

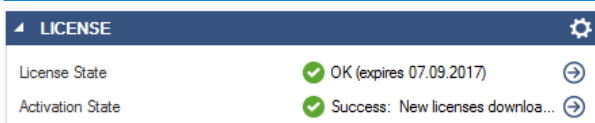
Getting Started - Control Center for Google Cloud

<https://campus.barracuda.com/doc/73719940/>

The Barracuda Firewall Control Center for Google Cloud is available as a Bring Your Own License (BYOL) image from Google Launcher. 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 Control Center in a high availability cluster.

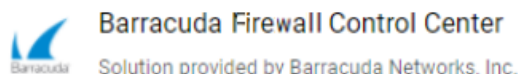
Before You Begin

- Deploy the Firewall Control Center for Google Cloud image from Google Launcher or by uploading the image. For more information, see [Google Cloud Platform Deployment](#) or <https://console.cloud.google.com/launcher/partners/barracuda-release>.
- Google Launcher automatically opens ports TCP 807, TCP 806 and TCP 692 for management traffic and remote management tunnel access to 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. The temporary root password for the Control Center instance is displayed on the post-install page:



Admin user	root
Admin password (Temporary)	qi7H6R-E
Management IP	10.138.20.108
Instance	firewall

2. Log into the box layer of the Control Center.
 - **IP Address/ Name** - Enter the public IP address. If connected to the VPC via client-to-site, you can also enter the private IP address that is associated with the Control Center.
 - **Username** - Enter root.
 - **Password** - Enter the temporary **Admin password** listed on the post-install page after deploying the Control Center via Google Launcher.



Firewall
 Control Center
 SSH

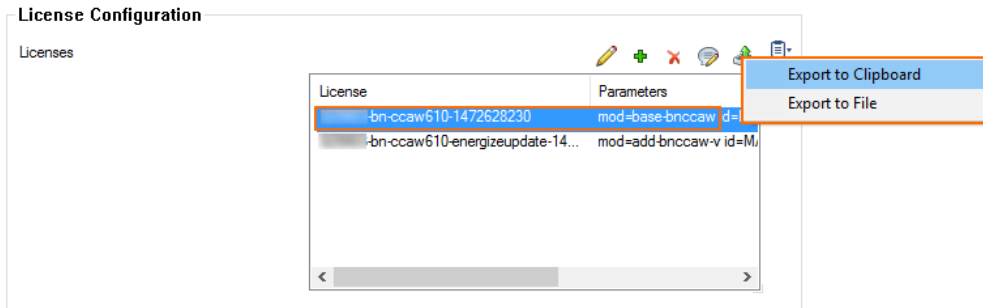
IP Address / Name: 52.210.192.189

Username: root

Password: [masked]

Sign in

- Open **CONFIGURATION > Configuration Tree > Box > Box Licenses**.
- Click **Lock**.
- 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.

- Log into the Control Center layer.



Firewall
 Control Center
 SSH

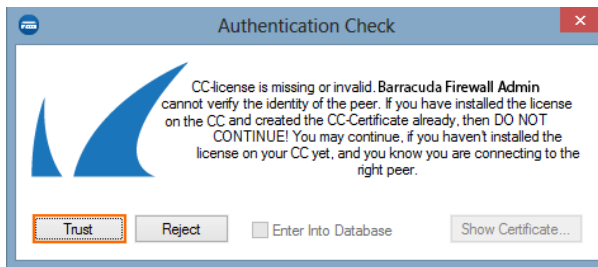
IP Address / Name: 52.210.192.189

Username: root

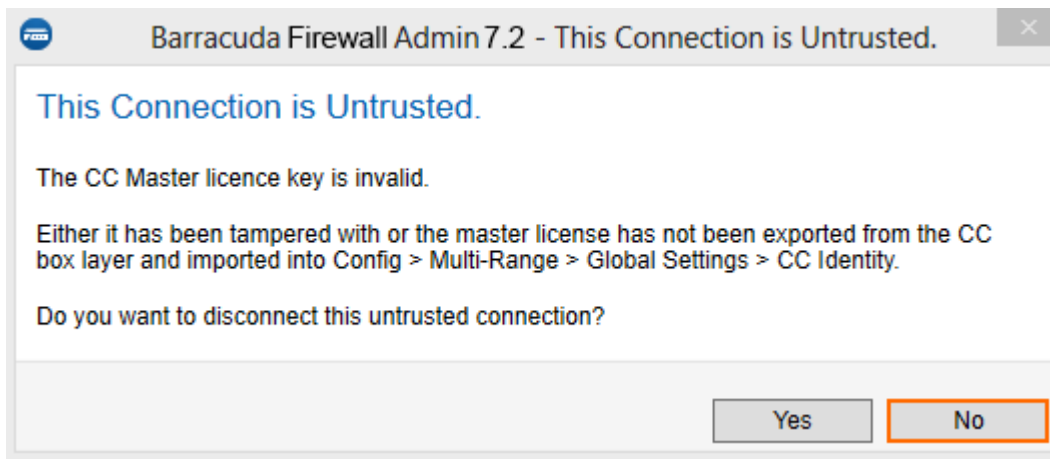
Password: [masked]

Sign in

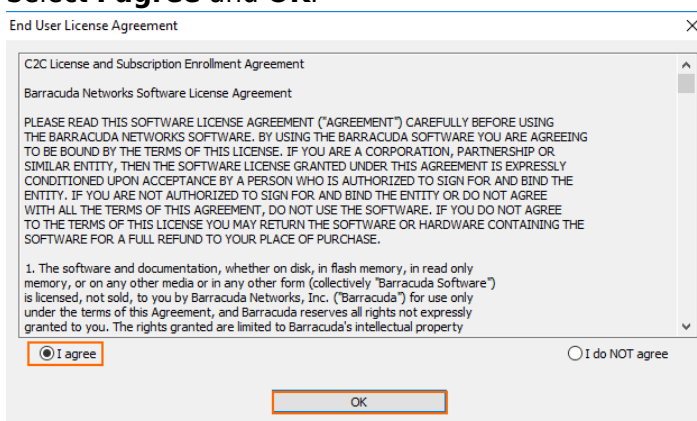
- Click **Trust**.



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 **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 Google Cloud according to your needs.

	Link
Create Admins	Control Center Admins
Configure Central Management	<ul style="list-style-type: none"> • Central Management • How to Manage Ranges and Clusters
Add Managed CloudGen Firewalls	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. awscs_01.png
2. default_pwd_NGCC_google1.png
3. awscs_06.png
4. awscs_02.png
5. awscs_05.png
6. azure_cc_021.png
7. azure_cc_031.png
8. awscs_03.png

© Barracuda Networks Inc., 2019 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.