CommandCenter® Secure Gateway Release 3.0.2

Thank you for your purchase of Raritan's CommandCenter® Secure Gateway Version 3.0.2. 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:

September 7, 2006

Applicability:

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

Release Status:

General Availability (GA)

General Upgrade Instructions:

If you are upgrading from a CommandCenter Secure Gateway with release 2.3 (H/W Model CC-SG-G1) to a CommandCenter Secure Gateway V1 (H/W Model CC-SG-V1) or CommandCenter Secure Gateway E1 (H/W Model CC-SG-E1), please refer to the CC-SG System Migration Guide which is packaged with your new CC-SG appliance. You will be requested to make a backup of your existing CC-SG 2.3 database prior to the upgrade as you will need to migrate your database from the CC-SG-G1 to the new CC-SG unit.

Customers with any version of CommandCenter Secure Gateway prior to release 2.3 must first upgrade to version 2.3 to ensure database compatibility.

Upgrading from release 3.0.0 on the CommandCenter Secure Gateway (H/W Model CC-SG-V1) to release 3.0.2 requires downloading two files from the Raritan web site (see URL below). Each of these files must then be uploaded into CC-SG. Follow the upgrade instructions that come within the zip file of the CC-SG 3.0.2 upgrade file for CC-SG 3.0.2 users.

Release Package Details:

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

1. User Guide – a user guide to features and functionality.
2. Admin Guide – an Administrators guide to features and functionality.
3. Quick Setup Guide – one page reference to quick setup instructions.
4. Digital Solution Deployment Guide – guide to deployment and configuration of devices.
5. Setup Guide – overview on preparing devices and installing CC-SG.

Please check the Raritan support website @

(http://www.raritan.com/support/sup_upgrades.aspx) for the following documents:

1. System Migration Guide – a guide to upgrade your current CC-SG G1 appliance with the new CC-SG V1 or CC-SG E1 appliance and migrate your existing database.
2. Upgrade Guide – procedures to upgrade your CC-SG G1 system from 2.3 to 3.0.2.
3. Release Notes – important information regarding this release of CommandCenter Secure Gateway.
4. 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 3.0 (3.0.0 / 3.0.2) Include:

1. **Command Line Interface** – Users can now establish SSH sessions to the CC-SG, the SX device, and to target servers and network devices.
2. **CommandCenter NOC 5.4 Integration** – Single sign-on and embedded links connect CC-NOC users through a CC-SG managed network to target servers and network devices.
3. **Consolidation of In-band Access Tools** – Provides new client application support through secure shell (SSH), remote windows desktop (RDP), and virtual network computing (VNC) applications. Serves as a gateway for access consolidation and connectivity to target servers and network devices.
4. **Diagnostic Console –** A set of screens for viewing CC-SG status and performing appliance maintenance using standard SSH clients.
5. **Notifications –** Task completion status can be forwarded by email or traps.
6. **Importing Files –** A CSV file containing system definitions of categories and elements can be built externally and then imported to CC-SG.
7. **IPMI Support –** Automated discovery of IPMI (1.5 or greater) devices and the ability to power control (on, off, recycle) the device through its IPMI BMC.
8. **Maintenance Mode –** This allows an administrator to place the CC-SG into quiet mode where existing user sessions are gracefully terminated and new sessions are prevented, while system maintenance is performed.
9. **Remote AAA Server Support –** Simultaneous support for a virtually unlimited number of remote Authentication servers.
10. **Searching –** The ability to quickly search for a port based on its name or IP address.
11. **Secure Chat –** All users (CC-SG and SX) accessing an SX port/target can collaborate in a common chat window.
12. **Security Updates –** Various login compliance procedures have been added.
13. **Task Scheduler –** An administrator can configure tasks to run on a predefined schedule. Tasks include operational functions (e.g. backup configuration, upgrade firmware) and running reports.
14. **AD Nested Groups –** Support for nested groups and recursive searches within groups on an Active Directory.

Important Release Information:

1. Dominion KX1.4 firmware is supported for KX116, KX216, KX232, KX416, and KX432, along with two new Dominion models, the KX 132 and KX 464.
2. After upgrading from CC-SG 2.3 when adding, editing, or deleting devices or ports an error message may appear stating "Unable to refresh security Cache". To update all groups user

needs to go to the device and port group menu and select every group and then click on the Update button (without making any changes). Associations>group manager and select port group manager and later on device group manager and make the update. [E 4528]

3. The latest list of open port scans and description can be found below.
4. A version of JRE is required on client system.
5. When using Firefox browser, JRE 1.4.2_05 needs to be pre-loaded onto the client PC.
6. In Dominion SX, only sys admin user (not “operator” or “observer”) has permission to add device.
7. In Firmware Manager, the format of device firmware versions may vary. Please check the product release notes or compatibility matrix to confirm firmware versions.
8. Element names are case sensitive when input, but not when selected. So do not add two Elements using different case, as only the first one entered can be used. [ST11180]
9. 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]
10. 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]
11. 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]
12. If using a CC-SG 3.0 in conjunction with CC-NOC 5.2/5.4, the time settings on both the CC-SG and CC-NOC 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.
13. When configuring the CC-SG for Active/Active networking mode, only one of the two Default Gateway fields should be filled in and the other left blank. Additional (non-default) Static IP routes can be added to either interface using the Diagnostic Console. [ST9150]
14. When using the Task Manager to upgrade KX device firmware, set the retry interval to 30 minutes or longer, as the upgrade takes ~20 minutes to complete. [ST11303]
15. The Japanese language user interface displays the “Shutdown CommandCenter” timer in seconds instead of minutes. [ST11298]
16. The German language user interface displays the Task Manager’s Recurrence Tab “Start At” time incorrectly as “Start bei” instead of “Start um”.
17. A task created using version 3.0.0 that is in the pending or scheduled state may not run after upgrading to 3.0.2. The task should be removed and added. [ST11789]
18. 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.
19. The time zone for GMT/Indianapolis will report one hour behind. Select a different GMT-5:00 location instead. [ST11661]
20. When configuring Active Directory on CC-SG, please refer to these instructions in place of CommandCenter Secure Gateway 3.0 Admin Guide, page 120, step 3:

    > ‘If not using anonymous binding, type a User name. The User name should be the Display Name, not the Logon, of the user account you want to use to query AD. The user account must be privileged to query AD.’

General Information:

1. For optimal operation, please disable the pop-up blocker in your browser.
2. 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).

3. Please enable or disable the SSL option in Security Manager before setting up CC in clustering mode. By default SSL is enabled.
4. When CC-SG is in cluster mode, the use of static IP addresses is recommended.
5. When device is under “Pause Management”, the ports on that device cannot be deleted.
6. When configuring CC-SG as an Active/Active mode, please enter only a single entry for default gateway in both fields.
7. In order to launch CommandCenter Secure Gateway 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.
8. For connections to KX connected targets JRE 1.5.0_02 is not supported.
9. When upgrading a KX device Raritan strongly recommends that the KX device be re-booted before the firmware upgrade is applied. You can reboot the KX devices directly from CommandCenter Secure Gateway by scheduling a reboot prior to upgrade for all KX devices using the Task Manager feature (under the Setup menu).
10. If upgrading a CC-SG from 3.0.0 to 3.0.2 you may see and can safely ignore an error message in the upgrade log about a “diagcon scriplet failure”.
11. To download the Thick Client to your desktop enter “http(s)://CC_IP_Address/cc.jnlp” 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.

Appendix: 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 Computer 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[1]	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: • RHSA-2004:120 • RHSA-2005:830. • RHSA-2003:101-01

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

[1] CVEs can be found on http://cve.mitre.org.

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 3.0.2
August 2006