CC-SG 6.0 Upgrade Guide

See the CC-SG version 6.0 release notes before proceeding with upgrade. Follow the upgrade path for your CC-SG version.

http://www.raritan.com/support/product/commandcenter-secure-gateway/commandcenter-secure-gateway-version-6.0.0

New Requirements for CC-SG 6.0 Upgrades

When upgrading a CC-SG virtual appliance from a previous version of CC-SG to version 6.0, you must meet three new requirements for a successful upgrade.

1: Delete all KX1, KSX1, KX-101, IP Reach, and PIISC Devices

- These devices are not supported in version 6.0. Upgrade will fail if any of these devices are being managed by CC-SG at the time of the upgrade.

Deleting a Device

You can delete a device to remove it from CC-SG management.

Important: Deleting a device will remove all ports configured for that device. All interfaces associated with those ports will be removed from the nodes. If no other interface exists for these nodes, the nodes will also be removed from CC-SG.

To delete a device:

1. Click the Devices tab and select the device you want to delete.
2. Choose Devices > Device Manager > Delete Device.
3. Click OK to delete the device. A message appears when the device has been deleted.

2: Add a Second Hard Disk to the Virtual Machine

- For CC-SG virtual machines only, add a second hard disk to your virtual machine. See ***Add a Second Hard Disk*** (see "***Adding a Second Hard Disk***" on page 1).

Adding a Second Hard Disk

This procedure applies to virtual CC-SG only.

1. Before adding the second hard disk, power off CC-SG in the Diagnostic Console. Choose Operation > Admin > CC-SG System Power OFF.
2. Login to vCenter and select the CC-SG virtual machine.
3. Right click Edit Settings on your virtual CC-SG to open the Virtual Machine Properties.
4. Click Add.
5. Select Hard Disk then click Next.
6. Select "Create a new virtual disk" then click Next.
7. Type 40 in Disk Size then click Next. **The disk size must be 40.**
8. Select SCSI(0:1) in Virtual Device Node then click Next.
9. Click Finish then click OK. You should see Hard disk 2 if you look in the Virtual Machine Properties again.
10. Power on the CC-SG virtual machine from vCenter.
11. Upgrade the CCSG with version 6.x upgrade file. The upgrade should take 30-40 minutes. After upgrade is finished, verify the upgrade is successful. You can then delete the old hard disk in vCenter if you want to save space.

3: Ensure CC-SG Does Not Use a License Server

CC-SG 6.0 no longer supports the Flexera lmadmin or lmgrd license servers. An external license server is not required anymore. If you are using a license server, you must get new license files from Raritan to migrate away from the license server. You must re-license before upgrading to CC-SG 6.0. Contact Raritan Technical Support to get the licenses, then use the CC-SG License Manager to upload them.

Upgrade Failure Messages

CC-SG upgrade will fail if the new requirements are not met.

If the upgrade fails, Diagnostic Console shows a Warning message: "Upgrade aborted. Please go to CommandCenter web page for details." Go to the CC-SG IP address to view a page with the reason for failure and instructions to resolve the problem.

Each upgrade failure requires CC-SG to reboot. You can then correct the problem, and try the upgrade again.

Upgrading CC-SG

You can find firmware files in the Support section of the Raritan website. To upgrade CC-SG from version 3.x to version 4.1, you must upgrade it to 4.0 first. To upgrade CC-SG from version 4.x to any version higher than 5.0, you must upgrade it to 5.0 first.

CC-SG version 4.0 or higher is not compatible with older G1 hardware. Do not upgrade a CC-SG G1 unit to version 4.0 or later.

Only users with the CC Setup and Control privilege can upgrade CC-SG.

You should back up CC-SG before upgrading, and send the backup files to a PC for safe keeping. See ***Backing Up CC-SG*** (on page 3) and ***Save a Backup File*** (on page 4).

You should check CC-SG's disk status before upgrading. See ***Check Disk Status*** (on page 3). **If there is an indication that a drive needs to be replaced or is questionable, or the RAID Array needs to be rebuilt or the status is questionable, contact Raritan Technical Support before proceeding with the firmware upgrade.**

If you are operating a CC-SG cluster, you must remove the cluster before upgrading. Upgrade each CC-SG node separately, then re-create the cluster. See Upgrading a Cluster.

Important: If you need to upgrade both CC-SG and a device or group of devices, perform the CC-SG upgrade first then perform the device upgrade.

CC-SG will reboot as part of the upgrade process. DO NOT stop the process, reboot the unit manually, power off, or power cycle the unit during the upgrade.

To upgrade CC-SG:

1. Download the firmware file to your client PC.
2. Log into the CC-SG Admin Client using an account that has the CC Setup and Control privilege.
3. Choose System Maintenance > Maintenance Mode > Enter Maintenance Mode. Enter password, delay time, and message for users. All users will be logged out when time delay ends.
4. Once CC-SG is in maintenance mode, choose System Maintenance > Upgrade.
5. Click Browse. Navigate to and select the CC-SG firmware file (.zip) then click Open.
6. Click OK to upload the firmware file to CC-SG.

   After the firmware file is uploaded to CC-SG, a success message appears, indicating that CC-SG has begun the upgrade process. All users will be disconnected from CC-SG at this time.
7. You must wait for the upgrade to complete before logging into CC-SG again. You can monitor the upgrade in the Diagnostic Console.
   a. Access Diagnostic Console using the admin account. See Access Administrator Console.
   b. Choose Admin > System Logfile Viewer. Select sg/upgrade.log then choose View to view the upgrade log.
   c. Wait for the upgrade process to run. The upgrade process is complete when you see the "Upgrade completed" message in the upgrade log. Alternatively, you may wait for the SNMP trap ccImageUpgradeResults with a "success" message.
   d. The server must reboot. The reboot process begins when you see the "Linux reboot" message in the upgrade.log. The server will shut down and reboot.

   Note: For upgrades from CC-SG 5.x to 6.0, and from 3.x to 4.0.x, the system will reboot twice, which is normal and expected.

   e. In approximately 2 minutes after the reboot, you may re-access the Diagnostic Console using the admin account, and monitor the progress of the upgrade process. **Optional.**
8. Click OK to exit CC-SG.
9. Clear the browser cache, then close the browser window. See ***Clear the Browser's Cache*** (on page 2).
10. Clear the Java cache. See ***Clear the Java Cache*** (on page 3).
11. Launch a new web browser window.
12. Log into the CC-SG Admin Client using an account that has the CC Setup and Control privilege.
13. Choose Help > About Raritan Secure Gateway. Check the version number to verify that the upgrade was successful.
    - If the version has not upgraded, repeat the previous steps.
14. Choose System Maintenance > Maintenance Mode > Exit Maintenance Mode. Click OK. All users will be able to login now.
15. Back up the CC-SG. See ***Backing Up CC-SG*** (on page 3).

Related Information

Clear the Browser's Cache

These instructions may vary slightly for different browser versions.

Internet Explorer:

1. Choose Tools > Internet Options.
2. On the General tab, click Delete Files then click OK to confirm.

In FireFox:

https://support.mozilla.org/en-US/kb/how-clear-firefox-cache#w_clear-the-cache

Clear the Java Cache

These instructions may vary slightly for different Java versions and different operating systems.

In Windows XP with Java 1.6:

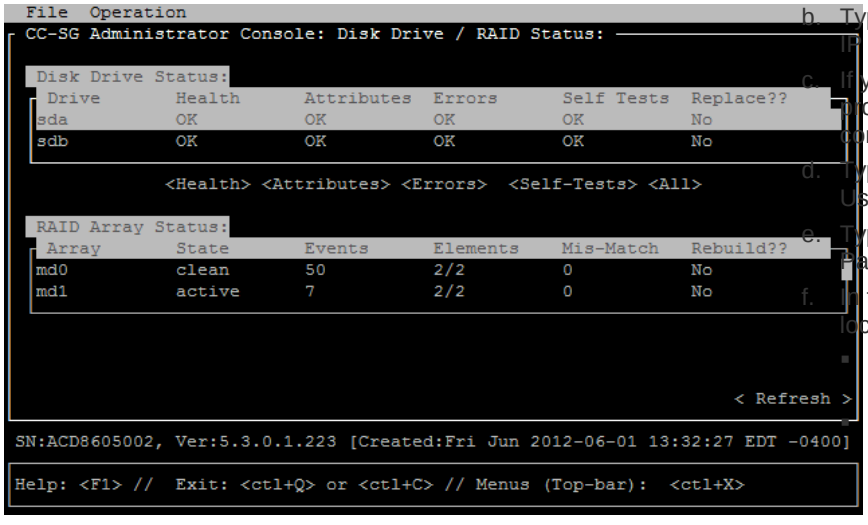
1. Choose Control Panel > Java.
2. On the General tab, click Settings.
3. In the dialog box that opens, click Delete Files.
4. Make sure the Applications and Applets checkbox is selected then click OK.

Check Disk Status

Before starting a CC-SG firmware upgrade, verify the CC-SG disk status. **If there is an indication that a drive needs to be replaced or is questionable, or the RAID Array needs to be rebuilt or the status is questionable, contact Raritan Technical Support before proceeding with the firmware upgrade.** See ***Upgrading CC-SG*** (on page 2).

To check disk status:

1. Choose Operation > Utilities > Disk Drive / RAID Status. This option allows you to view the status without the ability to initiate the Replace Disk Drive and Rebuild RAID Array operations.
2. Verify that disk drives do not need to be replaced, and do not indicate any questionable status.



Backing Up CC-SG

The best practice is to enter Maintenance Mode before backing up CC-SG. Entering Maintenance Mode ensures that no changes are made to the database while it is being backed up.

You can store up to 50 backup files on CC-SG. Once you have reached 50 backup files, you cannot create any new backups until you delete some old backup files from CC-SG. See Saving and Deleting Backup Files.

When you run the CC-SG backup as a task, select Automatic Delete when Maximum Reached to automatically delete the oldest backup file when the maximum number of backup files is reached. This setting is only available when creating a Backup CC-SG task. When a backup file is deleted as part of the backup CC-SG task, the audit log will contain an entry for each file deleted. See Schedule a Task.

To backup CC-SG:

1. Choose System Maintenance > Backup.
2. Type a name for this backup in the Backup Name field.
3. Type a description for the backup in the Description field. **Optional.**
4. Select a Backup Type: Full or Standard. See ***What is the difference between Full backup and Standard backup?*** (on page 4)
5. If you are setting this backup as a task from the Administration > Tasks page, select the Automatic Delete When Maximum Reached checkbox to allow CC-SG to delete the oldest backup file in storage locally when the maximum number of files is reached. Set the maximum number in the Maximum Backup Files field. The default number is 50 backup files. **Optional.**
6. To save a copy of this backup file to an external server, select the Backup to Remote Location checkbox. **Optional.**
   a. Select a Protocol used to connect to the remote server, either FTP or SFTP
   b. Type the IP address or hostname of the server in the IP Address/Hostname field. IPV6 is supported.
   c. If you are not using the default port for the selected Protocol (FTP: 21, SFTP: 22), type the Communications port used in the Port Number field.
   d. Type a username for the remote server in the Username field.
   e. Type a password for the remote server in the Password field.
   f. In the Directory (Relative Path) field, specify the location to save the backup file on the FTP server.
      - Leave this field blank to save the backup file to the default home directory on the FTP server.
      - Enter a path relative to the default home directory to save the backup file in a level below the default home directory on the FTP server. For example, to save the backup file in a folder called "Backups" under the default home directory, enter `Backups` in the Directory (Relative Path) field.
   g. In the "Filename (leave blank to use the default filename convention)" field, type a filename for naming the backup on the remote server, or leave blank to

accept the default name. The default name includes "backup" with a date and time.

h. Click Save As Default if you want to save current remote server settings as default values. A confirmation message appears. Click OK. **Optional.**

7. Click OK.

   A message appears when the backup completes. The backup file is saved in the CC-SG file system, and if specified in the Backup to Remote Location field, to a remote server as well. This backup can be restored at a later time. See Restoring CC-SG.

Important: The Neighborhood configuration is included in the CC-SG backup file so make sure you remember or note down its setting at the backup time. This is helpful for determining whether the backup file is appropriate for the CC-SG unit you restore.

What is the difference between Full backup and Standard backup?

Standard backup:

A standard backup includes all data in all fields of all CCSG pages, except for data in the following pages:

- Administration > Configuration Manager > Network tab
- Administration > Cluster Configuration

CCSG backup files stored on CCSG are also not backed up. You can view the list of backup files stored on CCSG in the System Maintenance > Restore page.

Standard backup also excludes other temporary data in fields, such as date ranges in Report pages.

Full backup:

A Full backup includes everything in the Standard backup, and also backs up the CC-SG firmware files, device firmware files, application files, and logs. Application files include AKC, VKC, RSC, and VNC.

Save a Backup File

1. Choose System Maintenance > Restore Command Center.
2. In the Available Backups table, select the backup you want to save to your PC.
3. Click Save to File. A Save dialog appears.
4. Type a name for the file and choose the location where you want to save it.
5. Click Save to copy the backup file to the specified location.