How to Grant SSH Support Access

https://campus.barracuda.com/doc/94540420/

In certain cases, you may have to grant SSH access to the Barracuda CloudGen WAN site appliance and/or the Barracuda CloudGen WAN gateway. Barracuda Networks Technical Support access via SSH is granted for 24 hours.

Before You Begin

- The public IP address of the site must be directly reachable.
- The Access Control list cannot be 0.0.0.0/0 and the maximum netmask can be up to a /30 network.
- The access is granted for two hours and can be renewed for another two hours starting from the moment the access has been renewed.
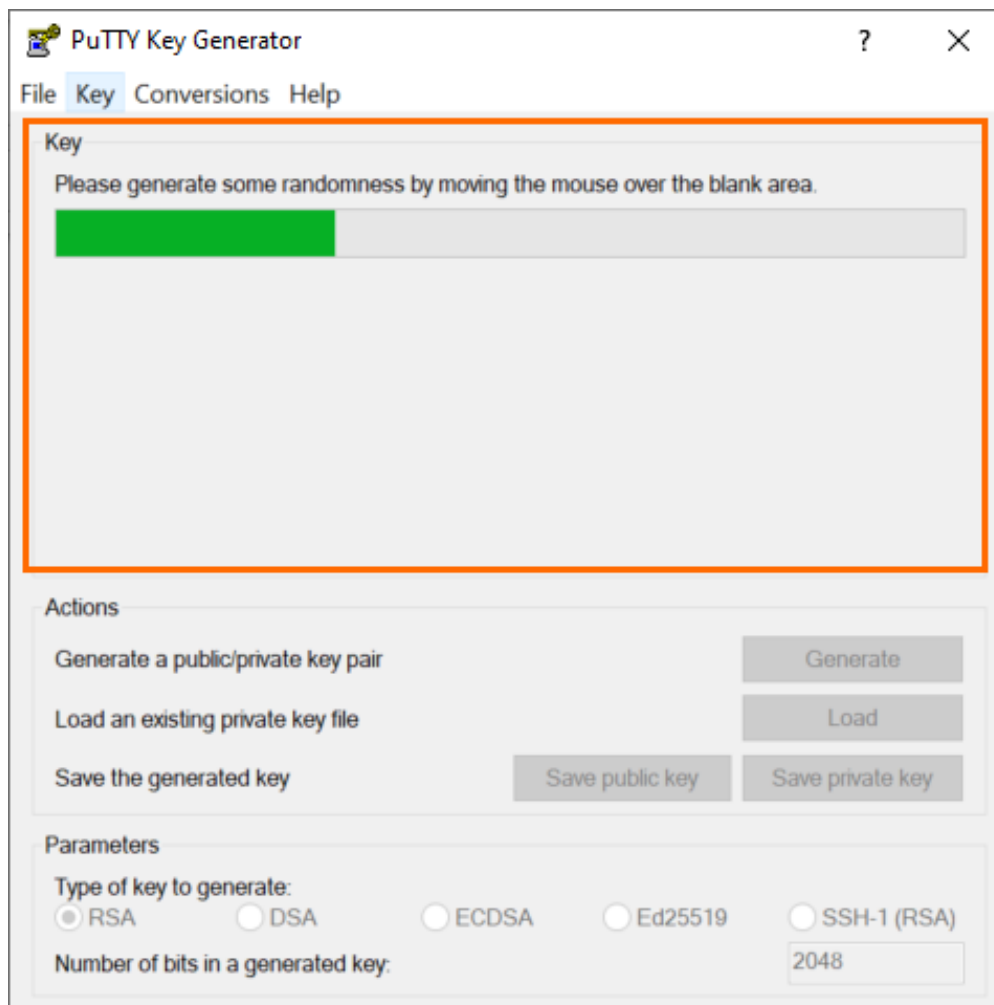
(Optional) Step 1. Create an SSH Key

In certain cases, you might have to create an SSH key yourself. However, in most cases, you can also use the key provided by Barracuda Networks Support.
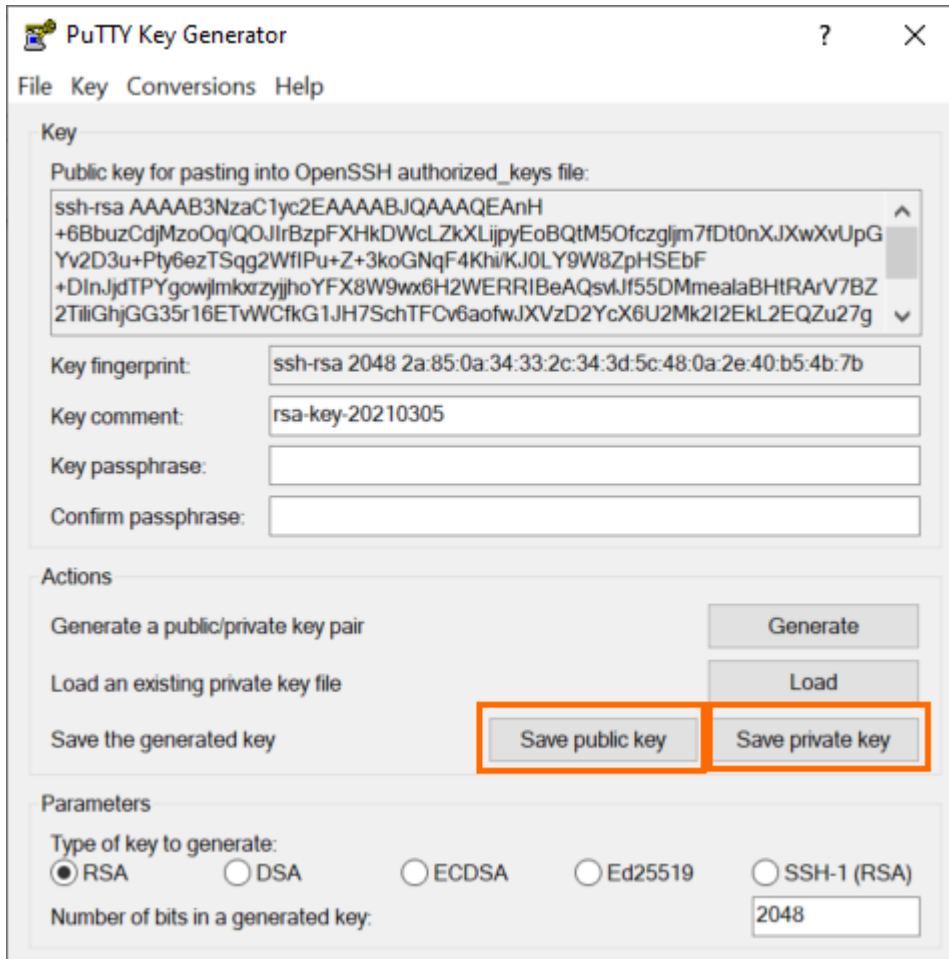
1. Download and install PuTTYgen from https://www.putty.org/.
2. Open PuTTYgen.
3. Click **Generate**.
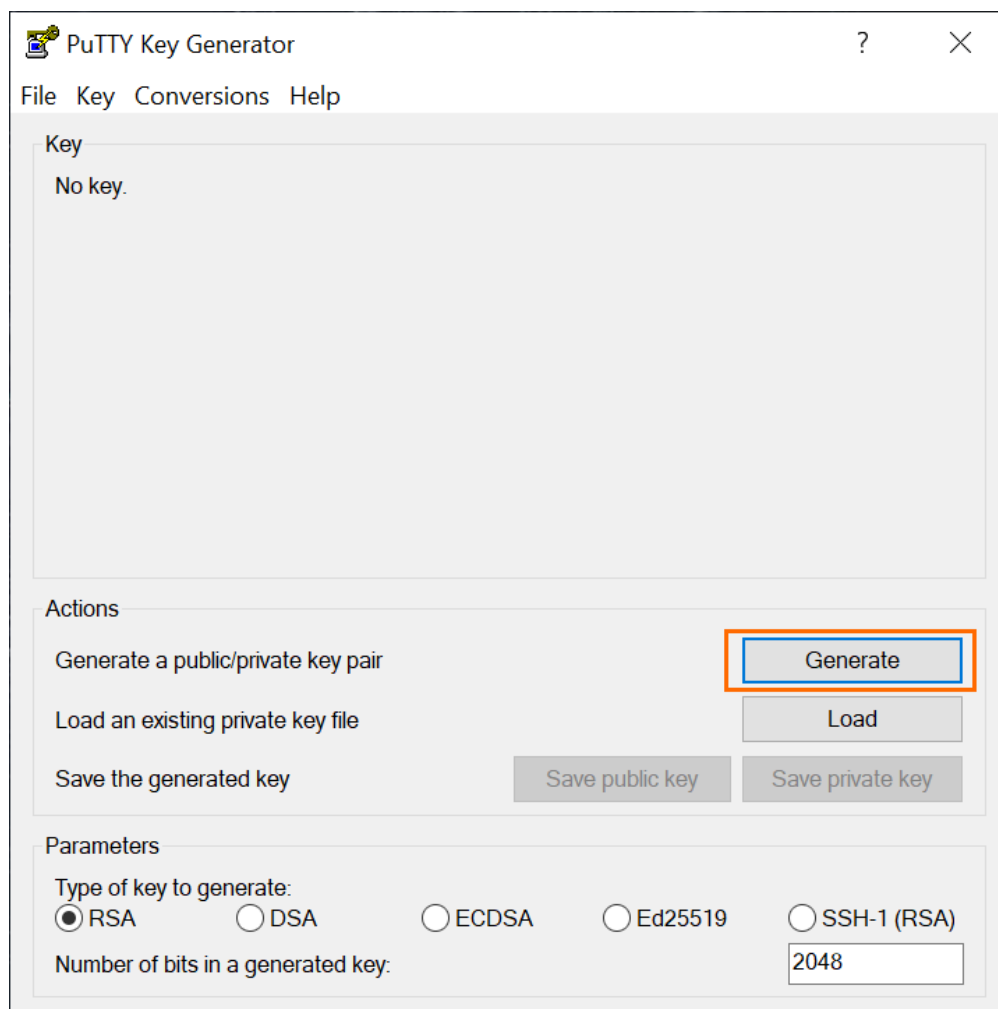
4. Move the mouse over the specified area to generate randomness.

5. Save the public and the private key for future reference.

6. Click **Save public key** and save it on your computer.
7. Click **Save private key** and save it on your computer.
8. Copy the public key from the text box to your clipboard.
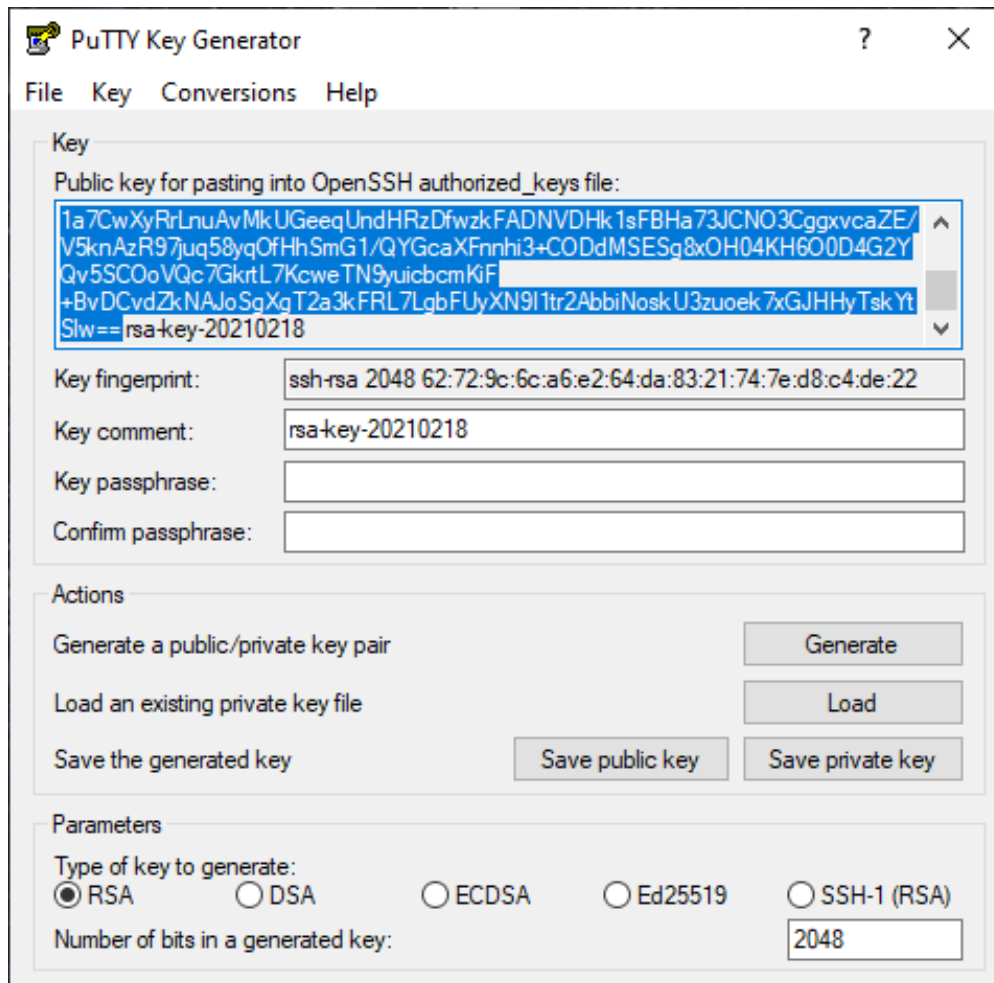
Copy only the highlighted part of the key as displayed in the picture above. Do not copy **rsa-key-20210218**.

Step 2. Grant Support SSH Access to a Site

Follow this step to grant support access to the site only. To grant access to both the site and the gateway, follow Step 2 and Step 3.

1. Go to https://cloudgenwan.barracudanetworks.com/ and log in with your existing Barracuda Cloud Control account.
2. At the top, select the workspace containing your site.
3. Click **SITES**.
4. Select the site you want to grant access to from the list of sites.
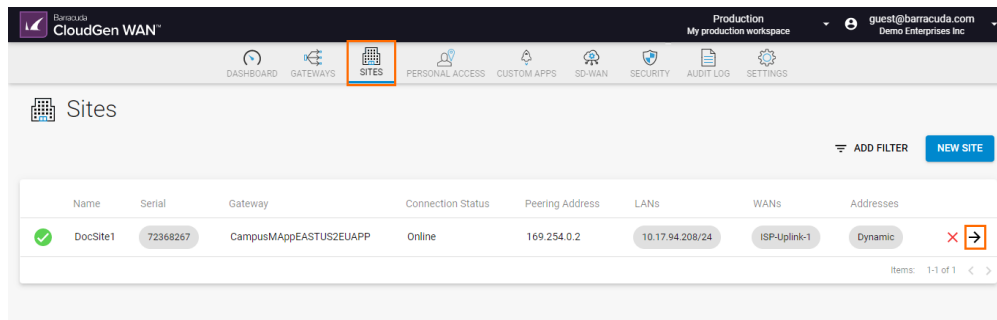
5. The site menu opens.
6. Click **SUPPORT ACCESS**.
7. The **Support Access** window opens. Specify values for the following:
    - **Support ACL** – Enter a comma-separated list of the networks you want to allow SSH access to the site. The Access Control list cannot be 0.0.0.0/0 and the maximum netmask can be up to a /30 network.
   - **SSH Public Key** – Enter the OpenSSH public key you want to allow SSH access to the site.

8. Click **SAVE**.

SSH access is granted to a site from the specified list of networks with the specified SSH public key. If you also want to grant SSH access to the gateway, continue with Step 3. If you want to grant SSH access for the site only, you are now finished.

Step 3. Grant Support SSH Access to a Gateway in Microsoft Azure

To grant support access to an Azure gateway, you must enable the configuration in this step and in Step 4. To grant support access to an on-premises gateway, go to Step 4.

1. Go to https://cloudgenwan.barracudanetworks.com/ and log in with your existing Barracuda Cloud Control account.
2. At the top, select the workspace containing your site.
3. Click **GATEWAYS**.
4. Click on the name of the gateway your site of Step 2 is connected to.
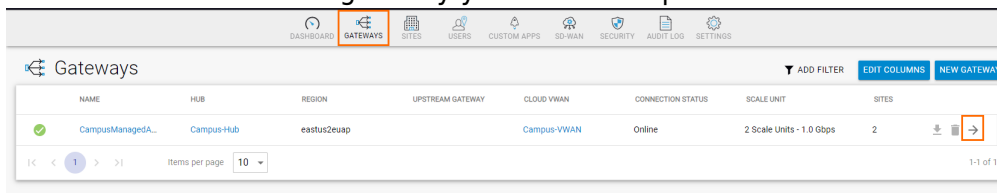
5. You are redirected to the managed app in Microsoft Azure. Log in with your Microsoft Azure credentials.
6. The managed application blade opens.
7. Click **Support access**.
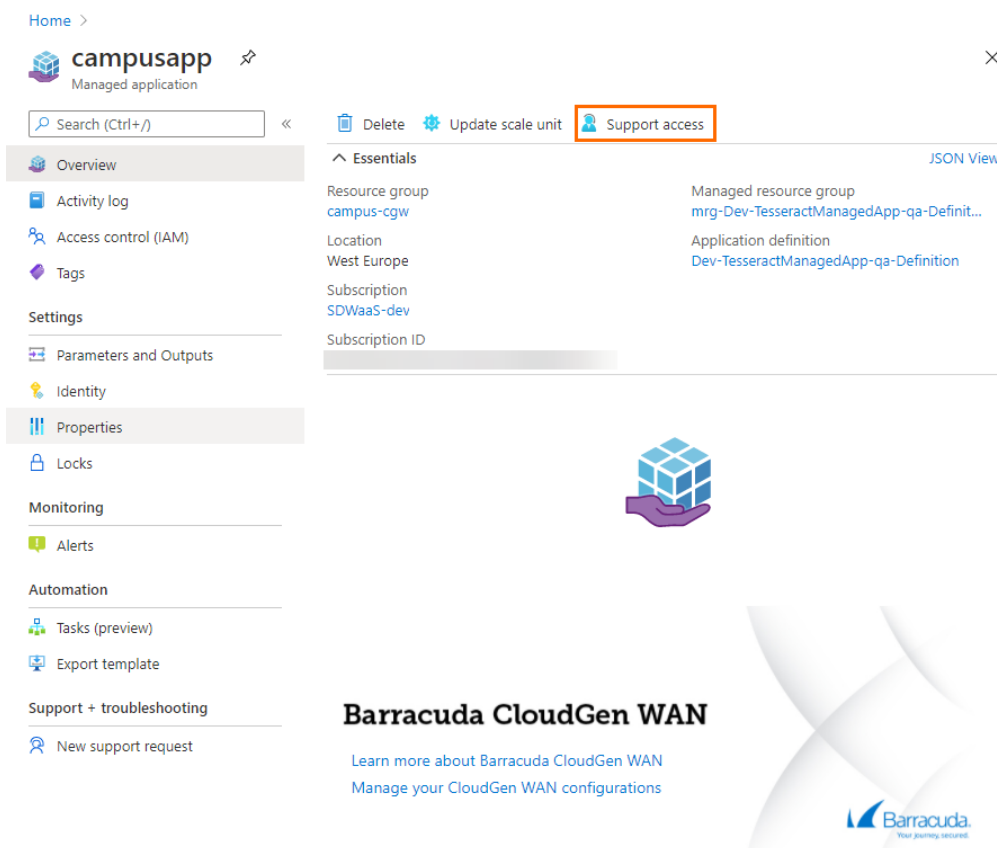
8. The **Support Access** blade opens.

- ○ **Support ACL** – Enter the same comma-separated list of the networks you entered in Step 2.

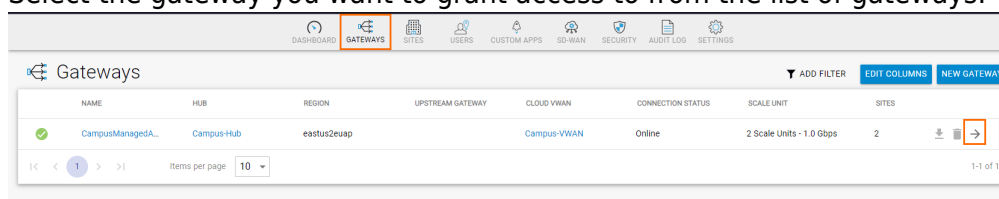9. Click **Review + submit**.
10. The **Review + create** blade opens.

11. Click **Submit**.

Step 4. Grant Support SSH Access in the CloudGen WAN Service

Note: To grant support access to an Azure gateway, you must first perform Step 3. To grant support access to an on-premises gateway, Step 3 is not required.
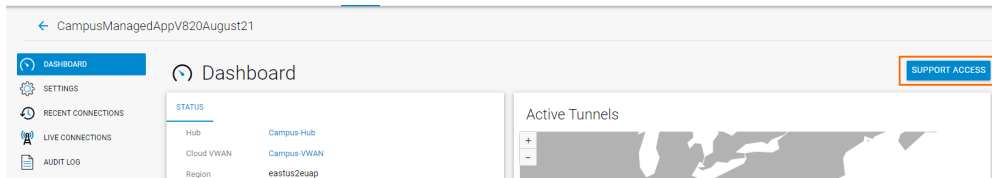
1. Go to https://cloudgenwan.barracudanetworks.com/ and log in with your existing Barracuda Cloud Control account.
2. At the top, select the workspace containing your site.
3. Click **GATEWAYS**.
4. Select the gateway you want to grant access to from the list of gateways.

5. The gateway menu opens.

6. Click **SUPPORT ACCESS**.

7. The **Support Access** window opens. Specify values for the following:
   - **Support ACL** – Enter a comma-separated list of the networks you want to allow SSH access to the gateway. The Access Control list cannot be 0.0.0.0/0 and the maximum netmask can be up to a /30 network.
   - **SSH Public Key** – Enter the OpenSSH public key you want to allow SSH access to the gateway.

8. Click **SAVE**.

SSH access is granted to the gateway from the specified list of networks with the specified SSH public key.

Figures

1. generate.png
2. generate_move.png
3. save.png
4. example_key.png
5. sites.png
6. key_cgw.png
7. gw1.png
8. mapp.png
9. sup_acl.png
10. submit.png
11. gw1.png
12. gw2.png
13. gw3.png