

## CommandCenter® Secure Gateway



### Release 5.2

Der Raritan CommandCenter Secure Gateway (CC-SG) bietet IT-Organisationen integrierte, sichere und einfache Zugriffs- und Überwachungsfunktionen für sämtliche technologische Plattformen auf der Anwendungs-, Betriebssystem- und BIOS-Ebene.

#### Funktionsübersicht

- ▶ Sichere, einmalige Anmeldung über eine einzige IP-Adresse zum Verwalten aller Raritan Dominion® KVM-over-IP-Switches, analogen Paragon II KVM-Geräte und intelligenten Dominion PXT™-PDUs
- ▶ Verfügbar als Hardware für die Installation im Rack oder als reine virtuelle Anwendung
- ▶ Ein einziger Zugriffs- und Prüfpunkt für physische Server (einschließlich Blade-Systeme und -Server), virtuelle Maschinen und die VMware™-Infrastruktur wie ESX™/ESXi-Server- und VirtualCenter-Umgebungen
- ▶ Remote Zugriff und Power Kontrolle ist auch möglich über HP® Integrated Lights-Out (iLO/iLO2), Dell® Remote Access Control (DRAC), IBM® Remote Supervisor Adaptor (RSA) und IPMI Service Processors sowie RDP, VNC, SSH und TELNET in-Band-Anwendungen
- ▶ Client-Schnittstelle für den HTML-Zugriff, mit der die Anwender einfach in individuell anpassbaren Übersichten zu den verwalteten Geräten navigieren können – einschließlich Favoriten und zuletzt aufgerufener Knoten
- ▶ Zentrale rollenbasierte Richtlinienverwaltung einschließlich kontrollierter Zugangsberechtigungen
- ▶ Ein erweiterter und flexibler Bereich der Anwendernutzung durch den integrierten mobilen Zugriff mittels Smart Phones.
- ▶ Universal Virtual Media Unterstützung über Dominion KX II-Geräte
- ▶ Konsolidierter Prüfpfad einschließlich ausführlicher Aktivitätsberichte

Eigenschaften	Funktionen	Vorteile
Unterstützung des Dominion KX II	Der CC-SG unterstützt den Zugriff auf Server und andere Geräte, die an den Dominion KX II angeschlossen sind. Der KX II verfügt über virtuelle Medien und die Absolute Mouse Synchronization™-Technologie. Der CC-SG bietet die Erkennungs-, Management-, Upgrade- und viele andere Verwaltungsfunktionen der KX II-Geräte.	Der CC-SG ermöglicht die nahtlose Integration von Zugriffsmöglichkeiten über verschiedene Dominion-Produkte, z.B. in gemischten Umgebungen mit Geräten vom Typ Dominion KX und Dominion KX II.
Unterstützung des Dominion SX	Der CC-SG unterstützt den Zugriff auf serielle Geräte, die am Dominion SX angeschlossen sind.	Mehrere SX-Geräte lassen sich zusammen mit anderen Raritan-Zugriffsgaräten zentral verwalten.
Virtualisierung: Integration von VMware	Der CC-SG ermöglicht Ihnen die einfachere Einrichtung eines einheitlichen Zugriffs auf Ihre virtualisierte Umgebung, das Erteilen virtueller Leistungsbeefehle an virtuelle Maschinen und Hosts sowie eine Topologie-Übersicht mit Verbindungen per Mausclick. Der CC-SG lässt sich in VMware-Umgebungen integrieren und unterstützt Funktionen wie die Verknüpfung mit VirtualCenter-Software, ESX/ESXi-Servern und VMotion™-Funktionen.	Sie erhalten einen konsolidierten Zugriffs-, Energieverwaltungs- und Prüfpunkt für Ihre physischen und virtuellen Server.  Die Verknüpfung mit virtuellen Maschinen bleibt auch dann erhalten, wenn sie von einem virtuellen Host auf einen anderen verlagert werden.

Eigenschaften	Funktionen	Vorteile
Unterstützung des Zugriffs auf Blade-Server, die an Dominion KX II-Geräte angeschlossen sind	Der CC-SG unterstützt den Zugriff auf Blade-Server, die an Raritan Dominion KX II-Switches angeschlossen sind. Zu den unterstützten Blade-Modellen gehören die meisten Blade-Server von Dell, HP und IBM.	Sie können von einem einzigen Client auf alle angeschlossenen Knoten zugreifen, einschließlich aller Blade- und Non-Blade-Server, IP-Tools, Serviceprozessoren, PDUs, virtualisierten Systeme und Geräte, die mit den Raritan KVM-Lösungen verbunden sind.
Unterstützung des Raritan Dominion PX	<p>Der CC-SG kann alle intelligenten Dominion PX Mehrfachstromanschlüsse im IP-Netzwerk erkennen und hinzufügen. Der CC-SG erkennt dabei automatisch die Firmware-Version, Seriennummer und Anzahl der am jeweiligen PX verfügbaren Stromversorgungsanschlüsse. Sobald der Dominion PX als verwaltbares Netzwerkgerät zum CC-SG hinzugefügt wurde, ermöglicht er nach einer einmaligen Anmeldung den Zugriff auf die Administrationsschnittstelle. Zusätzlich sind die Dominion PX Stromversorgungsanschlüsse zur Konfiguration und Belegung von bestehenden CC-SG-Knoten (-Servern) verfügbar.</p> <p>Hinweis: Die Möglichkeit zur CC-SG-Integration in den PX über physische Verbindungen mit den Dominion-Geräten über Stromversorgungskabel oder -CIMs ist nach wie vor möglich und wird weiterhin unterstützt.</p>	<p>Sie können umfangreiche zentrale Zugriffs- und Verwaltungsfunktionen nutzen.</p> <p>Ihre PX-Geräte lassen sich unabhängig von seriellen oder KVM-Switches steuern.</p>
Zugriff auf In-Band-Anwendungen und Embedded Service Processors	<p>TELNET wird als serielle in-Band Konsolenschnittstelle unterstützt.</p> <p>RDP, eine der am häufigsten eingesetzten seriellen in-Band Konsolenschnittstellen, lässt sich entweder im Konsolen- oder externen Anwendermodus nutzen. Bei der RDP-Konsole kann der IT-Administrator festlegen, dass er während der gesamten Sitzungsdauer der einzige RDP-Nutzer bleibt. Alle RDP-Sitzungen von externen Konsolennutzern werden dann automatisch beendet, sobald sich der Administrator an der RDP-Konsole anmeldet. Zusätzlich lässt sich die RDP-Oberfläche an die gewünschte Farbtiefe anpassen.</p> <p>Mit einem wechselseitig verschlüsselten MD5-Passwort lassen sich Service-Konten auf dem CC-SG erstellen und speichern. Service-Konten lassen sich bei allen in-Band-Schnittstellen zur externen und lokalen Authentifizierung nutzen. Wenn das Passwort eines Service-Kontos geändert wird, gilt das neue Passwort automatisch für alle CC-SG-Schnittstellen, die dieses Service-Konto nutzen. Dennoch lassen sich bei Bedarf weiterhin individuelle Passwörter für jede Schnittstelle festlegen.</p>	<p>Sie können über das TELNET-Protokoll Verbindungen mit seriellen Zielgeräten herstellen.</p> <p>Sie können Ihre RDP flexibler nutzen.</p> <p>Sie sparen bei Passwortänderungen wertvolle Konfigurationszeit.</p>

Eigenschaften	Funktionen	Vorteile
Stabile Sicherheit	<p>Linux<sup>®</sup>-basierte Anwendungsarchitektur mit niedrigem Sicherheitsprofil.</p> <p>Ein leistungsstarkes Richtlinienverwaltungstool ermöglicht Ihnen den Zugriff und die Kontrolle mit zahlreichen, vom Benutzer anpassbaren Kriterien wie Tageszeit, physischer Standort, Anwendung, Betriebssystem, Abteilung und Funktion.</p> <p>Für durchgängige Knotenzugriffsaktionen über AES-kompatible Dominion-Geräte ist eine 128-Bit- und 256-Bit- AES-Verschlüsselung verfügbar.</p> <p>Neben lokalen Authentifizierungs- und Autorisierungsfunktionen werden auch zahlreiche Authentifizierungsprotokolle wie LDAP, Active Directory<sup>®</sup>, RADIUS und TACACS+ unterstützt.</p> <p>Nutzergruppen lassen sich vom Active Directory importieren.</p> <p>Die Second-Factor-Authentifizierung mit SecureID<sup>®</sup> wird auf RADIUS-Servern unterstützt.</p> <p>IP-basierte Zugriffskontrolllisten (ACLs), mit denen sich der Nutzerzugriff für bestimmte IP-Adressen freigeben oder sperren lässt.</p> <p>Proxy-Modus für den sicheren Gerätezugriff über Firewalls/VPNs.</p> <p>Authentifizierung mit starken Nutzerpasswörtern sowie SAS 70-kompatibel, um die maximal zulässige Anzahl von fehlgeschlagenen Anmeldeversuchen und die Benutzer-ID-Sperrparameter festzulegen.</p>	<p>Der CC-SG ist eine leistungsstarke Plattform mit hoher Zugriffssicherheit, auf die sich alle IT-Verantwortlichen verlassen können, die ihren Anwendern einen Zugriff auf kritische Unternehmensressourcen ermöglichen müssen.</p>
Nachbarschaftskonfiguration	<p>Die Architektur ermöglicht eine parallele Implementierung von bis zu zehn CC-SG-Geräten, damit diese die Zugriffs- und Kontrollanforderungen des jeweiligen Unternehmens an seine IT-Infrastruktur gemeinsam erfüllen. Die Einheiten einer Nachbarschaft können aus Hardware und/oder virtuellen Anwendungen bestehen. Alle Einheiten müssen dieselbe Firmwareversion nutzen.</p>	<p>Skalierbarkeit: Sie können weitere CC-SGs hinzufügen, sobald Ihre Umgebung wächst.</p> <p>Die Ressourcenverteilung über mehrere CC-SGs führt zu einer Leistungssteigerung.</p> <p>Regionalisierung:</p> <ul style="list-style-type: none"> <li>▶ Sie ermöglicht eine lokale Authentifizierung für den lokalen Zugriff.</li> <li>▶ Der CC-SG sorgt für rund-um-die-Uhr verfügbare Geschäftsprozesse – so vermeiden Sie regionale Ausfallzeiten.</li> </ul> <p>Abteilungsbezogene Zuordnung/ lokale administrative Autonomie:</p> <ul style="list-style-type: none"> <li>▶ Mit dem CC-SG können Sie auf Netzwerk-Partitionierungen zugreifen.</li> <li>▶ Unterteilen Sie nach verwendeten Zugriffstools, Raritan-Gerätetypen, Benutzertypen usw.</li> </ul> <p>Sie können CC-SG-Geräte in verschiedenen Subnetzen anwenden.</p>

Eigenschaften	Funktionen	Vorteile
Nahtlose Backup-Konfiguration	Die „Cluster“-Konfiguration ermöglicht eine Geräte-Redundanz durch primäre und sekundäre CC-SG-Implementierungen in verschiedenen Subnetzen und/oder geografischen Standorten.  Bitte beachten Sie, dass die virtuelle Anwendung des CC-SG nicht in ein Cluster eingebunden werden kann. Raritan unterstützt das VMware High Availability feature zur Ausfallsicherung einer virtuellen Anwendung.	Falls ein primäres Gerät ausfällt, übernimmt ein sekundäres Gerät sofort nahtlos dessen Funktion.
Webbrowser-Zugriff auf den CC-SG	Der CC-SG unterstützt den Webbrowser-Zugriff auf eine IP-Adresse oder einen Hostnamen. Bei einigen Anwendungen, die das automatische Eintragen von Benutzername und Passwort zulassen, jedoch keine zusätzlichen Eingabefelder wie Sitzungs-ID erfordern, ist eine einmalige Anmeldung über die Webbrowser-Oberfläche möglich. Der Zugriff auf die Dominion PX-Weboberfläche und die Dell RAC6-Administrationsoberfläche sind zwei Beispiele für Webbrowser-Schnittstellen, die eine einmalige Anmeldung unterstützen.	Diese Funktion ermöglicht einen zentralen geprüften Zugriff auf jedes Gerät, das über einen Webserver verfügt, z.B. auf Mehrfachstromanschlüsse, integrierte Service Prozessoren und proprietäre webbasierte IT-Anwendungen.
Zugriff von Smart Phones	Der CC-SG's Mobile KVM Client (MKC) ermöglicht out-of-band KVM Zugriff und Leistungssteuerung von mobilen Endgeräten. Version 5.2 unterstützt iPad und iPhone® mit IOS 4.0 oder neuerer Software. Der Ausbau des Supports ist geplant.  Der MKC unterstützt out-of-band KVM Zugriff über Dominion KX II und Leistungssteuerung über CC-SG Schnittstellen für DRAC, iLO/iLO2/iLO3, IPMI, RSA und VMware virtual machines. Außerdem möglich ist eine Leistungssteuerung von Power IQ®-verwalteten PDUs und Raritan's PX Plattform.  Voraussetzung für dieses Feature: KX II 2.4 oder höher.	CC-SG Benutzer können ihr Smart Phone für KVM und Leistungssteuerung und –management nutzen.  Bietet die Flexibilität, von überall auf IT Ressourcen zuzugreifen und sie zu verwalten- bei der Arbeit, von zu Hause oder unterwegs.  Die perfekte Lösung für Anwender, die einen schlanken Browser bevorzugen.
Überprüfungen und Prüfpfad-Berichte	Der CC-SG-Administrator kann den Prüfpfadbericht nach Kategorien untergliedern. Zum Beispiel kann der Administrator festlegen, dass ausschließlich Authentifizierungsmittelungen für eventuell erforderliche Problemhebungen, Sicherheitsmeldungen für Überwachungszwecke oder Virtualisierungsmeldungen zur Aktivitätsverfolgung bei virtuellen Maschinen angezeigt werden. Der Administrator kann außerdem festlegen, dass nur Aufgaben, integrations- oder zugriffsrelevante Prüfmitteilungen angezeigt werden. Mit einer Platzhaltersuche kann der Administrator darüber hinaus nach speziellen Prüfmitteilungen suchen.  Knotenüberprüfung verlangt, dass Benutzer, die zu einer vom CC-SG-Administrator festgelegten Gruppe gehören, freie Textinformationen eingeben müssen, sobald sie auf eine Oberfläche zugreifen. Diese Informationen lassen sich im Prüfpfadbericht und in der Registerkarte Knotenüberprüfung anzeigen.	Der CC-SG ermöglicht eine granulare Prüfpfad-Aufgliederung für spezielle Zwecke wie Störungsbehebung, Sicherheit und Programmfehlerdiagnose.  Sie können Aktivitätsberichte nach Systembenutzern wie Auftragnehmern und Zeitarbeitern untergliedert erfassen.
Tools zur Fernüberwachung und Kapazitätsplanung	Der CC-SG bietet zahlreiche Tools, um die Leistung des CC-SG über einen bestimmten Zeitraum sowie in Echtzeit zu überwachen. Diese Tools lassen sich einzeln aktivieren, um Informationen zur CPU, zum Arbeits- und Festplattenspeicher usw. zu erfassen oder anzuzeigen.  Mit dem Echtzeit-Datenerfassungstool können sich die Kunden Informationen in einem grafischen Format anzeigen und beim Über- oder Unterschreiten selbst vorgegebener Schwellenwerte per E-Mail benachrichtigen lassen. Mit dem Zeitspannen-Datenanalyse-Tool können sich die Kunden ihre CC-SG-Leistung für einen bestimmten Zeitraum anzeigen lassen.	Der CC-SG unterstützt sichere externe Überwachungstools, die die Kunden aktivieren können, um die Leistung ihrer CC-SG-Hardware zu überwachen und sich benachrichtigen zu lassen, wenn ihr Eingreifen erforderlich sein könnte.

Eigenschaften	Funktionen	Vorteile
Verbesserte Bedienoberfläche und Benutzerfreundlichkeit	Im Verlauf seines gesamten Lebenszyklus wurde der CC-SG umfangreich verbessert, um das Benutzererlebnis zu optimieren. Beispielsweise können die CC-SG-Administratoren festlegen, dass jede Aktion, die sich auf die Stromversorgung auswirkt, ihre Zustimmung erfordert, z.B. das Ausschalten eines Servers. Zusätzlich wurde das Knotenprofil um eine benutzerfreundlichere Registerkartenstruktur erweitert, die dem Anwender mehr nützliche Informationen anzeigt.	Durch die fortlaufende Verbesserung der CC-SG-Bedienoberfläche profitieren die Raritan-Kunden stets von einem optimalen Benutzererlebnis.
Vereinfachter Firmware-Upgrade-Vorgang für Raritan-Geräte	<p>Mit der Geräte-Upgrade-Funktion des Task Managers lässt sich die Anzahl der Geräte einstellen, die gleichzeitig aktualisiert werden sollen. Zusätzlich kann der Anwender ein Zeitfenster für den automatischen Upgrade-Vorgang festlegen. Nach Ablauf dieses Zeitfensters startet der CC-SG keine weiteren Geräte-Upgrades. Um ein paralleles Upgrade auszuführen, können die Administratoren in einem einfachen Auswahl- und Verschiebefenster erkennen, welche Geräte Sie für einen Upgrade-Vorgang ausgewählt haben.</p> <p>Außerdem wurde die Funktion für den automatischen Geräte-Neustart verbessert. Der CC-SG-Administrator kann mehrere Geräte auswählen und festlegen, wann diese automatisch neu gestartet werden sollen. Diese Funktion erweist sich als besonders nützlich, wenn ein Gerätestart vor oder nach einem Geräte-Upgrade erforderlich ist.</p> <p>Nach dem Abschluss dieser Aufgabe wird zusätzlich zur automatisch generierten E-Mail-Benachrichtigung ein Upgrade-Statusbericht erzeugt. Der Upgrade-Statusbericht enthält eine Echtzeitbeschreibung des Geräte-Upgrade-Vorgangs. Der Bericht ändert sich je nachdem, welches Gerät gerade aktualisiert wird, bereits aktualisiert wurde oder noch aktualisiert werden wird.</p>	<p>Diese Funktion erweist sich speziell in Umgebungen als besonders nützlich, in denen zahlreiche Dominion-Geräte vom CommandCenter gesteuert werden – ganz gleich, ob in einem Rechenzentrum oder einer verteilten Umgebung. Als ebenso nützlich erweist sich diese Funktion für Rechenzentren, die rund um die Uhr betrieben werden sowie in Umgebungen, bei denen die Infrastrukturwartungs- und -ausfallzeiten minimal gehalten und streng überwacht werden müssen.</p> <p>Die Funktion zum automatischen Geräte-Upgrade wurde vereinfacht, damit Sie Ihre Raritan-Geräte schnell, effektiv und sicher aktualisieren können.</p>
Unterstützung von HP iLO, iLO2 und iLO3	Der CC-SG unterstützt nach einmaliger Anmeldung den Konsolenzugriff auf HP-Server, die mit iLO/2/3-Prozessoren ausgerüstet sind. Zusätzlich lassen sich diese HP-Server über den CC-SG ein-/ausschalten, aus dem Standby-Betrieb hochfahren und geordnet herunterfahren.	Der CC-SG steigert die Produktivität in Umgebungen, in denen iLO/2/3-Server zusammen mit dem CC-SG implementiert wurden.
Individuell konfigurierbare Ansichten durch Knotengruppen	Neben der Möglichkeit zum Konfigurieren individueller Ansichten über vordefinierte Kategorien lassen sich auch individuelle CC-SG 3.2-Ansichten durch vordefinierte Knotengruppen erstellen. Gruppenbasierte individuelle Ansichten lassen sich sowohl im Client für den HTML-Zugriff und in den Java™-basierten Administrationsclients erzeugen. Der CC-SG-Administrator kann individuelle Ansichten für alle Systemnutzer freigeben, und zusätzlich kann jeder Anwender seine eigene individuelle Ansicht mithilfe von Knoten- und Gerätegruppen erstellen.	<p>Für Kunden aus Großunternehmen oder großen verteilten IT-Umgebungen mit mehreren Gruppen können die Anwender einfach die Server oder IT-Systeme finden, auf die sie zugreifen möchten.</p> <p>Mit dem CC-SG können die IT-Mitarbeiter individuelle Ansichten erstellen und bei Bedarf jederzeit rasch modifizieren. Das vereinfacht ihre tägliche Arbeit und gibt ihnen wieder mehr Zeit für die Lösung von Problemen, anstatt umständlich nach Servern suchen zu müssen.</p>
Virtuelle Medien	Der CC-SG unterstützt die Kontrolle von Zugriffsrichtlinien für virtuelle Medien. Für virtuelle Medien sind drei Autorisierungsoptionen verfügbar: Ablehnen, Kontrolle und Schreibschutz. Virtuelle Medien sind nur für OOB-Knoten verfügbar, die über ein Virtual-Media-CIM mit einem Dominion KX II-Gerät verbunden sind, die vom CC-SG verwaltet werden. Virtuelle Medien lassen sich mit einem Client-System oder externen Netzwerklaufwerk mit USB-Anschluss verbinden.	Mit dieser Funktion lässt sich das Gerät einfach per Fernzugriff neu aufsetzen (mit einem neuen Betriebssystem versehen), starten oder aktualisieren.

Eigenschaften	Funktionen	Vorteile
WS-API-Unterstützung	Für die Nutzung mit dem CC-SG ist ein WS-API verfügbar.	Es ermöglicht den Zugriff auf den CC-SG, die verknüpften Knoten und andere CC-SG-Funktionen von Ihrer eigenen, individuell konfigurierten Client-Anwendung.
Synchronisieren von Daten mit Power IQ®	CC-SG zieht sich Daten von Power IQ für einfache, bequeme Datensynchronisierung.	Einheitliche Infrastrukturdaten bei CC-SG und Power IQ werden so gewährleistet. Die Arbeit für Dateneinträge muss nicht doppelt durchgeführt werden – so wird Zeit gespart. Knoten, Schnittstellen, Geräte, Ports – diese und mehr Informationen können leicht synchronisiert werden.
Datenimport/-export	Version 5.0 bietet Ihnen eine äußerst umfangreiche Import-/Exportfunktion. Sie ermöglicht den Import von CSV-Dateien, um die Konfiguration von Geräten, Knoten, Anwendern, Belegungen und PDUs zu beschleunigen. Der Import/Export von Dateien umfasst: <ul style="list-style-type: none"> <li>▶ den Import und Export von Kategorien und Elementen</li> <li>▶ den Import und Export von Anwendergruppen und Anwendern</li> <li>▶ den Import und Export von Knoten und Schnittstellen</li> <li>▶ den Import und Export von Geräten und Ports</li> <li>▶ die Power IQ™ Import- und Exportdatei</li> </ul>	Durch das Vorhalten der Informationen in einem Kalkulationsblatt mit IT-Infrastrukturprofilen können die Administratoren alle erforderlichen Daten einfach ändern und als .csv-Datei für den Import in den CC-SG speichern. Dadurch sparen Sie viel kostbare Zeit.  Die Administratoren können auf die bereits mit dem CC-SG verwalteten Daten zugreifen und diese einfach zum Erstellen einer Masterdatei aus dem CC-SG exportieren. Wenn sie alle erforderlichen Änderungen vorgenommen haben, lässt sich die Datei wieder in den CC-SG importieren oder in anderen Anwendungen weiternutzen.  Tauschen Sie einfach Daten zwischen dem CC-SG und Power IQ aus.
Steuern Sie die Stromversorgung von Servern, die mit einer von Power IQ unterstützten PDU verbunden sind	Ermöglicht die Steuerung der Stromversorgung von CC-SG-Knoten (Power IQ IT-Geräten), die mit PDUs von verschiedenen Herstellern verbunden sind und von Power IQ verwaltet werden – ohne ihren CC-SG-Client zu verlassen.	CC-SG-Nutzer, die auch Power IQ implementiert haben, können die Stromversorgung ihrer IT-Infrastruktur verwalten, ohne den CC-SG verlassen zu müssen. Die Geräte lassen sich an jeder PDU anschließen, die von Power IQ verwaltet wird – sogar an nicht von Raritan gefertigten Modellen. CC-SG-Nutzer, die auch Power IQ implementiert haben, können die Stromversorgung ihrer IT-Infrastruktur verwalten, ohne den CC-SG verlassen zu müssen.
Der virtuelle CC-SG: Testversion	Der CC-SG ist jetzt als reine Software-Testversion erhältlich, die sich auf virtualisierten Servern und PCs installieren lässt. Sie ist bis auf folgende Einschränkungen voll funktionsfähig: <ul style="list-style-type: none"> <li>▶ sie unterstützt höchstens 10 Schnittstellen</li> <li>▶ sie unterstützt nicht die optionale CC-SG WS-API.</li> </ul> <p>Bestellen Sie eine DVD (CCSG16-VA) oder laden Sie die Daten von der Raritan Website herunter. (<a href="http://www.raritan.com">www.raritan.com</a>)</p>	Den CC-SG können Sie jetzt auch ohne Installation der Hardware-Appliance testen. Installieren Sie einfach die virtuelle Version auf einem virtualisierten Server, auf dem entweder VMWare Server oder ESXi ausgeführt wird (beide Versionen sind kostenlos von VMWare erhältlich).

Eigenschaften	Funktionen	Vorteile
.NET Client-Unterstützung	Der CC-SG verfügt über einen „Aktiven KVM-Client“ (AKC), der statt Java die Microsoft® .NET-Technologie nutzt. Sowohl der Admin- als auch der Access-Client unterstützen .NET. Auf den Client-PCs lassen sich die Betriebssysteme Windows® XP, Windows Vista® und Windows 7 ausführen.	Dadurch können alle Anwender, die eine Windows-gestützte Architektur bevorzugen, einen .NET-Client nutzen.
Windows 7-Unterstützung	Der CC-SG unterstützt jetzt den Zugriff auf Zielgeräte, auf denen Windows 7 ausgeführt wird. Die Nutzung von Windows 7 auf Client-PCs wird ebenfalls unterstützt. Die Unterstützung funktioniert bei allen Versionen von Windows 7 (Home Premium, Professional und Ultimate).	Unternehmen, die Server und Client-Rechner implementieren, auf denen Windows 7 ausgeführt wird, können jetzt ein bequemes Upgrade ihrer vorhandenen CC-SG-Einheiten ausführen, um ihre aktualisierte Infrastruktur zu unterstützen – oder neue CC-SGs installieren, ohne sich um die Kompatibilität mit dem neuesten Microsoft-Betriebssystem sorgen zu müssen.
DRAC 6-Unterstützung	Neben der langjährigen Unterstützung von DRAC 4 und 5 unterstützt der CC-SG jetzt auch den Zugriff auf den Dell Remote Access Controller 6. Dieser ist über folgende Schnittstellen möglich: <ul style="list-style-type: none"> <li>▶ Telnet</li> <li>▶ SSH</li> <li>▶ Web Browser</li> <li>▶ IPMI Power</li> </ul>	Unternehmen mit Dell-Servern, die diese von DRAC 4 oder 5 auf DRAC 6 migriert haben, können jetzt auch bequem über den CC-SG darauf zugreifen.  Kunden, die einen KVM-Standardzugriff auf bestimmte Server und gleichzeitig einen Zugriff über DRAC auf andere Server benötigen, können nun über einen CC-SG-Client bequem auf alle Ressourcen zugreifen.