

Secure Connector WAN Connections

https://campus.barracuda.com/doc/17994/

Barracuda Secure Connectors can connect to the Internet using DHCP client, static, or Wi-Fi client connections. The connections can be configured through the Secure Connector Editor or, for troubleshooting purposes, directly on the web interface of the Secure Connector.

DHCP Client

The Secure Connector receives a public IP address from the DHCP client of the ISP. All traffic is automatically sent out through the WAN interface.

Configuration Using the Secure Connector Editor

- 1. Go to your cluster > Cluster Settings > Secure Connector Editor.
- 2. Click Lock.

- 3. Double-click to edit the device or Secure Connector template.
- 4. In the left menu, click WAN Settings.
- 5. (Template only) Enable WAN Interface Settings.

WAN Interface Settings

From the WAN Network Mode drop-down list, select DHCP-Client.

DHCP-Client	✓ I.
	Ē×
	Ŧ
24-Bit	✓
	DHCP-Client

7. Click OK and Activate.

Configuration Using Web Interface Override

Use the web interface override to temporarily restore connectivity. Correct any misconfigurations on the Control Center beforehand because the configuration on the Secure Connector will be overridden immediately after the configuration lock in the web interface has been released.

- 1. Log into the web interface.
- 2. Click the **Network** tab.
- 3. Click Retrieve Lock.
- 4. In the WAN Interface section, set DHCP Client to Yes.
- 5. Click Save.



- 6. On the top of the page, click **Activate Configs**.
- 7. To return to using the configuration stored on the Control Center, click **Release Lock**.

Static IP Address

You can configure a static IP address and route if you use a static IP address to connect to the Internet. Static IP addresses are unique to the device and, as such, cannot be configured via Secure Connector template.

Configuration Using the Secure Connector Editor

- 1. Go to your cluster > Cluster Settings > Secure Connector Editor.
- 2. Click Lock
- 3. Double-click to edit the Secure Connector.
- 4. In the left menu, click **WAN Settings**.
- 5. From the WAN Network Mode drop-down list, select Manual.
- 6. Enter the **IP Address**.
- 7. Select the **Subnet Mask**.

wan menace settings		
WAN Network Mode	Manual	 Image: second sec
DHCP Client		Ē
IP Address	54.229.172.87	Ē
Subnet Mask	24-Bit	~

- 8. In the left menu, click **Routing Settings**.
- 9. Click + to add a route to the **System Routes** table.
- 10. Enter a Name and click OK. The System Routes window opens.
- 11. From the Interface Name drop-down list, select WAN.
- 12. Enter the Gateway IP address.
- 13. Enter 0.0.0.0/0 as the **Target Network Address**.
- 14. From the **Type** drop-down list, select **gateway**.

Туре	gateway 🗸	Ē
Target Network Address	0.0.0/0	Ē
Gateway IP	64.99.0.1	Ē
Interface Name	WAN	Ē

15. Click **OK** and **Activate**.

Configuration Using Web Interface Override

Use the web interface override to temporarily restore connectivity. Correct any misconfigurations on the Control Center beforehand because the configuration on the Secure Connector will be overridden



immediately after the configuration lock in the web interface has been released.

- 1. Log into the web interface.
- 2. Click the **Network** tab.
- 3. Click Retrieve Lock.
- 4. In the **WAN Interface** section, set **DHCP Client** to **No**.
- 5. Enter the WAN IP Address.
- 6. From the **Subnet Mask** drop-down list, select the subnet mask.
- 7. Click Save.
- 8. In the Network Routes section, click + Add Route. The Add Network Route page opens.
- 9. From the **Device** drop-down list, select **WAN**.
- 10. Enter the **Gateway** IP address.
- 11. Enter 0.0.0.0/0 as the **Target Network**.
- 12. Click Add Route.
- 13. On the top of the page, click **Activate Configs**.
- 14. To return to using the configuration stored on the Control Center, click **Release Lock**.

Wi-Fi Client

When used in Wi-Fi client mode, the Secure Connector can connect to wireless networks to connect to the Internet.

Configuration Using the Secure Connector Editor

- 1. Go to your cluster > Cluster Settings > Secure Connector Editor.
- 2. Click Lock
- 3. Double-click to edit the device or template.
- 4. In the left menu, click **Wi-Fi Settings**.
- 5. From the **Wi-Fi Mode** drop-down list, select **Client-Mode**.
- 6. Click + in the **SSID** to add a wireless network.
- 7. Enter a Name and click OK. The SSID window opens.
- 8. Configure the following settings for the wireless network:
 - **SSID** Enter the **SSID** for your network.
 - Security Mode Select the security protocol used by the wireless network: None, WPA2-PSK, or WPA-PSK.
 - **Passphrase** Enter the passphrase of the wireless network.

The passphrase can consist of small and capital characters, numbers, and nonalpha-numeric symbols, except the hash sign (#).

• SSID valid for Wi-Fi Mode - Select Client.



Active		÷.
SSID	barracudaWIFI	×
Security Mode	WPA2-PSK V	Ξ. ·
Passphrase	yourpassphrase	T.
SSID valid for Wi-Fi Mode	Client	×
Interface Name	WIFI	Ē×

- 9. Click **OK**.
- 10. Select the **Network Mode**. The Barracuda Secure Connector supports 802.11b and 802.11g.

wi-ri seunys				
Wi-Fi Mode	Client-Mode		~	Ēv
SSID			💉 🕂 🗙 🔤 🗐 🗐	ŀ
	Name	Active	SSID	
	DemoAP	1	DemoAP	
	DemoClient	1	f280qa	
	<		>	
Network Mode	802.11g		~	Ē-

11. Click **OK** and **Activate**.

Configuration Using Web Interface Override

Use the web interface override to temporarily restore connectivity. Correct any misconfigurations on the Control Center beforehand because the configuration on the Secure Connector will be overridden immediately after the configuration lock in the web interface has been released.

- 1. Log into the web interface.
- 2. Click the **Wireless** tab.
- 3. Click Retrieve Lock.
- 4. In the Wi-Fi Configuration section, set Operating Mode to Client.
- 5. From the **Country** drop-down list, select your country.

WiFi Configuration		
Operating Mode	Off Client Access Point	
Country	AUSTRIA	٠
	SAVE CHANGES	

- 6. In the **Wi-Fi-Client Interface** section, configure the Wi-Fi interface settings:
 - DHCP Client Set DHCP Client to Yes.
 - Static IP address Set DHCP Client to No.
- 7. (Static IP address only) Configure the default route for the WAN interface:
 - 1. Enter the **IP Address** and select the **Subnet Mask**.
 - 2. Click Save.



- 3. Click the **Network** tab.
- 4. In the Network Routes section, click Add Route. The Add Network Route page opens.
- 5. From the **Device** drop-down list, select **WAN**.
- 6. Enter the Gateway IP address.
- 7. Enter 0.0.0.0/0 as the **Target Network**.
- 8. Click Add Route.
- 9. Click the Wireless tab.
- 8. In the Wi-Fi SSIDS section, select Scan. The Wi-Fi Scan page opens.
- 9. Locate the wireless network you want to connect to, and click **Add**. The **Add Wi-Fi SSID** page opens.
- 10. Enter the **Passphrase**.

The passphrase can consist of small and capital characters, numbers, and non-alphanumeric symbols, except the hash sign (#).

11. Click Add SSID.

- 12. On the top of the page, click **Activate Configs**.
- 13. To return to using the configuration stored on the Control Center, click **Release Lock**.

Wireless WAN Modem

Connect the Barracuda 3G/UMTS modem to the Secure Connector.

Configuration Using the Secure Connector Editor

- 1. Go to your cluster > Cluster Settings > Secure Connector Editor.
- 2. Click Lock
- 3. Double-click to edit the device or template.
- 4. In the left menu, click Wireless WAN Settings.
- 5. Select the **WWAN Active** check box.

Wireless WAN Settings			
WWAN Active			Ēv
Modem	Barracuda 4G Modem M40 [USB/internal]	2	Ē

- 6. Enter the Wireless WAN Connection Details matching your mobile provider: • Access Point Name (APN)
 - Access Point Name
 - SIM PIN
 - Phone Number



New	••••	Ē
Confirm	••••	
Strength	Weak	
	New Confirm Strength	New Confirm Strength Weak

7. Enter the **Authentication** settings matching your mobile provider:

- Authentication Method
- User Access ID

- User Access Sub-ID
- Access Password

SIM PIN and access password can consist of small and capital characters, numbers, and non-alpha-numeric symbols, except the hash sign (#).

Autrenucation			
Authentication Method	CHAP	~	Ēv
User Access ID	ppp@A1plu	s.at	Ē,
User Access Sub-ID			Ēv
Access Password	New	•••	Ē,
	Confirm	•••	
	Strength	Weak	

8. Click **OK** and **Activate**.

Configuration Using Web Interface Override

Use the web interface override to temporarily restore connectivity. Correct any misconfigurations on the Control Center beforehand because the configuration on the Secure Connector will be overridden immediately after the configuration lock in the web interface has been released.

- 1. Log into the web interface.
- 2. Click the **Modem** tab.
- 3. Click **Retrieve Lock**.
- 4. Enable WWAN. The Modem Config section opens.
- 5. Enter the configuration settings matching your mobile provider:
 - Access Point Name (APN)
 - SIM PIN
 - Phone Number
 - Authentication Method
 - Useraccess ID
 - Useraccess SubID
 - Access PW



Modem Config	
WWAN enabled	Enabled Disabled
Access Point Name (APN)	A1.net
SIM PIN	9654
Phone Number	*99***1
Authentication Method	CHAP V
Useraccess ID	ppp@A1plus.at
Useraccess SubID	
Access PW	PPP
	SAVE CHANGES

SIM PIN and access password can consist of small and capital characters, numbers, and non-alpha-numeric symbols, except the hash sign (#).

- 6. Click Save Changes.
- 7. Activate the configuration.
- 8. To return to using the configuration stored on the Control Center, click **Release Lock**.



Figures

- 1. sca_WAN_DHCP_01.png
- 2. sc_wan_dhcp01.png
- 3. sc_wan_static01.png
- 4. sc_wan_static02.png
- 5. sc wan wifi01.png
- 6. sc_wan_wifi02.png
- 7. sc_wif_client01.png
- 8. sc_wwan01.png
- 9. sc_wwan02.png
- 10. sc umts03.png
- 11. sc umts web ui.png

© Barracuda Networks Inc., 2025 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.