

Secure Connector WAN Connections

<https://campus.barracuda.com/doc/96026756/>

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

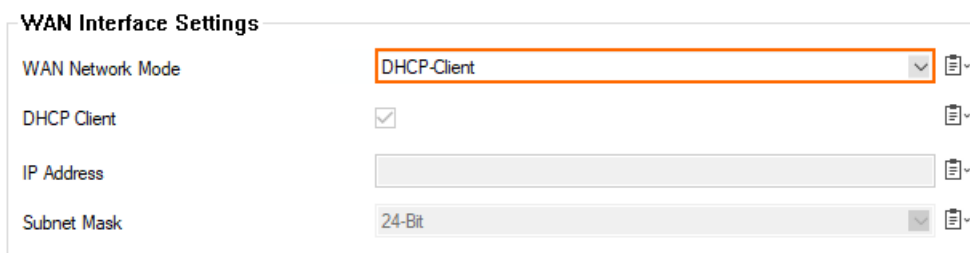
The Secure Connector receives a public IP address from the DHCP client of the ISP. All traffic is automatically sent out through the WAN interface.

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**.



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

A screenshot of the 'WAN Interface Settings' configuration form. The 'WAN Network Mode' dropdown is set to 'DHCP-Client' and is highlighted with an orange box. Below it, the 'DHCP Client' checkbox is checked. The 'IP Address' field is empty, and the 'Subnet Mask' dropdown is set to '24-Bit'. Each field has a copy icon to its right.

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**.

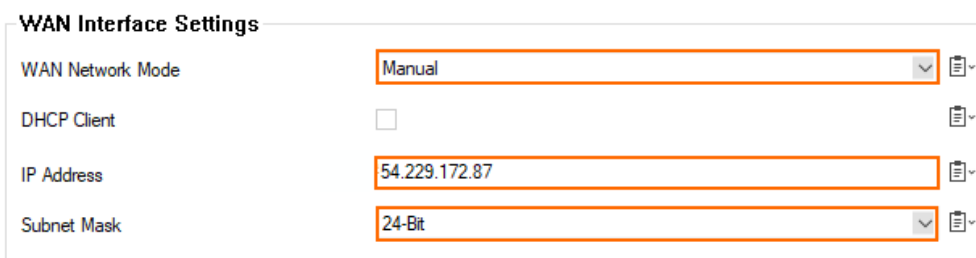
6. On the top of the page, click **Activate Configs**.
7. To return to using the configuration stored on the Control Center, click **Release Lock**.

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.

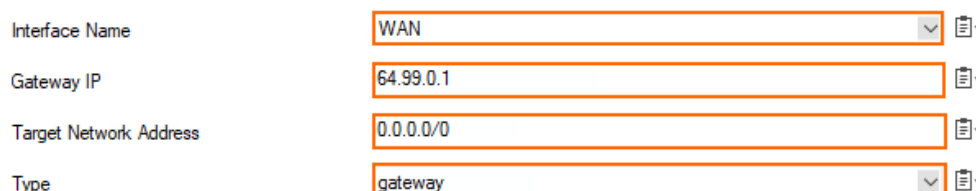
Configuration Using the Secure Connector Editor

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 Interface Settings	
WAN Network Mode	Manual
DHCP Client	<input type="checkbox"/>
IP Address	54.229.172.87
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**.



Interface Name	WAN
Gateway IP	64.99.0.1
Target Network Address	0.0.0.0/0
Type	gateway

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 non-alpha-numeric symbols, except the hash sign (#).
 - **SSID valid for Wi-Fi Mode** – Select **Client**.

Active	<input checked="" type="checkbox"/>	
SSID	<input type="text" value="barracudaWIFI"/>	
Security Mode	<input type="text" value="WPA2-PSK"/>	
Passphrase	<input type="text" value="yourpassphrase"/>	
SSID valid for Wi-Fi Mode	<input type="text" value="Client"/>	
Interface Name	<input type="text" value="WIFI"/>	

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

Wi-Fi Settings

Wi-Fi Mode	<input type="text" value="Client-Mode"/>										
SSID	<div> </div> <table> <thead> <tr> <th>Name</th> <th>Active</th> <th>SSID</th> </tr> </thead> <tbody> <tr> <td>DemoAP</td> <td>1</td> <td>DemoAP</td> </tr> <tr> <td>DemoClient</td> <td>1</td> <td>f280qa</td> </tr> </tbody> </table>		Name	Active	SSID	DemoAP	1	DemoAP	DemoClient	1	f280qa
Name	Active	SSID									
DemoAP	1	DemoAP									
DemoClient	1	f280qa									
Network Mode	<input type="text" value="802.11g"/>										

- 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.

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

WiFi Configuration

Operating Mode	<input type="radio"/> Off <input checked="" type="radio"/> Client <input type="radio"/> Access Point
Country	<input type="text" value="AUSTRIA"/>

SAVE CHANGES

- 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**.
- (Static IP address only) Configure the default route for the WAN interface:
 - Enter the **IP Address** and select the **Subnet Mask**.
 - 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**.

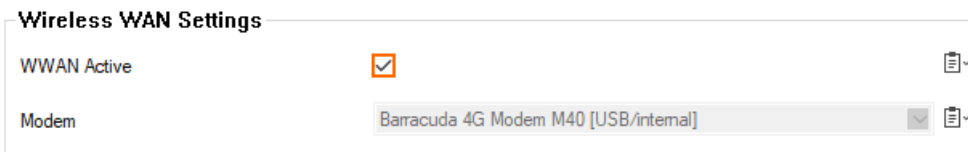
The passphrase can consist of small and capital characters, numbers, and non-alpha-numeric symbols, except the hash sign (#).
11. Click **Add SSID**.
12. On the top of the page, click **Activate Configs**.
13. To return to using the configuration stored on the Control Center, click **Release Lock**.

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 ☒

Modem Barracuda 4G Modem M40 [USB/internal]

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

Wireless WAN Connection Details

Access Point Name (APN)	A1.net		
SIM PIN	New	
	Confirm	
	Strength	<div><div>Weak</div></div>	
Phone Number	*99***1		

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 (#).

Authentication

Authentication Method	CHAP		
User Access ID	ppp@A1plus.at		
User Access Sub-ID			
Access Password	New	...	
	Confirm	...	
	Strength	<div><div>Weak</div></div>	

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	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Access Point Name (APN)	<input type="text" value="A1.net"/>
SIM PIN	<input type="text" value="9854"/>
Phone Number	<input type="text" value="*99***1"/>
Authentication Method	<input type="text" value="CHAP"/>
Useraccess ID	<input type="text" value="ppp@A1plus.at"/>
Useraccess SubID	<input type="text"/>
Access PW	<input type="text" value="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., 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.