Get Started with Barracuda IoT Connect

https://campus.barracuda.com/doc/90444698/

Barracuda IoT Connect is currently in Private Preview (Early Access). Please contact iot_connect@barracuda.com to request an invitation.

Deploy Barracuda IoT Connect in the cloud and configure the Secure Connector in the web user interface. Afterwards, just plug in the Secure Connector (WAN and power). The Secure Connector then automatically receives the configuration from the Zero Touch Deployment. Currently, IoT Connect is available in Microsoft Azure and Amazon AWS.

Step 1. Deployment in the Public Cloud

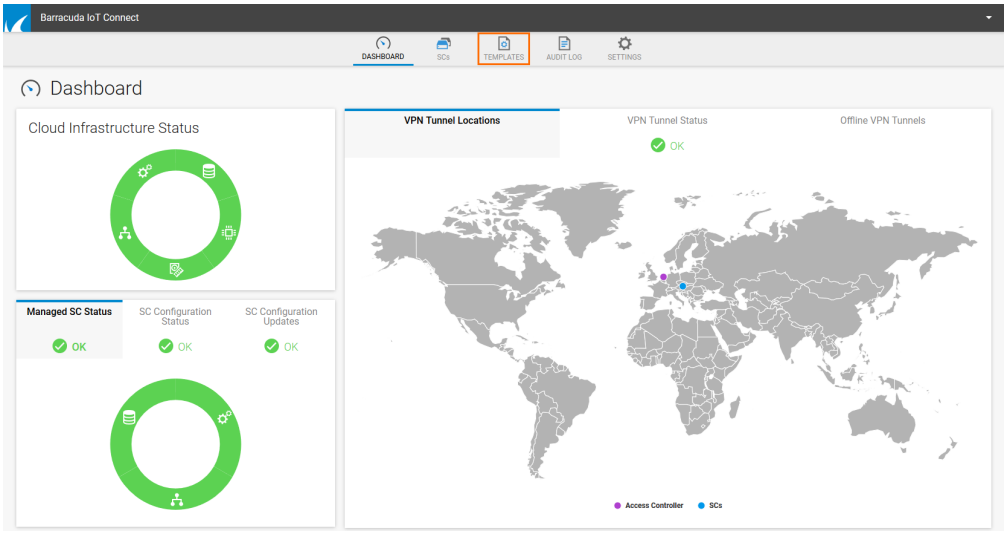
For instructions on the deployment process, follow the step-by-step guide for either Azure or AWS:

- Deployment of Barracuda IoT Connect in Microsoft Azure
- Deployment of Barracuda IoT Connect in Amazon AWS

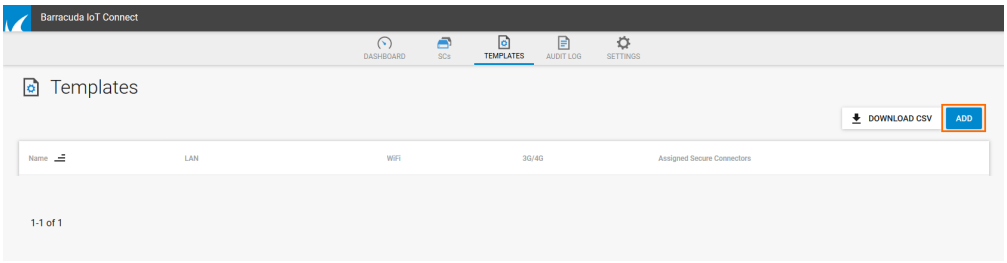
Step 2. Configure the Secure Connector in the Barracuda IoT Connect Web Interface

To manage the Secure Connector devices, you must first create a template and then assign the devices to the template. Devices can be assigned directly in the template creation wizard.

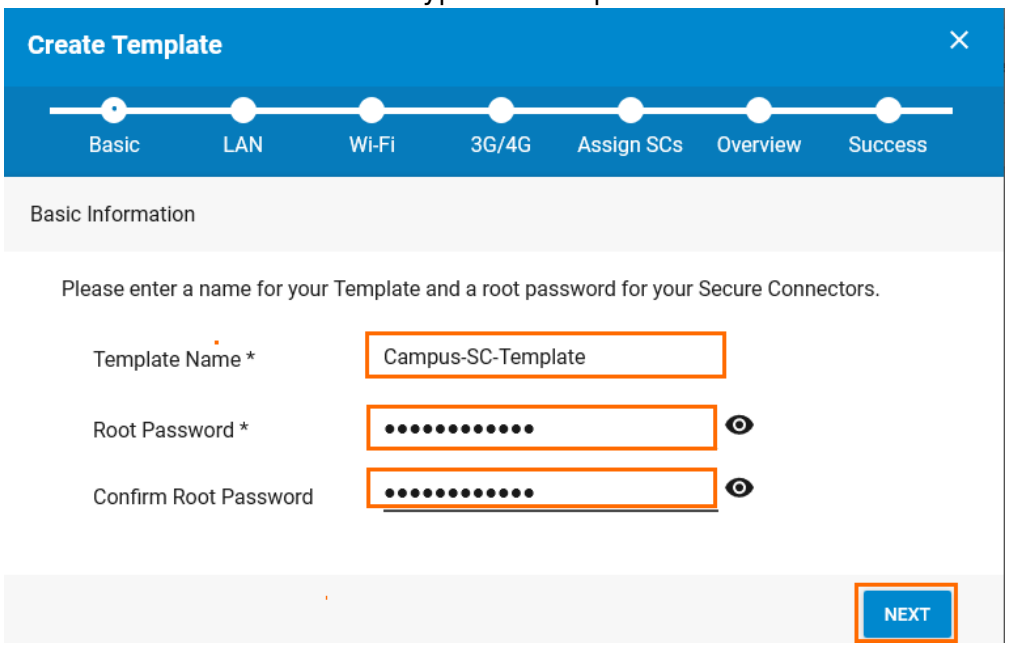
1. Go to https://iotc.barracudanetworks.com/.
2. Log in with your credentials.
3. Accept the cookies, and you will be forwarded to the IoT Connect **DASHBOARD**.



4. Click **TEMPLATES**.
5. Click **ADD**.

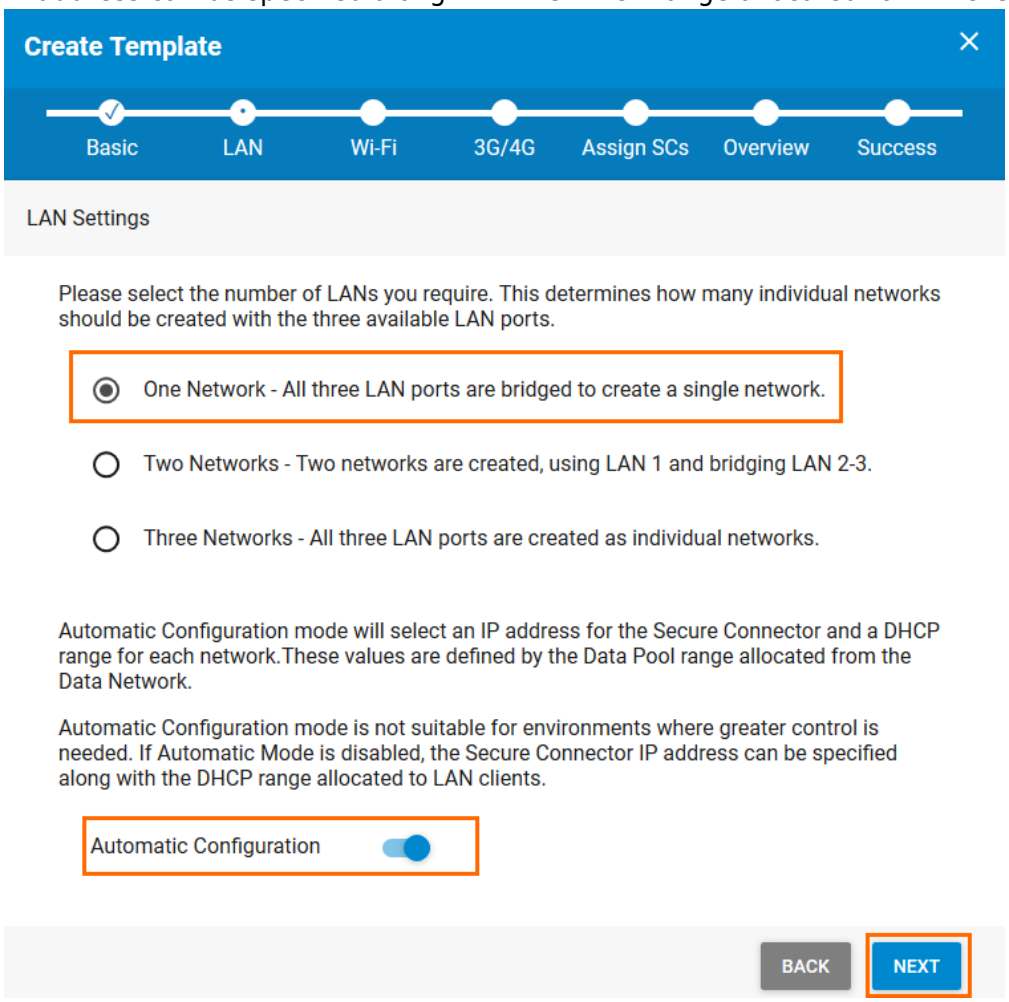


6. The **Create Template** wizard opens.
    1. In the **Basic** blade:
        1. **Template Name** - Enter a name for the template.
        2. **Root Password** - Enter the root password for the Secure Connector devices assigned to this template.
        3. **Confirm Root Password** - Retype the root password.

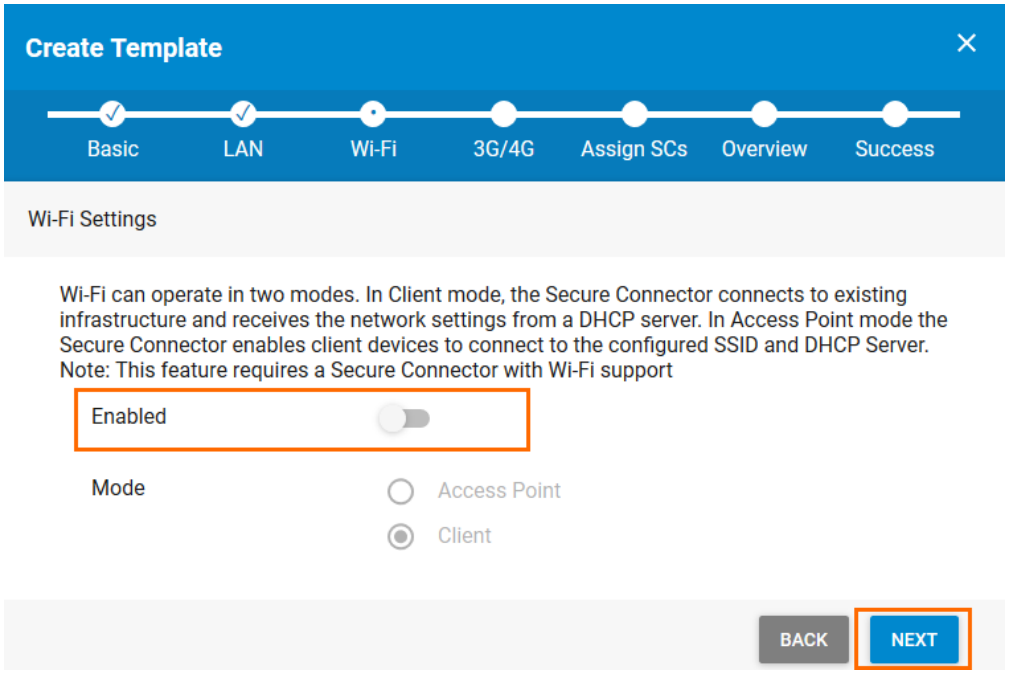


    4. Click **NEXT**.

2. In the **LAN** blade:
    1. Select either **One Network**, **Two Networks**, or **Three Networks**.
    2. **Automatic Configuration** - If Automatic mode is disabled, the Secure Connector IP address can be specified along with the DHCP range allocated to LAN clients.

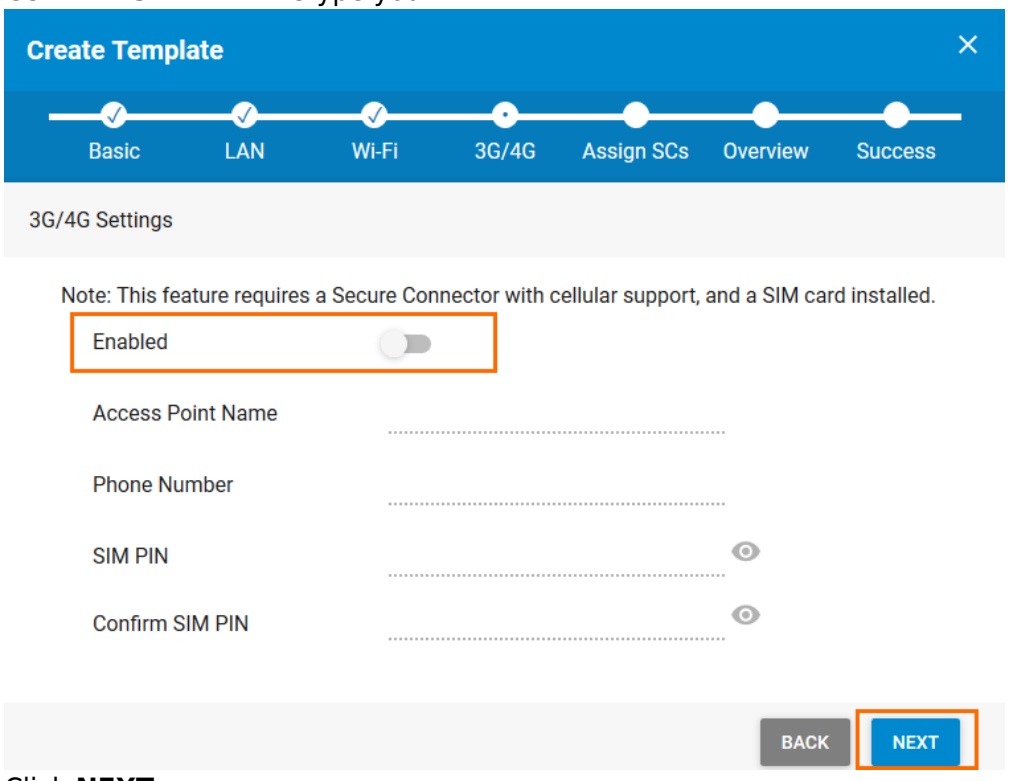


    3. Click **NEXT**.
3. In the **Wi-Fi** blade:
    1. **Enabled** - Enable to use Wi-Fi if your Secure Connector is Wi-Fi capable.
    2. **Mode** - Select either **Access Point** or **Client**. In Client mode, the Secure Connector connects to existing infrastructure and receives the network settings from a DHCP server. In Access Point mode, the Secure Connector enables client devices to connect to the configured SSID and DHCP server.



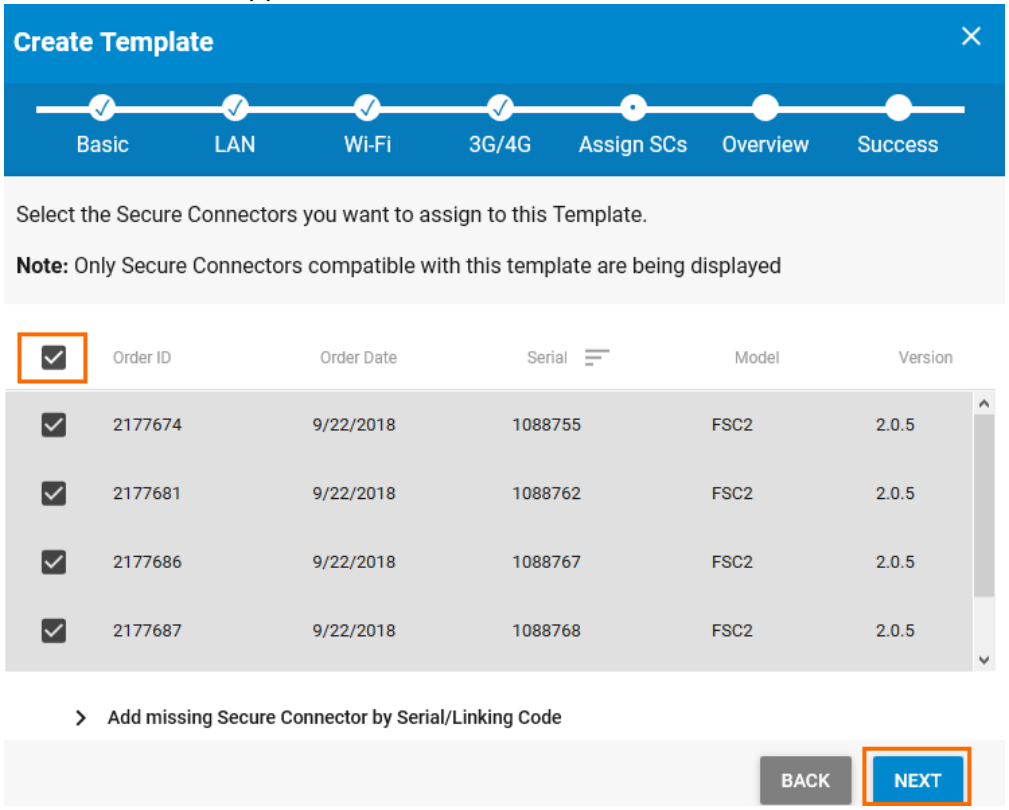
3. Click **NEXT**.

4. In the **3G/4G** blade:
   1. **Enabled** - Enable if you use a Secure Connector with cellular support and an installed SIM card.
   2. **Access Point Name** - Enter the name of your access point.
   3. **Phone Number** - Enter the phone number of the installed SIM card
   4. **SIM PIN** - Enter the PIN of the installed SIM card.
   5. **Confirm SIM PIN** - Retype your PIN.

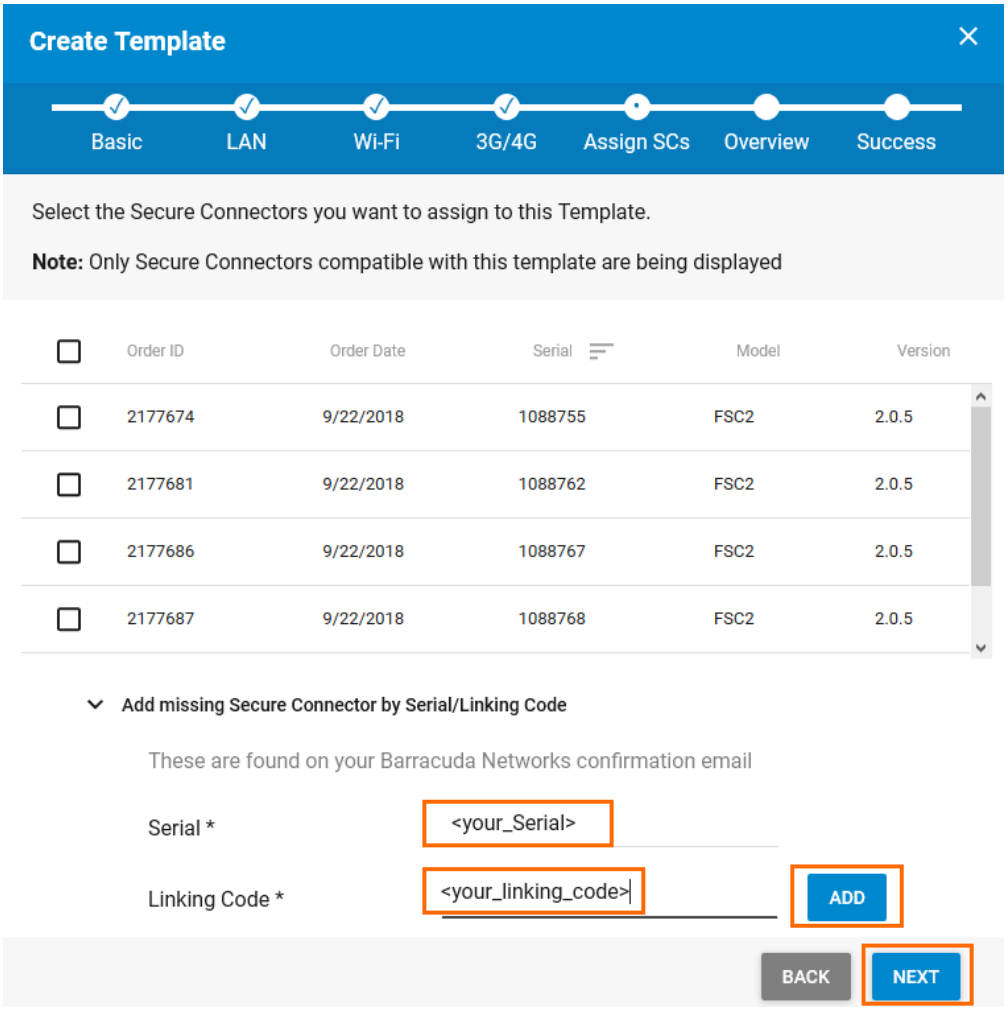


6. Click **NEXT**.

5. In the **Assign SCs** blade:
   1. All Secure Connector devices assigned to your account via Zero Touch Deployment (ZTD) that are compatible with the settings of this template can be selected by selecting the check box next to it. To select all Secure Connector devices, select the check box in the upper-left corner.

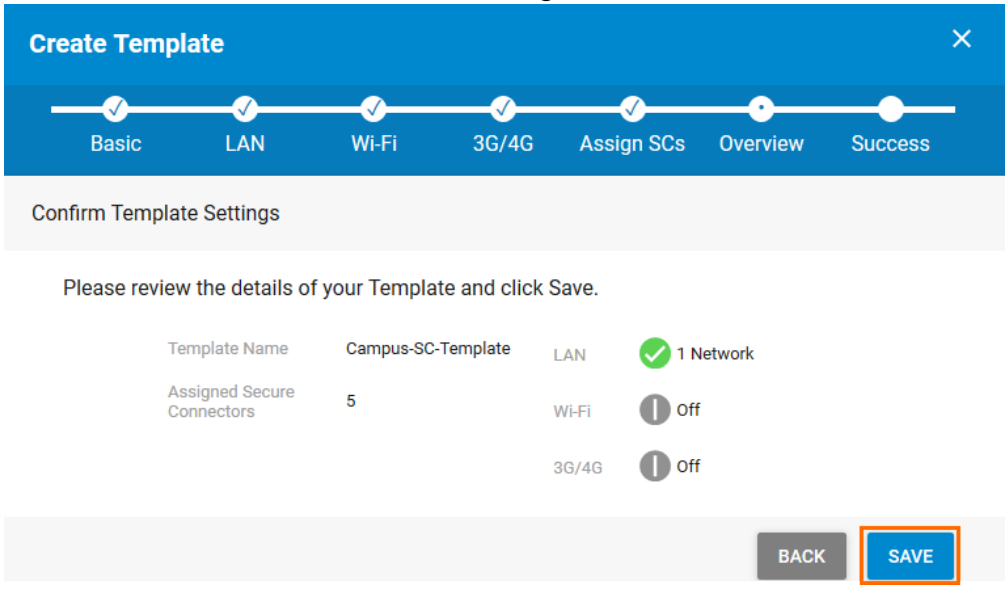


   2. Click **Add missing Secure Connector by Serial/Linking Code** to add Secure Connector devices that are not linked to your ZTD.
      1. **Serial** - Enter the serial number of your Secure Connector.
      2. **Linking Code** - Enter the linking code of your Secure Connector.

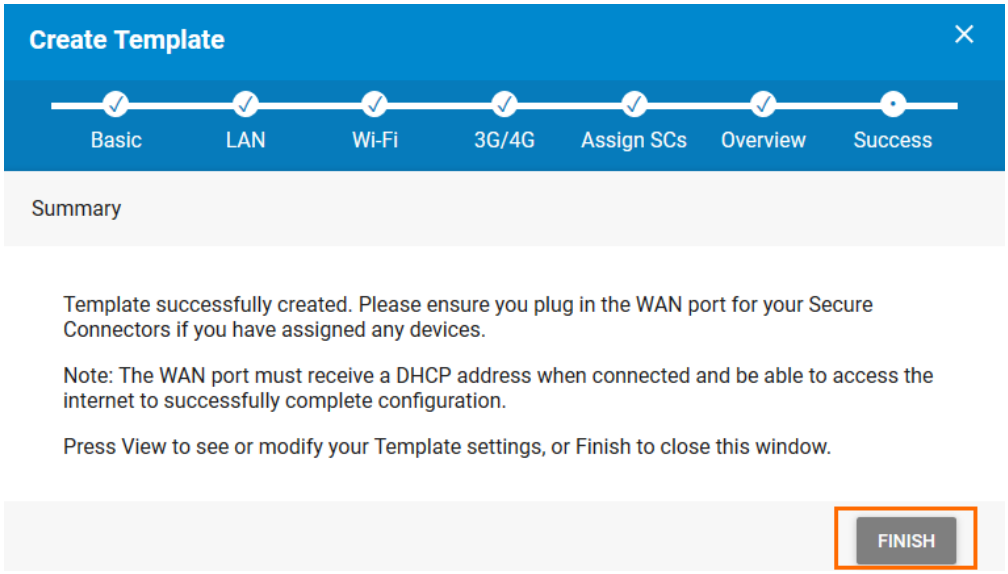


3. Click **NEXT**.

6. In the **Overview** blade, review the configuration and click **SAVE**.



7. Read the notes in the **Success** blade carefully and click **FINISH**.



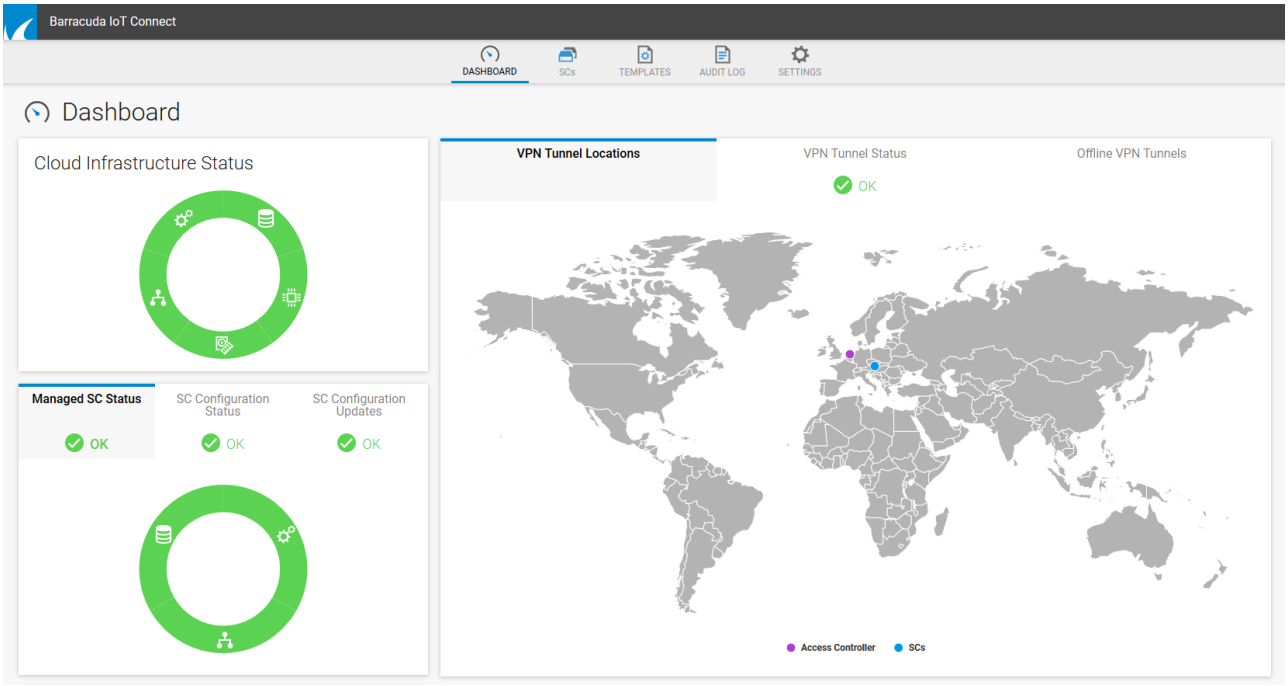
Step 3. Plug in the Secure Connector on Site

1. Plug a network cable of a network with Internet access into the WAN port of your Secure Connector.
2. Plug in the power cable of your Secure Connector.

The Secure Connector now receives its configuration and automatically connect to your IoT Connect infrastructure. After a few minutes, the Secure Connector will appear in your Barracuda IoT Connect **DASHBOARD**.

Step 4. (Optional) Verify that Your Secure Connector Devices Are Connected

1. Go to https://iotc.barracudanetworks.com/.
2. Log in with your credentials.
3. Accept the cookies and you will be forwarded to the IoT Connect **DASHBOARD**.
4. All connected Secure Connector devices appear as a blue dot on the map.



Next Step

Your IoT Connect infrastructure is now ready. Continue with forwarding your data traffic from the Secure Access Controller to your data center.

Figures

1. dashboard.png
2. templates.png
3. basic.png
4. lan.png
5. wifi.png
6. 3g4g.png
7. assign_sc_1.png
8. assign_sc_2.png
9. overview.png
10. success.png
11. iot_connect_dashboard_successfull.png