

CC-SG Virtual Appliance Evaluation

Quick Setup Guide for Virtual CC-SG 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 additional information on any aspect of the CommandCenter Secure Gateway, see the accompanying online help accessed from the CommandCenter Secure Gateway or from the CommandCenter Secure Gateway User Guide, which can be downloaded from the Firmware and Documentation section of Raritan's website (<http://www.raritan.com/support/firmware-and-documentation/>).

Evaluation Version Limitations

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

- Limit of 16 nodes.
- WS-API not supported.
- Clusters, Neighborhoods, and Upgrades not supported.

Prerequisites

- VMware Player 3.1 installed on a Windows 7 client
 - Available for free download from VMware's website, www.vmware.com
- CommandCenter Secure Gateway Virtual Appliance Evaluation .ZIP file downloaded to local client
 - Available for free download from Raritan's website, www.raritan.com

Install the Virtual Appliance Evaluation on VMware® Player

1. Unzip the Virtual Appliance Evaluation .ZIP file you downloaded from www.raritan.com.
2. Log in to VMware Player 3.1.
3. Choose File > 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.

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. The new password must be a strong password consisting of at least eight characters that are a combination of letters and numbers.
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. Wait a few minutes as CC-SG restarts.

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.

Next Steps

See the CommandCenter Secure Gateway Deployment Guide for information on deploying other Raritan devices for CC-SG management.

See the CommandCenter Secure Gateway Administrator Guide for information on configuring CC-SG.

Additional Information

For more information about the 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 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.