CommandCenter® Secure Gateway Release 5.2.0

Contents

(Note – numbers in parentheses throughout this document are reference numbers internal to Raritan.)

Introduction

These release notes contain important information regarding a new release of this product. Please read the entire document and the related documentation available for this release.

Release 5.2.0 includes several enhancements and maintenance items.

Release 5.2.0 documentation and upgrade firmware is available at http://www.raritan.com/support/commandcenter-secure-gateway/.

New Features and Updates in This Release

Access from Smart Phones and Tablet PC's

CC-SG 5.2.0 supports access and management of your IT resources from mobile devices, such as a smart phone or tablet PC. CC-SG now includes a new Mobile KVM Client (MKC), which enables out-of-band KVM access and power control from mobile devices. In 5.2, iPad and iPhone **with IOS versions 4.2.1 and 4.3.1** are supported. Additional mobile products will be supported in future releases.

The MKC supports out-of-band KVM access through Dominion KX II and power control through CCSG 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.

Requires CC-SG 5.2 and KX II 2.4.

CC-SG Extended Neighborhood Search

Users accessing CC-SG Network Neighborhoods are able to create a consolidated node list spanning multiple neighborhood units. Users can search from the Access Client for nodes that are managed directly by other neighborhood CC's and launch the interfaces for the discovered nodes.

Enhancement of Microsoft RDP Support to Enable Use of RSA SecurID 800

The CC-SG Microsoft RDP interface has been enhanced to support the use of local smart cards in remote sessions. This enables the use of smart cards and devices such as RSA SecurID 800 tokens for authentication when accessing a target server that requires this level of secure access.

Access & Power control of the Cisco UCS Platform

CC-SG supports access and management of Cisco Unified Computing System

(UCS) B-Series blade servers. Users can access KVM and IPMI functions via CCSG interfaces to the UCS' Integrated Management Controller (CIMC). CC-SG also supports standard KVM access to individual blades when using Dominion KX II.

CSV File Import Enhancement

The CSV Import feature has been enhanced to enable updating, adding and deleting of nodes and interfaces within the CC-SG database. Logging and SNMP traps related to this enhancement are also included. Further details can be found in the updated *Administration Guide*.

Updated VMware Support for Access & Management from CC-SG

VMware access & management support has been enhanced to include version 4.1. Please see the compatibility matrix for a full list of supported versions. This applies to CC-SG physical and virtual appliances.

Updated VMware Support for Running the CC-SG Virtual Appliance

The CC-SG Virtual Appliance (part number CCSG128-VA) release 5.2 can be installed on ESX/ESXi versions 4.0 and 4.1. Note that CCSG128-VA release 5.1 has not been tested with ESX/ESXi 4.1.

The evaluation version of the virtual CC-SG has also been expanded to run on VMware Player. The CC-SG evaluation runs on VMware Player version 3.1.4 and ESX/ESXi 4.1. The evaluation firmware can be downloaded from http://www.raritan.com/support/commandcenter-secure-gateway/ or ordered on DVD (CCSG16-VA). Please refer to the same location for the Virtual Evaluation Quick Setup Guide, which includes installation instructions.

Updated Service Processor Support

CC-SG 5.2 introduces support for HP's iLO3. The tested version is 1.16.

This release also includes updated support for DRAC5 (version 1.51) and DRAC6 (1.5). Please see the Compatibility Matrix for a complete list of supported versions.

Internet Explorer Version 9 Support and Firefox Version 4.x

CC-SG release 5.2 has been updated with support for IE9 and Firefox 4.x

Applicability

CC-SG 5.2.0 is applicable to the CommandCenter ® Secure Gateway physical appliance models CC-SG-V1, CC-SG E1 and the Virtual Appliance (CCSG128-VA).

Important note for CC-G1 customers: Raritan discontinued the CC-G1 model in

June of 2007. **Do not attempt to upgrade your CC-G1 to this release**. Please back up your CC-G1, restore the database to a CC-SG V1 or E1 hardware unit running the same firmware version, and upgrade the new V1 or E1 hardware unit to this release per the Upgrade Path instructions below.

Upgrade Path

To upgrade your CC-SG to this release you must be running firmware version 5.0.0 or higher (hardware appliance) or 5.0.5 (virtual appliance) or higher, as depicted in the diagram below. As indicated above, you can upgrade CC-SG V1 or CC-SG E1 but **not CC-G1** units to 5.2.0.

Please back up your CC-SG before and after any upgrade step. For detailed step by step instructions on upgrading, refer to the Readme file available with this CC-SG release. You may also need to upgrade your other Raritan devices. For a complete list of supported devices, refer to the CC-SG Compatibility Matrix, available at http://www.raritan.com/support/commandcenter-secure-gateway/. For instructions on upgrading managed Raritan devices, refer to the CC-SG Administrators Guide.

About Licensing

(*Note – this section applies only to **hardware appliance** upgrades from pre-5.0.0 versions; all others can disregard*).

In release 5.0.0, new licensing features were introduced in CC-SG. Licenses are now established and tracked through the new License Manager, located in the Administration menu of the Administration Client.

As seen in the upgrade path diagram above, if your unit is running a version lower than 5.0.0, **you must upgrade to 5.0.0 before moving up to 5.2.0**. During the upgrade to 5.0.0, CC-SG will establish a 128 node base license and will also build any applicable "add-on" licenses needed, **based on the quantity of nodes in the unit's database**. If there are more than 128 nodes in the database, a second license known as an "Add-On" license is created and added to the base license. The created Add-On license is rounded up, based on the following license levels:

CCL-64	64 node license
CCL-128	128 node license
CCL-256	256 node license
CCL-512	512 node license
CCL-1024	1024 node license
CCL-2048	2048 node license
CCL-4096	4096 node license
CCL-8192	8192 node license

For example, if there are 400 nodes in the database, an add-on license for 512 nodes will be established – **in addition to the 128 node base license**.

The process of upgrading and establishing the license(s) has been designed in a manner that is *as seamless as possible for current CC-SG customers*. During the upgrade, the new firmware release captures the unit's unique ID and current nodes – and uses this information to establish the new license(s). Upon completion of the upgrade, the licenses can be found in the new "License Manager" menu.

Once the upgrade to 5.0.0 is completed, your node licenses have now been established and the unit's node access will be limited to the amount of nodes as displayed in the License Manager. If you need to add to your node licenses in the future, please contact your Raritan sales representative.

Clustered Licensing: In a clustered configuration, in which a 2nd CC-SG serves as a failover unit to a primary unit, 'Cluster' licenses are shared. Examples of CC-SG part numbers for ordering a clustered solution include CC-2XE1-512 and CC-2XE1-1024.

The base and add-on licenses are bound to the two CC-SG node host IDs identified in the license files. License files should be added to, and features checked out, on the designated primary node in the cluster. They will be automatically transferred to the backup node when the two CC-SG nodes are joined into a cluster.

The licenses allow for the cluster to be temporarily deleted so that maintenance activity, such as firmware upgrades, may be performed.

Important: It is highly recommended that upgrading and/or license management is performed at a pre-arranged time, during which users are not accessing the system. The system requires that the required licenses are added and features are activated in order to be in the operational state. Until that time system access is limited, devices and nodes are not available.

If direct access to devices is needed while the CC-SG is not in the fully

operational state and the device indicates it is still under CC-SG management: Shut down the CC-SG application using System Maintenance > Shutdown. After the timeout period the devices will be directly accessible.

Note: If your CC-SG unit is relatively new, the database may include considerably less nodes than licensing that was purchased. Should this occur, please contact your closest Raritan office and report the issue to Customer Service, who will work with you to acquire the proper node license.

Security and Compliance Information

Refer to the CC-SG Administrators Guide 'Appendix B: CC-SG and Network Configuration' for specific settings.

Updated Product Documentation

Updated documents available with this release include:

- CC-SG 5.2.0 Upgrade Readme File
- Compatibility Matrix
- Administrators Guide
- Users Guide
- Quick Setup Guide

General Notes

1. If using Windows XP or Vista, CC-SG supports the 64 bit OS. However, if using a Java plug-in, only the 32 bit plug-in is supported. See http://java.sun.com/javase/6/webnotes/install/system-configurations.html for Java support information. (17855)
2. For optimal operations, disable the pop-up blocker in your browser.
3. Virtualization: During the first connection to a virtual machine, you may be asked to download an add-on from VMware. Once the add-on is installed, please restart your browser.
4. If you are using Firefox on Windows, you must add the IP address of the CC-SG to the Allowed Sites for Add-ons list and the Allowed Sites for Pop-ups list in the browser before connecting to a VMW Viewer interface.
5. Cluster rebuilds: When selecting a rebuild time, please be aware of possible differences in time zones between units.

6. During the CC-SG boot-up sequence, should the following message be displayed, it can be safely ignored (seen on the local KVM console port only):
7. `Memory for crash kernel (0x0 to 0x0) notwithin permissible range`
8. During boot-up, a normal delay of up to two minutes may occur after seeing the following message (local KVM console port only):

   `Red Hat nash version 5.1.19.6 starting`

Limitations and Restrictions

1. Mobile KVM Client notes:
   - There is a known issue that iPad/iPhone devices have with memory management. In order to prolong the time a session can run before encountering this problem, minimize the number of applications that are running and limit it to one mobile KVM client at a time.
     - On IPad1, with one CCSG Mobile Access client and one Mobile KVM client, sessions can be sustained for approximately 20 minutes. After this time, the memory management issues can cause the browser to stop running.
     - Sessions on iPad2 run significantly longer since it has more memory than iPad1.
     - Some guidelines to prolong the life of Mobile KVM session are:
       i. Run a maximum of one mobile KVM client.
       ii. Stop all the unused applications in the IPad, rather than having them sit idle in the memory. (Two quick presses on Home button will show all the apps resident in memory. Touch and hold any icon, until - sign shows up, then get rid of unused apps.)
   - Guidelines for number of concurrent Mobile KVM client sessions per CC-SG are as follows:
     - 12 concurrent sessions on model CC-SG-V1-1
     - 25 concurrent sessions on model CC-SG-E1-1
   - If Mobile KVM client is not properly closed, CC-SG Mobile Client Timeout will clean up any lingering sessions. The CC-SG Mobile Client Timeout setting is used to free resources from sessions which have not been properly terminated. In order to ensure optimal operation:
     - When ending a Mobile KVM client session, always 'Exit' from the Mobile KVM client toolbar Menu > 'Exit'. This ensures that session resources are freed quickly and available for other user sessions.
     - Otherwise, status will be updated by CC-SG after the timeout expires and resources are freed.
2. When setting up a Flexera License Server for use with virtual CC-SG appliance:
   - if using the license server hostname: ensure that DNS and reverse DNS lookups are correct and correspond to the hostname, include the

fully qualified domain name in the license file uploaded onto CCSG otherwise CCSG will not be able to locate the license server by hostname.

- if using the license server ip address: although the license file contains an ip address the license server will still perform DNS consistency checks, if these fail the license server will report an error. The workaround is to define an Environment Variable, FLEXLM_ANYHOSTNAME, set equal to 1. The FLEXLM_ANYHOSTNAME will cause the license server to in essence bypass the initial hostname checks.

3. When launching the iLO3 KVM app via CC, a warning 'do you wish to load unsecure content' will be presented to the user that needs to be accepted. This is because the HP applet is not signed.
4. Supported JRE versions for this release include 1.6.0_10 thru 1.6.0_26.
5. The “Bookmark Node” feature is not supported when using Internet Explorer version 8 (IE8). (20053, 20237)
6. RSA Remote Console cannot be launched from CC-SG when using JRE 1.6.0_10 and higher. IBM has a workaround: http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5080396.
7. If enabling AES 256, ensure that the jurisdiction files are installed on the client. Otherwise, you will be locked out of the CommandCenter.
8. When using a Linux client, the Virtualization topology view cannot be printed.
9. VMware Viewer and Firefox version 3.6.x are not compatible.
10. CC-SG cannot manage or access ESXi virtual nodes that use a free-trial license. (31078)
11. Firefox users of the Access Client are prompted to download a file named 140.JNLP each time a port connection is made. Select the "Do this automatically for files like this from now on" checkbox, so that Firefox can automatically download the file for future connections. (31893)
12. Single mouse mode does not function on Windows or Linux servers as targets when using VMware as a client. (36935)
13. When accessing DRAC5 targets, there is a limit of 4 concurrent SSH sessions. (35721)
14. If the version of DRAC does not support graceful shutdown, a “graceful shutdown not supported” message is received when executing a graceful shutdown operation for power control. (35722)
15. Licensing Notes:
    - When choosing a server on which to run the **Flexera License Server and Raritan vendor daemon**, please note the following:
        - Raritan’s testing has shown the following processor/OS combinations to be favorable:
            - Intel Pentium 4 with Windows XP

- Intel Pentium D with Windows Vista
- Intel Celeron with Windows 2003 Server
- AMD Opteron with Windows 2003 Server
- AMD Opteron with Windows 2003 Server
- AMD Opteron with Windows 7
- AMD Opteron with Windows 2008 Server
- AMD Athlon 64 with Windows Vista

- Raritan's testing has shown the following processor/OS combinations to be **unfavorable**:
  - Intel Xeon with Windows 2003 Server
  - Intel Xeon with Windows 2003 Server
  - Intel Pentium 3 with Windows 2003 Server
  - (32514)

- Per Flexera, The following steps are recommended as License Administrator best practices:
  - Do not use the default 2700 TCP port
  - Run the license server using a least privileged user account.
  - Utilize the recommended security settings offered by the Operating System (OS) vendors that resist the buffer/stack overflow attacks. For example, the Data Execution Prevention (DEP) feature on Windows helps in this regard. Most OS updates also include security features that take advantage of both hardware and software based protection mechanisms against malicious code execution.