Raritan
A brand of legrand

COMMANDCENTER® SECURE GATEWAY
Features and Benefits

Raritan's CommandCenter Secure Gateway (CC-SG) provides IT administrators and lab managers with consolidated, secure and simplified remote access and control of multiple technology platforms at the application, operating system and BIOS level.

Feature Summary

- Secure, single sign-on to a single IP address for managing all of Raritan's Dominion® KVM-over-IP switches, serial console servers, Paragon® II analog KVM switches and PX™ intelligent PDUs
- Single point of access to physical servers (including blade systems, PCs and servers), virtual machines and VMware® infrastructure such as the ESX/ESXi server and VirtualCenter environments
- Remote access and power control using HP® integrated Lights-Out (iLO), Dell® Remote Access Controller (DRAC), IBM® Remote Supervisor Adaptor (RSA) and IPMI service processors, plus RDP, VNC, SSH and Telnet in-band applications
- Available as a rack-mountable hardware solution or a VMware, Hyper-V or XenServer virtual appliance
- HTML Access Client interface, which allows the user to easily locate managed equipment in customizable views, including favorites and recently accessed systems
- Centralized, role-based policy management, including controlled access privileges
- Wide, flexible array of client choices, including mobile client for access from smart phones and tablets and Java-free Windows Client
- Universal Virtual Media™ support through Dominion KX II and KX III devices
- Consolidated logging and audit trail, including detailed activity reports

Features	Functionality	Benefits
CommandCenter® Secure Gateway		
Support for Dominion KX II and KX III	CC-SG supports access to servers, PCs and other IT equipment connected to the Dominion KVM-over-IP switches that provide virtual media and Absolute Mouse Synchronization™ technology. CC-SG provides discovery, management, upgrades and many other management capabilities of the KX II and KX III devices.	CC-SG provides seamless integration of access through different Dominion products such as environments with mixed Dominion KX II and Dominion KX III devices.
Support for Dominion SX & SX II	CC-SG supports access to serial devices connected to the Dominion SX and new SX II serial console servers.	You get centralized management of multiple SX & SX II units along with access to serial devices.
Virtualization: Integration of VMware	CC-SG provides streamlined, single sign-on access to your VMware virtualized environment, the ability to issue virtual power commands to virtual machines and hosts, and a topology view with one-click connections. CC-SG integrates with VMware environments and supports connectivity to VirtualCenter software, ESX/ESXi servers and VMotion™ functionality.	You get consolidated access, power control and auditing of both physical and VMware virtual servers. Connectivity to virtual machines is always available even when these are moved from one virtual host to another.
Access to Blade Servers Connected to Dominion KX II and KX III Devices	CC-SG supports access of blade servers connected to Raritan Dominion KX II and KX III switches. Supported blade models include Cisco, Dell, HP and IBM blade servers.	You can access all connected nodes from a single client, including blade servers, rack servers, IP tools, service processors, PDUs, virtualized systems and devices connected to Raritan's KVM

		solutions.
Support for Raritan's Dominion PX	CC-SG can discover and add Dominion PX "smart" power strips located on the IP network. Once added to the CC-SG as a network-managed device, the Dominion PX allows access to the administrative interface via a single sign-on. Additionally, Dominion PX outlets are available for configuration and association to existing CC-SG nodes (servers). Note: The option of CC-SG integration to the PX through physical connectivity to Dominion devices via a power Computer Interface Module (CIM) or power cable is still available and supported. For Raritan PX2-XXXX and PX3-XXXX models, CC-SG connects to these rack PDUs via integration with the Power IQ energy management system.	You enjoy comprehensive centralized access and management. Your control of PX units can be independent of KVM or serial switches.
Access to In-Band Applications and Embedded Service Processors	Telnet and SSH are supported as in-band serial console interfaces. RDP, a common in-band console interface, can be used in either console or remote user modes. The RDP console allows the IT administrator to be the only RDP user on the server while the session lasts. Service accounts can be created and stored on the CC-SG with an MD5 two-way encrypted password. Service accounts can be employed on all in-band interfaces to allow for use with remote or local authentication. Changing the service account password applies to all CC-SG interfaces using that service account.	You have the ability to connect to serial targets using the SSH and Telnet protocols. You'll add flexibility by using RDP. You'll reduce the configuration time required to reflect password changes.

Robust Security	Low security profile, Linux®-based appliance architecture. A powerful policy management tool allows access and control based on a broad range of user-customizable criteria, including time of day, physical location, application, operating system, department and function. Available 128-bit and 256-bit AES encryption for end-to-end node access activity through AES-enabled Dominion devices. Support for a broad range of authentication protocols, including LDAP, Active Directory®, RADIUS and TACACS+ in addition to local authentication and authorization capabilities. Ability to import user groups from Active Directory. Support for Two Factor Authentication with SecurID® on RADIUS servers. Security updates and hardening; immune to the Heartbleed, Poodle, Freak and Shellshock vulnerabilities. IP-based access control lists (ACLs), which grant or restrict user access by IP address. Proxy mode for secure access to devices through firewalls/VPNs. Strong user password authentication, SAS 70 compliance for configurable amounts of failed log-in attempts and user ID lockout parameters.	CC-SG is a powerful, hardened, secure access platform that delivers peace of mind to IT managers who need to provide secure access to vital corporate resources.
Neighborhood Configuration	A neighborhood of up to 10 CC-SG units can be deployed and work together to serve the IT infrastructure access and control needs of the enterprise. The units in a neighborhood may consist of hardware and/or virtual appliances. All units in a neighborhood must be running the same firmware version.	You can add more CC-SGs as your environment grows. Performance is enhanced through the distribution of resources across CC-SGs.

Cluster Configuration for Hardware Appliances	"Cluster" configuration provides appliance redundancy through primary and secondary CC-SG hardware appliances on different subnets and/or geographical locations. CC-SG virtual appliances are not physically clustered. Raritan supports the VMware "High Availability" and "Fault Tolerance" features for easy-to-use, cost effective high availability.	You get instant, seamless failover if the primary unit fails.
Web Browser Access to Various Web Based Devices and Systems	CC-SG supports Web browser access to various devices and systems via IP address or host name. Single sign-on via the Web browser interface is available in some applications that can accept automatic username and password entries. Access to the Dominion PX Web interface and Dell DRAC4 administrative UI are two examples of Web browser interfaces that support single sign-on.	CC-SG provides centralized and audited access to Web server-equipped devices such as KVM-over-IP switches, embedded service processors and many types of IP enabled devices.
Mobile access from Apple Smart Phones and Tablets	CC-SG's Mobile KVM Client (MKC) enables out-of-band KVM access and power control from mobile devices. Apple iPad and iPhone® with IOS 4.0 or later are supported. MKC supports out-of-band KVM access through Dominion KX II/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, including Raritan's PX platform.	CC-SG users enjoy the convenience of leveraging their smart phone or tablet for KVM and power control and management. Provides the flexibility of accessing and managing IT resources from anywhere — at work, at home or while traveling.
Auditing and Audit Trail Reporting	The CC-SG administrator can sort the audit trail report based on categories. For example, the administrator can choose to view only authentication messages for remediation purposes, security messages for monitoring purposes or virtualization messages for virtual machine-related activity tracking.	CC-SG permits granular audit trail sorting for specific purposes like remediation, security and debugging.
Remote Monitoring and Capacity Planning Tools	CC-SG provides a variety of tools to monitor real-time and historical performance of CC-SG. Once activated, these tools can capture or display information such as CPU, memory, hard disk space, etc. Using the real-time data capture tool, customers can view information in a graphic format and create email alerts based on thresholds they set. With the historical data trending reports, customers can see their CC-SG performance graphed over time.	CC-SG allows secure, remote monitoring tools that can be activated by customers to monitor their CC-SG hardware performance and alert them when action may be required on their part.

Streamlined Raritan Device Firmware Upgrade Process	The Task Manager can upgrade multiple devices concurrently. In addition, the user can determine a time window for the automated upgrade task. An improved Restart Device automated task has been created. The CC-SG administrator can choose multiple devices and restart them at a selected time. At the completion of the task, there is an Upgrade Status report generated in addition to an auto-generated email alert.	This feature is particularly valuable in environments where a large number of Dominion devices are managed by CC-SG, whether in a data center or distributed environment.
DRAC 6 Support	CC-SG provides access to Dell Remote Access Controller (DRAC) through the following interfaces: • Telnet • SSH • Web browser • IPMI power	Organizations with Dell servers who have migrated from DRAC 4 or 5 to DRAC 6 can conveniently access them through CC-SG. Customers who need standard KVM access to some servers and access through DRAC to others can conveniently manage all resources through a single CC-SG client.
HP iLO, iLO2, iLO3 and iLO4 Support	CC-SG supports single sign-on console access to HP servers equipped with iLO processors. In addition, CC-SG provides remote power on/off/cycle and graceful shutdown capabilities to these HP servers.	CC-SG increases productivity in environments where servers with iLO are deployed along with CC-SG.
Personal View Customization Using Node Groups	In addition to creating customized views by predefined categories, customized views can be created using predefined node groups. The CC-SG administrator can share custom views with all system users and, in addition, each user can create their own customized view using node groups and device groups.	Users can easily find the server or IT equipment they need to access. By easily creating custom views and modifying them on the fly, CC-SG makes the IT staff's work easier and more productive.
Virtual Media	CC-SG supports control of virtual media access policies. Three options of authorization are available for virtual media: deny, control and view only. Virtual media is available for systems connected through a virtual media CIM to Dominion KX II, KX III, KSX II and KX2-101-V2 devices managed by the CC-SG.	This feature makes it easy to load software, copy data, reimage (apply a new OS), boot or upgrade the device remotely.
WS-API Support	An optional Web Services API is available for customers to integrate their own systems with CC-SG.	This allows access of CC-SG, connected nodes and other CC-SG functions from customer applications.

Control Power for Servers Connected to any PDU Supported by Power IQ	Enables power control of CC-SG nodes (Power IQ IT devices) that are connected to multivendor PDUs being managed by Power IQ — without leaving CC-SG.	CC-SG users that have also implemented Power IQ enjoy the convenience of remote power control of their IT infrastructure without leaving CC-SG. Devices can be connected to any PDU that is managed by Power IQ — including non-Raritan models.
Synchronize Data with Power IQ	CC-SG pulls data from Power IQ for easy, convenient data synchronization.	Ensure that CC-SG and Power IQ have common infrastructure data. Save time by not duplicating data entry tasks. Node, interface, device, port and other information is easily synchronized.
Data Import/Export via CSV Files	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	By maintaining information in a spreadsheet, administrators can easily manipulate data and save it as a .csv file for importing into CC-SG, saving time. Administrators can leverage the data already in CC-SG, easily export data from CC-SG, make any necessary changes, then return it to CC-SG or use it in other applications. Can also share data between CC-SG and Power IQ.
Virtual CC-SG Evaluation Version	A software-only evaluation version of CC-SG is available, which can be installed on virtualized servers and PCs. The "Eval" is fully functional with a few exceptions: • Supports a maximum of 16 "interfaces" • Does not support the optional CC-SG WS-API The evaluation can be downloaded from the Raritan website (www.raritan.com).	CC-SG can be evaluated without installing the hardware appliance. Simply install the virtual appliance on any virtualized machine running either VMware Player, ESX or ESXi.
.NET™ KVM Client for Java-free Support	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, Windows Vista® and Windows 7/8 operating systems.	Provides the choice to use a .NET KVM client for those who prefer the Windows-based architecture.

Windows 7 & 8 Support	CC-SG supports the access of target devices running Windows 7 & 8. The use of Windows 7 & 8 on client PCs is also supported.	Organizations that are implementing servers and clients running Windows 7 & 8 can conveniently upgrade existing CC-SG units to support their updated infrastructure — or install new CC-SGs without worrying about compatibility with these Microsoft operating systems.