CommandCenter® Secure Gateway Release 4.1.0

This is to announce the General Availability
of CommandCenter® Secure Gateway
Firmware Release 4.1.0
January 31, 2009

Contents

Introduction 2
Applicability 2
Upgrade Path 3
New in This Release 3
Security and Compliance Information 7
Additional Release Documentation 7
Release Package Details 8
General Upgrade Instructions 8
Important Notes 9
Limitations and Restrictions 9
Troubleshooting 10
Raritan Support Contacts 12

(Note – numbers in parentheses throughout this document are reference numbers internal to Raritan.)

Introduction

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

Applicability

The CC-SG 4.1.x 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, releases 4.0 and later are not supported on the CC-G1 hardware. In order to benefit from the new updates and fixes included in this release you must replace your CC-G1 unit(s) with either of the current hardware models: CC-SG E1 or CC-SG V1 (note that if you are running multiple CC-SG units, they must be the same model). Please consult 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 G1 model:

1. Identify 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. Identify 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. Identify 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

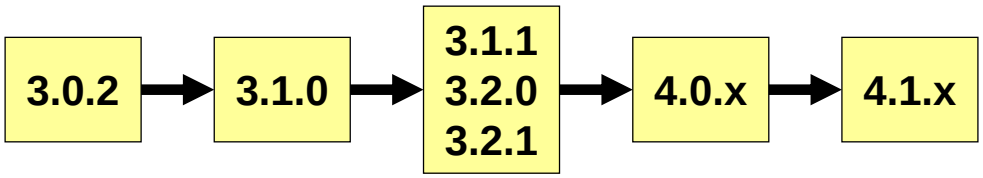
- In the System Information area at the Model field CC-SG-G1 will be indicated

Do not attempt to upgrade your CC-G1 to this release. Please back up 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 4.0.0 or 4.0.1. As indicated above, you can upgrade CC-SG V1 or CC-SG E1 but not CC-G1 hardware to 4.1.x.

For customers with firmware version 3.x.x, the following diagram depicts the possible upgrade paths for the CC-SG 4.1.x release:



Please back up your CC-SG prior and after any upgrade step. For detailed step by step instructions on upgrading, 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.

New in This Release

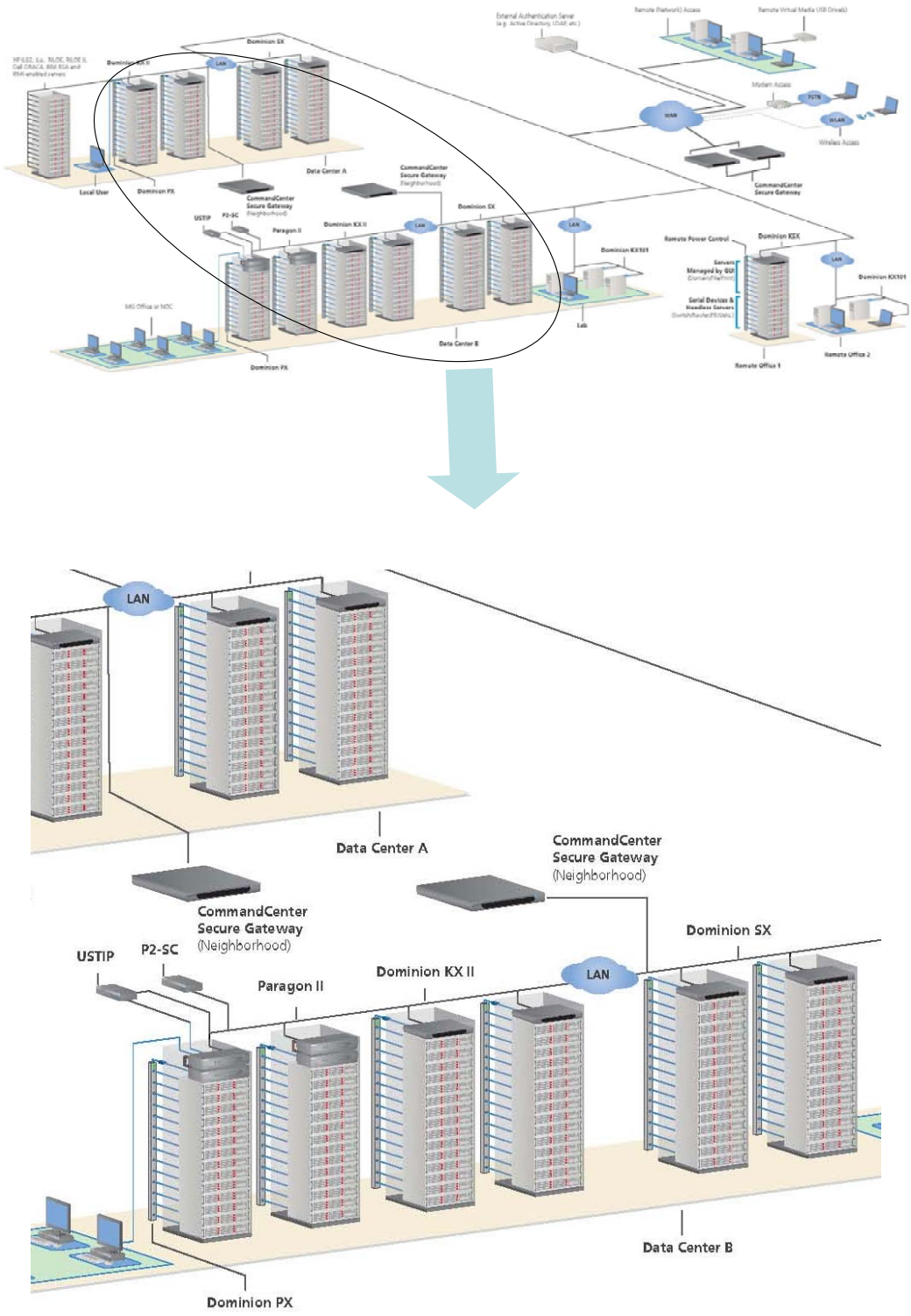
Primary Feature Enhancements

Support for Blade Servers connected to KXII Devices – CC-SG support the accessing of blade servers connected to Raritan Dominion KX-II KVM over IP switches, version 2.1 and higher. Supported blade models include most Dell, HP and IBM Blade Servers. Please see the KX-II 2.1 release notes for further information on supported blade models.

The CC-SG user and administration guides have been updated to include instructions on the use of this feature.

CC-SG Neighborhood – A Neighborhood is a collection of up to 10 CC-SG units, deployed together to serve the needs of the enterprise. As pictured, implementing a neighborhood helps to increase performance and redundancy by

- Distributing CC-SG units geographically
- Distributing bandwidth across CC-SG units



In such an environment, users access multiple CC-SG units with single sign-on using the Access Client. The accessing of different CC-SG's is seamless and transparent to the user.

Note that a CC-SG unit belongs to one Neighborhood only. Also, all CC-SG units in the same Neighborhood must be of the same firmware version and must be either standalone or Primary Nodes of clustered CC-SG units.

The CC-SG Neighborhoods feature provides several benefits:

- Scalability: add more CC-SG's as your environment grows and balance the load across multiple units
- Regionalization
  - Local authentication for local access
  - Around the clock global operations - avoid failures across regions
- Departmentalization / local administrative autonomy
  - Access network partitioning
  - Segment by access tools, Raritan device type, user type, etc.
  - Deploy CC-SG units across different subnets

Support for KX-II release 2.1 – CC-SG 4.1 has been developed to be compatible with KX-II release 2.1.

Dominion PX Support Enhancements –

- Security: Administrators can now edit the PX Device username and password fields (stored on CC-SG) that were used when adding the PX Device.
- Synchronization: Some changes incurred in managed PX devices are now reflected in CC-SG. Included are changes to an Outlet state, upgrades to the PX firmware, and changes to the username/password.
- Command failures are also logged.

VMware Virtualization Support Enhancements – The Virtualization Manager Add/Edit Control System (and Virtual Host) screens now include options to:

- Select / Deselect all or a subset of VMs
- Select / Deselect All by Interface type
- Sort the rows by column

Cluster Management Enhancements – When a failed CC-SG restarts it will automatically go into Waiting mode. It can also be configured to automatically go into Backup mode during a configurable timeframe.

Previously, returning the pair to Primary/Backup status was a manual process. Now, it is automated. (16584) Additional enhancements and improvements include:

- Simplified Cluster Creation Procedure (16582)
- DNS Support for Improved Usability
- Automatic Redirection to Primary Node (If backup IP address is entered and backup system is running)
- Automatic Rebuilding of a Cluster in Case of Failure
- On Demand switching of the Primary and Waiting systems

Minor Enhancements

Updated MIB – The MIB has been updated to account for the new customer SNMP traps. (17939)

Disc Drive Field Upgradability – The CC-SG's two disk drives may now be upgraded in the field. To ensure proper replacement, drives can only be obtained through Raritan Tech Support. A new user interface for step-by-step diagnosis is included in this release and written instructions are provided with the drive(s). The drives are hot-swappable and may only be used with the current E1/V1 CC-SG platform. In order to implement the replacement, the CC-SG unit must be running this new release. Note that there are two drives available; one for the E1 and one for the V1. (15275, 17339, 17712, 17713)

Device Configuration File Backup and Restore – This new feature enables a backup configuration file to be used on a new or replacement unit to avoid needing to re-enter the information. Customers are encouraged to back up their device configuration files regularly and often in order to receive the benefit this feature provides.

Device Configuration Copy Support – This feature allows administrators to use CC-SG to conveniently copy the configuration from one Raritan device to another. For example, users can copy one KX2 device's configuration to other KX2 devices managed by CC-SG. This is also true for SX, KSX-II, and KX2-101.

Enhanced AES Support – For compatibility with new KX-II features, release 4.1 includes AES-256 support. When AES is enabled, it's now possible to specify the strength of the AES encryption (AES-128 or AES-256). The default value is AES-128. Please see the admin guide for special configuration notes regarding this feature. To use AES encryption, first ensure that your web browser supports this stronger encryption. (17417)

SNMP Trap Enhancements – Several traps have been added related to cluster status and node changes.

Upgrade Enhancements – A few adjustments have been made to

messages seen during the upgrade process that are clearer and more user-friendly.

User Interface Enhancements – The CC-SG Backup command and Backup Task screens have been enhanced:

- The Password field is saved along with the other fields when the "Save as Default" option is clicked.
- The default values now apply to both the Backup command and the Backup Task.
- Once a Backup Task has been created, changes to the default values do not affect that task, regardless of its state (running, pending, or scheduled). The saved default values (IP Address, Username, Password, Directory, Filename) are reset to factory defaults (blank) if the administrator uses the CC-SG Reset command. (16287)

Browser Support – CC-SG may be accessed with Firefox 3.0.x. Please see the CC-SG compatibility matrix for a full list of supported browsers.

Client Support – CC-SG now supports 64 bit client operating systems, including Windows Vista 64 bit and Windows XP Professional x64 Edition. Please reference the compatibility matrix for any limitations (JRE version, etc.). (15169)

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.

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 4.1 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: scc41_upgrade_p22_rpm_rfp.zip

General Upgrade Instructions

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

Special Upgrading Notes:

1. When upgrading from 4.0 to 4.1, any web browser interfaces that were configured in 4.0 with an https URL will have the TCP port set to 80 after upgrade (If you click edit on the interface, 80 may be displayed, even though 443 is being used.) When editing an existing Web Browser interface that is configured for SSL, make sure to change the displayed TCP port from 80 to 443. By default, the port reverts to 80. Please make this change or TCP port 80 will be saved to the database and the connection will not be made. (17492/17334)
2. Users of 4.0 that upgraded their DRAC application to 1.5 using the JAR file downloaded from raritan.com need to again download the file. If not reloaded, the existing DRAC interfaces will launch the DRAC 1.35 JAR file. (17780)
3. 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.

Important Notes

1. As of CC-SG 4.2, which is planned for release mid-2009, **access to CC-NOC from CC-SG will no longer be supported**.
2. Raritan recommends using JRE 1.6.0_05 or 1.6.0_07 with CC-SG 4.1. This version has been proven not to support JRE 1.6.0_03, 1.6.0_10, or 1.6.0_11. CC-SG is also compatible with JRE 1.5.0. (18041)
3. If using Windows and using the client applet, JRE will only work with Windows 32. See http://java.sun.com/javase/6/webnotes/install/system-configurations.html for Java support information. (17855)
4. If you have a CC-SG E1 unit, LAN1 port on the back of your E1 must be connected to Ethernet before performing an upgrade to this release. If your LAN2 is connected to Ethernet in addition to LAN1 (recommended configuration), you do not need to check Ethernet ports prior to the upgrade. However, if only one port is connected, we recommend you make sure that LAN1 and not LAN2 is used. If the ports on the back of your CC-SG E1 unit are not labeled, then LAN1 is the top Ethernet port and LAN2 is the bottom one.
5. For optimal operations, disable the pop-up blocker in your browser.
6. Virtualization: During the first connection to a virtual machine, you may be asked to download an add-on from VMware. Once the add-on is installed, please restart your browser.
7. 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.
8. Cluster rebuilds: When selecting a rebuild time, please be aware of possible differences in time zones between units.

Limitations and Restrictions

1. The number of characters that may be used in the various fields within CC-SG has been noted in Appendix J of the admin guide. (14203)
2. There is a caching period of thirty minutes when passwords are changed. As a result, after changing a password, the prior password can be used for an additional thirty minutes. This applies only to customers using Windows 2003 for Active Directory. Local password changes are not

affected. (17007)

3. When clicking Connection - Exit to close MPC for targets connected to KX-II, 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.
4. A port with a connected Dominion PX managed power strip may not be visible in a custom view when using Device Group filter.
5. For Dominion KX-II if using CC-SG in Proxy mode change the default in the Default Application tab in Application manager to Virtual KVM Client. Note that virtual media is not supported in Proxy mode.
6. CC-NOC Sync keys are not accepted when CC-SG uses LAN2 port. (17550)
7. “Restore Type” options are not available while restoring CC-SG via SSH. (16631)
8. AES encryption (128 and 256) will only work with a Vista/IE7 combination or Firefox.
9. IE6 does not support AES-256 encryption and XP with IE6/IE7 does not support AES-256 encryption.
10. If enabling AES 256, ensure that the jurisdiction files are installed on the client. Otherwise, you will be locked out of the CommandCenter.
11. AES-256 is not supported when communicating with CC-NOC.
12. When using a Linux client, the Virtualization topology view cannot be printed.
13. Clusters should be implemented with identical CC-SG units:
    - All units should either be V1 or E1 units
    - All firmware should be identical

Troubleshooting

1. 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
2. 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:

- Choose Start > Control Panel.
- Double click the Java icon. The Java icon may be listed under Other Control Panel Options.
- On the Java tab, click the View button in the Java Applet Runtime Settings section. The Java Runtime Settings dialog appears.
- Select the line with the highest version number. Double click in the Java Runtime Parameters box for that line.
- Enter -Xmx300m in the box and click OK. This parameter sets the Java maximum heap size to 300MB.
- Click OK.
- 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