

## CommandCenter® Secure Gateway



### Version 4.1.0

Question	Answer
What is CommandCenter Secure Gateway (CC-SG)?	<p>CommandCenter Secure Gateway (CC-SG) 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 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, Dell DRAC, IBM RSA, IPMI, and in-band software solutions such as RDP, VNC, SSH, Telnet and Web browser.</p>
What are the different CC-SG hardware options supported?	<p>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.</p> <p>The CC-G1 hardware model was discontinued in June of 2007. In order to enjoy the benefits of new features and fixes available in release CC 4.0.0 and later, CC-G1 customers must upgrade to the E1 or V1 models. A trade-in offer is available for customers upgrading their CC-G1 to a new hardware. Note that the product warranty for CC-G1 will be honored as long as that warranty is still in effect.</p> <p>For more information, visit <a href="http://www.raritan.com/products/centralized-management/commandcenter-secure-gateway/">http://www.raritan.com/products/centralized-management/commandcenter-secure-gateway/</a></p>

Question	Answer									
<p>How do I identify if I have a CC-G1?</p>	<p>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:</p> <p><u>Using the Appliance Serial Number</u></p> <ul style="list-style-type: none"> <li>▶ Locate your serial number underneath the appliance</li> <li>▶ If your serial number starts with the letters XG, your appliance is a G1</li> </ul> <p><u>Using the Admin Client GUI</u></p> <ul style="list-style-type: none"> <li>▶ Log in to the CC-SG administrative interface</li> <li>▶ In the Administration drop down menu, select the Configuration option</li> <li>▶ Select the SNMP tab</li> <li>▶ In the System Description area you will identify your hardware model</li> </ul> <p><u>Using the Diagnostic Console CLI</u></p> <ul style="list-style-type: none"> <li>▶ With SSH client (e.g., PuTTY) make a connection using port number 23 to the CC-SG IP address</li> <li>▶ Login using "status" account</li> </ul> <p>In the System Information area at the Model field, CC-SG G1 will be indicated.</p>									
<p>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?</p>	<p>You can identify CC-SG V1 or E1 using the GUI</p> <ol style="list-style-type: none"> <li>1. Login to the Admin Client by entering URL &lt;YOUR_CC-SG_IP_address&gt;/admin&gt; into a web browser</li> <li>2. In the top menu go to Administration&gt;Configuration</li> <li>3. Select the SNMP tab</li> <li>4. Above the "Update Agent Configuration" button you will see your CC-SG firmware and hardware model</li> </ol> <p>Alternatively you can identify CC-SG V1 or E1 using the CLI</p> <ol style="list-style-type: none"> <li>1. Open SSH session using port 23 to the CC-SG IP address</li> <li>2. Login as "status"</li> <li>3. Look for the Model field</li> </ol> <p>In either case, use the following table to identify your hardware and processor:</p> <table border="1" data-bbox="566 1547 1219 1648"> <thead> <tr> <th>Hardware</th> <th>AMD</th> <th>Intel</th> </tr> </thead> <tbody> <tr> <td>CC-SG E1</td> <td><b>CC-SG-E1-0</b></td> <td><b>CC-SG-E1-1</b></td> </tr> <tr> <td>CC-SG V1</td> <td><b>CC-SG-V1-A</b></td> <td><b>CC-SG-V1-1</b></td> </tr> </tbody> </table> <p>(continued)</p>	Hardware	AMD	Intel	CC-SG E1	<b>CC-SG-E1-0</b>	<b>CC-SG-E1-1</b>	CC-SG V1	<b>CC-SG-V1-A</b>	<b>CC-SG-V1-1</b>
Hardware	AMD	Intel								
CC-SG E1	<b>CC-SG-E1-0</b>	<b>CC-SG-E1-1</b>								
CC-SG V1	<b>CC-SG-V1-A</b>	<b>CC-SG-V1-1</b>								

Question	Answer									
<p>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?</p>	<p>If the CC-SG is either still inside the carton packaging or is outside the packaging, but is not accessible via the IP network use the following table to identify your hardware and processor:</p> <ol style="list-style-type: none"> <li>1. Look for either the ID label located underneath the CC-SG chassis or either one of the carton labels located on the sides of the CC-SG carton packaging.</li> <li>2. Identify the field titled "H/W Rev" or "H/W" on the label.</li> <li>3. Use the following table to identify which model you have:</li> </ol> <table border="1" data-bbox="566 577 1396 896"> <thead> <tr> <th data-bbox="566 577 726 645">H/W: or H/W Rev.:</th> <th data-bbox="726 577 1045 645">AMD</th> <th data-bbox="1045 577 1396 645">Intel</th> </tr> </thead> <tbody> <tr> <td data-bbox="566 645 726 768">CC-SG E1</td> <td data-bbox="726 645 1045 768"><b>Chassis CC-SG-E1-0C</b> (instead of 0C, it is possible that you may find 0A or 0B)</td> <td data-bbox="1045 645 1396 768"><b>Chassis-II CC-SG-E1-1A</b> (instead of 1A, it is possible that you may find 1B or 1C)</td> </tr> <tr> <td data-bbox="566 768 726 896">CC-SG V1</td> <td data-bbox="726 768 1045 896"><b>Chassis CC-V1-AC</b> (instead of 0C, it is possible that you may find 0A or 0B)</td> <td data-bbox="1045 768 1396 896"><b>Chassis-II CC-SG-V1-1A</b> (instead of 1A, it is possible that you may find 1B or 1C)</td> </tr> </tbody> </table>	H/W: or H/W Rev.:	AMD	Intel	CC-SG E1	<b>Chassis CC-SG-E1-0C</b> (instead of 0C, it is possible that you may find 0A or 0B)	<b>Chassis-II CC-SG-E1-1A</b> (instead of 1A, it is possible that you may find 1B or 1C)	CC-SG V1	<b>Chassis CC-V1-AC</b> (instead of 0C, it is possible that you may find 0A or 0B)	<b>Chassis-II CC-SG-V1-1A</b> (instead of 1A, it is possible that you may find 1B or 1C)
H/W: or H/W Rev.:	AMD	Intel								
CC-SG E1	<b>Chassis CC-SG-E1-0C</b> (instead of 0C, it is possible that you may find 0A or 0B)	<b>Chassis-II CC-SG-E1-1A</b> (instead of 1A, it is possible that you may find 1B or 1C)								
CC-SG V1	<b>Chassis CC-V1-AC</b> (instead of 0C, it is possible that you may find 0A or 0B)	<b>Chassis-II CC-SG-V1-1A</b> (instead of 1A, it is possible that you may find 1B or 1C)								
<p>Why would I need the CC-SG?</p>	<p>As more data center servers and appliances are deployed, IT management is becoming increasingly complex, IT staffs are being stretched to the limit and the demand for actionable information that helps address uptime issues is on the rise. CC-SG allows an IT administrator to access, manage and view all equipment, manage users and access permissions from a single remote device.</p>									
<p>Which Raritan products does CC-SG support?</p>	<p>CC-SG can manage Raritan's Dominion KX and KX II KVM-over-IP switches, Dominion SX serial-over-IP console servers, Dominion KSX remote office appliances and CommandCenter NOC. When deployed with the Paragon II System Controller (P2-SC), CC-SG supports access and control of multiple Paragon II switches. CC-SG also enables centralized remote power management by providing connectivity to Raritan's Dominion PX intelligent rack power management solutions.</p>									
<p>How does CC-SG support virtualization?</p>	<p>With CC-SG firmware version 4.0 and later, you can add 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.</p>									
<p>How does CC-SG integrate with other Raritan products?</p>	<p>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.</p>									

Question	Answer
Does CC-SG support access of blade servers?	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.
What is a CC-SG "Cluster"?	A CC-SG Cluster uses two CC-SG nodes, one Primary node and one Secondary node, for backup security in case of Primary node failure. Both nodes share common data for active users and active connections, and all status data is replicated between the two nodes.
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.
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 down time.
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?	<p>Yes. Information about firmware or firmware availability may be downloaded from the Raritan Web site at <a href="http://www.raritan.com/support/CommandCenter-Secure-Gateway/">http://www.raritan.com/support/CommandCenter-Secure-Gateway/</a></p> <p>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.</p>
How many login accounts can be created for CC-SG?	There is no specified limit to the number of login 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?	<p>Passwords are encrypted using MD5 encryption, a one-way hash. This provides additional security to prevent unauthorized users from accessing the password list.</p> <p>Additionally, users can be authenticated remotely using Active Directory, Radius, LDAP or TACACS+ servers. Password is not stored or cached on CC-SG when using remote authentication.</p>
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?	<p>Newly-added nodes should automatically appear in the user's node table. To update the table, and see the newly-assigned node, click the [Refresh] button.</p> <p>Note: Clicking refresh on the CC-SG toolbar will not close the session. Only the browser refresh button will close the session.</p>

Question	Answer
Which version(s) of Java does CC-SG support?	<p>Please check the compatibility matrix to identify which JRE version is required for a given CC-SG firmware release.</p> <p>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.</p> <p>Note: JRE is required for use of 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.</p>
Specifically what type of changes can a management system monitor and alert on?	<p>CC-SG will log user activity (login/logout, 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.</p>
What is the recommended use of Computer Interface Modules (CIMs) being moved or swapped at the physical level with changes to the logical database?	<p>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.</p>
How does CC-SG integrate with blade chassis products?	<p>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 iLO and RiLOEII, Dell DRAC4, 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.</p>
Will the current Paragon solution work with CC-SG?	<p>Raritan has introduced an interface device – Paragon II System Controller (P2-SC) – that integrates Raritan's Paragon II analog Cat5 KVM switches with CC-SG.</p> <p>Visit <a href="http://www.raritan.com/products/analog-kvm/paragon-ii/">http://www.raritan.com/products/analog-kvm/paragon-ii/</a> for more information.</p>
How will I know if someone else is logged into a Raritan device managed by CC-SG?	<p>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 bolded when looking at the device tree view from the CC-SG GUI. In addition, a bolded node and a bolded interface name of a node would indicate that it is currently being accessed by a user.</p>

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?	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 (CIM.)
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 the CC-SG's RAID drive(s) fail, 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 on-screen 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.