Release Notes

CommandCenter® Secure Gateway Release 4.2.0

This is to announce the General Availability

of CommandCenter® Secure Gateway

Firmware Release 4.2.0

July 15, 2009

Contents

(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 4.2.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

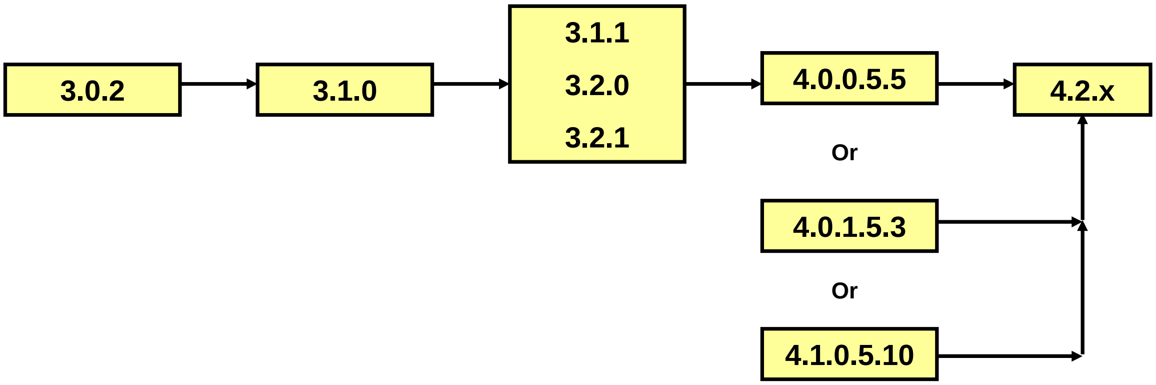
be indicated

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 or 4.1.0.5.10 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** hardware to 4.2.0.

For customers with firmware version 3.x.x, the following diagram depicts the possible upgrade paths for the CC-SG 4.2.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 in This Release

Primary Feature Enhancements

Import/Export

Release 4.2 includes a very comprehensive import/export capability. CSV files can be imported to help expedite the process of configuring devices, nodes, users, associations, and PDUs. A few benefits of using this feature include:

- Save time by using data maintained in a spreadsheet of IT infrastructure profiles; administrators can manipulate it and save it as a .csv file for importing into CC-SG.
- Leverage the data already in CC-SG; administrators can export from CC-SG for use in other applications.
- **Share data between CC-SG and PowerIQ**.

Import/Export files include:

- Import and Export of Categories and Elements
- Import and Export of User Groups and Users
- Import and Export of Nodes and Interfaces
- Import and Export of Devices and Ports
- PowerIQ Import and Export File

(5410, 5464, 13037, 15941, 18774, 18775, 18776)

WS-API Enhancements

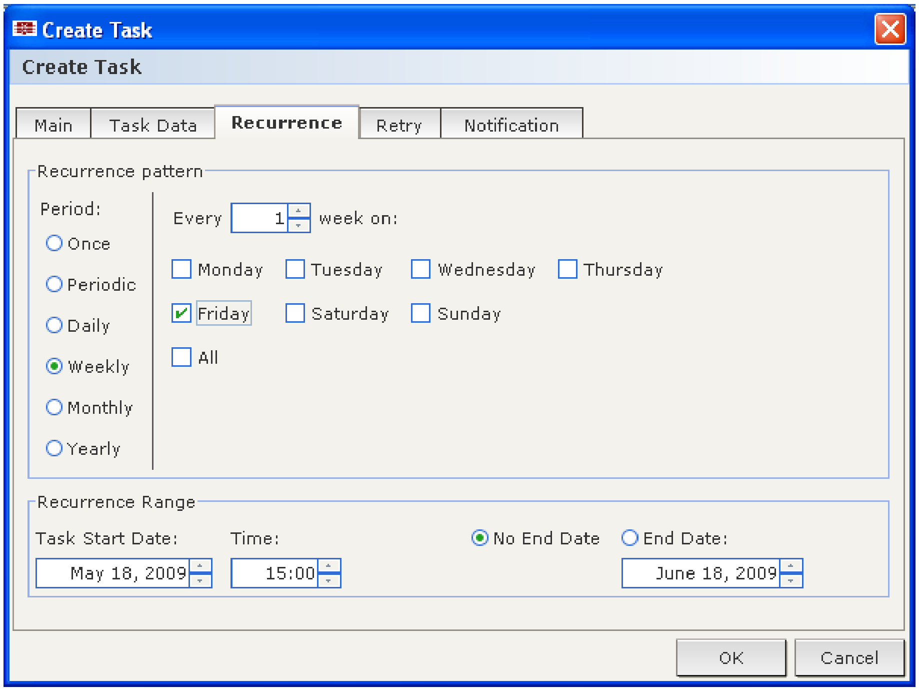
Two new features have been added to the optional WS-API:

- Automated Node Renaming
- Automated adding/removing Users from User Groups

The CC-SG WS-API and its support option have been added to the Raritan price list.

Active Directory Enhancements

Prior to release 4.2, CC-SG allowed administrators to configure a daily synchronization with an Active Directory database. With this release, this feature has been expanded to allow a more flexible synchronization schedule, as seen in the following Task Manager menu samples:



Create Task

Create Task

Main | Task Data | **Recurrence** | Retry | Notification

Recurrence pattern

Period:
○ Once
○ Periodic
○ Daily
● Weekly
○ Monthly
○ Yearly

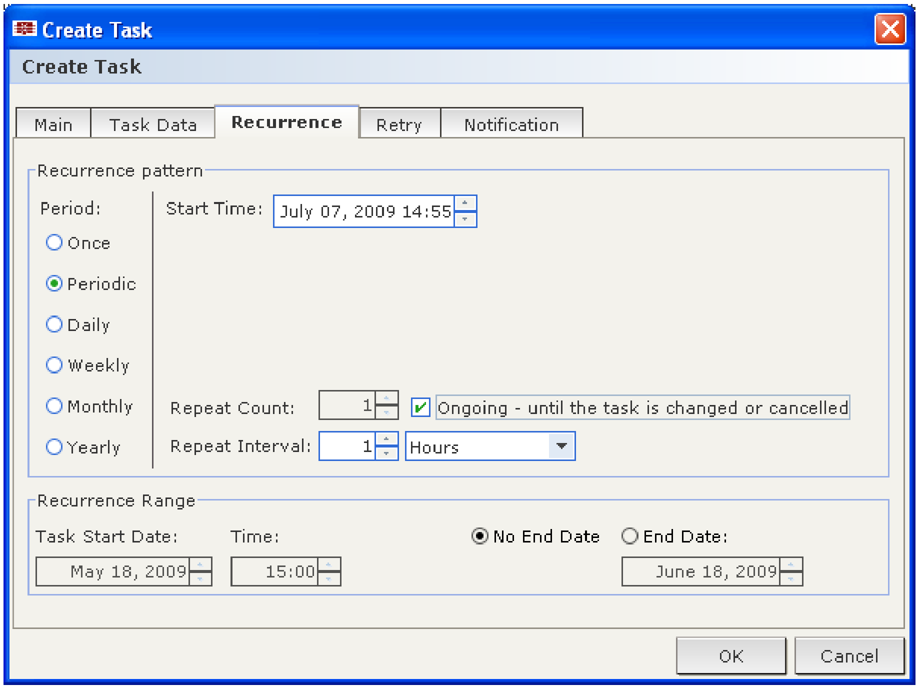
Every 1 week on:

□ Monday □ Tuesday □ Wednesday □ Thursday
☑ Friday □ Saturday □ Sunday
□ All

Recurrence Range

Task Start Date: May 18, 2009
Time: 15:00
● No End Date
○ End Date: June 18, 2009

OK Cancel



Create Task

Create Task

Main | Task Data | **Recurrence** | Retry | Notification

Recurrence pattern

Period:
○ Once
● Periodic
○ Daily
○ Weekly
○ Monthly
○ Yearly

Start Time: July 07, 2009 14:55

Repeat Count: 1 ☑ Ongoing - until the task is changed or cancelled
Repeat Interval: 1 Hours

Recurrence Range

Task Start Date: May 18, 2009
Time: 15:00
● No End Date
○ End Date: June 18, 2009

OK Cancel

(12123, 13323, 13211, 17510, 18496, 19061)

CCSG-KXII-Paragon Integration

KX II is now supported as an IP access point to Paragon II. You can also connect Paragon II to a KX II device that is managed by Raritan's

CommandCenter Secure Gateway (CC-SG), allowing access to Paragon II from the CC-SG client. For complete compatibility when using CC-SG, it is recommended that the KX II device connected to Paragon II is running version 2.1 or later.

Minor Enhancements

Support of Virtual Media in Proxy Mode

When accessing the Dominion KX II from CC-SG, proxy mode is now supported when using the VKC client and the virtual media CIM. (Proxy mode allows you to connect to a node or port by passing all data through CC-SG.) The MPC client is not supported in proxy mode.

Note that proxy mode increases the load on your CC-SG, which may cause slower connections. However, proxy mode is recommended if you are more concerned about the security of the connection. Please reference the updated *CC-SG Administrators Guide* for further details.

(19257)

KX II 832 and 864 Upgrades

These new 8-user Dominion KX II models can be upgraded from CC-SG.

Sorting of Node Groups and Device Groups

Prior to this release, when Node (or Device) Group Manager is opened, the existing Groups were not sorted in the left panel. When a new Group was added it did not appear in any particular order and could be difficult to locate. In 4.2, when the Node (or Device) Group Manager is opened, all existing Node (or Device) Groups are sorted in the left panel in alphabetical order. Also, when a new Group is created it is inserted into the left panel in alphabetical order.

(16249)

Miscellaneous

- "Messages" column of the Access Report now displayed in the Admin Client (16263)
- Ability to edit the name of the VirtualCenter (17976)
- Added IPMI status to availability report (19243)
- More log information added when exception occurs from Virtualization API (18658)
- Full Name field added to new user form for better identification (17097)

- Support of Internet Explorer version 8 (19248)

Decommissioned Features

The following features or products are no longer supported in 4.2.0:

- Access to CC-NOC
- Active-Active network configuration

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 4.2 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 4.2 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 4.2**, 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 4.2. (18717)
5. The system’s built-in Compatibility Matrix, which is available from the drop-down “Administration” menu, indicates compatibility with only the current and previous version of Dominion KX II (releases 2.1.0 and 2.1.10). However, the new 8-port models run on release 2.1.8, which *is* compatible with CC-SG 4.2.

Important Notes

1. Release 4.2 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) notwithin 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. When switching Paragon II channels in a PCCI configuration, the CC-SG client closes. To work around this issue, disable the “tabbed browsing” feature in IE7. (20212, 18908)
3. When switching Paragon II channels in a PCCI configuration, the MPC or RRC client may become exhausted with connections and freeze. (19429)
4. 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)

5. As of the date of this release, CC-SG is not supported for use with Firefox 3.0.11. Version 3.0.10 is recommended. (20430)
6. 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)
7. The number of characters that may be used in the various fields within CC-SG has been noted in Appendix J of the Administrators Guide. (14203)
8. 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)
9. A port with a connected Dominion PX managed power strip may not be visible in a custom view when using Device Group filter.
10. 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.
11. CC-NOC Sync keys are not accepted when CC-SG uses LAN2 port. (17550)
12. “Restore Type” options are not available while restoring CC-SG via SSH. (16631)
13. AES encryption (128 and 256) will only work with a Vista/IE7 combination or Firefox.
14. IE6 does not support AES-256 encryption and XP with IE6/IE7 does not support AES-256 encryption.
15. If enabling AES 256, ensure that the jurisdiction files are installed on the client. Otherwise, you will be locked out of the CommandCenter.
16. When using a Linux client, the Virtualization topology view cannot be printed.
17. Certificates generated from the Administration > Security > Generate Certificate Signing Request option and Generate Self Signed Certificate option are not restored when a complete backup is taken and restored on another CC. (20434)
18. When using the WS-API provided by Raritan for CC-SG, an IP address must be used – not a hostname. (20353)
19. When using the WS-API, the certificate has to be regenerated when CCSG is restored. (20381)
20. 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)

21. 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.