

## 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](mailto: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

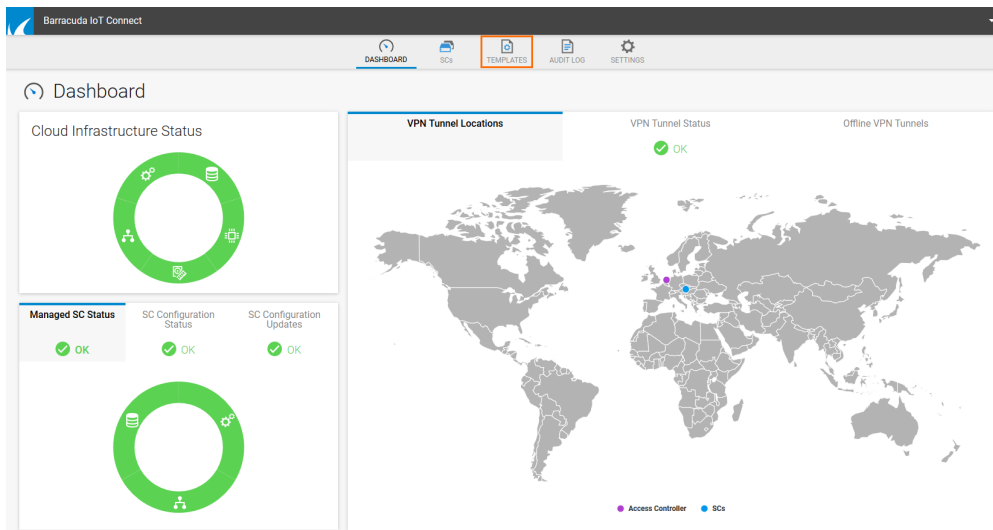
For instructions on the deployment process, follow the step-by-step guide for either Azure or AWS:

- [Deployment of Barracuda IoT Connect in Microsoft Azure](#)
- [Deployment of Barracuda IoT Connect in Amazon AWS](#)

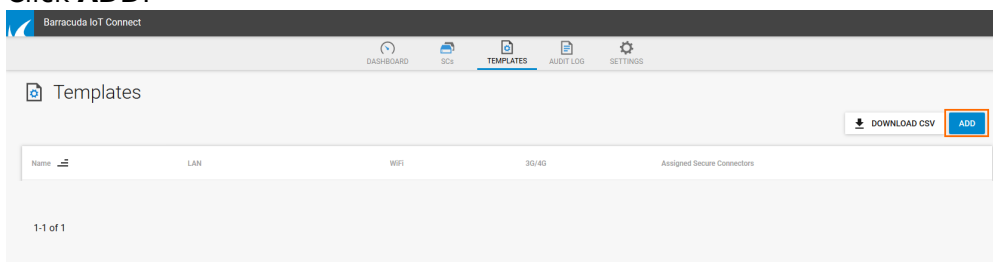
### Step 2. Configure the Secure Connector in the Barracuda IoT Connect Web Interface

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.

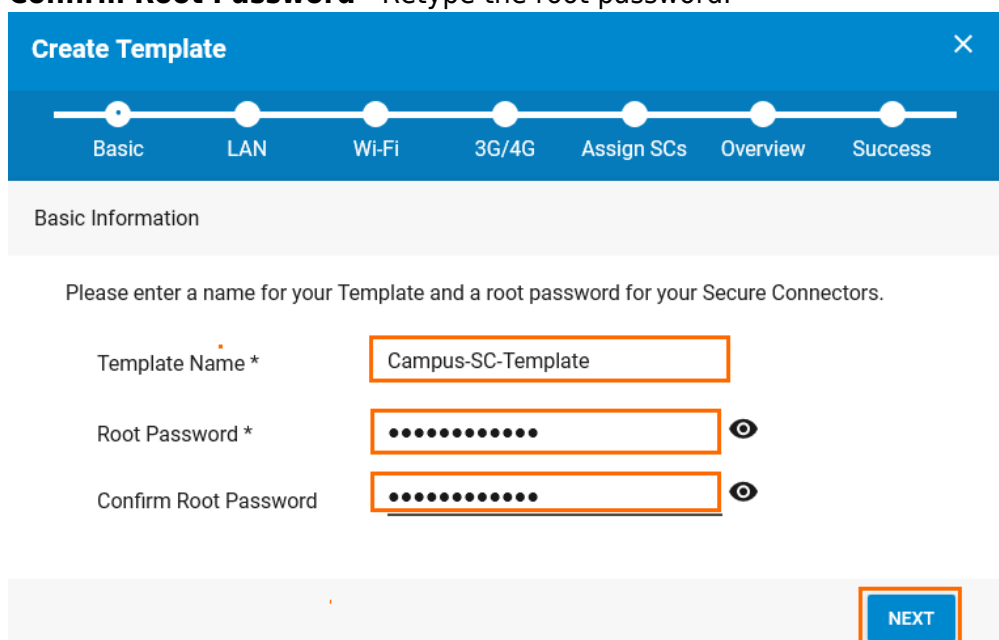
1. Go to <https://iotc.barracudanetworks.com/>.
2. Log in with your credentials.
3. Accept the cookies, and you will be forwarded to the IoT Connect **DASHBOARD**.



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



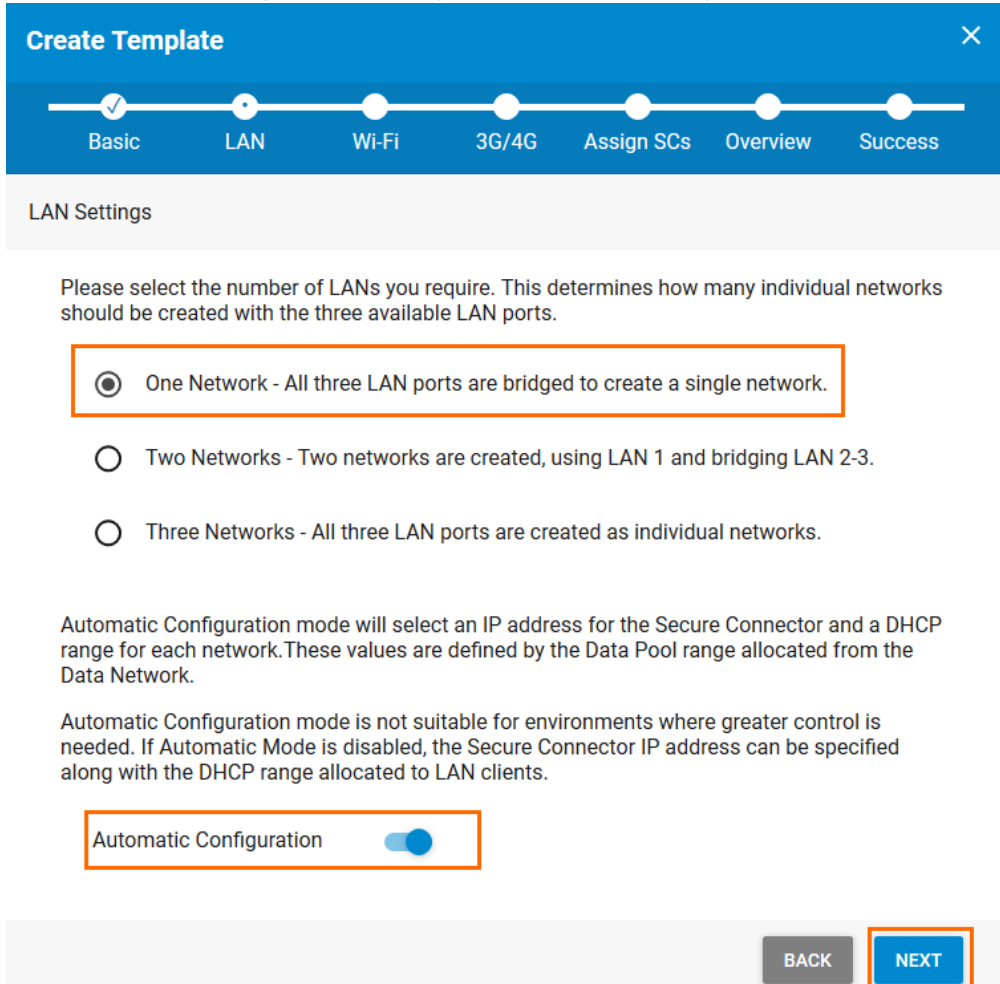
6. The **Create Template** wizard opens.
  1. In the **Basic** blade:
    1. **Template Name** - Enter a name for the template.
    2. **Root Password** - Enter the root password for the Secure Connector devices assigned to this template.
    3. **Confirm Root Password** - Retype the root password.



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.



The screenshot shows the 'Create Template' wizard in the LAN Settings section. A progress bar at the top indicates the current step is 'LAN', with 'Basic' completed and 'Wi-Fi', '3G/4G', 'Assign SCs', 'Overview', and 'Success' remaining. Below the progress bar, the 'LAN Settings' section contains the following text and options:

Please select the number of LANs you require. This determines how many individual networks should be created with the three available LAN ports.

- One Network - All three LAN ports are bridged to create a single network.
- Two Networks - Two networks are created, using LAN 1 and bridging LAN 2-3.
- Three Networks - All three LAN ports are created as individual networks.

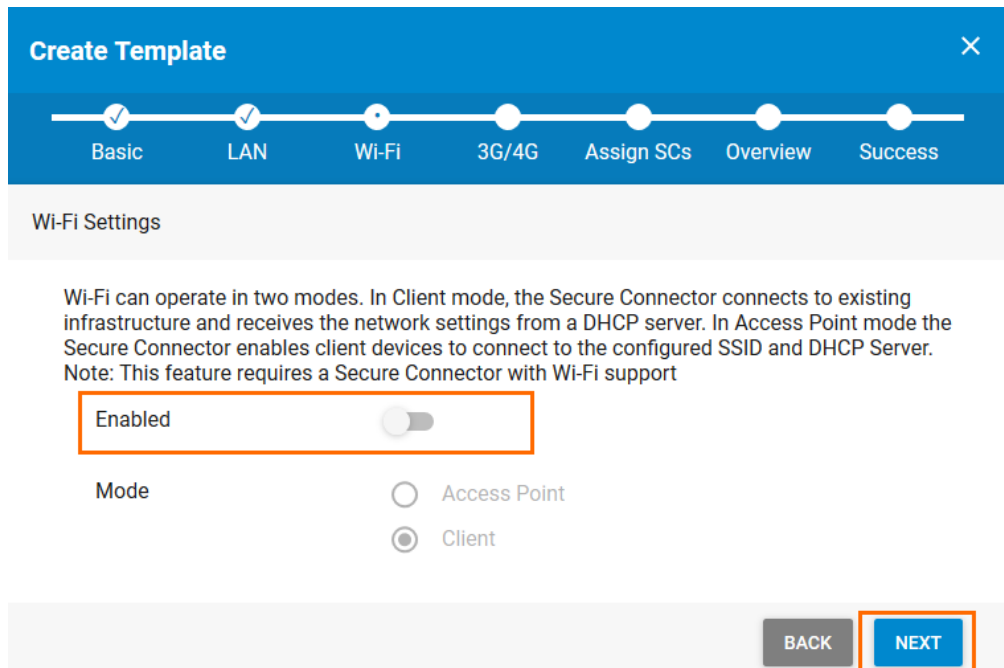
Automatic Configuration mode will select an IP address for the Secure Connector and a DHCP range for each network. These values are defined by the Data Pool range allocated from the Data Network.

Automatic Configuration mode is not suitable for environments where greater control is needed. If Automatic Mode is disabled, the Secure Connector IP address can be specified along with the DHCP range allocated to LAN clients.

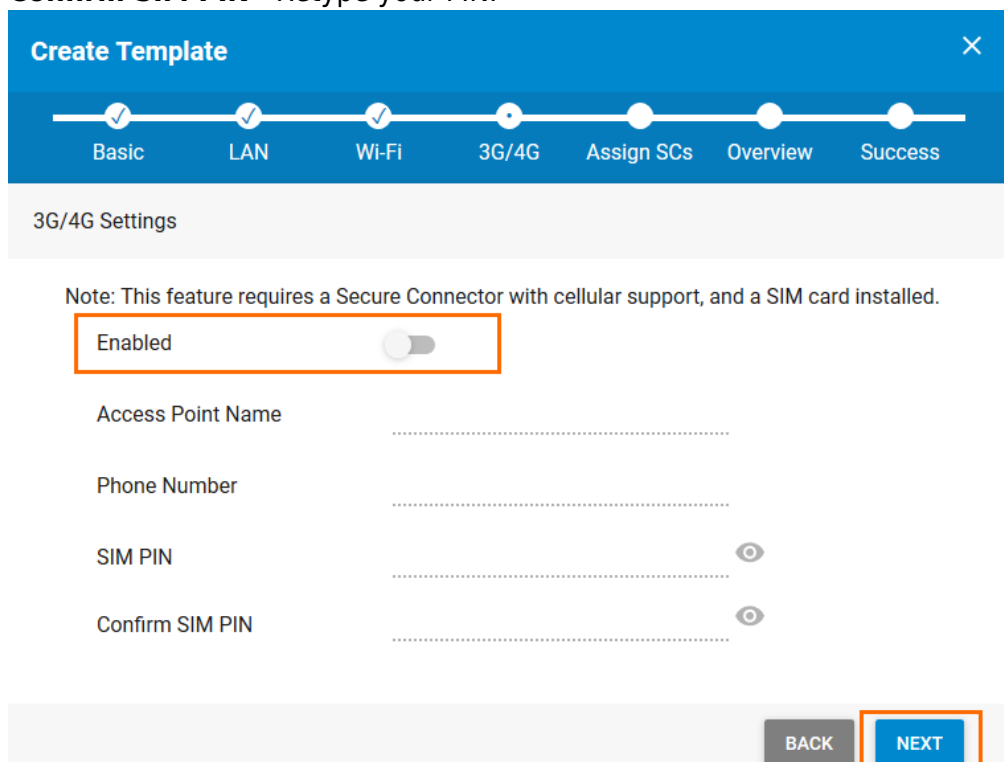
At the bottom of the form, there is a toggle switch for 'Automatic Configuration' which is currently turned on. At the very bottom right, there are 'BACK' and 'NEXT' buttons, with the 'NEXT' button highlighted with an orange border.

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.



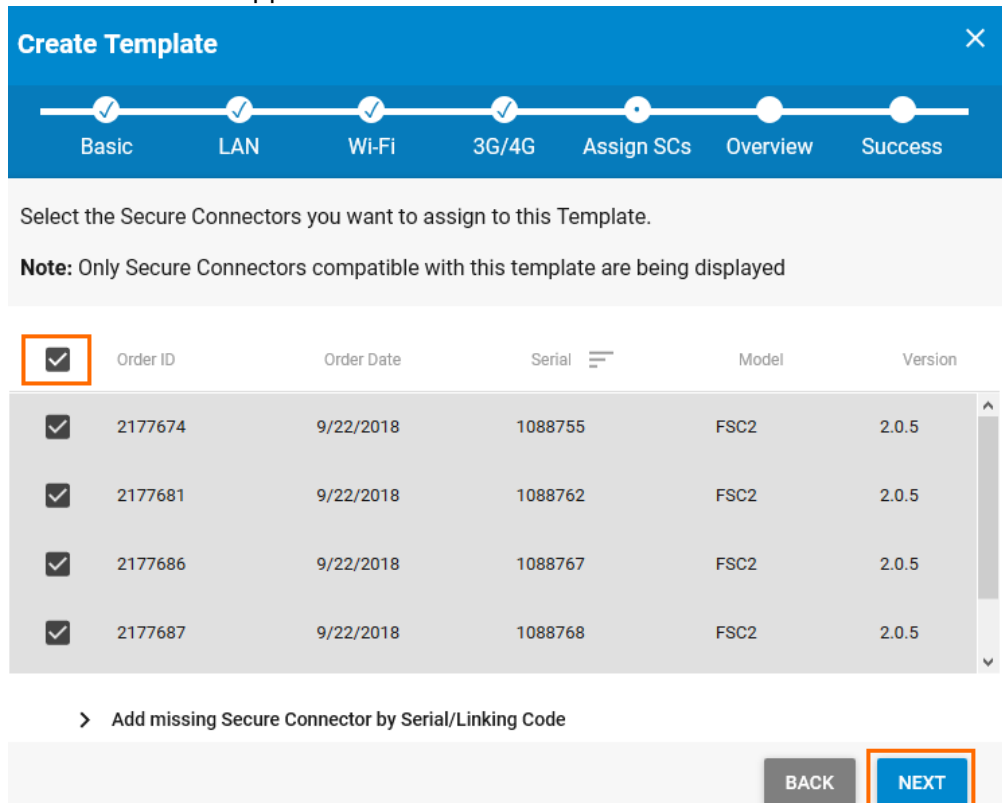
3. Click **NEXT**.
4. In the **3G/4G** blade:
  1. **Enabled** - Enable if you use a Secure Connector with cellular support and an installed SIM card.
  2. **Access Point Name** - Enter the name of your access point.
  3. **Phone Number** - Enter the phone number of the installed SIM card
  4. **SIM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



**Create Template** ✕

Basic LAN Wi-Fi 3G/4G Assign SCs Overview Success

Select the Secure Connectors you want to assign to this Template.

**Note:** Only Secure Connectors compatible with this template are being displayed

<input checked="" type="checkbox"/>	Order ID	Order Date	Serial	Model	Version
<input checked="" type="checkbox"/>	2177674	9/22/2018	1088755	FSC2	2.0.5
<input checked="" type="checkbox"/>	2177681	9/22/2018	1088762	FSC2	2.0.5
<input checked="" type="checkbox"/>	2177686	9/22/2018	1088767	FSC2	2.0.5
<input checked="" type="checkbox"/>	2177687	9/22/2018	1088768	FSC2	2.0.5

> Add missing Secure Connector by Serial/Linking Code

BACK NEXT

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.

### Create Template ✕

✓ ✓ ✓ ✓ ● ● ●  
Basic LAN Wi-Fi 3G/4G Assign SCs Overview Success

Select the Secure Connectors you want to assign to this Template.

**Note:** Only Secure Connectors compatible with this template are being displayed

<input type="checkbox"/>	Order ID	Order Date	Serial	Model	Version
<input type="checkbox"/>	2177674	9/22/2018	1088755	FSC2	2.0.5
<input type="checkbox"/>	2177681	9/22/2018	1088762	FSC2	2.0.5
<input type="checkbox"/>	2177686	9/22/2018	1088767	FSC2	2.0.5
<input type="checkbox"/>	2177687	9/22/2018	1088768	FSC2	2.0.5

▼ Add missing Secure Connector by Serial/Linking Code

These are found on your Barracuda Networks confirmation email

Serial \*

Linking Code \*  ADD

BACK
NEXT

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

### Create Template ✕

✓ ✓ ✓ ✓ ✓ ● ●  
Basic LAN Wi-Fi 3G/4G Assign SCs Overview Success

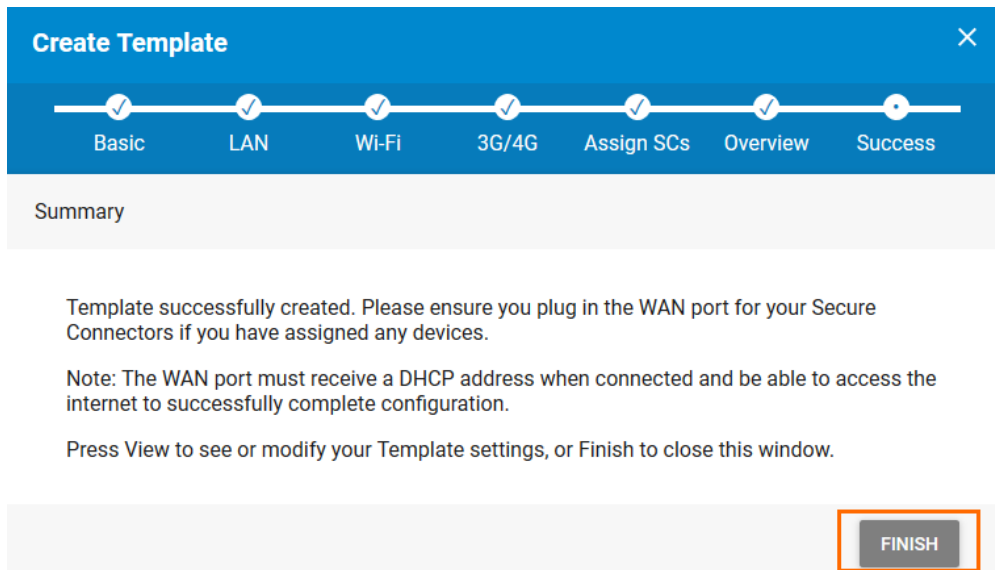
Confirm Template Settings

Please review the details of your Template and click Save.

Template Name	Campus-SC-Template	LAN	<span style="color: green; font-weight: bold;">✓</span> 1 Network
Assigned Secure Connectors	5	Wi-Fi	<span style="border: 1px solid gray; border-radius: 50%; padding: 2px 5px;">1</span> Off
		3G/4G	<span style="border: 1px solid gray; border-radius: 50%; padding: 2px 5px;">1</span> Off

BACK
SAVE

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



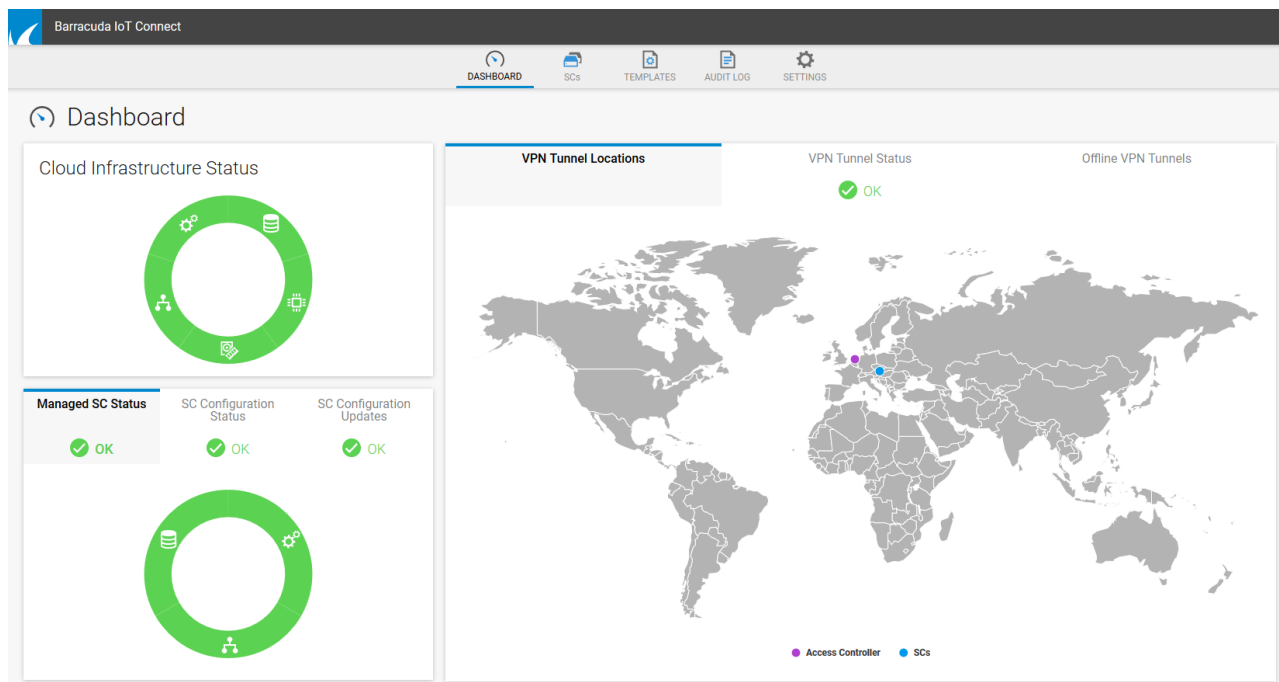
### Step 3. Plug in the Secure Connector on Site

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

© Barracuda Networks Inc., 2020 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.