CommandCenter Secure Gateway (CC-SG) Release 6.0.0.5.14

Release Notes v4

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 6.0.0.5.14 contains: (1) all features in the original 6.0.0.5.2 release (available in April), (2) a fix for the "Heartbleed" security vulnerability in the OpenSSL cryptographic software library used by the CommandCenter and (3) additional enhancements and fixes.

The Release 6.0.0.5.14 firmware and documents are available to CC-SG customers with up-to-date maintenance contracts at **http://www.raritan.com/support/commandcenter-secure-gateway/**.

Updated Product Documentation

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

- CC-SG Administrators Guide, User Guide & Online Help
- CC-SG 6.0 Upgrade Guide (has detailed firmware upgrade instructions)
- Quick Setup Guide for CC-SG Virtual Appliance - No License Server
- CC-SG WS-API Programming Guide

Release 6.0.0.5.14 New Features and Updates

CC-SG Release 6.0.0.5.14 includes the following features and updates:

1. **OpenSSL Library Heartbleed Vulnerability**. Patch and fix the "Heartbleed" security vulnerability (CVE-2014-0160) in the OpenSSL cryptographic software library used by CC-SG. See "heartbleed.com" for information on this vulnerability. Raritan recommends that customers consult their security experts and take appropriate actions to recover from this vulnerability including installing new SSL certificates and changing passwords.
2. **Erroneous CC-SG E1 Appliance Overheat LED.** Fixes the operation of the CPU Overheat LED on the front panel of the new, updated CC-SG E1 Physical Appliances, which would erroneously light.
3. **Remote IPMI Access**. For security reasons, we have blocked remote IPMI Access via the CC-SG standard LAN port of the new CC-SG E1 Physical Appliances.
4. **Other fixes and security improvements**.

Release 6.0.0.5.2 New Features and Updates

The previous CC-SG 6.0 Release (6.0.0.5.2) included the following features and updates:

1. **Dominion KX III Support**

   The new Dominion KX III high performance, KVM-over-IP appliances (DKX3-xxx) are supported. Dominion KX II switches (DKX2-xxx) continue to be supported, although CC-SG 6.0 does not support the first generation Dominion KX devices (see below).

2. **Java 7 Support**

   Support for the latest Java 7 Runtime Environment (up to 7u51) for added security. Java 6 is no longer supported and Release 6.0 has not been tested with Java 8. Consult the compatibility matrix for supported versions.

3. **First Generation Dominion KX Switches No Longer Supported**

   The first generation Dominion devices are no longer supported: Dominion KX (DKX-xxx), KSX (DKSXxxx), KX-101 (DKX-101) and the Paragon IP-Reach (IPR-xx). These devices are end-of-life and end-of-support. **You must remove these switches from CC-SG before upgrading to Release 6.0**.

4. **First Generation Dominion Clients No Longer Supported**

   The first generation MPC (KVM), RRC (KVM) and RC (Serial) Clients are no longer supported. For KVM-over-IP, customers should use the Windows-based Active KVM Client (AKC) or the Java-based Virtual KVM Client (VKC). For serial, use the Raritan Serial Client (RSC).

5. **Flexera lmadmin and lmgrd License Servers (used by the CC-SG Virtual Appliance) Not Supported**

   For the Virtual CC-SG Appliance, CC-SG 6.0 no longer supports the Flexera lmadmin or lmgrd License Servers. An external license server is not required anymore. If you are using a license server, then you must get new license file(s) from Raritan to migrate away from the license server. You must re-license before upgrading to CC-SG 6.0. Please contact Raritan Technical Support and then use the CC-SG License Manager to upload the new license(s).

6. **Integrated Lights-Out iLO4 Support**

   Support for the HP iLO4 embedded management.

7. **Chrome Browser and Internet Explorer 11**

   The Chrome Browser and Internet Explorer 11 are now available for use with CC-SG.

8. **Reporting CC-SG Firmware Upgrade Failures**

   Should a CC-SG upgrade fail, the CC-SG Diagnostic Console will show that the firmware upgrade failed. The user is provided with the reason for the failure, as well as any recommended actions.

9. **Security Enhancements**

   Increased security. Addressed multiple security vulnerabilities. Updated OS, Apache and OpenSSH versions. New Verisign certificates. Increased CC-SG Super User Password length. SSL Certificate key length increased to 2048 bits.

10. **CC-SG API Updates**

    For the getDevice() function in the device management service , the DeviceData wsdl file has been changed. There are two new fields for the device's model and portCount. The port count reflects the number of feature ports such as KVM, serial, power, and outlets. Consult the API Guide for more information.

Upgrade Path to Version 6.0.0.5.14

Customers using 6.0.0.5.2 can upgrade directly to 6.0.0.5.14. The upgrade path for other releases depends on the type of CC-SG (physical or virtual) and the type of licensing:

1. Physical Appliance (CC-SG V1 and E1):

- All 5.x CC-SG versions can upgrade directly to CC-SG 6.0.0.5.14.
- 3.x and 4.x versions should upgrade to version 5.0 according to the diagram below. And then upgrade to CC-SG 6.0.0.5.14.

2. Virtual Appliance with No License Server (versions 5.3 & 5.4).

- Upgrade directly from 5.3 or 5.4 to version 6.0.0.5.14.

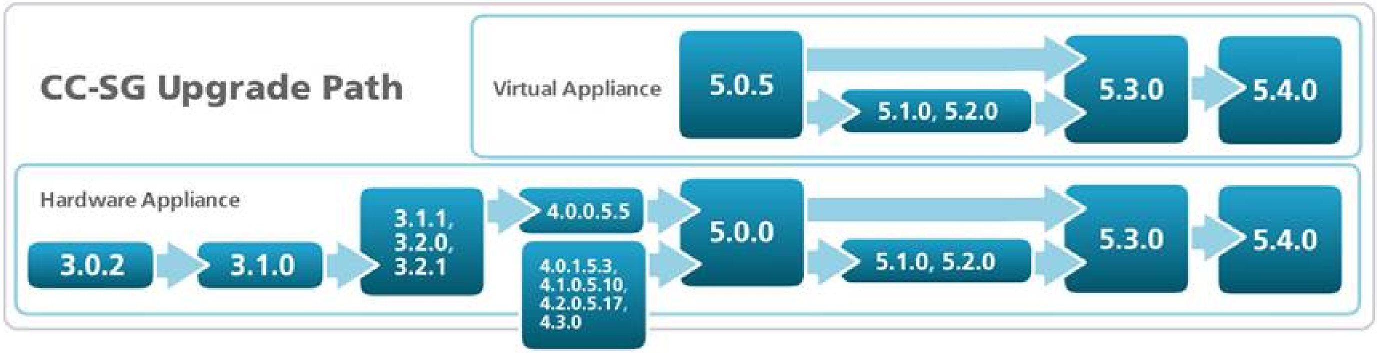
3. Virtual Appliance with License Server (versions 5.0.5, 5.1, 5.2, 5.3 & 5.4)

1) Versions 5.0.5, 5.1, 5.2 should upgrade to version 5.3.
2) As CC-SG 6.0.0.5.14 no longer supports the Flexera lmadmin or lmgrd License Servers, you must obtain new license file(s) to migrate away from these license servers. Please contact Raritan Technical Support to get new license files and then use the CC-SG License Manager to upload the new license(s). You must

re-license before upgrading to CC-SG 6.0.0.5.14.

3) You can then directly upgrade from version 5.3 or 5.4 to 6.0.0.5.14.

If instructed above to upgrade to a specific version, please consult the following diagram.



Additional Upgrade Information

For the CC-SG Virtual Appliance, you must add a second hard disk to your virtual machine before you upgrade.

You can upgrade CC-SG V1 or CC-SG E1, but not the older CC-G1 units to 6.0.0.5.14.

Please back up your CC-SG before and after any upgrade step.

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.

For detailed step by step instructions on upgrading, refer to the CC-SG 6.0 Upgrade Guide.

If you have any questions, please contact Raritan technical Support**.**

Special Notes and Limitations

1. The Microsoft RDP client cannot be launched via a CC-SG bookmark. To be fixed in a future update.
2. IPv6 - Please note the following when utilizing CC-SG in IPv4/IPv6 Dual Stack Mode:
   - The Administration Client cannot be launched in an IPv6 network when using Firefox 6, 7, 8, 9, 10, 11, 12. A workaround is available that includes installation of a user certificate. Details are provided in the Administrators Guide.
   - 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.
3. When adding VNC and RDP interfaces for Windows 7, please make sure that ICMPv4 and ICMPv6 are allowed by your Windows 7 firewall.
4. 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.
5. Supported JRE versions include: Java 7 up to JRE 1.7 update 51. Unsupported versions include: 1.7.0_11 and 1.7 update 9-bo5. Certain embedded service processors versions have not been updated for the recent Java changes and

may require the Java Security Slider to be lowered or use of the Exception Site List in the Java Control Panel's Security Tab.

6. The "Bookmark Node" feature is not supported when using Internet Explorer version 8 (IE8).
7. 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**.
8. If enabling AES 256, to avoid lockout from CC-SG ensure that the jurisdiction files are installed on the client PC or device.
9. VMware Viewer and Firefox version 3.6.x are not compatible.
10. CC-SG cannot manage or access ESXi virtual nodes that use a free trial license.
11. Single mouse mode does not function on Windows or Linux servers as targets when using VMware as a client.
12. When accessing DRAC5 targets, there is a limit of 4 concurrent SSH sessions.
13. 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.
14. 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.