

# Secure Connector Deployment via Configuration File

https://campus.barracuda.com/doc/96026753/

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 <u>Infrastructure</u> <u>Set-Up</u>.
- Configure the Secure Connector using the Secure Connector Editor. For more information, see <u>Secure Connector Setup and Configuration</u>.

## 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**.

CONTROL CONFIG	URATION DA	TADAGE ADMIN	IS STATISTICS E	EVENTS NETWORK ACCESS CLIENT						
Configuration Secure Connector × Editor (1 1) - 1 [7.1]										
Secure Connector Data Networks (Cluster1 1)										
Add SC	Import SC									
SC List										
					•					
Name	Template	Release	Country	Unit	VPN	Description	VPN Mode			
FSC 1	FSC-Template	SCA-1.0.0	Austria	Table	0-	Pacuda Next-Gen Secure Connector 1	Operative			
FSC2	-	SCA-1.0.0	Austria	Align views vertically		acuda Next-Gen Secure Connector 1	Operative			
			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.

Barracuda Secure Connector
Username
admin
•••••
SIGN IN

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



All Files (\*.\*)

Open Cance

	Barracuda Secure Connector									Signe	d in as admin Sign out
			DASHBOARD LOG N	A 🔒 ETWORK DHCP	(e) VPN	الطّ MODEM					
	Dashboard										LOCK
8.	In the <b>Backup</b> section, click <b>Ch</b>	oose I	File and	select	the	sca.	.conf fi	le create	ed in	Step 2.	
	Backup	© Open							×		
	Path	Choose File N	← → ∽ ↑	→ This PC →	Desktop	> 801 > MI	801 > MFA ~ (			Search MFA	٩
			Organize 🔻 New folder							• •	
	Firmware Update		o Creative Clou	d Fil ^ Nam	e	^		Date modified	Туре	Size	^
		FSC-2.0.8 Choose File No	This PC	Ps b	Ps backup.png			01.08.2019 12:46	PNG File	90 KB	
	Firmwara Version		20 Objects	Ps e	nable_goo	ogle_auth1.pn	g	13.06.2019 09:36	PNG File	4 KB	
	Path		3D Objects	Ps e	enable_totp	p_auth.png		13.06.2019 09:41	PNG File	7 KB	
			🗠 📃 Desktop	Ps e	enter_toker	n.png		31.07.2019 13:58	PNG File	13 KB	

File name: sca.conf

9. Click Apply backup.

UMTS Info

- 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.

## Barracuda CloudGen Firewall



#### Figures

- 1. export\_sc.png
- 2. web\_login.png
- 3. web\_retrieve.png
- 4. choose\_file.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.