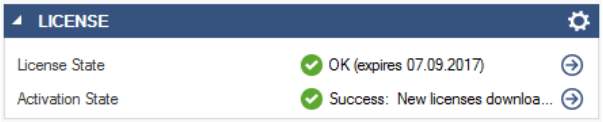
Getting Started - Control Center for AWS

https://campus.barracuda.com/doc/73719436/

The Barracuda Firewall Control Center for AWS is available as a Bring Your Own License (BYOL) image from the AWS Marketplace. Two models are available. The VCC610 supports two ranges and unlimited clusters, the VCC400 one range and one cluster. The Control Center can manage both on-premises hardware and virtual firewalls, as well as CloudGen Firewalls in the public cloud. It is not possible to use the AWS Control Center in a high availability cluster.

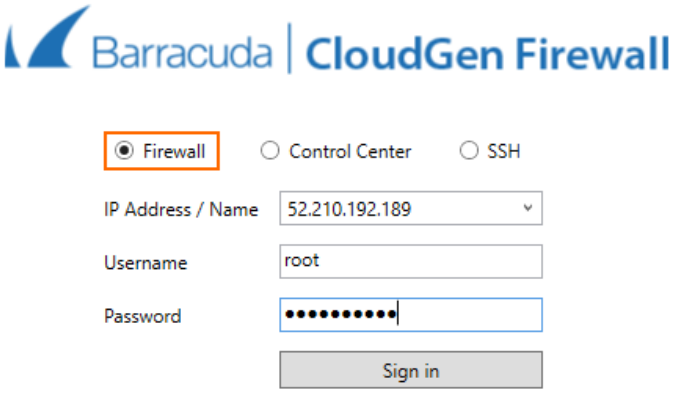
Before You Begin

- Deploy the Barracuda Firewall Control Center for AWS image from the Marketplace. For more information, see Amazon AWS Deployment.
- Verify that you are not blocking TCP 807 and TCP 806, as these ports are required for management access to the Control Center.
- Open TCP 692 for remote management tunnels if CloudGen Firewalls, which are not in the same VPC, are managed by the Control Center.
- Activate the license on the box layer of the Control Center. For more information, see How to Activate and License a Stand-alone Virtual or Public Cloud Firewall or Control Center.

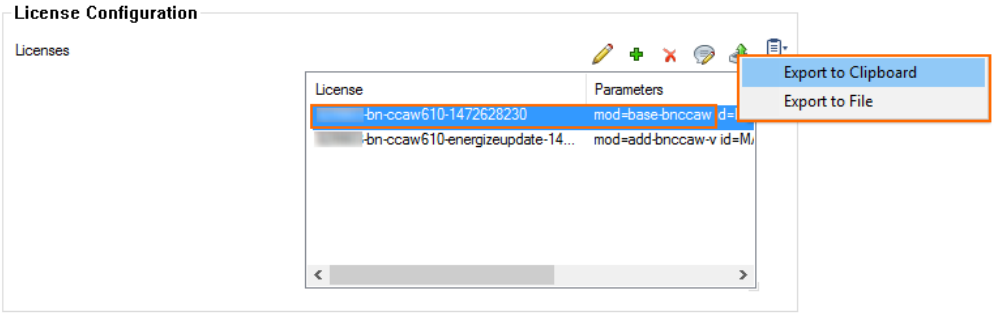


Step 1. Export the Base License on Box Layer

1. Log into the box layer of the Control Center.
   - **IP Address/ Name** – Enter the public IP address, or if connected to the VPC via client-to-site, the private IP address associated with the Control Center.
   - **Username** – Enter `root`.
   - **Password** – Enter the instance ID of the Control Center instance.



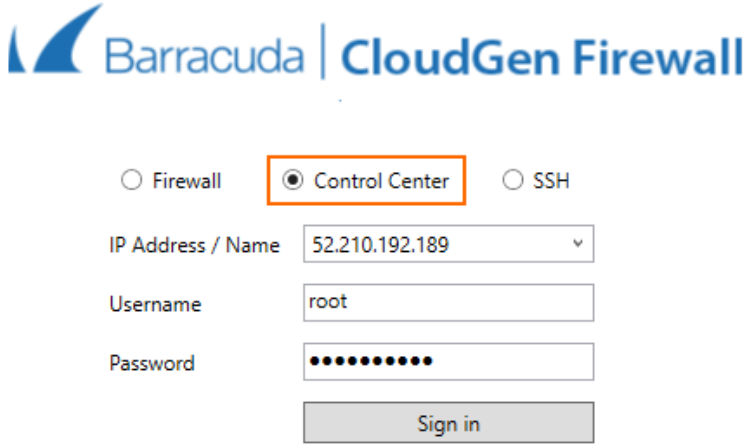
2. Open the **CONFIGURATION > Configuration Tree > Box > Box Licenses** page.
3. Click **Lock**.
4. In the **Licenses** table, select the **Base License**. Then, click **Im/ Export** and select **Export to Clipboard** or **Export to File**.



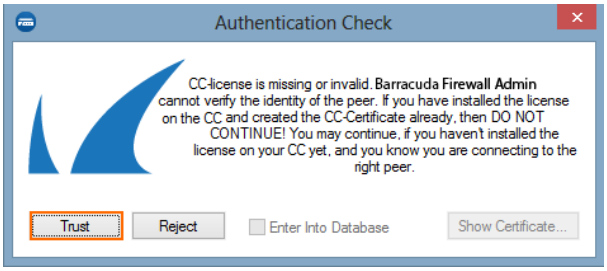
Step 2. Configure CC Identification Settings

The **CC Identification** settings are required to secure communication between the Control Center and the CloudGen Firewalls it manages.

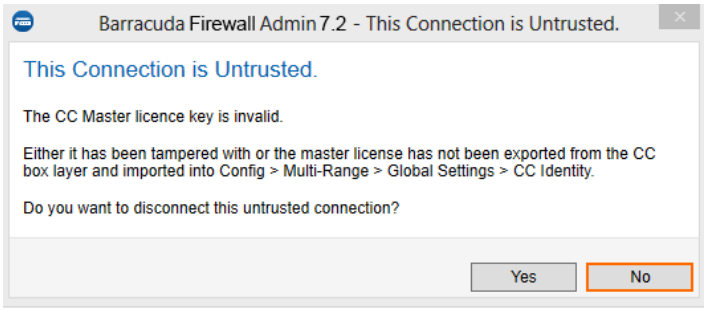
1. Log into the Control Center layer.



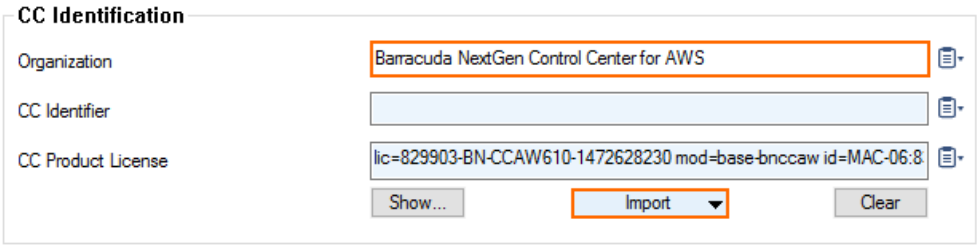
2. Click **Trust**.



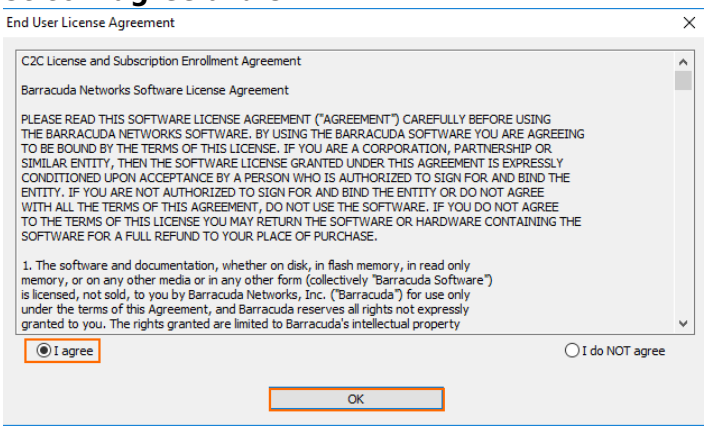
3. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > CC Identity**. The **This Connection is Untrusted** pop-up opens.
4. Click **No**.



5. Click **Lock**.
6. In the **Organization** field, enter your organization name.



7. In the **CC Identification** section, click **Import** and select either **Import from Clipboard** or **Import from File** to import the base license exported in Step 3. The **Certificate View** window opens.
8. Click **OK**. The **End User License Agreement** window opens.
9. Select **I agree** and **OK**.



10. In the left menu, click **Trust Chain**.
11. Define the keys and certificates required for secure communication between the Control Center and the CloudGen Firewalls that it will manage:
    - **CC Private Key –** Click **New Key** and specify the key length.
    - **CC Certificate –** Click **Edit** and specify the certificate settings.
    - **CC SSH Key –** Click **New Key**.
12. Click **Send Changes** and **Activate**.

Step 3. (optional) Complete the Auto-Activation Form

To automatically activate managed firewall licenses, you must enter the data for the auto-activation

form once.

1. Log into the Control Center layer.
2. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > CC Parameters**.
3. In the left menu, select **Activation Template**.
4. Click **Lock**.
5. Enter the **Owner** and **Purchase Information**.
6. Click **Send Changes** and **Activate**.

Next Steps

Continue with the steps below to set up the Control Center in AWS according to your needs.

	Link
Create Admins	Control Center Admins
Configure Central Management	• Central Management • How to Manage Ranges and Clusters
Add Managed CloudGen Firewalls	• How to Configure a Remote Management Tunnel for a CloudGen Firewall • How to Import an Existing CloudGen Firewall into a Control Center
License Managed CloudGen Firewalls	• How to Assign and Activate Single Licenses on a Control Center • How to Install and Assign Pool Licenses on a Control Center
Revision Control System (RCS)	Revision Control System (RCS)

Figures

1. awscc_01.png
2. awscc_06.png
3. awscc_02.png
4. awscc_05.png
5. azure_cc_021.png
6. azure_cc_031.png
7. awscc_04.png
8. awscc_03.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.