FSC WAN Connections

https://campus.barracuda.com/doc/53248310/

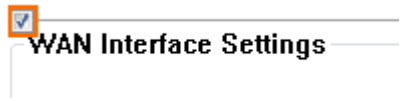
Barracuda NextGen Secure Connectors can connect to the Internet using DHCP client, static, or Wi-Fi client connections. The connections can be configured through the Secure Connector Editor or, for troubleshooting purposes, directly on the web interface of the Secure Connector.

DHCP Client

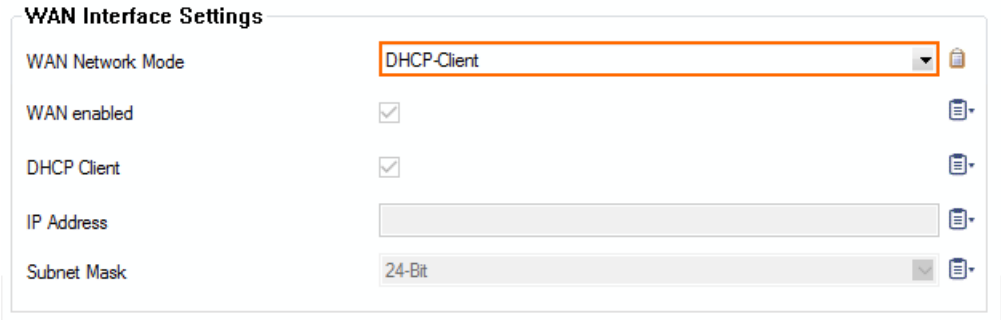
The Secure Connector receives a public IP address from the DHCP client of the ISP. All traffic is automatically sent out through the WAN interface.

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**.



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. Go to **CONFIGURATION > Network**.
3. Click **Retrieve Lock**.

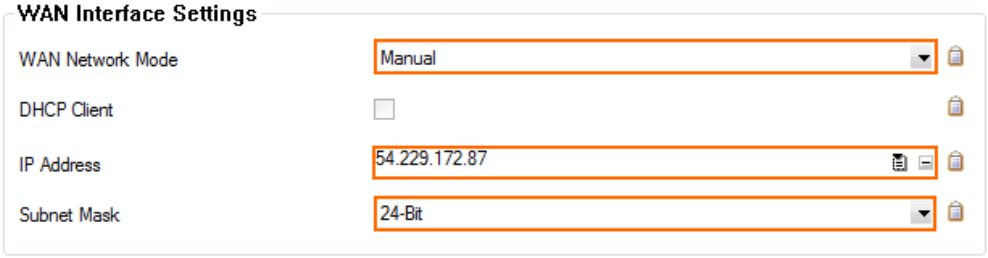
4. In the **WAN INTERFACE** section, set **DHCP Client** to **Yes**.
5. Click **Save Changes**.
6. On the top of the page, click **Activate Configs**.
7. To return to using the configuration stored on the Control Center, click **Release Lock**.

Static IP Address

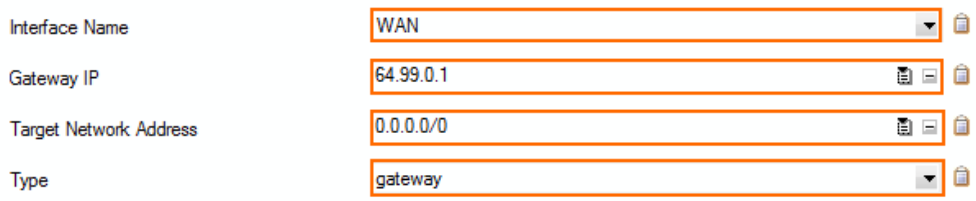
You can configure a static IP address and route if you use a static IP address to connect to the Internet. Static IP addresses are unique to the device and, as such, cannot be configured via Secure Connector template.

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**.



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 the `0.0.0.0/0` as the **Target Network Address**.
14. From the **Type** drop-down list, select **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.

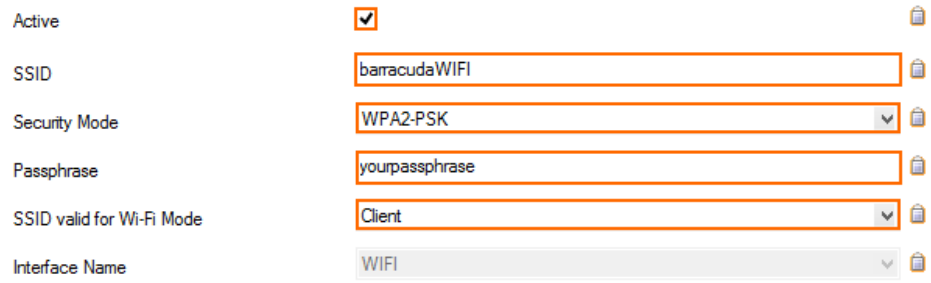
1. Log into the web interface.
2. Go to **CONFIGURATION > Network**.
3. Click **Retrieve Lock**.
4. In the **WAN INTERFACE** section, set **DHCP Client** to **No**.
5. Enter the WAN **IP Address**.
6. From the **Subnet Mask** drop-down list, select the subnet mask.
7. Click **Save Changes**.
8. In the **NETWORK ROUTES** section, click **+ Add Route**. The **Edit 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

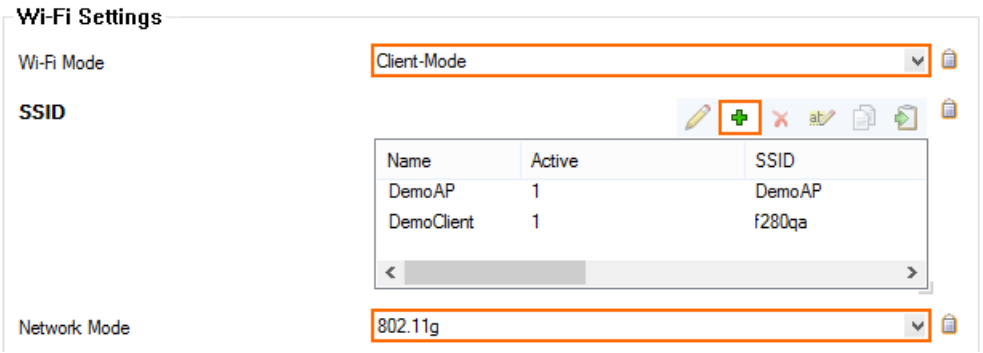
When used in Wi-Fi client mode, the Secure Connector can connect to wireless networks to connect to the Internet.

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**.



9. Click **OK**.
10. Select the **Network Mode**. The FSC supports 802.11b and 802.11g.

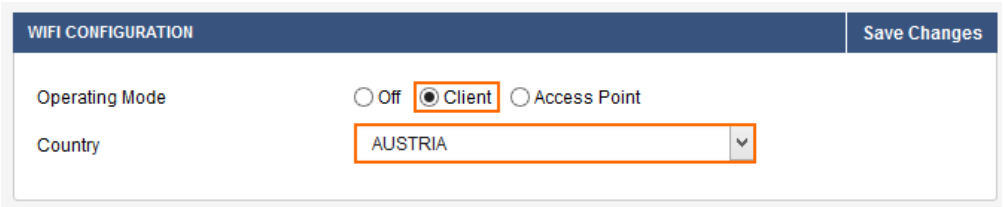


11. Click **OK** and **Activate**.

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. Go to **CONFIGURATION > Wireless**.
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.

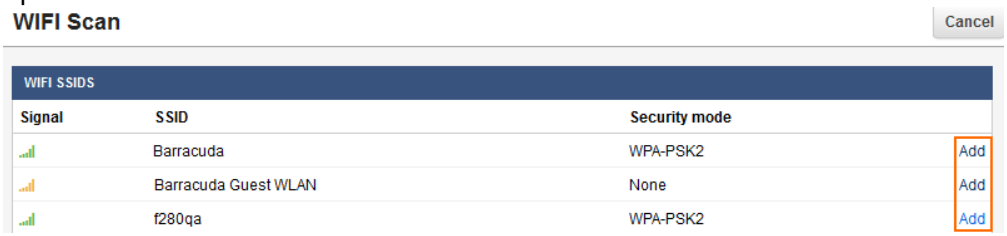


6. In the **Wi-Fi-CLIENT INTERFACE** section, configure the Wi-Fi interface settings:
   - **DHCP Client** – Set **DHCP Client** to **Yes**.
   - **Static IP address** – Set **DHCP Client** to **No**.
7. (Static IP address only) Go to **CONFIGURATION > Network** and configure the default route for the WAN interface:
   1. Enter the **IP Address** and select the **Subnet Mask**.
   2. Click **Save Changes**.
   3. In the **NETWORK ROUTES** section, click **+ Add Route**. The **Edit Network Route** page

opens.

4. From the **Device** drop-down list, select **WAN**.
5. Enter the **Gateway** IP address.
6. Enter `0.0.0.0/0` as the **Target Network**.
7. Click **Add Route**.
8. Go to **CONFIGURATION > Wireless**.

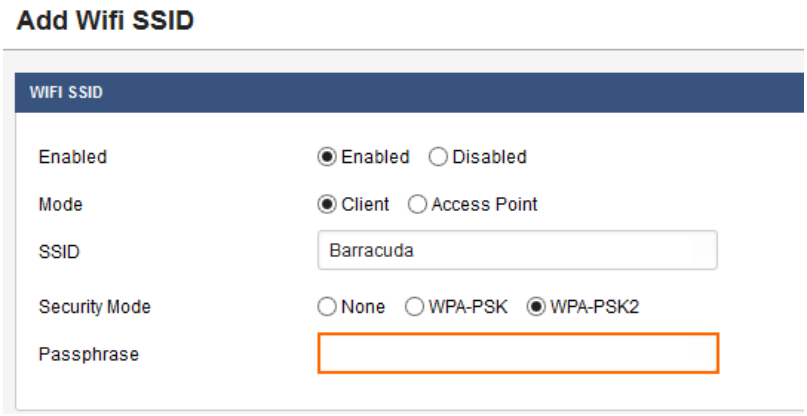
8. In the **Wi-Fi SSIDS** section, select **Scan**. The **Wi-Fi Scan** page opens.
9. Locate the wireless network you want to connect to, and click **Add**. The **Add Wi-Fi SSID** page opens.



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

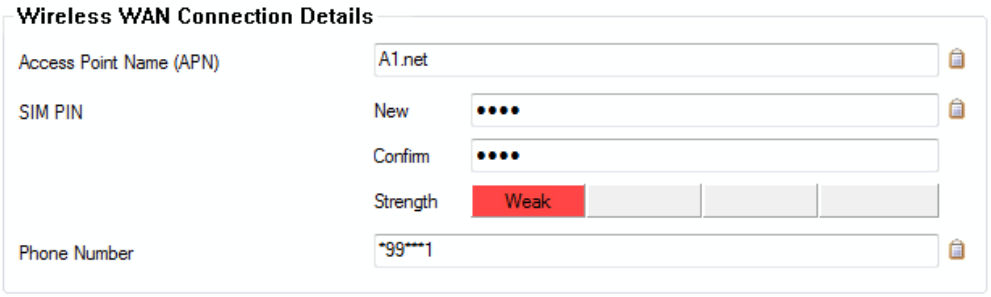
Connect the Barracuda 3G/UMTS modem to the Secure Connector.

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**.

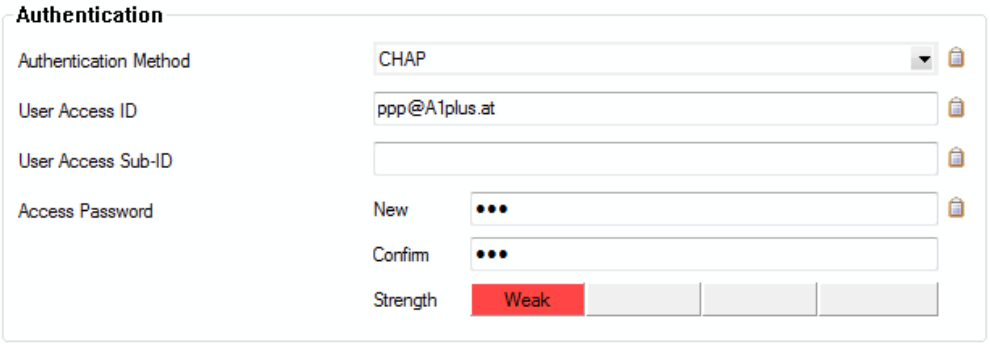
5. Select the **WWAN Active** check box.

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



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 (#).



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

Configuration Using Web interface Override

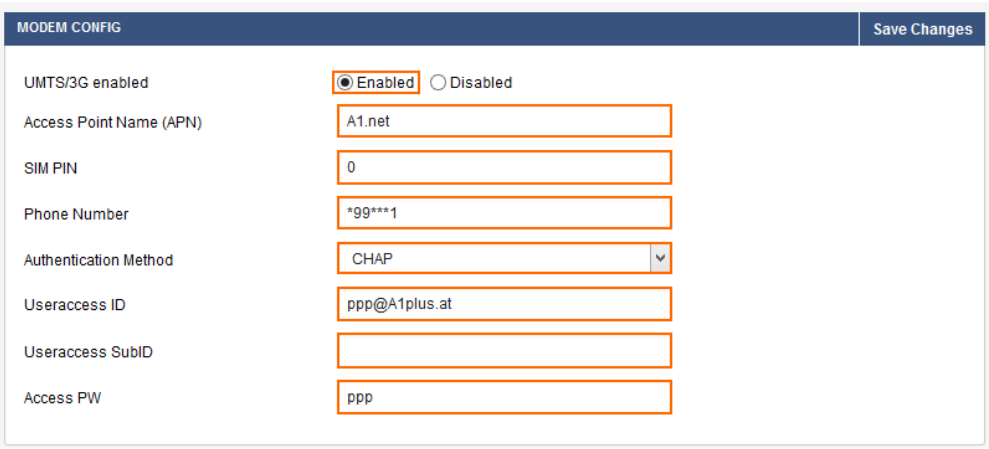
Use the web interface override to temporarily restore connectivity. Correct any misconfigurations on the Control Center beforehand because the configuration on the Secure Connector will be overridden immediately after the configuration lock in the web interface has been released.

1. Log into the web interface.
2. Go to **CONFIGURATION > Modem**.
3. Click **Retrieve Lock**.
4. In the **MODEM CONFIG** section, set **UTMS/3G enabled** to **Enabled**.
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**

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

Modem



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

Figures