CommandCenter Secure Gateway (CC-SG) Release 6.1

Release Notes

Introduction

These release notes contain important information regarding CommandCenter Secure Gateway Release 6.1.0.

Release 6.1 contains: (1) all features in the previous 6.0.0.5.4 release, plus new features, fixes and updates.

The Release 6.1 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 6.1 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 6.1 New Features and Updates

CC-SG Release 6.1 includes the following features, enhancements and updates:

1. **Dominion SX II Support.** Support for the new, next-generation Dominion SX II Console Servers.
2. **Dominion KX III Release 3.2.** Support for the upcoming Dominion KX III Release 3.2.
3. **CC-SG Hyper-V Virtual Appliance.** CC-SG is now available as a Microsoft Hyper-V Virtual Appliance
4. **CC-SG XenServer Virtual Appliance.** CC-SG is now available as a XenServer Virtual Appliance.
5. **New 64 Node Virtual Appliance**. Customers can purchase a 64 node CC-SG Virtual Appliance, which provides a lower cost entry to CommandCenter management. Raritan part number CCSG64-VA.
6. **Extensive Security Updates.** Significant security upgrades and enhancements. See below.
7. **Support VMware Version 5.5.** Support this VMware version.
8. **KVM "view only" Permission.** Support view only permission for Dominion KX III switches with Release 3.1 and higher. Other switches will require future firmware updates.
9. **Dominion KX KVM Client Support:** Several enhancements to the Dominion KVM Clients: (1) Java-free Active KVM Client (AKC), and (2) Java-based Virtual KVM Client (VKC), including:
   a. CC-SG will now launch AKC on Windows platforms when the Auto-Detect option is selected.
   b. Remote power control is now available from inside AKC & VKC.
   c. Support VKC and AKC KVM-over-IP Sessions for the Chrome Browser.
   d. Support AKC for KX2-101-V2 Release 3.6 and above
   e. Can launch the CC-SG Admin Client from the Chrome browser (45 and above)
10. **CSV Delete Device.** Can now delete a device using a CSV file.
11. **Support latest version of Java 8.** Check the compatibility matrix for the supported versions. CC-SG should work with future Java versions. The software may need to be updated if the Java developers make incompatible changes to new Java versions**.** Please call Raritan Tech Support if you have any issues**.**
12. **Miscellaneous customer fixes.**

Release 6.1 Security Updates

A large number of security upgrades and hardening are included in this release, including the following:

1. Support TLS and optionally disable SSLv3 (POODLE issue)
2. CC-SG to use and generate SHA-2 Certificates
3. New Verisign code signing SHA-2 Certificate
4. Block TCP/IP ports 4446 and 4457
5. Upgrade OpenSSH version to address vulnerabilities
6. Upgrade OpenSSL version to address Freak and other vulnerabilities
7. Patch OpenSSL to fix TLS Man-in-the-Middle vulnerability
8. Increase key size to 4096 bits for certificate generation
9. Run Nessus Security Scan
10. Address cross scripting vulnerability in CCSG Web user interface
11. Address BASH security vulnerability
12. Address CCS Injection OpenSSL & GNUtils vulnerabilities

Upgrade Path to Version 6.1

Customers using 6.0.0.5.x can upgrade directly to 6.1. 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 should upgrade directly to CC-SG 6.0.x and then to CC-SG 6.1.
- 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.x and then to CC-SG 6.1.

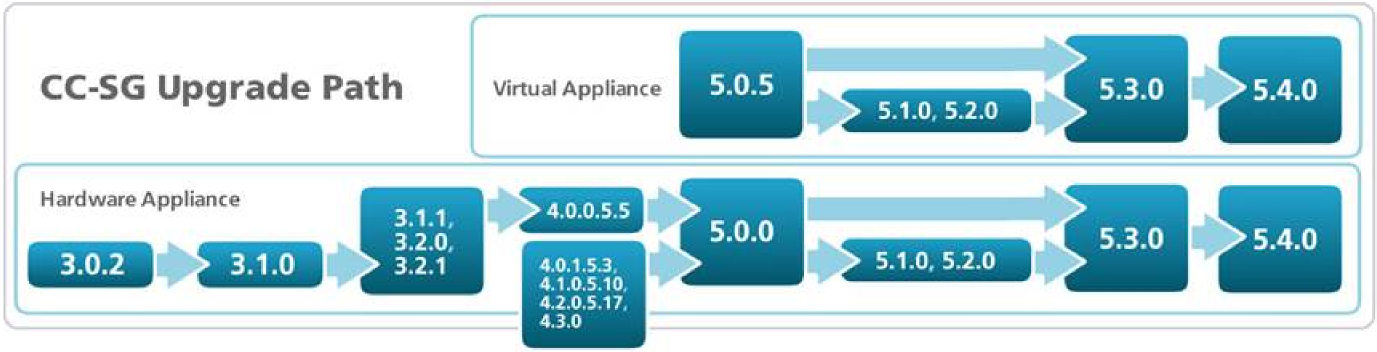
2. Virtual Appliance with No License Server (versions 5.3 & 5.4).

- Upgrade directly from 5.3 or 5.4 to CC-SG 6.0.x and then to version 6.1

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 6.0.5 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 6.0.5.x.
3) You can then directly upgrade from version 5.3 or 5.4 to CC-SG 6.0.5.x and then to 6.1.0.

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 to 6.0.5.x.

You can upgrade CC-SG V1 or CC-SG E1, but not the older CC-G1 units to 6.1. 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 6.1 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. Unsupported Java 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. Cannot login to CC-SG via IPv6 with java 1.7.0.7_71. Previous versions have worked as well as Java 8.
7. The “Bookmark Node” feature is not supported when using Internet Explorer version 8 (IE8).
8. 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**.
9. If enabling AES 256, to avoid lockout from CC-SG ensure that the jurisdiction files are installed on the client PC or device.
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.
15. Chrome versions 45 (and above) and the Edge browser cannot launch in-band interfaces in the CC-SG HTML-based Access Client. If you plan to use the in-band interfaces, for best results, we recommend other browsers. If you must use these browsers for this purpose, then use the Java-based CC-SG Admin client to access your in-band interfaces, however iLO, DRAC and RSA will not launch.