Release Notes for CommandCenter Secure Gateway (CC-SG) Release 11.0

Introduction

These release notes contain important information regarding CommandCenter Secure Gateway Release 11.0. Release 11.0 contains: all features in the previous 10.0 release, plus new features, fixes and updates.

Release 11.0 is available to CC-SG customers with up-to-date maintenance contracts at:

http://www.raritan.com/support/commandcenter-secure-gateway/.

Release 11.0 New Features and Updates

CC-SG Release 11.0 includes the following features, enhancements, and updates:

1. Added support for TLS v1.3
2. Added the ability to enable/disable specific TLS ciphers
3. Removed support for SSL v3.0
4. Default IP address mode changed to DHCP
5. Strong passwords and account login failure lock out now enforced by default
6. Fixed bug where IP Access Control lists do not load automatically on system restart
7. Added CSV import capability for bulk password changes
8. Added WS-API call for bulk password changes
9. Added DKX3 CIM serial info in CC-SG GUI and reporting
10. Added WS-API call to retrieve DKX3 CIM serial info and node data
11. Added capability to perform a “certificate reset” as one of the reset options
12. Added the ability to run an asset report on managed User Stations
13. Added the ability for an admin “custom view” in the client GUI to be shared with other users

Important CC-SG Information

- Release 11.0 does not officially support the old, single-port models DKX-101, DKX2-101 models.
- Firmware version 4.6 is required for the Dominion KX III & IV User Stations (DKX3-UST, DKX4-UST) to integrate with CommandCenter Secure Gateway Release 11.0.
- The Dominion KX II models (DKX2-xxx) are no longer officially supported in CC-SG version 8.0 and later.

Updated Product Documentation

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

- CC-SG Administrators Guide, User Guide & Online Help

- Quick Setup Guide for CC-SG Virtual Appliance - No License Server
- CC-SG WS-API Programming Guide

Upgrade Path to Version 11.0

Customers can upgrade to Release 11.0 from CC-SG Releases 9.0. Customers using previous versions should consult the Upgrade Guides for those releases. Contact tech support if there are any questions on upgrade compatibility or the correct path to follow.

Important Note: customers upgrading to Release 11.0 with CC-SG virtual appliances upgraded from previous releases (5.x or 6.x), may have two hard drives as a result of these prior upgrades. Before upgrading to 11.0, the original (older) hard drive (disk 1) **must be** removed. Please consult the information on the CommandCenter Support page or call Raritan Technical Support if you need assistance

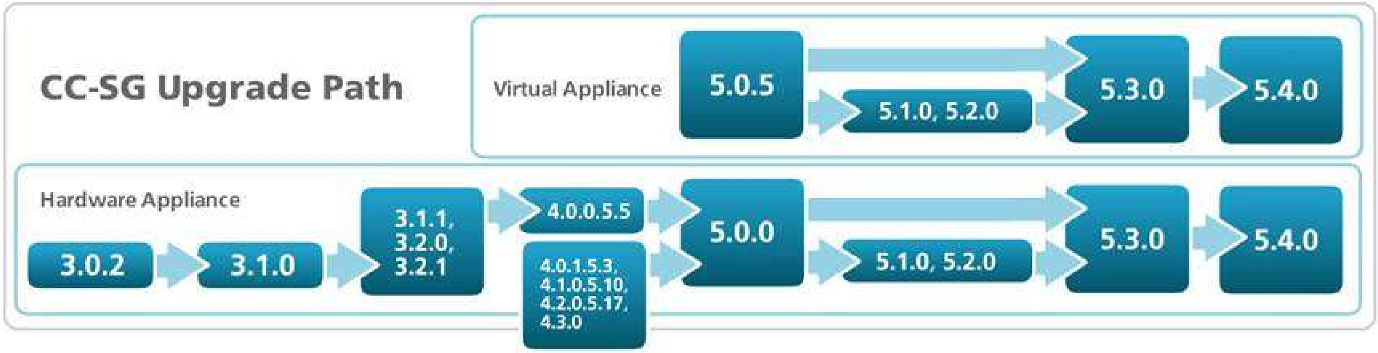
The upgrade path for older releases depends on the type of CC-SG (physical or virtual) and the type of licensing:

1. **Physical Appliance** (CC-SG V1 and E1):
   - All 5.x CC-SG versions should upgrade directly to CC-SG 6.0 and then to CC-SG 7.0.
   - 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, and then to CC-SG 7.0.
   - **The following older versions cannot upgrade to 7.0: CC-SG-V1-A, CC-SG-V1-1 (2009 and earlier), CC-SG-E1-0**

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 and then to version 7.0

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 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.
   3) You can then directly upgrade from version 5.3 or 5.4 to CC-SG 6.0 and then to 7.0.

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



Additional Upgrade Information:

For the CC-SG Virtual Appliances:

- **Four (4) GBs of RAM are required**
- **You must add a second hard disk to your virtual machine before you upgrade to Release 7.0. Consult the Release 7.0 Upgrade Guide for more information.**
- **Your virtual machine must only have one hard disk when you upgrade to Release 11.0**

You can upgrade CC-SG V1 or CC-SG E1, but not the older CC-G1 units to 7.0.

Older CC-SG units not supported include:

- CC-SG-V1-A
- CC-SG-V1-1 (2009 and earlier)
- CC-SG-E1-0

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 9.0 Administrators Guide or the online help.

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

Special Notes and Limitations

1. HSC & HKC in proxy mode uses TCP port 2401, which is different from the other KVM Clients. Check the documentation for proxy mode.
2. SSL 3.0 is disabled by default for security reasons. As it may be required for CC-SG to communicate with older devices, you can enable it if desired.
3. TLS 1.0 is needed to use the following Raritan devices: KX2 v2.7, KSX2 v2.7, LX v2.7, KX2-101v2 v3.7
4. To use the Power Control Menus inside the KVM/Serial Clients, you must connect the Raritan PX PDU's to a Dominion appliance.
5. To disable java in browsers and automatically launch HKC: on the Java Control Panel, under the Security Tab, untick option "Enable Java in the browser."
6. To use the new VMware Web Viewer, you must install a certificate. Follow the prompts and then re-connect.
7. The Microsoft RDP client cannot be launched via a CC-SG bookmark. To be fixed in a future update.
8. 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 to 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.
   - A list of features and functions that cannot be used with IPv6 is provided in the Administrators Guide.
9. When adding VNC and RDP interfaces for Windows 7, please make sure that ICMPv4 and ICMPv6 are allowed by your Windows 7 firewall.
10. 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.
11. Unsupported Java versions include: Java 6 and Java 7. 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.
12. RSA Remote Console can't be launched from CC-SG when using JRE 1.6.0_10 and higher. IBM has provided a workaround: http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5080396.
13. If enabling AES 256, to avoid CC-SG lockout ensure that jurisdiction files are installed on the client PC or device.
14. CC-SG cannot manage or access ESXi virtual nodes that use a free trial license.
15. Single mouse mode does not function on Windows or Linux servers as targets when using VMware as a client.
16. When accessing DRAC5 targets, there is a limit of 4 concurrent SSH sessions.
17. 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.
18. 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.
19. 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.