CommandCenter Secure Gateway (CC-SG) Release 5.4.0

Release Notes v2

Introduction

These release notes contain important information regarding a new release of CommandCenter Secure Gateway. Please read the entire document and the related documentation available for this release.

Release 5.4.0 includes several new features and maintenance enhancements.

Release 5.4.0 firmware and all documents & files mentioned in these release notes are available at **http://www.raritan.com/support/commandcenter-secure-gateway/**.

The Release 5.4 firmware is available to CC-SG customers with up-to-date maintenance contracts.

Updated Product Documentation

This following CC-SG documents have been updated for this release:

- CC-SG Administrators Guide
- CC-SG User Guide
- CC-SG Virtual Appliance and lmadmin License Server Management Quick Setup Guide
- CC-SG Virtual Appliance and lmgrd License Server Management Quick Setup Guide
- CC-SG Virtual Appliance No License Server Quick Setup Guide
- CC-SG WS-API Programming Guide

Upgrade Path

To upgrade your CC-SG to version 5.4.0, **you must be running firmware version 5.3.0** as depicted in the diagram below.   If your CC-SG is not running firmware version 5.3.0, then consult the diagram below and follow the required upgrade steps.   You can upgrade CC-SG V1 or CC-SG E1 but not the older CC-G1 units to 5.4.0.   If you have any questions, please contact Raritan technical Support.
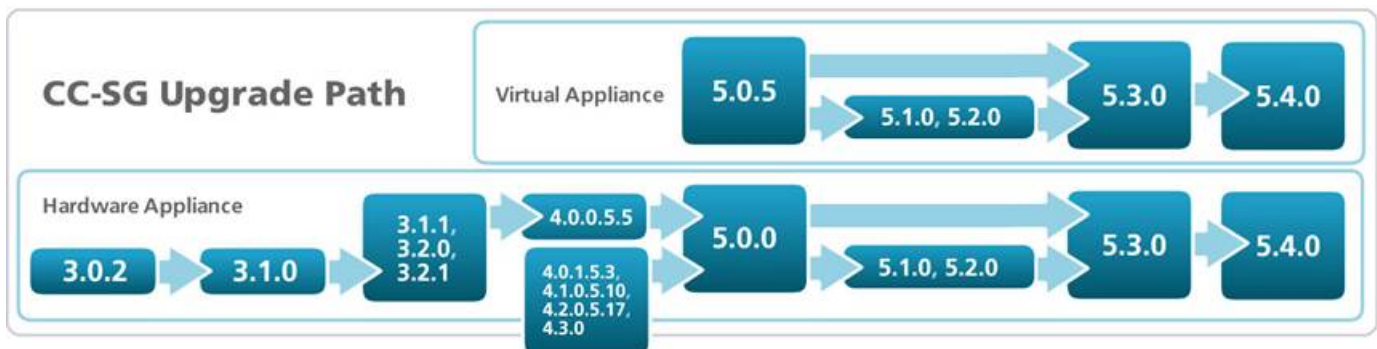
Please back up your CC-SG before and after any upgrade step. For detailed step by step instructions on upgrading, refer to the Readme file for this CC-SG release. You may also need to upgrade your other Raritan devices. For a complete list of supported devices, refer to the CC-SG Compatibility Matrix.   For instructions on upgrading managed Raritan devices, refer to the CC-SG Administrators Guide.

New Features and Updates

CC-SG Release 5.4 includes the features and updates listed below.   Please see the Administrators Guide and User Guide for details on using each new feature.

1. **Updated E1 hardware platform**

   A new, updated E1 hardware platform with increased performance will begin shipping in July 2013.

2. **Java 7 support**

   Support for the latest Java 7 Runtime Environment for added security and performance.   Java 6 is also supported. Consult the compatibility matrix for supported versions.   Java 6 will not be supported in future CC-SG releases.

3. **Proxy mode support for Microsoft RDP client**

   CC-SG's Microsoft RDP Client is now available in proxy mode, supporting RDP connections to the latest Windows operating systems in proxy mode.

4. **VMware VSphere 5.1 support**

   Support for VMware vSphere version 5.1.   CC-SG may also be deployed as a VSphere 5.1 virtual appliance.   The VMware 4.x Remote Console is an option for users wanting virtual media support.

5. **Additional web browser interface control**

   Increased ability to support single-sign-on for additional non-Raritan devices and systems.

6. **Additional CC-SG web services API's**

   New API's have been added to the CC-SG Web Services API for added integration with customer software systems.

7. **Address security vulnerabilities**

   Increased security by addressing security vulnerabilities.   New Verisign certificate.   Upgraded Apache version.

8. **Additional IPv6 support**

   IPv6 support for Dominion KX2-101-V2 Release 3.5 and KSX Release 2.5

9. **Dominion products support**

   CC-SG 5.4 includes support for Dominion KX2-101-V2 Release 3.5, SX Release 3.4 and KSX 2.5

10. **Configurable min and max lengths for "weak" CC-SG passwords**

    Ability to set lengths for "weak" (non-strong) passwords.

Special Notes and Limitations

1. IPv6 - Please note the following when utilizing CC-SG in IPv4/IPv6 Dual Stack Mode:
   - The Administrators Client cannot be launched in an IPv6 network when using Firefox 6, 7, 8, 9, 10, 11, 12.   This is a certificate bug caused by Firefox.   A workaround is available that includes installation of a user certificate.   Details are provided in the Administrators Guide.   Please contact Raritan Tech Support for assistance.
   - If using VNC in an IPv6 network, please select "Prefer On" in the Real VNC server settings.
   - If adding static routes for IPv6, please note:
     1. Upon reboot of CC-SG, the values are not retained
     2. In the event of IP failover, the values are not retained.
   - A list of features and functions that cannot be used with IPv6 is provided in the Administrators Guide.
2. When adding VNC and RDP interfaces for Windows 7, please make sure that ICMPv4 and ICMPv6 are allowed by your Windows 7 firewall.

3. When launching the iLO3 KVM app via CC, a warning 'do you wish to load unsecure content' will be presented to the user that needs to be accepted. This is because the HP applet is not signed.

4. Supported JRE versions for this release include: (1) Java 6 1.6 updates 10 through 43, (2) Java 7 up to JRE 1.7 update 21. Unsupported versions include: 1.7.0_11 due to bugs in that release and 1.7 update 9-bo5

5. The "Bookmark Node" feature is not supported when using Internet Explorer version 8 (IE8).

6. RSA Remote Console cannot be launched from CC-SG when using JRE 1.6.0_10 and higher. IBM has provided a workaround here: **http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5080396**.

7. If enabling AES 256, to avoid lockout from CC-SG ensure that the jurisdiction files are installed on the client PC or device.

8. VMware Viewer and Firefox version 3.6.x are not compatible.

9. CC-SG cannot manage or access ESXi virtual nodes that use a free trial license.

10. Single mouse mode does not function on Windows or Linux servers as targets when using VMware as a client.

11. When accessing DRAC5 targets, there is a limit of 4 concurrent SSH sessions.

12. If your version of DRAC does not support graceful shutdown, a "graceful shutdown not supported" message is received when executing a graceful shutdown operation for power control.

13. If using the SNMPv3 option and the MGSOFT MIB Browser, authentication and privacy passwords cannot be the same. CC-SG will send the traps but the browser will ignore them.