

CommandCenter® Secure Gateway Release 4.3.0

This is to announce the **General Availability**
of CommandCenter® Secure Gateway
Firmware Release 4.3.0
January 15, 2010

Contents

Introduction	2
Applicability	2
Upgrade Path.....	3
New Features in This Release	4
Security and Compliance Information	7
Additional Release Documentation	7
Accessing the Updated Firmware	7
General Upgrade Notes	8
Important Notes.....	8
Limitations and Restrictions	9
Troubleshooting.....	10

(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 4.3.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

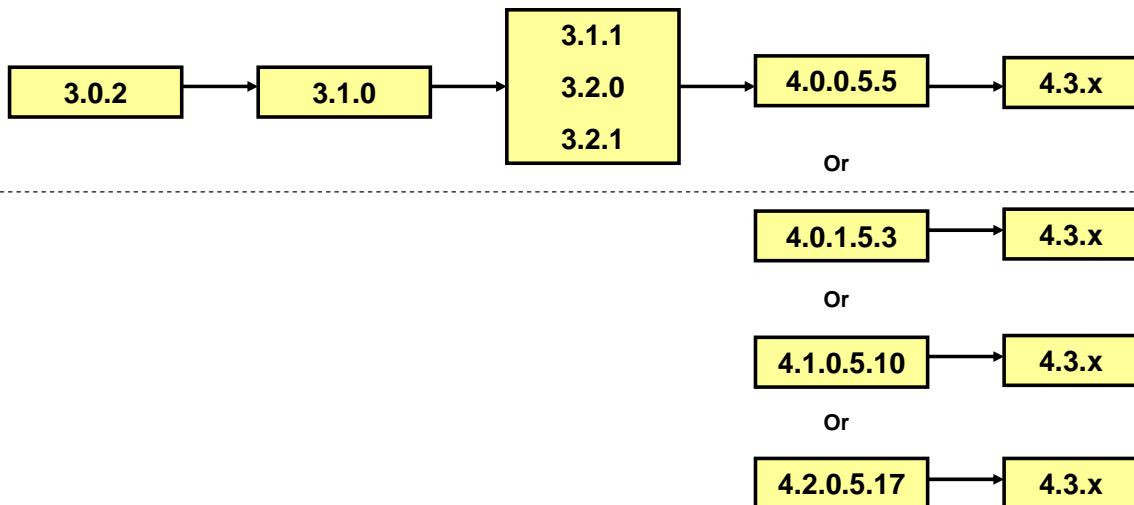
be indicated

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 4.0.0.5.5 and above, as depicted in the diagram below. There may also be additional upgrade steps to take, depending on your current version. As indicated above, you can upgrade CC-SG V1 or CC-SG E1 but **not CC-G1** units to 4.3.0.

For customers with firmware version 3.x.x, the following diagram depicts the possible upgrade paths for the CC-SG 4.3.x release:



Please back up your CC-SG before 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 Features in This Release

Primary Feature Enhancements

Control Power for Servers Connected to Any PDU Supported by Power IQ

In addition to the existing support for Raritan's PX Rack PDU's, this feature enables remote power control of CC-SG nodes (Power IQ IT Devices) that are connected to any non-Raritan Rack PDUs that can be managed by Power IQ. This feature requires the use of Power IQ version 1.5 or higher.

In this release, the Import/Export function introduced in release 4.2 is used to provide node information from Power IQ to CC-SG. There is also the option to export node data from CC-SG for import into Power IQ. Both options are available in order to allow customers to manage this function in the manner that best meets their particular operation. (23694)

Virtual CC-SG Evaluation

A software-only evaluation version of CC-SG is now available, which can be installed on VMware capable virtualized servers and PC's. The "Eval" is fully functional with a few exceptions:

- Supports a maximum of 10 "interfaces"
 - Examples are one node with 10 interfaces or 10 nodes with one interface each.
 - An interface can be a target server, serial device, outlet, DRAC connection, etc. Interfaces can also be out-of-band KVM (KX, SX, IPR, etc), and in band targets, such as SSH, Telnet, VNC, RDP and the embedded targets such as ILO, DRAC, RSA.
- The optional CC-SG WS-API is not supported.

No special licenses are required. The CC-SG Eval is available in DVD format or as a download from www.raritan.com. Note that the file is very large and sufficient time should be allotted if downloading. The DVD may also be ordered by contacting Raritan's sales department and requesting part number CCSG10-VA. There is no charge for the CC-SG virtual trial.

The CC-SG Eval is supported to run on VMWare ESXi and VMWare Server.

Important: The purpose of the virtual version of CC-SG is to enable an easy and convenient way to evaluate the product; it is not available with full functionality. To obtain full functionality, the CC-SG E1 and V1 appliances are available.

WS-API Enhancements

The optional WS-API available for use with CC-SG has been enhanced to enable the following functions:

- User Management: Provides the ability to add, delete, get, get all, edit, add user(s) to a group and delete user(s) from a group. (18918)
- Accessing the HTML Client: now provides the ability to retrieve the full URL for the CC-SG HTML access client. (20593)
- Support of Node Power Control (23525): Enables power control of CC-SG nodes.
 - Power IQ interfaces
 - Managed power strips
 - Embedded IT resources (DRAC, iLO, RSA)
- Audit Log: Allows users of the API to access a consolidated audit log containing information about access and connectivity activity. (23523)

.NET client support

Users may now access target servers connected to Dominion KX II switches, through CC-SG with the new Windows based "Active KVM Client" (AKC), which utilizes Microsoft's .NET technology. AKC is supported on the Windows' XP, Vista and Windows 7 operating systems.

CC-SG acts as the download server for AKC. You can trust CC-SG as the download server or explicitly require AKC Download Server Certificate validation, which requires upload or creation of a CC-SG SSL certificate with a valid host designation, expiry period and signed by a trusted root CA. If not installing AKC Download Server certificates, the CC-SG administrator must be running JRE 1.6.0_10 or above in order to set up the certificates.

Note that the Internet Explorer browser must be used when opening this client. Please refer to the Compatibility Matrix for the supported IE versions.

Windows 7 Support

CC-SG now supports the access of target devices running Windows 7. The use of Windows 7 on client PC's is also supported. Each version of Windows 7 is supported (Home Premium, Professional and Ultimate).

DRAC 5 Support

In addition to the longstanding support for DRAC 4, CC-SG now provides access to Dell Remote Access Controller 5. (20975)

Minor Feature Enhancements

- Direct remote access to KX-II switches that are under CC-SG control.
- Microsoft RDP Client: In addition to the already-provided RDP client, the Microsoft RDP Client has been added as an additional option. This version of the client is especially beneficial when using Windows 7, Windows 2008 Server and the Japanese editions of Windows.
- With this release, the access method for existing devices or a new device can be applied easily. Changes can also be selectively applied to existing devices. (24464)
- Support of virtual media in proxy mode when using the MPC client (this support was added in 4.2, but was restricted to using the VKC client).
- Option to allow administrators of CC-SG to define the maximum number of user KVM sessions per Raritan device. (23603)
- Windows 2008 Server Support – access to target servers running Windows 2008 is supported.
- Power control interface for HP IA 64 Integrity iLO2 Support. (19421)
- “Backspace” Consistency - In Windows Telnet, the “Delete” key is used for backspacing. The CC-SG backspace was executed with CTRL+Backspace. For consistency, the CC-SG Telnet method is also now the Delete key. (20689)
- Prior to 4.3, the “Switch Primary and Backup” button was enabled during the “Waiting” cluster state. The intention is to make it available only when the backup unit becomes active. The button is now disabled when the backup unit is in the “Waiting” state. Note that the term “IP Failover” is now used in CC-SG instead of Primary or Backup. (20245)

Recommissioned Feature

“IP Isolation”, a feature formerly known as “Active-Active” has been reinstated. This feature allows clients to be isolated from devices by placing them on separate networks and requiring out-of-band node access to pass through CC-SG. The name change is reflected in the product GUI and its documentation.

- - -

For more detailed information about the features described above and how to configure and use these features refer to the CC-SG Administrators and User Guides.

Security and Compliance Information

Refer to the CC-SG Administrators Guide 'Appendix B: CC-SG and Network Configuration' for specific settings.

Additional Release Documentation

The following updated documents and files can be found at www.raritan.com/support/CommandCenter-Secure-Gateway/

- **CC-SG 4.3 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's guide to features and functionality.
- **Quick Setup Guide** – a short guide to quick setup. CC-SG E1 and CC-SG V1 each 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.

Accessing the Updated Firmware

The new firmware can be accessed in the release 4.3 section at <http://www.raritan.com/support/commandcenter-secure-gateway/>.

General Upgrade Notes

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

Special Upgrading Notes:

1. When upgrading from **4.0 to 4.3**, 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 several minutes. To view the upgrade progress you can login to the Diagnostic Console.
4. If upgrading from release 4.1.x, CC-SG allows administrators to run hard drive diagnostics. Administrators should perform this function before upgrading to 4.3. (18717)

Important Notes

1. Release 4.3 has been validated for use with JRE 1.5.0_10, 1.5.0_12, 1.6.0_05, 1.6.0_07, and 1.6.0_10 thru 1.6.0_13. This version has proven not to support JRE 1.6.0_03. (18041)
2. If using Windows XP or Vista, CC-SG supports the 64 bit OS. However, if using a Java plug-in, only the 32 bit plug-in is supported. See <http://java.sun.com/javase/6/webnotes/install/system-configurations.html> for Java support information. (17855)
3. For optimal operations, disable the pop-up blocker in your browser.
4. 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.
5. 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.

6. Cluster rebuilds: When selecting a rebuild time, please be aware of possible differences in time zones between units.
7. The Admin Client has occasionally shown to "crash" when left idle for extended periods of time. (19619)
8. During the CC-SG boot-up sequence, should the following message be displayed, it can be safely ignored (seen on the local KVM console port only):

Memory for crash kernel (0x0 to 0x0) not within permissible range

9. During boot-up, a normal delay of up to two minutes may occur after seeing the following message (local KVM console port only):

Red Hat nash version 5.1.19.6 starting

Limitations and Restrictions

1. The "Bookmark Node" feature is not supported when using Internet Explorer version 8 (IE8). (20053, 20237)
2. VMW Viewer interface cannot be accessed with Firefox 3.x when using Windows 7 (a Windows issue). (25753)
3. The "Exit" option in the MPC client's "Connection" menu does not function when running on Linux. Use the X in the corner of the window as an alternative. This issue has been seen when using the following:
 - Fedora Core 6: JRE 1.6.0_13; Firefox 3.0.10
 - Fedora Core 7: Firefox 2.0.0.14, JRE 1.5.0_13 and JRE 1.6.0_13
 - Red Hat Enterprise - Release 5.2: Firefox 3.0.10, JRE 1.6.0_07 and JRE 1.6.0_13(19999)
4. Unable to launch RSA Remote Console from CC-SG when using JRE 1.6.0_10 and higher. Downgrade to 1.6.0_07. This is a SUN issue, and when fixed will no longer be a restriction in CC-SG. (19651)
5. If using Firefox, FireFox 3.6 and higher require JRE 1.6_10 and higher.
6. There is a caching period of thirty minutes when remote 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)
7. A port with a connected Dominion PX managed power strip may not be visible in a custom view when using Device Group filter.

8. When a Dominion PX in a managed power strip configuration is rebooted, the power strip outlets in CCSG are deleted. 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. (25166)
9. PX Power Strip outlets are deleted when power strip is re-booted. (16502)
10. "Restore Type" options are not available while restoring CC-SG via SSH. (16631)
11. AES encryption (128 and 256) will only work with a Vista/IE7 combination or Firefox.
12. IE6 does not support AES-256 encryption and XP with IE6/IE7 does not support AES-256 encryption.
13. If enabling AES 256, ensure that the jurisdiction files are installed on the client. Otherwise, you will be locked out of the CommandCenter.
14. When using a Linux client, the Virtualization topology view cannot be printed.
15. When using the WS-API provided by Raritan for CC-SG, an IP address must be used – not a hostname. (20353)
16. When using the WS-API, the certificate has to be regenerated when CCSG is restored. (20381)
17. When generating a self signed certificate from CC-SG, don't use the special char "\$" (dollar sign) otherwise, the certificate won't be installed on CC-SG, even though the message indicates that it has been created successfully. (20282)
18. Clusters should be implemented with identical CC-SG units:
 - All units should either be V1 or E1 units
 - All firmware should be identical

Troubleshooting

Please refer to the troubleshooting sections of the CC-SG Administrators guide if issues should occur during the upgrade process.