CommandCenter® Secure Gateway
Frequently Asked Questions

Question	Answer
CommandCenter Secure Gateway Overview	
What is CommandCenter Secure Gateway (CC-SG)?	CommandCenter Secure Gateway is an easy to deploy, plug-and-play appliance that provides unified, secure browser or CLI-based access to KVM, serial and power control devices in the data center, lab and remote offices. CC-SG is available as a rack-mountable hardware solution or as a virtual appliance (runs on VMware®, Microsoft Hyper-V or XenServer). CC-SG consolidates multiple access technologies, providing a single point of remote access and control for devices, software applications and other solutions. These include Raritan's Dominion® series, Paragon® II, PX™ intelligent power distribution units, embedded service processors like HP® iLO, Dell® DRAC, IBM® RSA, IPMI, and in-band software solutions such as RDP, VNC, SSH, and Telnet. Access to many other systems and devices is available with a Web browser Interface.
What are the different CC-SG hardware options?	Raritan offers multiple hardware versions to address both small and medium size businesses as well as large enterprises with thousands of servers and other IT devices. CC-SG E1 is targeted at large deployments as well as environments where dual power supply is required for redundancy. The economical CC-SG V1 is a powerful KVM and in-band access and power management appliance for small and medium environments.
On which Virtualization Platform can I install CC-SG?	The CC-SG virtual appliance can be installed on a VMware, Microsoft Hyper-V and XenServer virtualization systems. Please see the CC-SG compatibility matrix for the supported versions.
Which Raritan products does CC-SG support?	CC-SG can manage Raritan's Dominion KX II, KX III, KX II-101 and KX II-101-V2 KVM-over-IP switches, Dominion SX & SX II serial-over-IP console servers, Dominion KSX II remote office appliances and Paragon II*. CC-SG also enables centralized remote power management by providing connectivity to PowerIQ and Dominion PX, PX2 and PX3 intelligent rack power management solutions. Serial connections via Dominion Serial Access Modules (DSAM) connected to the Dominion KX III are also supported. *Supports Paragon II access via direct connection to Dominion KX II or KX III.
I purchased a Dominion KX III, which CC-SG version should I use?	CC-SG version 6.0 and above supports the Dominion KX III. Versions 4.x and 5.x do not.
I purchased a Dominion SX II, which CC-SG version should I use?	CC-SG Version 6.1 and above supports the Dominion SX II serial console server. Previous versions do not.
Does CC-SG support the first generation Dominion products?	CC-SG Releases 6.0 and later do not support the first generation Dominion devices: Dominion KX (DKX-xxx), KSX (DKSXxxx), KX-101 (DKX-101) as well as the Paragon IP-Reach (IPR-xx). These devices are end-of-life and end-of-support. We recommend upgrading to the latest models. Customers continuing to use these devices should stay with the CC-SG 5.x versions.

How does CC-SG integrate with other Raritan products?	CC-SG uses a powerful proprietary search-and-discovery technology that identifies and connects to Raritan devices. Once CC-SG is connected and set up, device connection is transparent and administration is simple.
Does CC-SG support Java-free IP KVM and Serial access?	Yes, with the HTML-based CC-SG Access Client, users get many forms of Java-free access with the Dominion KX III HTML and .NET KVM Clients and the Dominion SX II HTML Client.
How does CC-SG connect to servers and other devices connected to Raritan devices?	CC-SG offers three connection modes: Direct, Proxy, and Both. Direct Mode allows you to connect to a node or port directly, without passing data through CC-SG. Proxy Mode allows you to connect to a node or port by passing all data through CC-SG. Both Mode allows you to configure CC-SG to use a combination of Direct and Proxy modes.
Why would I use proxy mode?	Proxy Mode allows users to connect to a node or port by passing all data through CC-SG. Proxy Mode increases the load on your CC-SG server, which may cause slower connections. However, Proxy Mode is recommended if you would like to centralize user access to devices and systems through the CC-SG. You need to keep the CC-SG TCP ports 80, 8080, 443, and 2400 open in your firewall. Note: Some interfaces only work in "direct mode" even though you configure CC-SG to use Proxy mode. These interfaces include ILO, RSA, DRAC, Web Browser and VMware Viewer. Microsoft and Java RDP interfaces can be used in proxy mode. The new HTML KVM and Serial Clients do not work in proxy mode at this time.
Does CC-SG have a software maintenance program?	Yes. Software maintenance, which includes software updates and access to Raritan Software Support, is included for the first year of your CC-SG purchase. After the first year, additional software maintenance can be purchased. It's important to obtain the extended coverage before the end of the first year to ensure continuous coverage and access to software updates.
How do I get access to new CC-SG updates and releases?	Customers with up-to-date CC-SG software maintenance can get access to new CC-SG releases and updates on the raritan.com Support page by logging in.
If I buy the CC-SG virtual appliance, can I run it on multiple virtual servers?	The software can be installed multiple times, but a different license is needed for multiple virtual CC-SG's to run.
Can two Virtual CC-SG appliances be set up as a cluster?	No, but seamless and power high availability operation is available using VMware. The CC-SG virtual appliance can utilize the VMware "high availability" and "fault tolerance" availability features for seamless and powerful redundancy. For Hyper-V and XenServer, redundancy may be available depending on your environment.
Can I access CC-SG from a smart phone?	Yes, the Mobile KVM Client (MKC) enables out-of-band KVM access and power control from Apple mobile devices. The MKC supports out-of-band KVM access through Dominion KX II and KX III, and power control through CC-SG power interfaces for DRAC, iLO, IPMI, RSA and VMware virtual machines. Also supported is power control of Power IQ®-managed PDUs and Raritan's PX platform.

Is CC-SG a licensed product?	Yes. CC-SG, like many software products, is a licensed product. CC-SG is licensed via nodes (see below). Licenses are administered using the "Software License Key Management" page available on the Support section available on raritan.com. CC-SG administrators can manage licenses using the License manager in CC-SG.
What are node licenses?	CC-SG is licensed based on the number of nodes under management. A node is a system or device managed by the CC-SG. For example, servers, PC's and networking devices connected to Raritan Dominion devices count as nodes. The CC-SG base product (for both the hardware and virtual appliances) is provided with a certain number of nodes. Additional node licenses can be purchased as your infrastructure grows.
Does CC-SG support access and management of virtual servers?	Yes. You can add a VMware virtualization environment to CC-SG to enable a connection from CC-SG to virtual machines, virtual hosts and control systems. This virtualization feature includes: (1) streamlined setup of single sign-on access to your virtualization environment, (2) the ability to issue virtual power commands to virtual machines and virtual hosts, and (3) a topology view with one-click connections. CC-SG integrates with VMware environments and can support features like connectivity to the Virtual Center software, ESX servers and VMotion™ functionality.
Does CC-SG support direct KVM access to blade servers?	Yes. CC-SG supports access to and management of blade servers that are connected to the Dominion KX II or KX III. CC-SG allows for convenient and easy access to blade servers and their chassis.
How does CC-SG integrate with blade chassis products?	As there are multiple types of blade servers and multiple blade server manufacturers, Select Cisco, Dell, HP and IBM blade models are supported. CC-SG integrates with blade servers in different ways. CC-SG supports blade servers with and without integrated KVM switches, in conjunction with Raritan's Dominion KX II or KX III. In addition, other types of access can be configured, i.e. RDP, SSH and VNC. CC-SG can also utilize a blade servers embedded management cards, such as HP iLO and RiLOE II, Dell DRAC and IBM RSA II. Consult the CC-SG and Dominion KX II or III documentation for more information.
What is a CC-SG "Cluster"?	A CC-SG Cluster consists of two CC-SG hardware appliances: one primary and one secondary, for backup security in case of primary unit failure. Both units share common data for active users and active connections, and all status data is replicated between the two.
Do I need to buy additional licenses for the backup cluster unit?	No. Because only one CC-SG is active at a time, node licenses are not needed for the second CC-SG. A single license file is created by utilizing the ID's of each CC-SG in the cluster.
What is a CC-SG "Neighborhood"?	A CC-SG neighborhood is a collection of up to 10 CC-SG units, deployed and working together to serve the IT infrastructure access and control needs of the enterprise. A Neighborhood implementation allows for significant scalability and distribution of CC-SGs for improved performance in large or geographically dispersed configurations.

How do I find servers and devices that are managed by another CC-SG in a Neighborhood?	Users can search from the CC-SG Access Client for nodes that are managed directly by another CC-SG in a neighborhood and then launch the interfaces for the discovered nodes. Users can then create a consolidated node list spanning multiple neighborhood units — providing easy, convenient access when needed.
Can Clusters and Neighborhoods be implemented together?	Absolutely. By deploying CC-SG in a combination Cluster/Neighborhood configuration, not only is performance improved, but automatic failover ensures the elimination of or decrease in downtime.
Can a Neighborhood be built with virtual appliances?	Yes. It is operated the same way as a Neighborhood with hardware appliances. Virtual and hardware CC-SG appliances can be connected in a neighborhood.
If I buy a CC-SG virtual appliance, can I easily migrate to it from a CC-SG hardware appliance?	Yes. As of release 5.1, the system configuration and database can be easily transferred. Both appliances must be running the same firmware release for easy migration.
Can I upgrade to newer versions of CC-SG as they become available?	Customers with up-to-date CC-SG software maintenance have access to CC-SG upgrades (new firmware releases). Information about firmware or firmware availability may be downloaded from the Raritan website at http://www.raritan.com/support/CommandCenter-Secure-Gateway/ Upgrades are done through CommandCenter Secure Gateway's Graphical User Interface. Additionally, the CC-SG appliance has a CD/DVD-ROM drive to facilitate install/upgrades. To ensure secure operations and compatibility with the latest browser, operating systems and device versions, Raritan recommends upgrading to new releases when they are available.
How many log-in accounts can be created for CC-SG?	There is no specified limit to the number of log-in accounts that can be created.
Can I assign specific node access to a specific user?	Yes. Administrators have the ability to assign access to specific nodes per user or per group.
How are passwords secured in CC-SG?	Passwords are encrypted using MD5 encryption, a one-way hash. This provides additional security to prevent unauthorized users from accessing the password list. Additionally, users can be authenticated remotely using Active Directory®, RADIUS, LDAP or TACACS+ servers. The password is not stored or cached on CC-SG when using remote authentication.
Does CC-SG support two-factor authentication? (2FA)	Yes, CC-SG supports Two Factor Authentication with RSA SecurID® on RADIUS servers.
An administrator added a new node to the CC-SG database and assigned it to me, but I cannot see it in my Device Selection table. Why?	Newly added nodes should automatically appear in the user's node table. To update the table and view the newly assigned node, click the [Refresh] button.

Do I have to manually add all information to CC-SG, such as device and user information?	No. CC-SG includes a very comprehensive import/export capability. CSV files can be imported to help expedite the process of configuring devices, nodes, users, associations and PDUs. Import/export files include: • Import and export of categories and elements • Import and export of user groups and users • Import and export of nodes and interfaces • Import and export of devices and ports • Power IQ import and export file
Which version(s) of JavaTM does CC-SG support?	Please check the CC-SG Compatibility Matrix to identify which JRE versions are supported for a given CC-SG firmware release. The CC-SG administrator has the ability to set his or her own required JRE version for CC-SG users and also provide Hyperlink to this JRE version. Note: JRE is required to use the CC-SG Java-based Admin Client and for Raritan client applications such as VKC and RSC. The CC-SG Access Client and the Dominion Active KVM Client (AKC) do not use Java.
Given the recent security issues with Java, I'm concerned about Java use. What can I do?	Java is not required for use with the CC-SG HTML-based Access Client used by most users. Non-administrative users can use this client to access remote systems and devices. The Microsoft .NET-based Active KVM Client (AKC), a KVM Client used by the Dominion KX II, KX III, KX2-101-V2, and KSX II, does not use Java. We recommend the use of this client when running on Windows operating systems. The new, Dominion KX III HTML KVM Client (HKC) is available for Linux and Mac platforms. For customers looking to minimize their use of Java, this HTML-based KVM Client runs in the browser and does not utilize Java or .NET. The new, Dominion SX II HTML KVM Client (HKC) is available for Java-Free serial access. This HTML-based Serial Client runs in the browser and does not utilize Java or .NET. Users accessing serial devices connected to the Dominion SX & SX II can utilize a SSH client of their choice to access serial devices. Users can also make use of the CC-SG "Thick Client," which is Java based, but is not launched from a browser, thus avoiding browser based vulnerabilities.
Specifically what type of changes can CC-SG monitor and alert on?	CC-SG will log user activity (log-in/log-out, connect/disconnect) and configuration changes for both CC-SG and managed Raritan appliances, along with status changes of the connected appliances. All of the above can be forwarded to a network management system via SNMP or syslog.
Does CC-SG support remote power control using Raritan's PX Intelligent Rack PDU's?	Yes, Raritan PX, PX2 and PX3 PDU's can be added to CC-SG and then associated with server nodes to give users the ability to power on, off or cycle these servers. Raritan PDU's can also be connected to Dominion KVM and Serial devices to give users the ability for out-of-band power control of servers connected to these Raritan devices.

Is CC-SG integrated with Power IQ?	Yes. CC-SG does have several points of integration with Power IQ power management solution. First, Power IQ data, such as node, interface, outlet and device information, can be pulled into CC-SG to eliminate time-consuming data entry into both databases. Alternatively, data that's exported from either product can be imported into the other for fast, easy sharing and synchronization. Also, CC-SG users can control the power of nodes that are connected to Raritan PX and multivendor PDUs managed by Power IQ — without leaving their CC-SG client.
Will the current Paragon solution work with CC-SG?	Yes. Simply connect Paragon II to the Dominion KX II/III and set up the KX II/III as a connected device. Please refer to the Paragon II User Guide for details.
How will I know if someone else is logged into a Raritan device managed by CC-SG?	CC-SG presents the list of users logged into a device and can show which users are currently accessing a node through the active users report. Currently accessed devices will be in bold when looking at the device tree view from the CC-SG GUI. In addition, a bold node and a bold interface name of a node would indicate that it is currently being accessed by a user.
Does CC-SG have the ability to look at multiple device screens? How is this presented?	Users can simultaneously view and control multiple devices, provided they have the appropriate access privileges.
Is SSL encryption internal (LAN) or external (WAN)?	Both. The session is encrypted regardless of source, i.e., LAN/WAN. Note that SSLv3 is disabled by default and TLS used for security reasons. It can be enabled by the administrator.
Can audit/logging abilities track down who switched a power plug on/off?	Yes. Direct power switch off is not logged, but the power on/off through the CC-SG GUI is recorded in the audit trail and can be viewed in an audit trail report.
Does CC-SG support Certificate Signing Requests?	Yes. Under CC-SG, navigate to Security Manager and on the Certificates tab, you can generate a certificate signing request (CSR) to be sent to a certificate authority to apply for a digital identity certificate, generate a self-signed certificate, or import and export certificates and their private keys.
Does CC-SG support virtual media?	Yes. CC-SG supports Virtual Media in conjunction with Dominion KVM-over-IP devices. The use of virtual media on the Dominion KX II, KX III and KSX II devices also requires a virtual media Computer Interface Module.
Does CC-SG support the new KX III DSAMs?	Serial connections via Dominion Serial Access Modules (DSAM) connected to the Dominion KX III are supported. You will see any connected DSAMs in the Device View in the left hand navigator. The DSAM ports will appear as nodes in the Node View. Users can connect to the connected serial devices via the new HTML Serial Client.
Does CC-SG support the Firefox® and Chrome browsers?	Yes. Please see the CC-SG Compatibility Matrix for a full list of supported Web clients. CC-SG 6.1 includes changes to support running Java applications on Chrome versions 45 and above.
If I have an existing IT management application, can I integrate it with CC-SG?	Yes. Raritan offers an optional Web Service API (WS-API) for this purpose. It allows access of CC-SG, connected nodes and other CC-SG functions from your own customized client application.

If the CC-SG's RAID drive(s) fail(s), can I get a new drive?	Yes, for CC-SG's under warranty. Please see the Administrator's Guide for further information and troubleshooting if you suspect issues with the RAID drive(s). There is an onscreen diagnostics menu to help identify any issues. Please contact Raritan Tech Support for assistance.
Does CC-SG support AES-256?	Yes. AES-256 can be selected in the Admin GUI. AES-128 is the default setting.
Is there an evaluation version of CC-SG?	Yes. There is an evaluation version of CC-SG that can be installed on VMware Player, ESX or ESXi. You can download it from our website. The "Eval" is fully functional with a few exceptions : • Supports a maximum of 16 "interfaces" • Does not support the optional CC-SG WS-API
Is there a Windows version of the KVM Client?	Yes. CC-SG includes an "Active KVM Client" (AKC), which utilizes Microsoft®'s .NET technology instead of Java. Both the CC-SG Admin and Access Clients support AKC. Client PCs may run on Windows XP®, Vista®, Windows 7, 8 and 10 operating systems.
Is there an HTML5 KVM Client to avoid Java?	Yes, there are HTML KVM and Serial Clients for the KX III and SX II respectively. These run in the browser and do not use Java. Note that these do not run in proxy mode at the current time.
Which KVM Client does CC-SG use?	This is determined by the CC-SG administrator via the Application Manager screen. The administrator can select a particular client or use "Auto-Detect," which directs CC-SG to launch the appropriate client based on the Raritan device and the user's browser and operating system.
What are all the applications needed on the client machines in order to use CC-SG?	CC-SG has been designed to avoid adding any extra burden to client administrators. CC-SG stores and provides all the client applications, which means next to nothing needs to be specially maintained on your client devices. The only exception is that a compatible version of Java (JRE) is installed if you are going to use the CC-SG Java-based Admin Client (used by administrators) or a Java-based Raritan console application such as VKC. Java is not required for use with the CC-SG web-based Access Client, the new KX III HTML KVM Client, the new SX II HTML Serial Client or the .NET based Active KVM Client (AKC), used by the Dominion KX II, KSX II and KX III.
Does CC-SG support Windows 7, Windows 8, Windows 10 and Windows 2008 & 2012 Server?	Yes. CC-SG supports target devices running Windows 7, Windows 8, Windows 10 and Windows 2008 Server. The use of either OS on Client PCs is also supported. Each version of Windows 7 is supported (Home Premium, Professional and Ultimate).
Does CC-SG support IPv6?	Yes, in IPv4/IPv6 dual stack mode. As of 5.4.0, CC-SG does not support IPv6 only mode. Administrators can enable dual stack mode. The default setting is IPv4 only. Note that IPv6 support is being phased in over a few releases. Please refer to the release notes and Administrator's Guide for information about features and functions that are not supported when using IPv6.
Which version of SNMP does CC-SG support?	Support for SNMP is version 3.

How do I identify if I have the first generation CC-SG G1 hardware appliance?

If you purchased and received your CC-SG before May 2006, you have CC-SG G1 hardware. If you received your CC-SG after May 2006, and are not sure about your hardware mode, use one of the following three methods to identify if you have a CC-SG G1 hardware model:

Using the Appliance Serial Number

- Locate your serial number underneath the appliance
- If your serial number starts with the letters XG, your appliance is a G1

Using the Admin Client GUI

- Log in to the CC-SG administrative interface
- In the Administration dropdown menu, select the Configuration option
- Select the SNMP tab
- In the System Description area, you can identify your hardware model

Using the Diagnostic Console CLI

- With SSH client (e.g., PuTTY), make a connection using port number 23 to the CC-SG IP address
- Log in using "status" account
- In the System Information area at the Model field, CC-SG G1 will be indicated

I have a CC-SG V1/CC-SG E1. However, I don't know if this unit has an AMD or Intel® processor. How do I find out?

You can identify CC-SG V1 or E1 using the GUI

1. Log in to the Admin Client by entering URL <YOUR_CC-SG_IP_address>/admin> into a Web browser
2. In the top menu, go to Administration>Configuration
3. Select the SNMP tab
4. Above the "Update Agent Configuration" button, you will see your CC-SG firmware and hardware model

Alternatively, you can identify CC-SG V1 or E1 using the CLI

1. Open SSH session using port number 23 to the CC-SG IP address
2. Log in as "status"
3. Look for the Model field

In either case, use the following table to identify your hardware and processor:

Hardware	AMD	Intel
CC-SG E1	CC-SG E1-0	CC-SG E1-1
CC-SG V1	CC-SG V1-A	CC-SG V1-1

Where can I get more detailed information about CC-SG features?

Look in the Support section of raritan.com for the CC-SG Admin Guide, On-line Help and other docs.

The on-line help is a good way to quickly search for information on any given topic.