

SC Deployment via SC Configuration File

<https://campus.barracuda.com/doc/46208889/>

When deploying a new SC, create the configuration on the Control Center and then import the configuration on the SC. The SC will then automatically connect to its assigned SAC and Control Center.

In this article:

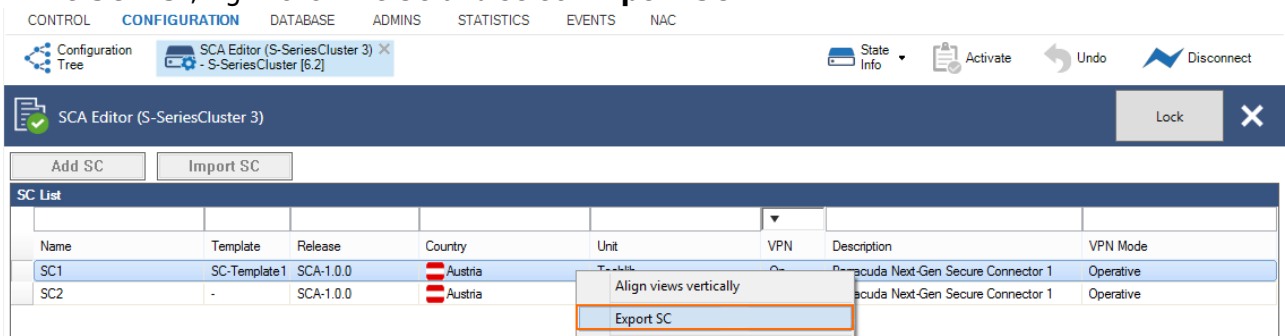
Before You Begin

- Configure the SAC and Control Center. For more information, see [Secure Access Concentrator and Control Center Deployment](#).
- Configure the SC using the Secure Connector Editor. For more information, see [How to Add a Secure Connector Configuration](#).

Step 1. Export the SC Configuration File

Export the **sca.conf** configuration file.

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



The screenshot shows the 'SCA Editor (S-SeriesCluster 3)' interface. At the top, there are navigation tabs: CONTROL, CONFIGURATION (selected), DATABASE, ADMINS, STATISTICS, EVENTS, and NAC. Below the tabs are several icons: Configuration Tree, SCA Editor (S-SeriesCluster 3) (selected), State Info, Activate, Undo, and Disconnect. The main area contains a table titled 'SC List' with columns: Name, Template, Release, Country, Unit, VPN, Description, and VPN Mode. The table has two rows: SC1 and SC2. A context menu is open over the SC1 row, with 'Export SC' highlighted. Other menu items include 'Align views vertically'.

Name	Template	Release	Country	Unit	VPN	Description	VPN Mode
SC1	SC-Template1	SCA-1.0.0	Austria			Barracuda Next-Gen Secure Connector 1	Operative
SC2	-	SCA-1.0.0	Austria			Barracuda Next-Gen Secure Connector 1	Operative

4. Enter **sca** as the **File name** and click **Save**.

The file must be called **sca.conf**. Otherwise, you will not be able to import it on the SC.

Step 2. Copy the Configuration File to the SC

You can copy the configuration file to the SC either via USB cable, where the SC acts as a USB mass storage device, or via web interface. As 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 SC with a USB cable to your client PC and copy the SC configuration file to the device. The configuration is automatically applied when the SC is rebooted.

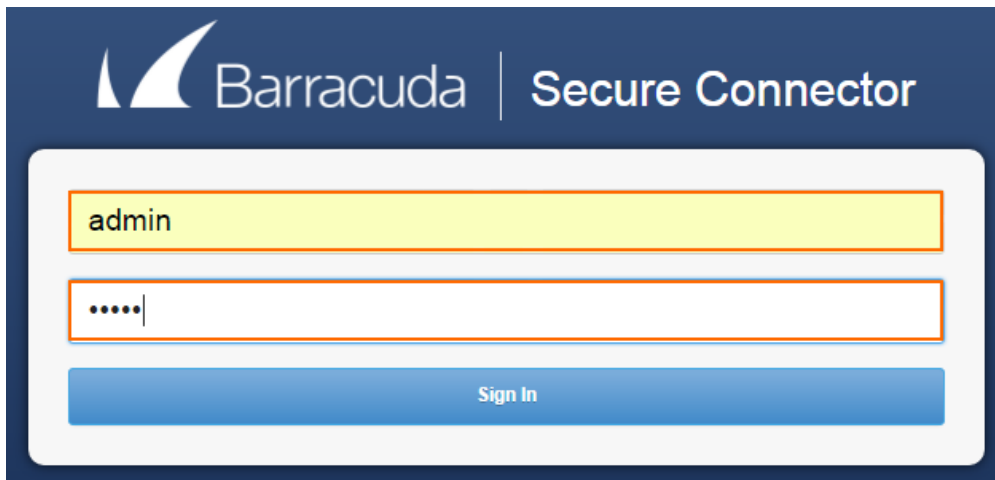
1. Use a micro to standard USB cable to connect the OTG port with a USB port on your client PC.
2. Wait for your client PC to recognize the SC as a mass storage device.
3. Verify the file name of the SC configuration file is **sca.conf**.
4. Copy `sca.conf` to the USB storage of the SC.
5. Unplug the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

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

Import the File via SC Web Interface

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

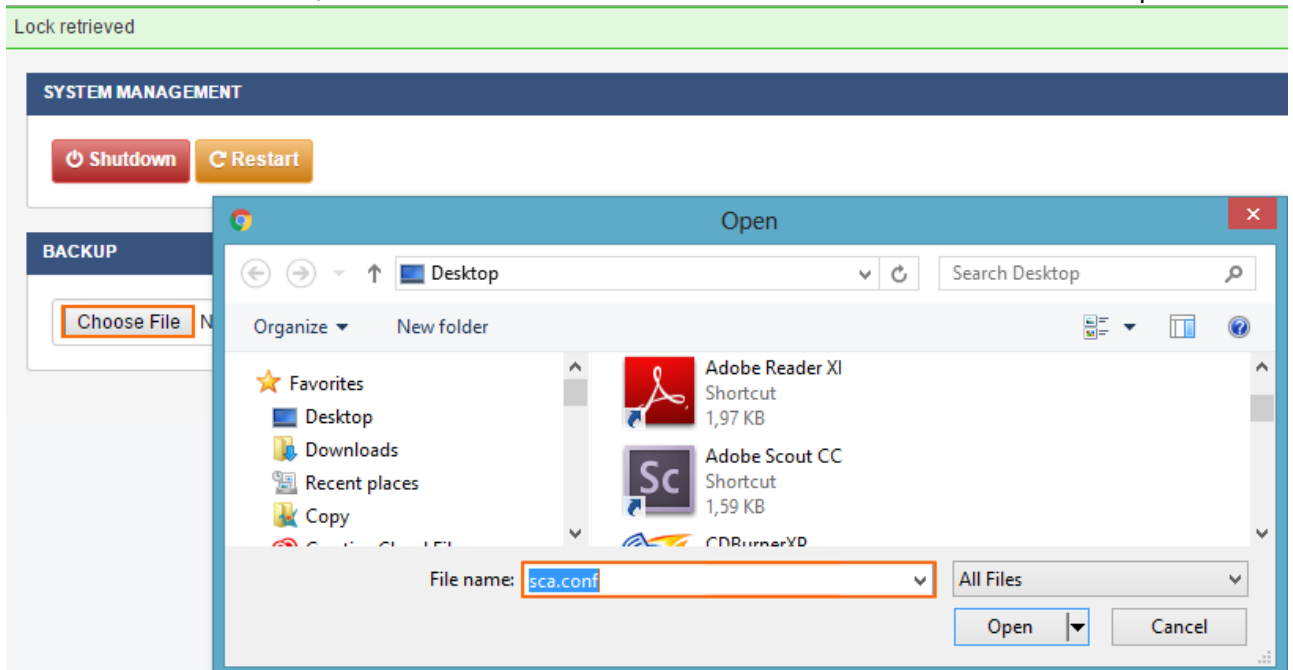
1. Change your client PC IP address to:
 1. **IP address** - 192.168.200.100
 2. **Netmask** - 255.255.255.0
 3. **Gateway** - 192.168.200.200
2. Connect your client PC to the **LAN** port of the SC.
3. Open a browser and go to **https://192.168.200.200**.
4. Log into the Secure Connector:
 - **Username**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



6. Go to **CONFIGURATION > Administration**.
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. Click **Activate Configs**.
11. Click **Release Lock**.



Your SC now automatically connects to its assigned SAC. The WAN LED turns green and the VPN LED red when a connection has been established. The device is now visible on the VPN page of the SAC and Status Map of the Control Center

[Status Map](#)
[Geo Maps](#)
[Configuration Updates](#)
[File Updates](#)
[Sessions](#)
[Barracuda Activation](#)
[Floating Licenses](#)
[Statistics Collection](#)
[Remo Exec](#)

Scope: All
 State: (0) 3 1 1 (6)
 [Range](#)

Name	Description	Access IP	Version	C...	Appli...	Server	Se...	N...	Li...	Ad...	R...	VPN	Co...
Range 3													
CH-AC1	Access Concentrator 1	10.0.15.66	6.2.1-042.nightbuild	VF2000	ACVIRT1								
SC1	Barracuda Next-Gen Secure Connector 1	10.33.0.1	SCA-1.0.0										

[DASHBOARD](#)
[CONFIGURATION](#)
[CONTROL](#)
[FIREWALL](#)
[VPN](#)
[LOGS](#)
[STATISTICS](#)
[EVENTS](#)
[SSH](#)

[Site-to-Site](#)
[Client-to-Site](#)
[Status](#)

[Filter](#)
 NAC: 0 (0) - Clients: 0 (0) - SSL: 0
 [Refresh if active](#)
 [Refresh \(F5\)](#)
 [Disconnect](#)

Name	Tunnel	Local	Peer	Info	Transport	Encryption	Auth.	Compression	bps10	Total	Idle	
/ single transport tunnel (1)												
	3-S-SeriesCluster-SC1	TINA	10.0.15.6	89.144.212.75		TCP	AES 128	SHA	0%	0 B	30 K	1 s

[DASHBOARD](#)
[CONFIGURATION](#)
[CONTROL](#)
[FIREWALL](#)
[VPN](#)
[LOGS](#)
[STATISTICS](#)
[EVENTS](#)
[SSH](#)

[Site-to-Site](#)
[Client-to-Site](#)
[Status](#)

[Access Cache](#)
[Drop Cache](#)
[Client Downloads](#)
[Filter](#)
[Refresh \(F5\)](#)
[Disconnect](#)

Tunnel	Name	Type	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last Info
	TINA	3-S-SeriesCluster-SC1		FW Tunnel	ACTIVE	10	0	18s	89.144.212.75	Access Granted

Figures

1. export_sc.png
2. sc_login.png
3. retr_lock.png
4. sc_browse.png
5. rel_lock.png
6. SC_CC_Status_Map.png
7. SC_SAC_VPN_02.png
8. SC_SAC_VPN_01.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.