CommandCenter Secure Gateway Firmware Release Notes REV

Firmware Version: CC-SG 11.5.0

Release Status: General Availability (GA)

Date: May 10, 2024

CommandCenter Secure Gateway (CC-SG) Overview

Raritan's CommandCenter® Secure Gateway (CC-SG) is an easy to deploy, plug-and-play appliance that provides IT administrators and lab managers with a secure, single point of remote access and control. Raritan's CC-SG consolidates multiple remote access technologies, including Dominion® KVM-over-IP switches and serial console servers, Raritan PX PDUs, service processors, and in-band methods such as RDP, SSH and VNC.

With CC-SG, users can access and control their entire IT infrastructure from a single system, featuring BIOS-level, out-of-band KVM and serial access to a wide variety of computer and serial devices.

Release 11.5.0 Firmware Overview

CC-SG Release 11.5.0 is a General Availability (GA) Release. This release may include performance and productivity improvements, support for new products and accessories, new features and enhancements, bug fixes, and general fixes for specific model families. Specific updates are outlined below.

Release 11.5.0 is available to CC-SG customers with up-to-date maintenance contracts at:

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

Important Note

CC-SG users need 11.0.0 installed prior to going to 11.5.0. Any CC-SG running on a previous release (10.0.0 or earlier) must follow the upgrade steps defined below before upgrading to release 11.5.0.

Firmware Version	*Upgrade Steps*
6.x	» 6.x » 7.0.0 » 9.0.0 » 11.0.0 » 11.5.0
7.0.0 or 8.x	» 7.0.0 or 8.x » 9.0.0 » 11.0.0 » 11.5.0
9.x or 10.0.0	» 9.x or 10.0.0 » 11.0.0 » 11.5.0
11.0.0	» 11.0.0 » 11.5.0

The new hardware (CC-SG-E1-5) requires firmware version ≥ 11.5.

Please contact technical support with any questions or issues.

Applicability

Please review the CC-SG Compatibility Matrix Release 11.5 for additional details.

General Guidelines for this Release

Please check the **Support & Compatibility** section below. Or contact Raritan Support if you are unsure of the model number of your unit—it is typically viewable from the GUI's *Device Information* page and is also printed on a label located on the device.

Release Highlights

New Features & Enhancements

Issue ID	*Description*
81262	SAML Authentication – Okta
	Smartcard access to CC-SG
81592	CSV Import Capability – Password Changes
81600	New Hardware E1-5 replaces EoL CC-SG E1-4*
81696	Generic Authentication Failed Message

***Hardware Comparison Chart**:

Raritan Command Center Secure Gateway Hardware Comparison Specifications		
Part Number	CCSG-E1-5 (AAEON)	CCSG-E1-4 (Supermicro)
Vendor	AAEON	SuperMicro
Processor	Intel® 13th/12th Gen (Raptor Lake-S/Alder Lake-S) Core™ Processors install with Intel i7-12700E	Intel® CoreTM i7-7700 Processor (8M Cache, up to 4.20 GHz)
Chipset	Q670 chipset	Intel® C236 Express PCH
Memory	DDR4 2666 MHz, 8 GB x 1	DDR4 2400Mhz 4GB x 2
Storage	128G SATA SSD x 2	128GB Innodisk 2.5" SATA SSD 3MG2-P series
LED Indicators	Power/Disk/NIC1/NIC2/Overheat (Not Used)	Power/Disk/NIC1/NIC2/Power Failure
Rear I/O	- USB 3.2 Gen2 x 5 - USB 3.2 Gen2x2 (20G) Type C x 1 - 1GbE LAN by Intel I210 w/ LED x 2 - VGA x1 + Display x 1 + HDMI x 1 - Audio (Mic, Line-in, Line-out) - Dual AC-in - Power module alarm reset button x 1	- USB 3.0 x 4 (2 rear + 2 header) - USB 2.0 x 9 (2 rear + 6 header + 1 Type A) - DP x 2 , DVI-I x 1, VGA x 1 - Integrated IPMI 2.0 with KVM and Dedicated LAN - Onboard I/O device : HD Audio, 2 COM ports (2 headers) - Dual AC
Front I/O	- HW Reset Button (behind the front bezel) - Power Button	- HW Reset Button (behind the front bezel) - Power Button

Please consult the appropriate User Guide for more information on these firmware features at raritan.com/support.

CommandCenter Secure Gateway Documentation

The following user documentation is available for the CommandCenter Secure Gateway:

- Quick Setup Guide for CC-SG Virtual Appliance - VMware, HyperV
- Quick Setup Guide for CC-SG Cloud Appliance - AMS, Azure
- Enterprise MIB
- E1 Quick Setup Guide
- V1 Quick Setup Guide

- Admin and User Online Help
- Admin Guide
- User Guide
- Admin Desktop Clients Installation Guide
- API Guide
- Virtual Evaluation Quick Setup Guide
- Cloud Evaluation Quick Setup Guide

The CC-SG documentation is available from the CC-SG web-based user interface and on the Raritan.com website: www.raritan.com. Go to the Support section and select CommandCenter Secure Gateway. Click on the appropriate release. Historical firmware version downloads can be found on raritan.com/support.

CC-SG Online Help

An Online Help System is available. Click on Help – Online Help in the left-hand information panel and the Online Help system will launch. You can browse to the appropriate topic via the Contents, Index and Search tabs. The entire CC-SG User guide is available, including text and images, with an extensive set of links. Online help for the Raritan products is available on http://www.raritan.com/support/online-help/

Release Package Details

The CC-SG 11.5.0 Firmware is a General Availability release package and will be posted on the Raritan support website at raritan.com/support.

Firmware Upgrades

Raritan provides new firmware upgrade releases that contain software enhancements, new features, and improvements. These upgrades are available on the Raritan Website: www.raritan.com. Please go to the Support page and click on Dominion KX III in the "Choose a Product" button, or go directly to:

https://www.raritan.com/support/product/commandcenter-secure-gateway

Locate the entry for the new firmware release. Release Notes are available with: (a) brief descriptions of new features/enhancements, (b) important operating instructions, and (c) firmware upgrade instructions. Follow the Release Notes instructions to upgrade the device.

Firmware Upgrade Prerequisites

If you have any questions, or do not meet the pre-requisites listed below, please STOP and contact Raritan Technical Support for further instructions. Please read the entire instructions (this document) before proceeding.

Support & Compatibility with CC-SG 11.5.0

1. Release 11.5 supports both the new and previous CC-SG hardware versions.
2. Release 11.5 does not officially support the old, single-port models DKX-101, DKX2-101 models.
3. 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 11.5.

4. The Dominion KX II models (DKX2-xxx) are no longer officially supported in CC-SG version 8.0 and later.

Upgrade Path to Version 11.5

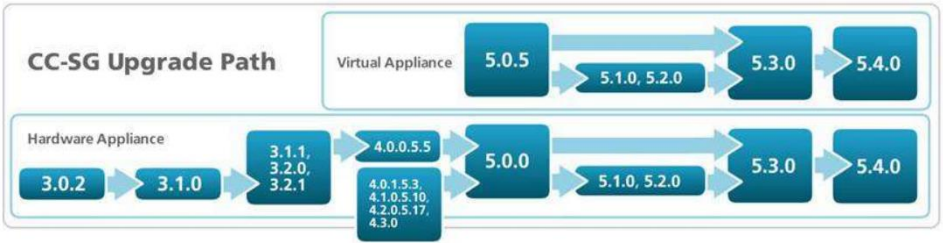
Customers can upgrade to Release 11.5 from CC-SG Release 11.0. Customers using previous versions should consult the Upgrade Guides for those releases. Contact tech support if there are any questions on upgrade compatibility or the correct path to follow.

Important Note: customers upgrading to Release 11.5 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 11.5, 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)
    - Versions 5.0.5, 5.1, 5.2 should upgrade to version 5.3.
    - 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.
    - 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 11.5**

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 11.5 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.

Contact Us

Go to raritan.com/support for contact options.