Frequently Asked Questions

CommandCenter® Secure Gateway

Release 5.2

Question	Answer
What is CommandCenter Secure Gateway (CC-SG)?	CommandCenter Secure Gateway is a management appliance that provides unified, secure browser or CLI-based access to the KVM, serial and power control devices in the data center and remote offices. CC-SG is available as a rack-mountable hardware solution or as a virtual appliance (runs on VMware®).
	CC-SG manages Raritan's Dominion® series, Paragon® II, IP-Reach® and Dominion PX™ intelligent power distribution units to provide centralized policy and security management for user access to servers and devices. CC-SG uses different access and power control methods to provide centralized management of devices, software applications and other solutions in the data center. These include Raritan devices, embedded service processors like HP® iLO/2/3, Dell® DRAC, IBM® RSA, IPMI and in-band software solutions such as RDP, VNC, SSH, Telnet and Web browser.
What are the different CC-SG hardware options?	Raritan offers hardware versions to address both small- and medium-size businesses as well as large enterprises with thousands of servers and other IT appliances. CC-SG E1 is targeted at large deployments as well as environments where dual power supply is required for redundancy. The CC-SG V1 is a powerful KVM and in-band access and power management appliance designed to address network redundancy or subnet proxy environments.
	The CC-SG G1 hardware model was discontinued in June 2007. In order to enjoy the benefits of new features and fixes available in release CC-SG 4.0.0 and later, CC-SG G1 customers must upgrade to the E1 or V1 models. A trade-in offer is available for customers upgrading their CC-SG G1 to new hardware. Note that the product warranty for CC-SG G1 will be honored as long as that warranty is still in effect.
On which Virtualization Platform can I install CC-SG?	CC-SG can be installed on a VMware virtual machine. 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 and KX II and KX II-101 KVM-over-IP switches, Dominion SX 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 Raritan's Dominion PX intelligent rack power management solutions.
	*Supports Paragon II access via direct connection to Dominion KX II.
How does CC-SG integrate with other Raritan products?	CC-SG uses a powerful, proprietary search-and-discovery technology that identifies and connects selected Raritan devices. Once CC-SG is connected and set up, device connection is transparent and administration is simple.
Does CC-SG have a software support program?	Yes. Software support, which includes product updates and access to Raritan Technical Support, is included for the first year of your CC-SG purchase. After the first year, extended software support can be purchased. It's important to obtain the extended coverage before the end of the first year to ensure against a period without support.
If I buy the CC-SG virtual appliance, can I run it on multiple virtual servers?	A different license is needed for each virtual machine on which it runs.

Question	Answer
Can I access CC-SG from a smart phone?	Yes. Introduced in release 5.2, the Mobile KVM Client (MKC) enables out-of-band KVM access and power control from mobile devices. In 5.2, iPad® and iPhone® with IOS 4.0 or later are supported. Additional device support is planned.
	The MKC supports out-of-band KVM access through Dominion KX II and power control through CC-SG power interfaces for DRAC, iLO/iLO2/iLO3, IPMI, RSA and VMware virtual machines. Also supported is power control of Power IQ®-managed PDUs and Raritan's PX platform.
	Use of this feature also requires KX II 2.4 or higher.
What are node licenses?	CC-SG is licensed based on the number of nodes and interfaces that you want it to be able to access. The base product (for both the hardware and virtualized solutions) is provided with a 128-node license. Additional licenses can be added as needed to meet your needs as your organization changes and grows.
How do I identify if I have a CC-SG G1?	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 into 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

Question	Answer
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: <table><tr><td>Hardware</td><td>AMD</td><td>Intel</td></tr><tr><td>CC-SG E1</td><td>CC-SG E1-0</td><td>CC-SG E1-1</td></tr><tr><td>CC-SG V1</td><td>CC-SG V1-A</td><td>CC-SG V1-1</td></tr></table>
Does CC-SG support access and management of virtual servers?	Yes. With CC-SG firmware version 4.0 and later, you can add a virtualization environment to CC-SG to enable a connection from CC-SG to virtual machines, virtual hosts and control systems. The new virtualization feature includes streamlined setup of single sign-on access to your virtualization environment, ability to issue virtual power commands to virtual machines and virtual hosts and 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 KX II. CC-SG allows for convenient and easy organization in its GUI of blade servers and the chassis that houses them.
How does CC-SG integrate with blade chassis products?	CC-SG can support any device with a KVM or serial interface as a transparent pass-through. All blade chassis come with one KVM connection for the management of the blade system. Some blade servers allow KVM connections on a blade basis through a proprietary add-on connector from the blade server manufacturer. This would allow access and control of the blade server through Raritan devices. In addition, CC-SG can incorporate access and power management through embedded cards such as HP iLO2 and RiLOE II, Dell DRAC (4/5/6) and IBM RSA II. Typically, these cards are located on the blade chassis and control the whole enclosure. CC-SG also provides power management through power strips connected to Raritan devices. CC-SG can also provide centralized access to individual blades with RDP, VNC or SSH. In release 5.2, support for Cisco®'s UCS platform was added. Users can access KVM and IPMI functions via CC-SG interfaces to the UCS' Integrated Management Controller (CIMC).
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.

Question	Answer
Can two CC-SG virtual appliances be clustered?	No. For failover of a virtual appliance, we support using VMware's High Availability feature.
Do I need to buy additional licenses for the backup Cluster unit?	No. Because only one unit is active at a time, node licenses are not needed for the second unit.
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 Neighborhood appliance?	Users can search from the Access Client for nodes that are managed directly by other neighborhood CC-SGs and 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.
Can a virtual and hardware appliance be included in the same Neighborhood?	Yes. Note that all appliances in a neighborhood must be running the same firmware version.
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.
Is the status of CC-SG limited by the status of the devices that it proxies?	No. CC-SG software resides on the dedicated appliance. This means that even if the device being proxied by CC-SG is not operating, users can still access CC-SG.
Can I upgrade to newer versions of CC-SG as they become available?	Yes. 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 client Graphical User Interface. Additionally, the CC-SG appliance has a CD/DVD-ROM drive to facilitate install/upgrades.
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. However, licensing restrictions or system specifications will limit the number of concurrent users or the number of nodes associated with the CC-SG based on the configuration deployed.
Can I assign specific node access to a specific user?	Yes, for users with Administrator permissions. Administrators have the ability to assign specific nodes per user.
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.

Question	Answer
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. Note: Clicking Refresh on the CC-SG toolbar will not close the session. Only the browser [Refresh] button will close the session.
Do I have to manually add all information to CC-SG, such as device and user information?	No. CC-SG, as of release 4.2, 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 Java^{TM} does CC-SG support?	Please check the compatibility matrix to identify which JRE version is required 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 console applications such as MPC and VKC. JRE is not required for use with the CC-SG HTML-based Access Client.
Specifically what type of changes can a management system monitor and alert on?	CC-SG will log user activity (log-in/log-out, connect/disconnect) and configuration changes at both CC-SG and managed Raritan appliances, and status changes of the connected appliances. All of the above can be forwarded to a network management system or enterprise notification system via SNMP or syslog.
What is the recommended use of Computer Interface Modules (CIMs) being moved or swapped at the physical level with changes to the logical database?	Each CIM includes a serial number and a target system name. Raritan systems devices assume that a CIM remains connected to its named target when its connection is moved to another switch. This move is automatically reflected in the system configuration and is propagated to CC-SG. If the CIM is moved to another server, an administrator must rename the CIM.
Is CC-SG integrated with Power IQ?	Yes. CC-SG does have several points of integration with Raritan's 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 being 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 and set up the KX II 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.

Question	Answer
Does CC-SG have the ability to look at multiple device screens? How is this presented?	If there are many devices connected to the CC-SG, users can scroll through the screens to view them all, provided they have the appropriate access privileges. Multiple screens can be opened, each one corresponding to one node, but will be restricted on the KVM side by the capacity of the KVM-over-IP channels.
Is SSL encryption internal (LAN) or external (WAN)?	Both. The session is encrypted regardless of source, i.e., LAN/WAN.
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 Client Certificate Request?	Yes. Under CC-SG, navigate to Security Manager under Setup.
Does CC-SG support virtual media?	Yes. CC-SG supports Virtual Media Deny, View and Control access policies. Customers can take advantage of the virtual media capabilities of CC-SG by using a Dominion KX II product managed by CC-SG. The use of virtual media on the Dominion KX II also requires a special virtual media Computer Interface Module.
Does CC-SG support Firefox®?	Yes, including Firefox 3.0.x. Please see the compatibility matrix for a full list of supported Web clients.
If I have an existing IT management application or client, can I integrate it with CC-SG?	Yes. Raritan offers an optional WS-API for this purpose. It allows access of CC-SG, connected nodes and other CC-SG functions from your own customized client application. Ordering information can now be found in our price list.
If the CC-SG's RAID drive(s) fail(s), can I get a new drive?	Yes. Please see the Administrator's Guide for further information and troubleshooting if you suspect issues with the RAID drive(s). As of release 4.1, 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 may either order the software from Raritan (part no. CCSG16-VA) or 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 .NET™ version of CC-SG clients?	Yes. CC-SG includes an "Active KVM Client" (AKC), which utilizes Microsoft®'s .NET technology instead of Java. Both the Admin and Access Client support .NET. Client PCs may run on Windows XP®, Vista® and Win7 operating systems.
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 small exception is that a compatible version of Java (JRE) is installed if you are going to use the CC-SG Java-based Admin Client or Raritan console applications such as MPC and VKC. JRE is not required for use with the CC-SG HTML-based Access Client.
Does CC-SG support Windows 7 and Windows 2008 Server?	Yes. CC-SG supports target devices running Windows 7 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).