CommandCenter® Secure Gateway Release 3.1.0

Thank you for your purchase of Raritan's CommandCenter® Secure Gateway Version 3.1.0. These Release Notes contain important information regarding the release of this product, so please read them carefully. We strongly recommend you read the entire document and the related documentation available for this product.

Effective:

January 16, 2007

Applicability:

CommandCenter ® Secure Gateway (H/W Models CC-SG-G1, CC-SG-V1, CC-SG E1)

Release Status:

General Availability (GA)

General Upgrade Instructions:

Raritan strongly recommends that you backup your existing database prior to upgrading your CC-SG. Make sure that your backup is stored on a network location different from the CC-SG appliance you are about to upgrade.

In order to upgrade to this release you must be running either CommandCenter Secure Gateway firmware version 3.0.2 or 3.0.0. Note that this upgrade process would make updates to the database. Therefore, the database must also be included with your CC-SG 3.0.2 or 3.0.0 prior to upgrade.

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.

As part of this upgrade 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.

Thick Client Installation Instructions:

Install it 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

Release Package Details:

The zip file provided for this upgrade includes 3 components:

1. Firmware file
2. Readme file
3. Active Directory Important Note

Please check the Raritan support website @ (http://www.raritan.com/support/sup_prdmanuals.aspx) for the following documents:

- User Guide – a user guide to features and functionality.
- Admin Guide – an Administrators guide to features and functionality.
- Quick Setup Guide – one page reference to quick setup instructions. CC-SG E1, V1, and G1 each have its own version of the Quick Setup Guide.
- Deployment Guide – guide to deployment and configuration of devices.
- Compatibility Matrix – matrix containing supported firmware 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.

Expiration Date of Content:

This document will be obsolete when the next generally available release is posted on the Raritan web-site. Contact Raritan Customer Support or check our Web-site (http://www.raritan.com/support) for updated versions of the CommandCenter Secure Gateway software, release notes and user documentation.

Updates in CommandCenter Secure Gateway 3.1.0 Include:

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).
2. **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).
3. **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.
4. **Embedded Card Access** –support for Dell DRAC 4 and IBM RSA II embedded cards.
5. **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.
6. **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
7. **Customizable Banners and Message of the Day** – Login page provides customizable electronic notifications, corporate graphical logos, and post login messages of the day.
8. **Active Directory Group Search Enhancements** – Recursive searches for AD Groups and Nested AD groups.
9. **LDAP Authentication over SSL** – provided that the LDAP server is configured for SSL

support, CC-SG can now provide an SSL secure session.

10. **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.
11. **Guided Setup** – Simplified creation of groups, associations, and privileges.
12. **Mouse over operations** – Provides node level information
13. **New Raritan Serial Client (RSC) -** New application for Dominion SX devices
14. **Enhancement to Dominion SX CLI commands –** reflecting node and interface list, connect, and disconnect commands
15. **Enhancements to Search functions** – selectable 'wild card' or string match search format
16. **Graceful Shutdown command –** the graceful shutdown command is available through the IPMI, DRAC4, and RSAII interfaces.
17. **Custom views** – System-wide custom views can be created by administrators and shared with users.
18. **AD User Group Report** – new report

We strongly recommend that you review the 'What's new in this release' presentation available on the www.raritan.com/support website to understand how these changes improve user and administrator experience with CC-SG.

Important Release Information:

1. When changing password, non CC Super-users are not allowed to use any one of the 5 previous passwords even if Strong Password is disabled in the Security Manager, Local Settings. Using the old password displays an error that Password is already used. [E4199]
2. Categories and Elements can be created and assigned within the user interface. However, the CSV file Import Category function is not available. [E3087]
3. When edit the outlet name for the Power Control interface associate with a Dominion KX port, a new association between the KX port and the new outlet is not created and the port has to be associated manually to the outlet. Another possible workaround is instead of using edit to change the outlet name or move an outlet from one power strip to another, delete & then add the power strip. [E4192]
4. If Security Profile is enabled via Dominion SX local access while the SX is in Pause management from CC-SG, device management cannot resume. Changing security enables strong passwords, which in turn cause current password on SX to expire. Two possible workarounds are available. The workaround is to create another username after security profile is enabled, and provide this username to CC-SG when resume management is attempted. In case edit already took place, delete the SX from CC-SG, enable security profile on SX, then add SX to CC. [E4152]
5. In the Admin Client, all nodes associated with a device are shown as locked during upgrade of that device. They are not shown as locked in HTML client. Note that if an In-band interface is available for the note it is accessible at all times via both clients [E2939]
6. When going back from Pause Management to Resume Management in IP-Reach version 3.20 or KSX version 3.23 ports still appear as down for about 30 seconds. In order to refresh port status wave your mouse over the port to change status. [E4124]
7. While configuring ports with "Select All" option, ports are not configured with the default application selected in the "Default application" tab. Instead ports are configured with "Auto-Detect" option. [E3956]
8. When upgrading, 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]
9. When outlet port is associated to KVM/Serial port, then one node is created for both

interfaces (according to PSD 7990). The created node takes the category elements of the KVM/Serial port. This is not specified in the PSD but it seen logical that the category elements of the KVM/Serial port are more important. [E3715]

10. The "Access Report" is only available to users of the default "System Administrators" group. [E3961]
11. 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]
12. The service banner message is displayed in the Diagnostic Console even when disabled. Note that it is not displayed for all client access when disabled. [E2150]
13. Even if the checkbox for required AES encryption may be selected in the Security Manager, General tab, clients to CC-SG sessions not supporting AES may still be established. [E4612]
14. Restricted Service Agreement is no required prior to access in the Diagnostic Console even if enabled. Note that it is required for all client access when enabled. [E2146]
15. In the Admin Client when device is unavailable (e.g., being configured) user is able to select a port of the device and edit port settings. When attempting to update the port changes an error message is displayed and the port settings are not upgrade. [E547]
16. 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]
17. 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]
18. When saving a report using the manage reports button, the fields are separated using a semicolon instead of a comma. You should change your client application delimiter from comma to semicolon or all data will appear in one column. [ST10090, E547]
19. If the configure ports command is running on the primary node of a CC-SG cluster when a power failure occurs, these ports cannot be configured or deleted using the backup node. [ST10711]
20. 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]
21. 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 takes ~20 minutes to complete. [ST11303, E517, E2942]
22. 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.
23. In the manage report data window, on Saving the Log records to a CSV file, in each record, field values are separated with semicolon. For field to be separated to CSV columns, you must change the list separator on your PC to a semicolon. [E549].
24. 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].

General Information:

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, 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. When using Firefox browser, JRE 1.4.2_05 needs to be pre-loaded onto the client PC.
4. For optimal operation, disable the pop-up blocker in your browser.
5. When a device is in PC-Share mode, CC-SG will allow RRC and MPC to connect to any target connected to a device. In reality there are a limited number of active targets determined by the device model number (e.g. 1 for KX1xx, 1 for KSXxxx, 2 for KX2xx, and 4 for KX4xx).
6. Enable or disable the SSL option in Security Manager before setting up CC-SG in clustering mode.
7. When device is under "Pause Management," the ports on that device cannot be deleted.
8. In order to launch CommandCenter Secure Gateway Admin client from your web browser, JRE version 1.4.2_05 or later is required. If your client PC has an older version, CommandCenter Secure Gateway will guide you through the JRE installation.
9. For connections to KX-connected targets JRE 1.5.0_02 is not supported.
10. When upgrading a Raritan device it is strongly recommends that the device be re-booted before the firmware upgrade is applied. You can reboot the devices directly from CommandCenter Secure Gateway by scheduling a reboot prior to upgrade for all Raritan devices using the Task Manager feature.
11. To download the Thick Client to your desktop enter "http(s)://CC_IP_Address/install" in your web browser.

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
Phone: (800) 724-8090 or 732-764-8886
Fax: (732) 764-8887
tech@raritan.com

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

Japan
Phone: (81) 3-5833-6360
Fax: (81) 03-5833-6336
sales@raritan.co.jp

Outside of these areas
Phone: (886) 2-8919-1333
Fax: (886) 2-8919-1338
sales.asia@raritan.com

Release Notes: CommandCenter Secure Gateway Version 3.1.0, January 2007