

CommandCenter Secure Gateway Firmware Release Notes



Firmware Version: CC-SG 14.0

Release Status: General Availability (GA)

Date: June 23, 2026

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 14.0 Firmware Overview

CC-SG Release 14.0 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 14.0 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 v12 is the fence release for CC-SG v14. CC-SG users need v12.0 installed prior to going to v14.0. Then they need 11.0 or 11.5 installed prior to going to 12.0. Any CC-SG running on a previous release (10.0 or earlier) must follow the upgrade steps defined below before upgrading to release 14.0.

<i>Firmware Version</i>	<i>Upgrade Steps</i>
13.0	» 13.0 » 14.0
12.0	» 12.0 » 14.0
11.5	» 11.5 » 12.0 » 14.0
11.0	» 11.0 » 12.0 » 14.0
9.x or 10.0	» 9.x or 10.0 » 11.0 » 12.0 » 14.0
7.0 or 8.x	» 7.0 or 8.x » 9.0 » 11.0 » 12.0 » 14.0
6.x	» 6.x » 7.0 » 9.0 » 11.0 » 12.0 » 14.0

The new hardware (CC-SG-E1-5) requires firmware version $\geq$ 11.5.

Please contact technical support with any questions or issues.

Applicability

Please review the CC-SG Compatibility Matrix Release 14.0 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 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

<i>Issue ID</i>	<i>Description</i>
88871, 88870, 88866	Patch File to eliminate Dirty Frag CVEs
88767	Support for Running on Proxmox
88654, 88350, 87491, 75004	Support Other Virtual Platforms
88551	DOC: Recommended max for CC-SG Database is 500 devices or 5000 nodes
88538, 86444	New Message when cluster is broken
88424, 88422, 86821, 86773, 86678, 81204	Support OpenJDK to launch CCSG Admin Client
88352, 88335, 87657	Support NodeGrid Serial Devices
88336, 86677	REST API
88457, 88267, 86470, 86469, 86434, 86184	Update Firmware Manager & Compatibility Matrix for v14
88005	Update OpenSource License List
87776	Diagcon Password Settings
87749, 86362	Import Devices: Add, Update or Delete with CSV File
87739	Update Upgrade Guide for v14
87713	Update the Code Signing Certificate
87705, 86925, 86374	iPV6 Certification
87704, 87500, 82459	Inband Interface, Java RDP removed from Admin GUI
87702, 82854	Add Windows File Server Option for Configuring Backup to Remote Location
87593	SNMPv3 Protocols for ServerTech Pro3X
87446	Menus are displayed in Japanese based on local settings in the client
87268	RDP to Support 1920x1080
86679	Update Rocky Linux
86676	Run Nessus Scanner

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
- 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 14.0 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 CommandCenter Secure Gateway 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 14.0

1. Release 14.0 supports CC-SG hardware versions E1-4 & E1-5.
2. User Station Firmware version 5.3 is required for the Dominion KX III & IV User Stations (DKX3-UST, DKX4-UST) to integrate with CommandCenter Secure Gateway Release 14.0.
3. Dominion EOL Legacy devices are not permitted in the database and need to be removed prior to upgrading.

Upgrade Path to Version 14.0

Customers can upgrade to Release 14.0 from CC-SG Release 12 or 13.0. 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 14.0 with CC-SG virtual appliances upgraded from 12.0 may have two hard drives as a result of the 12.0 upgrade. Before upgrading to 14.0, the original (older) hard drive (disk 1) must be removed. Please refer to the CCSG 14.0 Upgrade Guide found 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 E1-4 and E1-5):
 - E1-3 hardware is no longer supported starting in 13.0.

Additional Upgrade Information:

For the CC-SG Virtual Appliances:

- Four (4) GBs of RAM are required
- **Your virtual machine must only have one hard disk when you upgrade to Release 14.0**

Older CC-SG units not supported include:

- CC-SG-V1-A
- CC-SG-V1-1 (2009 and earlier)
- CC-SG-E1-0
- CC-SG-E1-3

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 14.0 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. To use the Power Control Menus inside the KVM/Serial Clients, you must connect the Raritan PX PDU's to a Dominion appliance.
3. To use the new VMware Web Viewer, you must install a certificate. Follow the prompts and then re-connect.
4. The Microsoft RDP client cannot be launched via a CC-SG bookmark.
5. 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.
6. When adding VNC and RDP interfaces for Windows 7, please make sure that ICMPv4 and ICMPv6 are allowed by your Windows 7 firewall.
7. If enabling AES 256, to avoid CC-SG lockout ensure that jurisdiction files are installed on the client PC or device.
8. CC-SG cannot manage or access ESXi virtual nodes that use a free trial license.
9. Single mouse mode does not function on Windows or Linux servers as targets when using VMware as a client.
10. When accessing DRAC5 targets, there is a limit of 4 concurrent SSH sessions.
11. 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.
12. 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.
13. 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.

© 2026 Legrand. All Rights Reserved. Trademarks are the property of their respective owners. The industry-leading brands of Ortronics, Raritan, Server Technology, and Starline empower Legrand's Data, Power & Control to produce innovative solutions for data centers, building networks, and facility infrastructures. Our division designs, manufactures, and markets world-class products for a more productive and sustainable future. The exceptional reliability of our technologies results from decades of proven performance and dedication to research and development.