Secure Connector Deployment via Configuration File

https://campus.barracuda.com/doc/91128304/

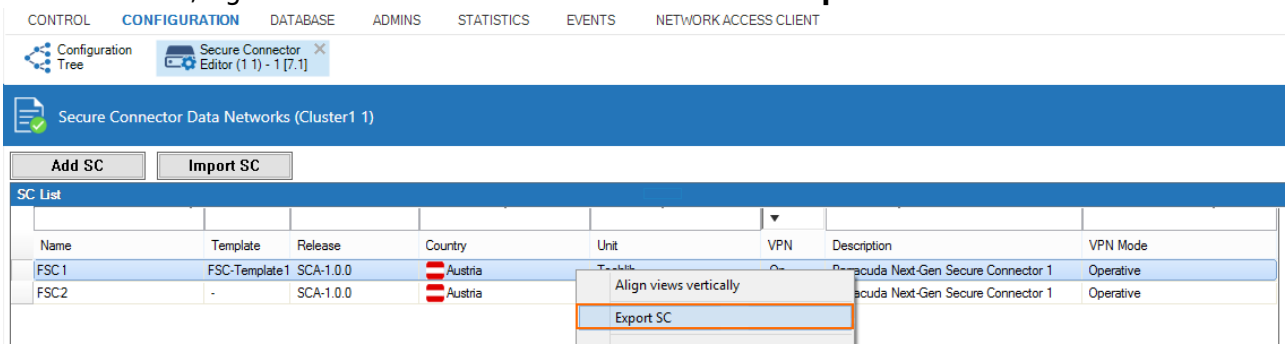
When deploying a new Secure Connector, create the configuration on the Control Center and then import the configuration via USB OTG or web interface. On the next boot, the Secure Connector automatically connects to its assigned Access Controller and Control Center.

Before You Begin

- Configure the Access Controller and Control Center. For more information, see Infrastructure Set-up.
- Configure the Secure Connector using the Secure Connector Editor. For more information, see Secure Connector Setup and Configuration.

Step 1. Export the SCA.CONF Configuration File

1. Go to ***your cluster*** **> Cluster Settings > Secure Connector Editor**.
2. In the **SC List**, right-click the Secure Connector and select **Export SC**.



3. Enter `sca` as the **File name** and click **Save**.

The file must be called sca.conf.

Step 2. Copy the Configuration File to the Secure Connector

You can copy the configuration file to the Secure Connector either via USB cable, where the Secure Connector acts as a USB mass storage device, or via web interface.

Because the sca.conf file contains sensitive information, such as certificates and network settings, do not use unsafe distribution methods, such as unencrypted emails or cloud storage,

to distribute the configuration.

Import the File via USB Mass Storage (OTG)

Connect the Secure Connector with a USB cable to your client PC and copy the Secure Connector configuration file to the device. The configuration is automatically applied when the Secure Connector is rebooted.

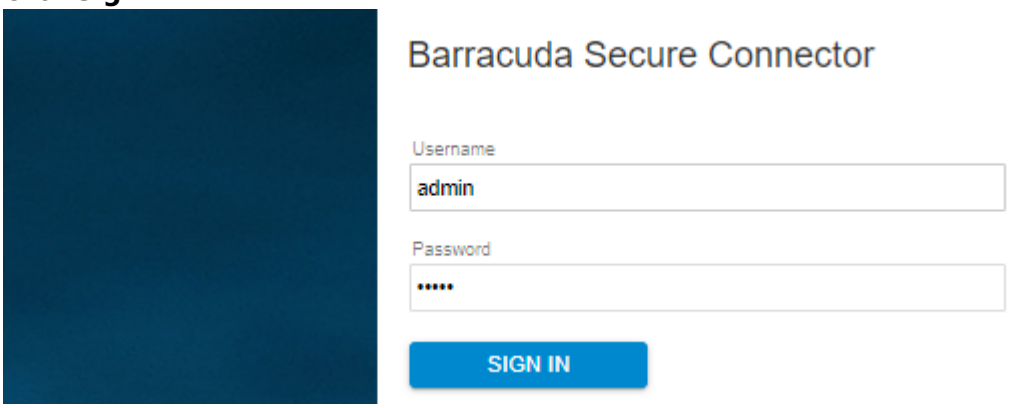
1. Use a micro to standard USB cable to connect the OTG port with a USB port on your client PC.
2. Wait for your client PC to recognize the Secure Connector as a mass storage device.
3. Verify the file name of the Secure Connector configuration file is **sca.conf**.
4. Copy sca.conf to the USB storage of the Secure Connector.
5. Unplug the USB cable and reboot.

The configuration is automatically applied on first boot. The Secure Connector configuration file is not removed from the device, but only applied once.

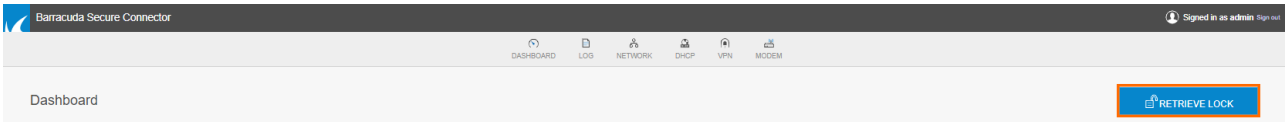
Import the File via Secure Connector Web Interface

The Secure Connector listens on 192.168.200.200 on the LAN port. You must configure your client PC to connect to the Secure Connector and then use the web interface to upload the configuration file.

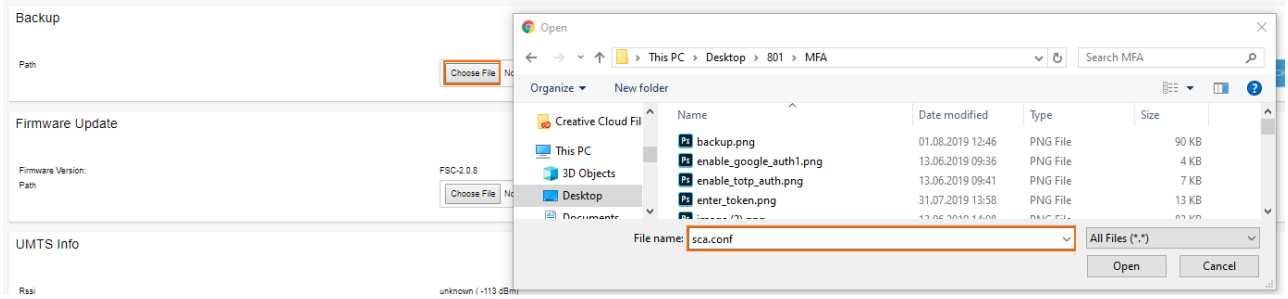
1. Change your client PC IP address to:
   - **IP address** – 192.168.200.100
   - **Netmask** – 255.255.255.0
   - **Gateway** – 192.168.200.200
2. Connect your client PC to the **LAN** port of the Secure Connector.
3. Open a browser and go to **https://192.168.200.200/**.
4. Log into the Secure Connector:
   - **Username** – Enter `admin`.
   - **Password** – Enter `admin`.
5. Click **Sign In**.



6. The web interface **Dashboard** page opens.
7. Click **Retrieve Lock**.



8. In the **Backup** section, click **Choose File** and select the **sca.conf** file created in Step 2.



9. Click **Apply backup**.
10. On the top of the page, click **Activate Configs**.
11. Click **Release Lock**.

Your Secure Connector now automatically connects to its assigned Access Controller. The WAN LED turns green and the VPN LED red when a connection has been established. The device is now visible on the **VPN > Site-to-Site** page and **VPN > Status** page of the Access Controller and on the **Status Map** page of the Control Center.

Figures

1. export_sc.png
2. web_login.png
3. web_retrieve.png
4. choose_file.png