

CC-SG Virtual Appliance Evaluation

This Quick Setup Guide explains how to install and configure the CommandCenter Secure Gateway. CommandCenter Secure Gateway is Raritan's management software platform engineered to consolidate secure access and control of IT devices.

For details on using the CommandCenter Secure Gateway, access online help from the application or the *Support page* <http://www.raritan.com/support> on the Raritan website. Online help is your primary resource but a PDF version of the help is also available on the Support page.

Evaluation Version Limitations

The virtual evaluation version of CommandCenter Secure Gateway provides full functionality, with several exceptions:

- Limit of 16 nodes.
- Limit of 1 NIC. IP Isolation Mode and IP Failover Mode not supported.
- WS-API not supported.
- Clusters, Neighborhoods, and Upgrades not supported.

Prerequisites

The CC-SG virtual appliance evaluation can be installed on either the free VMware Player, or on ESXi.

- ▶ **For both VMware Player and ESXi installations, you need:**
 - 10GB datastore
 - 4GB free memory
- ▶ **To install on VMware Player, you need:**
 - VMware Player 14.0.
 - Available for free download from VMware's website, www.vmware.com
 - CommandCenter Secure Gateway Virtual Appliance Evaluation zipped .VMX file downloaded to local client.
 - Available for free download from Raritan's website.
 - Go to <http://www.raritan.com/support/commandcenter-secure-gateway/> and click the CC-SG Virtual Appliance Evaluation link, then download the version for VMware Player. Registration may be required.
- ▶ **To install on VMware ESX or ESXi, you need:**
 - VMware ESXi 5.5, 6.0, or 6.5.
 - CommandCenter Secure Gateway Virtual Appliance Evaluation zipped .OVF file downloaded to local client
 - Available for free download from Raritan's website.
 - Go to <http://www.raritan.com/support/commandcenter-secure-gateway/> and click the CC-SG Virtual Appliance Evaluation link, then download the version for ESXi. Registration may be required.

Install the Virtual Appliance Evaluation on VMware® Player

1. Unzip the Virtual Appliance Evaluation file you downloaded from www.raritan.com. The `vccsg_eval_<release number>.VMX` file is included in the .ZIP.
2. Log in to VMware Player.
3. Click Open a Virtual Machine.
4. Locate the `vccsg_eval_<release number>.VMX` file and select it. Click Open.
5. The virtual machine displays in the library. Click "Play virtual machine".
6. A message displays. Select "I copied it" then click OK.
7. You may see a message about adding removable media to the virtual machine. Click OK.
8. Click Remind Me Later in the message about installing VMware Tools.
9. Wait several minutes while the virtual appliance starts. The local console opens. See *Log in to Diagnostic Console to Set CC-SG IP Address* (on page 2) for next steps.

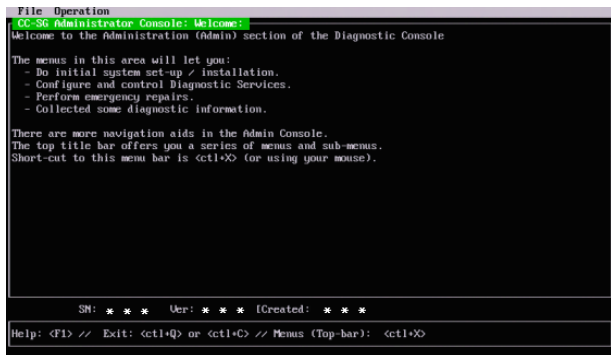
Install the Virtual Appliance Evaluation on VMware ESXi

1. Unzip the Virtual Appliance Evaluation file you downloaded from www.raritan.com. The `vccsg_eval_<release number>.OVF` file is included in the .ZIP.
2. Connect to the ESXi from your client computer using vSphere.
3. Log in as a user that has permission to create, start, and stop virtual machines.
4. Choose File > Deploy OVF Template.
5. Select Deploy From File then click Browse to go to the directory where you unzipped the files.
6. Select the .OVF file. Click Next.
7. Details about the virtual machine display. You can change the default name of the virtual machine. Click Next.
8. Select the inventory location. Click Next.
9. Select the Host where you want to deploy the CommandCenter Secure Gateway. Click Next.

10. If you selected a cluster, select the specific host. Click Next.
11. Choose the datastore where all files will be stored. Make sure the datastore has 10GB free. Select thin provisioned if the datastore supports it. Click Next.
12. Choose the network your CC-SG is being deployed on. Click Next.
13. View the summary then click Finish. Wait several minutes while the virtual machine is created.
14. Power on the virtual machine.
15. Open the Console tab to access the Diagnostic Console of CC-SG. See *Log in to Diagnostic Console to Set CC-SG IP Address* (on page 2) for next steps.

Log in to Diagnostic Console to Set CC-SG IP Address

1. Log in as *admin/raritan*. Usernames and passwords are case-sensitive.
2. You will be prompted to change the local console password.
 - a. Type the default password (*raritan*) again.
 - b. Type and then confirm the new password.
3. Press CTRL+X when you see the Welcome screen.



4. Choose Operation > Network Interfaces > Network Interface Config. The Administrator Console appears.
5. In the Configuration field, select DHCP or Static. If you select Static, type a static IP address. If needed, specify DNS servers, netmask, and gateway address.
6. Select Save.

Default CC-SG Settings

IP Address: 192.168.0.192

Subnet Mask: 255.255.255.0

Username/Password: admin/raritan

Reboot the System After a DHCP Configuration

If you configured the CC-SG to use DHCP, you must reboot the system.

- In the local console, choose Operation > Admin > CC-SG System Reboot.

Log in to CC-SG

Once CC-SG has restarted, you can log in to CC-SG from a remote client.

1. Launch a supported browser and type the URL of the CC-SG: <https://<IP address>/admin>.
For example, <https://192.168.0.192/admin>.

Note: The default setting for browser connections is HTTPS/SSL encrypted.

2. When the security alert window appears, accept the connection.
3. You will be warned if you are using an unsupported Java Runtime Environment version. Follow the prompts to either download the correct version, or continue. The Login window appears.
4. Type the default username (*admin*) and password (*raritan*) and click Login.

The CC-SG Admin Client opens. You are prompted to change your password. Strong passwords are enforced for *admin*.

Next Steps

See the CommandCenter Secure Gateway online help at <https://www.raritan.com/support/product/commandcenter-secure-gateway>.

Additional Information

For more information about CommandCenter Secure Gateway and the entire Raritan product line, see Raritan's website (www.raritan.com). For technical issues, contact Raritan Technical Support. See the Contact Support page in the Support section on Raritan's website for technical support contact information worldwide.

Raritan's products use code licensed under the GPL and LGPL. You can request a copy of the open source code. For details, see the Open Source Software Statement at (<http://www.raritan.com/about/legal-statements/open-source-software-statement/>) on Raritan's website.