CommandCenter® Secure Gateway Release 4.0.0

This is to announce the General Availability
of CommandCenter® Secure Gateway
Firmware Release 4.0.0
as of date:
September 3, 2008

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 release.

Applicability

The CC-SG 4.0.0 release is applicable to CommandCenter ® Secure Gateway hardware Models CC-SG-V1 and CC-SG E1 only.

Important note for CC-G1 customers: Raritan discontinued the CC-G1 model in June of 2007. While CC-G1 customers can upgrade their CC-SG to any firmware versions in the 3.x series, release 4.0 is not supported on the CC-G1 hardware. In order to benefit from the new updates and major fixes included in this release you must upgrade your CC-G1 to any one of the new hardware models: CC-SG E1 or CC-SG V1. Refer to your Raritan reseller or partner for CC-G1 trade-in information and other offers available.

Use one of the following three methods to identify if your hardware is a CC-G1:

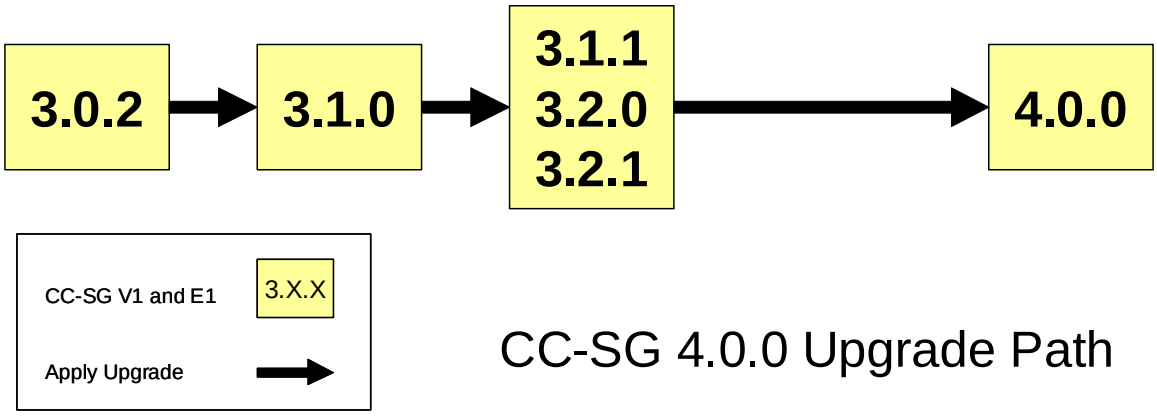
1. Identifying CC-G1 hardware model using the appliance Serial Number:
    - Locate your serial number underneath the appliance
    - If your serial number starts with the two letters XG, your appliance is a G1
2. Identifying your CC-G1 hardware model in the Admin Client:
    - Login to the CC-SG administrative graphical user interface
    - In the Administration drop down menu select the Configuration option
    - Select the SNMP tab
    - In the System Desc area you will see your HW model
3. Identifying your hardware model using the Diagnostic Console command line interface:
    - Using an SSH client (e.g., PuTTY) make a connection using port number 23 to the CC-SG IP address
    - When the Diagnostic Console interface appears login using ‘status’ account
    - In the System Information area at the Model field CC-SG-G1 will be indicated

Do not attempt to upgrade your CC-G1 to this release. You need to backup your CC-G1, restore the database to a CC-SG V1 or E1 hardware unit running the same firmware version, and upgrade the new V1 or E1 hardware unit to this release per the Upgrade Path instructions below.

Upgrade Path

To upgrade to this release you must be running CC-SG firmware version 3.1.1 or higher. As indicated above, you can only upgrade CC-SG V1 or CC-SG E1 but not CC-G1 hardware to 4.0.0.

For customers with firmware version 3.x.x, the following diagram depicts the possible upgrade paths for the CC-SG 4.0.0 release:



We recommend you backup CC-SG prior and after any upgrade step. For detailed step by step instructions on upgrade refer to the Readme file available for this CC-SG release. You may also need to upgrade your Raritan devices. For a complete list of supported devices, refer to the Compatibility Matrix. For instructions on upgrading devices, refer to the CC-SG Administrators Guide.

Updates in This Release

For customers upgrading CC-SG to release 4.0.0 updates include:

- **Support for Virtualization Systems** – Add virtualization environment to CC-SG to enable connection from CC-SG to virtual machines, virtual hosts, and control systems. The new virtualization feature includes streamlined setup of single-sign-on access to your virtualization environment, ability to issue virtual power commands to virtual machines and virtual hosts, and a topology view with one click connections. CC-SG integrates with VMware™ environments and can support features like connectivity to the Virtual Center software, ESX servers, and VMotion™ functionality.
- **Integration of Dominion PX PDU via the IP Network** – Dominion PX can now be either added or discovered on the network when assigned with an IP address. Individual outlets can be assigned to a node in order to allow power on/off/cycle command to that node (server). When integrated via IP (i.e., not connected to another Raritan device), the Dominion PX will appear in Device Tab as a Raritan device, PX administrative interface can be launched directly from CC-SG with no need for another sign on, and PX is included in the Device Asset Report.

  Dominion PX in a managed power configuration, where the PX is connected to a Dominion KX, SX, or KSX via a power CIM or power cable, is still supported in this release as it was in earlier releases.
- **RDP Console Access and Color resolution Enhancements –** a redesigned interface is now available. The RDP interface now allows for setup of both screen size and color depth [E9564, E13930]. Furthermore, when configuring the RDP interface the CC-SG Admin can determine if the RDP interface will behave as a Remote User or Console. [E3562]

- **In-band Software Applications can be used in Direct Mode –** in-band applications such as RDP and SSH can be used in either Direct or Proxy mode. The mode selection is determined based on the Connection Mode configured in the Administration>Configuration setup in the Admin Client.
- **Single Sign on to all In-band Software applications** – username and password can now be used on all in-band interfaces to allow for single sing on.
- **Telnet Interface Support –** a new In-band interface has been added to support connection to devices operating with the Telnet command line protocol. [E9432, E15175]
- **Service Accounts –** Service Accounts are applicable to In-band interfaces such as software applications (e.g., RDP, SSH), embedded service processors (e.g., iLO, DRAC, IPMI), and virtualization. Service Accounts can now be assigned instead of username/password values and can be used in both remote and local authentication to simplify the password change process. A change of the Service Account password will instantly apply to all interfaces using that Service Account without the need for further changes in individual interfaces. Assign Service Account functionality was added to simplify the process of assigning Service Accounts to large groups of interfaces.
- **Text Note Entry to Audit Trail –** the administrator can require selected user groups such as contractors and temporary workers to enter information describing their activity prior to accessing any interface. Once entered, this information is recorded in the audit trail and Access Report and is also displayed in the Node Audit Tab in the node profile. [E12171]
- **Improved Node Profile Including New Tab Design**
    - Interfaces tab – always displays when the node is being selected and provides all Out-of-band, In-band, and Power Control interfaces available to the user.
    - Associations tab – includes all the categories and elements describing the node or the device.
    - Locations and Contacts tab – include location (Department, Site, and Location) and contact (Name, Phone Number, and Cell Phone) information related to the node or device.
    - Notes tab – can be used to capture reminders or other information a user may wish to communicate with other users of this node. The information is kept for reference only and is not captured in the Audit Trail.
    - Audit tab – lists all node access activities done by users required to enter audit. In addition to other information captured in the Access Report for this node, information will include a Free Text Note entered by selected users (see Free Text Note Entry to Audit Trail feature below).
    - Virtualization Data tabs – applicable to virtual machines, virtual hosts, or control system nodes only:
        - Virtual Machine Data – contains information about the operating system, storage, and status of the virtual machine. Additionally, information and hyperlinks are available to the virtual host and control system managing this virtual machine.
        - Virtual Host Data – contains information about the server used, network and routing information. Virtual host Reboot and Forced Reboot

capabilities are available for users with appropriate privileges. A hyperlink to the associated control system node is available.

  - Control System Data - contains data about the control system version, SAN in use as well as virtual host name and other information.

- **Custom JRE Incompatibility Message –** the JRE incompatibility warning message can now be customized by the administrator. The administrator can control the lowest required JRE version from all CC-SG users [E8634]. Administrator selected JRE version cannot be lower than the minimum version provided in the CC-SG Compatibility Matrix.
- **Configurable Power Operation Confirmation Message –** the administrator can now configure a popup message prompting for user confirmation prior to any power control operation [E9058, E12377].
- **Remote Authentication and Authorization Enhancements**
  - Lockout settings policy for failed login may now be applied to remote authentication users. This function has to be enabled by the administrator otherwise, only the remote authentication system enforces their failed login policy [E12928].
  - The maximum length of Active Directory password is now extended from 16 to 32 characters [E10698].
  - The maximum length of TACACS+ key field is extended from 16 to 128 digits [E14199].
  - IP addresses of all Active Directory Domain Controllers returned from the DNS server are cached and used in a case where the DNS server is down [E12378, E13131].
  - "On Demand AD Synchronization" does not require CC-SG to be in Maintenance Mode [E13630].
- **SNMP Enhancements –** on new systems SNMP daemon is disabled by default and requires activation. If the daemon is off, no traps can be sent from CCSG and no Set or Get SNMP commands can be executed from any SNMP manager application [11944]. For customers upgrading to this release, the daemon is enabled if any traps are enabled prior to the upgrade. Additionally, new traps are added to reflect added CC-SG 4.0 functionality. Refer to the MIB v2 file for a complete list of available CC-SG traps.
- **CC-SG Reset –** granular reset options are now available to the administrator also in the Admin Client. Now you can reset IP-ACL in the addition to all other reset options [E11985].
- **Enhanced Reporting Capabilities –** following reports have been enhanced:
  - Audit Trail report can now filter based on Virtualization, Security, Embedded, and other activities audited by the CC-SG.
  - Node Asset report now has a URL field that represents the node Bookmark [E12464]. A Bookmark, sometime referred to as Direct Port Access (DPA), can be used open the node's default interface from a web browser without accessing the CC-SG GUI (CC-SG login will be required). Additionally, this report includes Raritan port ID [E10339].

- All Users Data report now includes a list of privileges and nodes available to each user [E7689].
- Syslog report now also includes Access Report information [E9844].

- **Remote System Monitoring and Historical Data Trending –** remote monitoring can now be activated via the Diagnostic Console. Monitoring includes real time and historical information about system performance including variables such as CPU utilization, processor performance, and disk space availability [E11109].

For more detailed information about the features described above and how to configure and use these features refer to the CC-SG Administrator and User Guides. For those customers upgrading to this release we strongly recommend that you review the 'What's new in this release' presentation in order to understand how these and other changes improve user and administrator experience with CC-SG. The presentation is available on www.raritan.com/support/CommandCenter-Secure-Gateway website in the version 4.0.0 folder.

Major Fixes in This Release

1. Customers with firmware version 4.0.0.5.3 experiencing the following issue may choose to upgrade their firmware: In HTML-based Access Client double clicking one of the nodes in the node tab results in the user being booted out of the client to the login screen. [E16168]
2. CC-SG backup command and automated backup task no longer require breaking up a CC-SG cluster. This includes both local backup and backup to a remote ftp location. [E13282]
3. Embedded service processor card polling interval for each console and power interface is increased from 3 minutes to 10 minutes. This includes IBM RSA, Dell DRAC, and HP iLO. [E13286]
4. Client login timeout on the HTML Access Client is now set for 1 minute, same as in the Admin Client. [E14698]
5. CC-SG backup file name and description are not saved in a readable format in some cases in a non-English version. Correct character mapping is now in place and file name is readable. [E13169]
6. User with no "Device, Port and Node Management" privilege is now able to see nodes in custom view filtered by group. [E14177]

Internal notes: E13913, E 14355, E13210, E13207, E12726, E14147, E14008, E13333 and E15494.

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
www.raritan.com/support/CommandCenter-Secure-Gateway/

- **CC-SG 4.0 Upgrade Readme File –** step by step instructions for customers upgrading to this release.
- **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.
- **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 and CC-SG V1each have their own version of the Quick Setup Guide.
- **MIB File –** this file can be used to upload trap definitions onto an SNMP manager applications such as HP Open View.

Release Package Details

The file provided for this upgrade includes the following components:

- Firmware file: scc40_upgrade_p23_rpm_rfp.zip

General Upgrade Instructions

Refer to the Readme file for detailed step by step upgrade instructions.

When upgrading the CC-SG, a pop-up message will be seen once the upgrade has "completed". The pop up will indicate that the CC-SG will be accessible after 8 minutes. While typically the process takes about 8-10 minutes, depending on the CC-SG database size, it may actually take 30 - 60 minutes before a user can login. To view the upgrade progress you can login to the Diagnostic Console. SNMP trap for upgrade results can be enabled. [E 15245, E 15492]

Important Notices

1. For optimal operations, disable the pop-up blocker in your browser.
2. CC-SG 4.0 Compatibility Matrix indicates DRAC4 1.35 (Build 09.27). If your DRAC 4 cards have version 1.5, you need to update the DARC Remote Console file in CC-SG. Download the file from the Raritan website to a network location and upload it from the Administration>Applications menu onto the CC-SG. Note that you can only use either DRAC 4 1.35 or 1.50 but not both. [E15445]

Important notices for users of the new Virtualization feature:

3. The first time you connect to a virtual machine, using any supported browser, you may be asked to download an add-on from VMware. Once the add-on is installed, restart your browser.
4. If you are using Firefox on Windows, you must add the IP address of the CC-SG to the Allowed Sites for Add-ons list and the Allowed Sites for Pop-ups list in the browser before connecting to a VMW Viewer interface.

Limitations and Restrictions

1. When clicking Connection - Exit to close MPC for targets connected to KX2, KSX2, KX, and KSX the window does not close. A page comes up saying "Page cannot be displayed". To close MPC click on the X at the top right corner of the MPC window or by disconnecting port from CCSG. [E14379]
2. When a Dominion PX in a managed power strip configuration is rebooted, the power strip outlets in CCSG are deleted. [E12777]. Note that this issue does NOT apply to a Dominion PX configured as a device managed by the IP network. Workaround: prior to rebooting the PX, pause management on the Raritan device managing the Dominion PX. Only after the Dominion PX is fully booted, resume the managing device. [E15440]
3. A port with a connected Dominion PX managed power strip may not be visible in a custom view when using Device Group filter. [E14359]
4. When restoring the CC-SG, the only two functional Restore Types are:

- Standard: This restores the database portion of the CC-SG.
- Custom: Select only from Restore Data, Restore Logs, and Restore Firmware Binaries. Selecting Restore CC Firmware or Restore Applications will cause the Restore to fail. [E15033]

5. Scheduled tasks like Access Nodes Report, Audit Trail Report, Access Report, and Error Log all have a limit of 5000 lines only. Any activity beyond the 5000th line will not be included in the report. Workaround: make the time span for the report shorter such that within the provided period less than 5000 lines are included. [E15488]
6. 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] Note that virtual media is not supported in Proxy mode.
7. 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, E15645]

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
- If the Java-based Admin Client becomes unresponsive you may need to increase your Java Applet memory. For example, to increase the Java Applet memory limit of a Windows XP machine running Java version 1.6 follow these steps:
  1. Choose Start > Control Panel.
  2. Double click the Java icon. The icon may be listed under Other Control Panel Options.
  3. On the Java tab, click the View button in the Java Applet Runtime Settings section. The Java Runtime Settings dialog appears.
  4. Select the line with the highest version number. Double click in the Java Runtime Parameters box for that line.
  5. Enter -Xmx300m in the box and click OK. This parameter sets the Java maximum heap size to 300MB.
  6. Click OK.
  7. Restart your browser.

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 NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

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

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

India

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

Japan

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

Europe

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

United Kingdom
Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

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

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

Korea

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

Melbourne, Australia

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

Taiwan

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