node Power Control option and then pressing OK to save. The predefined CC Super user, System Administrator, and CC user groups are provided Node Power Control privilege.
3. For optimal operation, disable the pop-up blocker in your browser.
4. When device is under “Pause Management,” the ports on that device cannot be deleted.
5. When upgrading a Raritan device it is strongly recommends that the device is re-booted before the firmware upgrade applied. You can reboot the devices directly from CC-SG by scheduling a reboot prior to upgrade for all Raritan devices using the Task Manager feature.

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

- When using the Task Manager to upgrade Dominion SX and KX device firmware, set the retry interval to 30 minutes or longer, as the upgrade may take 20 minutes or more to complete. [ST11303, E517, E2942]

Raritan Support Contacts:

U.S./Canada/Latin America

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

Europe

Phone: (31) 10-284-4040
Fax: (31) 10-284-4049
tech.europe@raritan.com

Japan

Phone: +81-(0)3-3523-5991
Fax: +81-(0)3-3523-5992
support.japan@raritan.com

Raritan Asia Pacific

Phone: (886) 2-8919-1333
Fax: (886) 2-8919-1338
Support.APAC@raritan.com

India

Phone: +91 124 410 7881
(9.00 a.m - 6.00 p.m)
Cell: +91 98 714 60002,
+91 98 714 60004
Fax: +91 124 410 7880
enquiry.india@raritan.com