CC-SG Cloud Appliance Evaluation

Quick Setup Guide

This Quick Setup Guide explains how to install and configure the CommandCenter Secure Gateway cloud appliance for evaluation. CommandCenter Secure Gateway is Raritan's management software platform engineered to consolidate secure access and control of IT devices. Access the online help from the application or the Support page on the Raritan website.

Evaluation Version Limitations

The 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.
- Clusters, Neighborhoods, and Upgrades not supported.

Supported Cloud Services

- Amazon Web Services (AWS)
- Microsoft Azure Cloud (Azure)

Installing Cloud CC-SG Evaluation on AWS

1. Go to https://www.raritan.com/landing/free-ccsg-download to register, then download the evaluation .ZIP file for AWS.
2. Extract the .VHD file from the .ZIP.
3. Upload the .VHD file into your AWS storage.
4. Using either the AWS Image Builder service or the API, create/import an Amazon Machine Image with the uploaded VHD file.
5. Launch an instance from the image, and then select an instance type that supports at least 2 CPUs and 4G RAM, such as t2.medium or t2.large.
6. Set the network interface to use DHCP.
7. Edit the VM security group to allow all ports used by CC-SG. Go to https://help.raritan.com/ccsg/v13.0/en/#1999.htm for details on open ports.

8. Start the VM, then go to the VM profile to find the IP address for the cloud CC-SG evaluation.

Installing Cloud CC-SG Evaluation on Azure

1. Go to https://www.raritan.com/landing/free-ccsg-download to register, then download the evaluation .ZIP file for Azure.
2. Extract the .VHD file from the .ZIP.
3. Upload the .VHD file into your Azure storage.
4. Using either the Azure portal or Azure PowerShell command to create an image with the uploaded VHD file.
5. Create a new VM with the image, and then select a size that supports at least 2 CPUs and 4G RAM, such as Standard_B2s.
6. Set the network interface to use DHCP.
7. Edit the network security group to allow all ports used by CC-SG. Go to https://help.raritan.com/ccsg/v13.0/en/#1999.htm for details on open ports.

8. Start the VM, then go to the VM profile to find the IP address for the cloud CC-SG evaluation.

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.

Note: The client version is visible on the login page.

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

After evaluating , you can create a backup file of your test configuration and restore it to a full-version CC-SG.

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 (https://www.raritan.com/about/legal-statements/open-source-software-statement/) on Raritan's website.