CC-SG 14.0.0 Upgrade Guide

This guide outlines the supported upgrade paths to CC-SG release 14.0.0. See: Upgrade Path (on page 8)

Note: Release 12.0 serves as the required fence release before upgrading to 14.0.

Are you upgrading from an earlier release? Go to www.raritan.com/support and download special instructions for your upgrade.

Upgrade Requirements:

► *Hardware Appliance Models:*

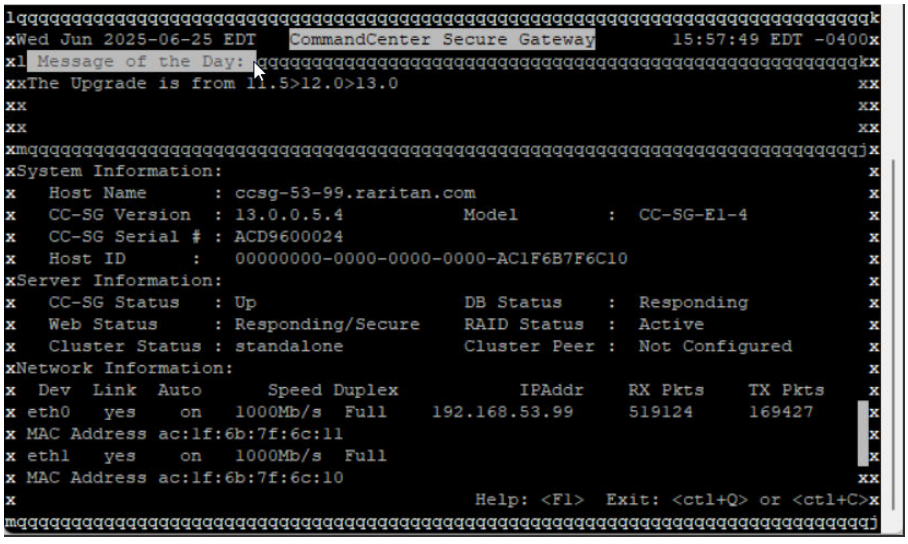
- E1-4
- E1-5

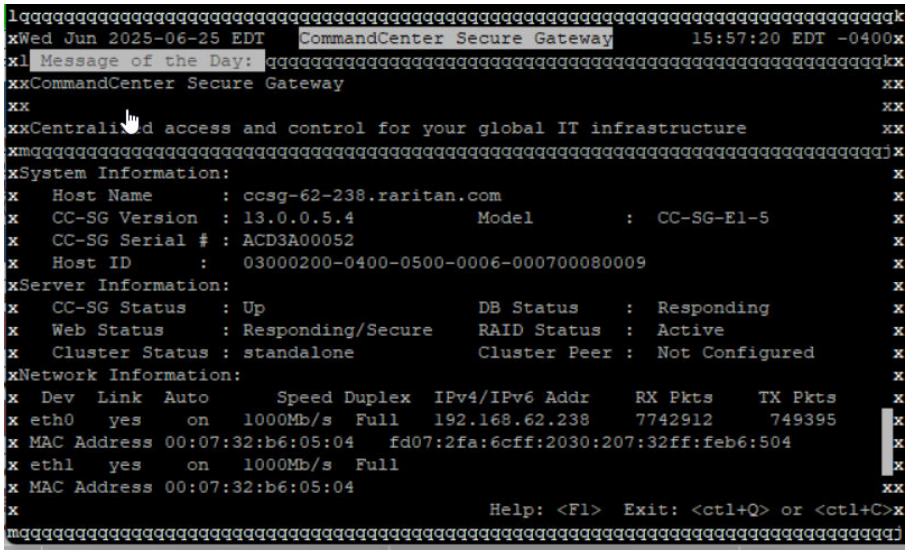
► *Virtual Appliances:*

- Requires at least 4GB of RAM
- Requires a second hard disk

E1 Model Support

1. Access the CC-SG diagnostic console over SSH port 23.
2. Login as "status", no password required.
3. Look for Model in the System Information section.





Verify RAM before Upgrade

CC-SG 14.0.0 requires at least 4GB of RAM. Verify recommended 4GB of RAM before upgrade or the upgrade will fail.

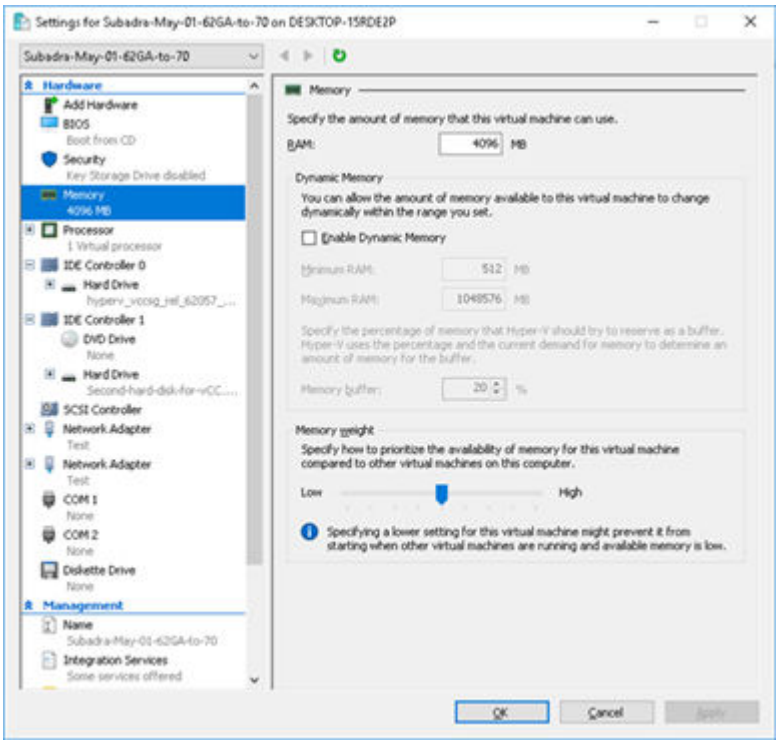
Before proceeding, power OFF the CC-SG from the Diagnostic Console: Choose Operation> CC-SG System Power Off.

► *VMware:*

- CC-SG virtual machines on VMware recommended at least 4GB of RAM in previous releases. Confirm the virtual machine settings before upgrade.

► *Hyper-V:*

- Hyper-V: In Hyper-V Manager, open the CC-SG virtual machine settings. Go to the Memory tab. Increase RAM to at least 4096MB. Click OK.



► *Physical Appliances:*

Adding RAM to physical appliances is not supported. If your model does not have enough RAM, upgrade will fail, and a support message will display with instructions if your appliance cannot be supported.

Virtual Appliances

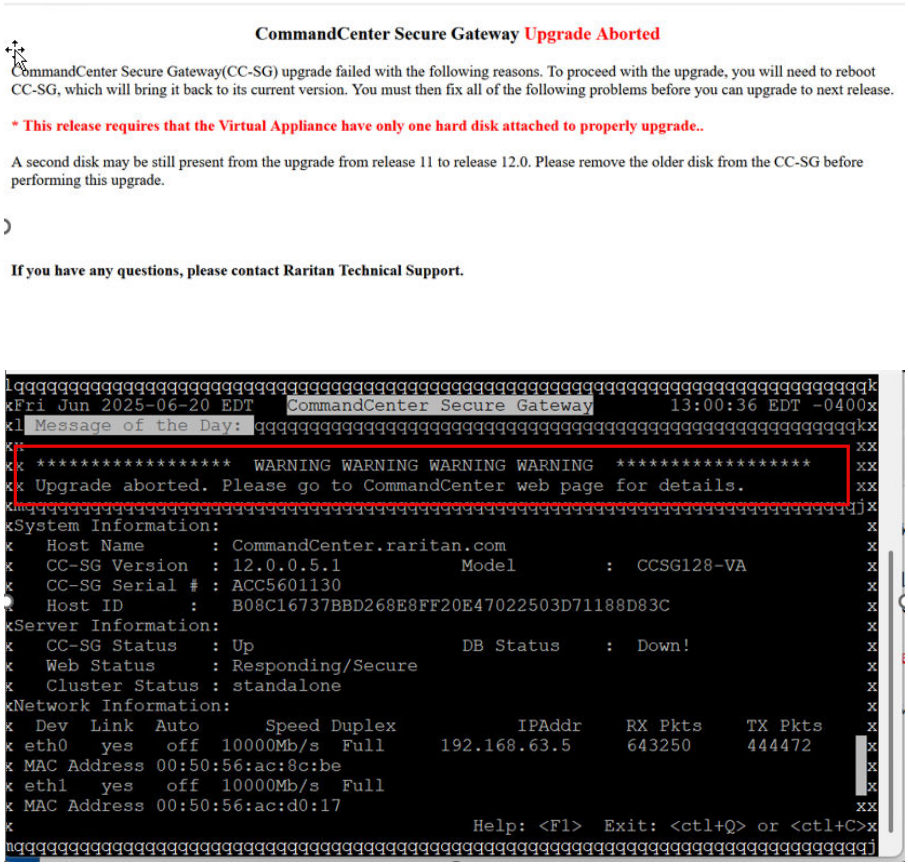
Remove the Second Hard Disk

Important: Ensure to have a current backup of your virtual machine before making any changes.

If you are upgrading to Release 12.0 with CC-SG virtual appliances upgraded from previous releases (11.0 or 11.5) may have two hard drives as a result of the prior 12.0 upgrade. Before upgrading to 14.0, a hard drive (Disk 1) must be removed.

During the upgrade to CC-SG 14.0.0, the process will abort if more than one hard disk is detected, as this release requires a single-disk configuration.

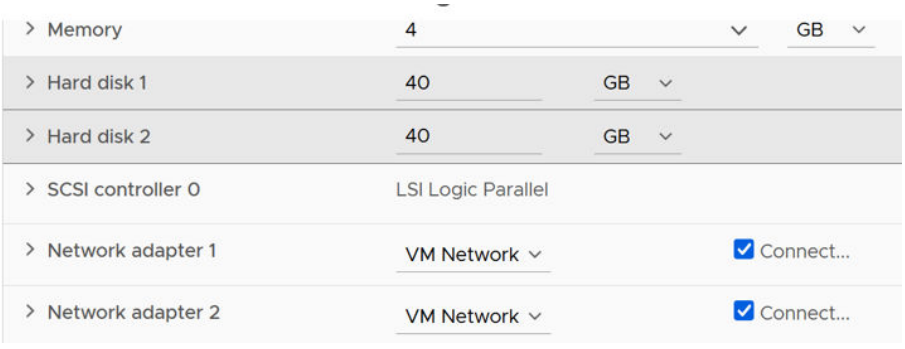
Note: Previous versions of the virtual appliance were configured with two hard disks.

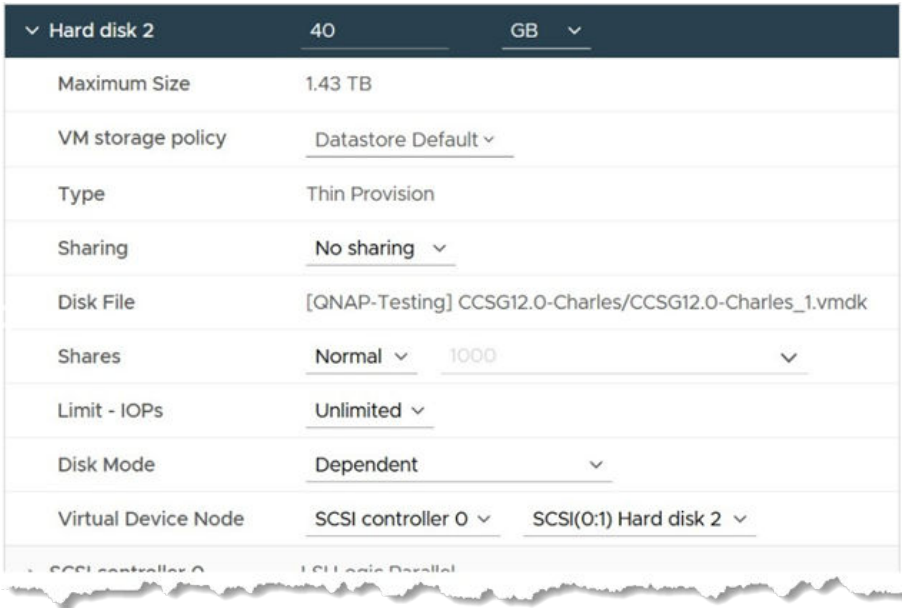


To regain access reboot the CC-SG to restore it to the currently installed version.

► *VMWare Environment:*

1. Power on the CC-SG virtual machine from vCenter.
2. Select VM and right click Edit Settings.

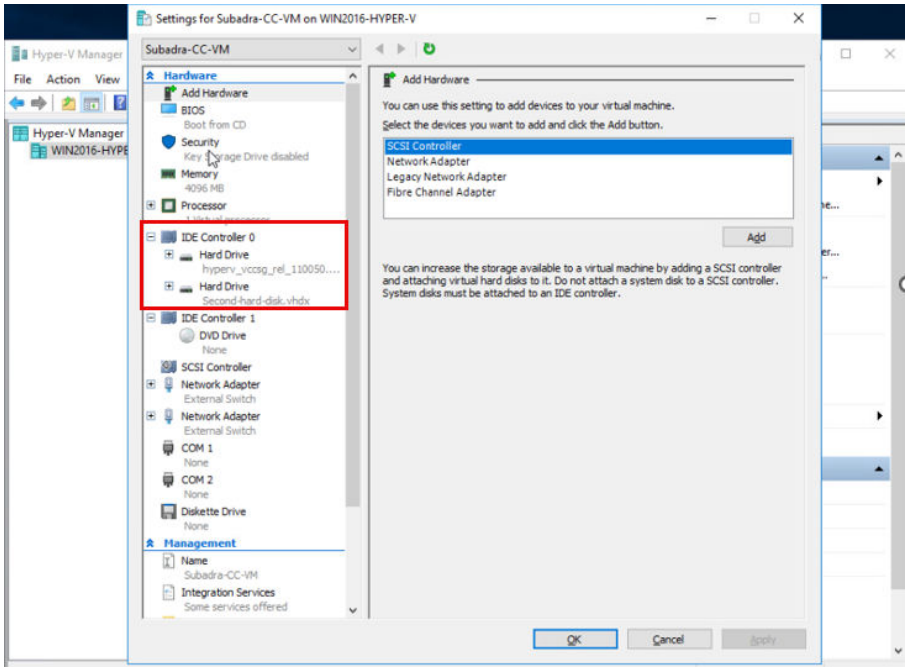




3. Remove Hard Disk 1, which is configured as SCSI (0:0).
4. Power on the VM.
5. Upgrade the CC-SG VM with 14.0.0 firmware version.

► *Hyper-V Environment:*

1. Power off the Hyper-V VM, and go the Settings.
2. Under IDE Controller 0, remove the disk labeled with the older release (e.g., 11_110050) assigned to (0:0).



3. Power on the VM.
4. Upgrade the CC-SG VM with 14.0.0 firmware version.

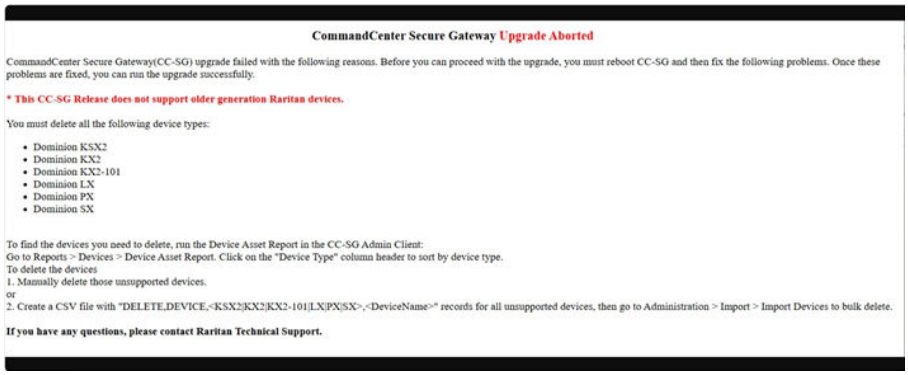
Remove Unsupported Raritan Devices

CC-SG 14.0 no longer supports legacy Raritan End-of-Life (EOL) devices.

The following devices must be deleted prior to upgrading from CC 12.0 or CC 13.0 to CC 14.0 GA:

- Dominion KX2
- Dominion KSX2
- Dominion SX
- Dominion LX
- Dominion KX2-101
- Dominion PX

If any of these devices are still added in CC-SG during the upgrade process, the upgrade will stop. Abort message will appear with a list of the required corrections. Users must remove these devices before proceeding with the upgrade.



CommandCenter Secure Gateway Upgrade Aborted

CommandCenter Secure Gateway(CC-SG) upgrade failed with the following reasons. Before you can proceed with the upgrade, you must reboot CC-SG and then fix the following problems. Once these problems are fixed, you can run the upgrade successfully.

*** This CC-SG Release does not support older generation Raritan devices.**

You must delete all the following device types:

- Dominion KSX2
- Dominion KX2
- Dominion KX2-101
- Dominion LX
- Dominion PX
- Dominion SX

To find the devices you need to delete, run the Device Asset Report in the CC-SG Admin Client:
Go to Reports > Devices > Device Asset Report. Click on the "Device Type" column header to sort by device type.
To delete the devices
1. Manually delete those unsupported devices.
or
2. Create a CSV file with "DELETE,DEVICE,<KSX2|KX2|KX2-101|LX|PX|SX>,<DeviceName>" records for all unsupported devices, then go to Administration > Import > Import Devices to bulk delete.

If you have any questions, please contact Raritan Technical Support.

Upgrading CC-SG

You can find firmware files in the Support section of the Raritan website.

Warning: Before upgrading, check the firmware Release Notes for the latest information on your specific upgrade path.

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

You should back up CC-SG before upgrading, and save the backup files to a different location for safe keeping. See Backing Up CC-SG (on page 9) and Save a Backup File (on page 11).

You should check CC-SG's disk status before upgrading. See Check Disk Status (on page 9). 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 in the Online Help.

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. You must use the greater firmware version than the current version to upgrade.
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 in the Online Help.
   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.

Upgrade Path

Note: Releases 11.0 and 11.5 can be upgraded directly to Release 12.0, which serves as the mandatory fence release prior to upgrading to Release 14.0.

Supported Upgrade Paths:

- From Release 13.0 → 14.0
- From Release 12.0 → 14.0
- From Release 11.5 → 12.0 → 14.0
- From Release 11.0 → 12.0 → 14.0
- From Release 11.0 → 11.5 → 12.0 → 14.0
- From Release 9.x or 10.0 → 11.0 → 12.0 → 14.0
- From Release 7.0 or 8.0 → 9.0 → 11.0 → 12.0 → 14.0
- From Release 6.x → 7.0 → 9.0 → 11.0 → 12.0 → 14.0

Always check the Support page for the release for any special upgrade guides and to see the latest updates from Raritan Tech Support.

Related Information

Clear the Browser's Cache

These instructions may vary slightly for different browser versions.

► *In FireFox:*

Clear Cache of FireFox Browser

► *In Edge:*

Clear Cache of Edge Browser

► *In Chrome:*

Clear Cache of Chrome Browser

Clear the Java Cache

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

► *In Windows:*

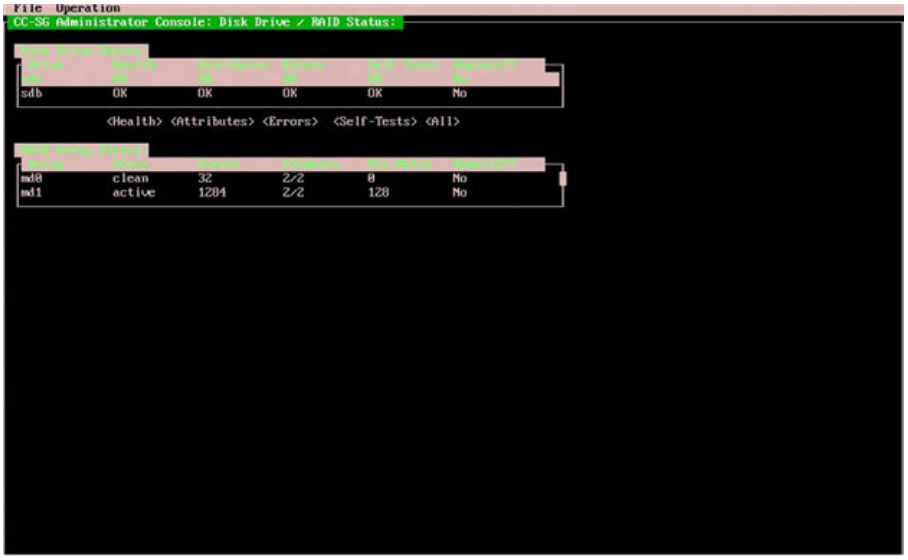
1. Choose Control Panel > Java.
2. On the General tab, click Settings.
3. In the dialog box that opens, click Delete Files.
4. Make sure the Applications and Applets checkbox is selected then click OK.

Check Disk Status

Before starting a CC-SG firmware upgrade, verify the CC-SG disk status.

► *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.

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.

Warning:Backups generated from pre versions of CC-SG cannot be restored to current version of CC-SG.

► *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 Full Backup vs Standard Backup (on page 11)
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. For the FTP protocol select either Active or Passive FTP Transfer Mode.
   b. Type the IP address or hostname of the server in the IP Address/Hostname field. IPV6 is supported. You should set FTP server for the chosen mode to save backups successfully by CC-SG.
   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.

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.

Full Backup vs Standard Backup

► *Standard backup:*

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

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

CC-SG backup files stored on CC-SG are also not backed up. You can view the list of backup files stored on CC-SG 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, Logs, CC-SG files and Licenses.

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.