Setting up ATR for Cisco Meraki Firewall

https://campus.barracuda.com/doc/30183/

What ATR does

ATR determines whether an alert is malicious.

If the alert is identified as malicious, the IP Address is automatically added to the firewall or network security solution block list, depending on how malicious ATR determines it to be.

For more information about Automated Threat Response (ATR), see Setting up ATR.

Setting up ATR

The documentation below outlines the requirements for the Barracuda XDR Automated Threat Response. All action items listed under the Customer Requirements must be completed. All required data must be uploaded to the XDR Dashboard in the **ATR Settings** > **Firewalls** section.

> These instructions are only for customers using a Cisco Meraki Firewall.

To set up ATR for Cisco Meraki Firewall, do the following:

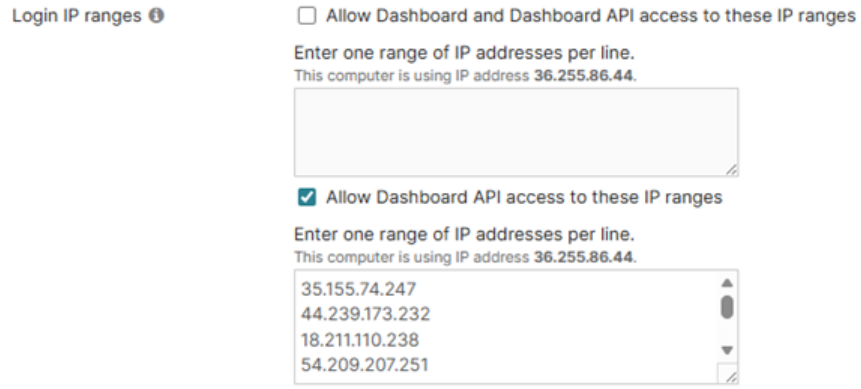
- To enable API Access and generate an API Key from the Meraki Dashboard
- To collect the Organization ID
- To ensure the IP address can make inbound connections to the firewall
- To configure the Barracuda XDR Dashboard

To enable API Access and generate an API Key from the Meraki Dashboard

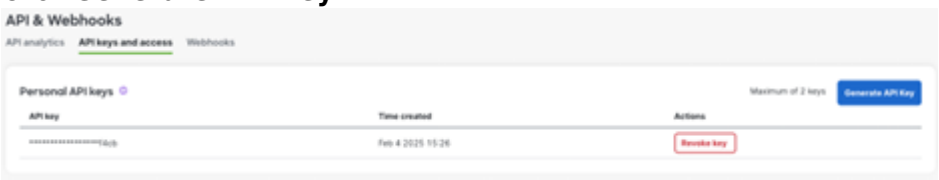
For access to the API, enable the API for your organization.

1. Log in to the Meraki dashboard: https://dashboard.meraki.com.
2. Navigate to **Organization** > **Settings**.
3. Ensure Barracuda's endpoints can make API calls to the Meraki Dashboard by adding the following IPs:
    - 35.155.74.247
    - 44.239.173.232

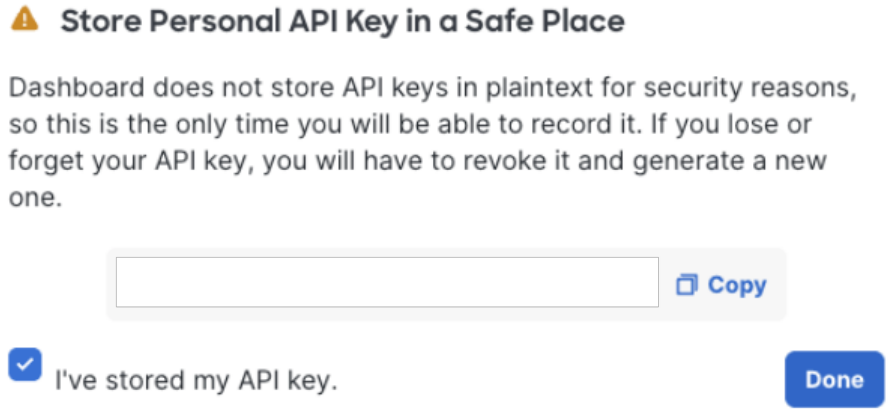
- 18.211.110.238
- 54.209.207.251



4. Navigate to **Organization** > **API & Webhooks** > **API keys & access**.
5. Click **Generate API Key**.



6. Scroll down to **API Access** to generate the API key.
7. Copy, then store the API key in a safe place.

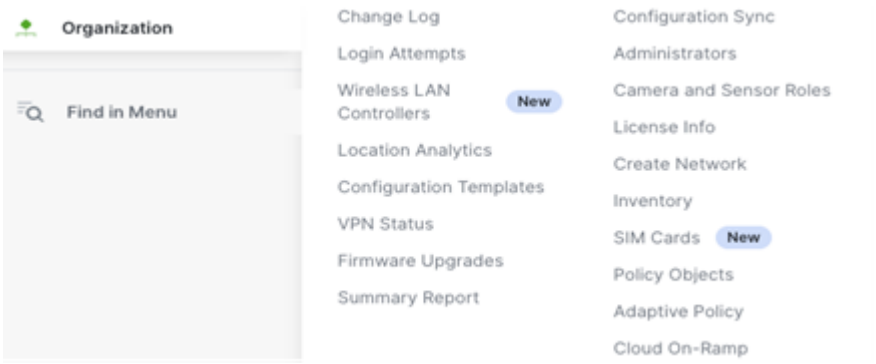


8. Click **Done**.

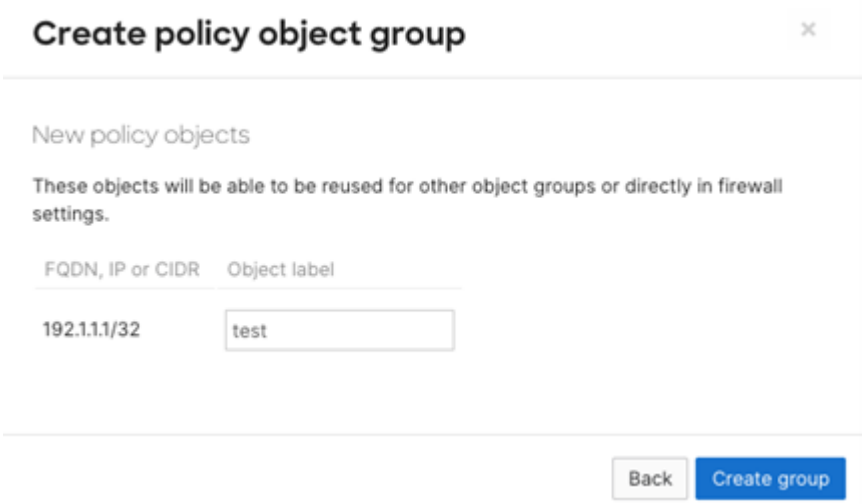
To collect the Organization ID

1. From the Meraki dashboard, from the bottom of the page, copy the **Organization ID** and store it in a safe place.

2. Navigate to **Organization** > **Policy Objects**.

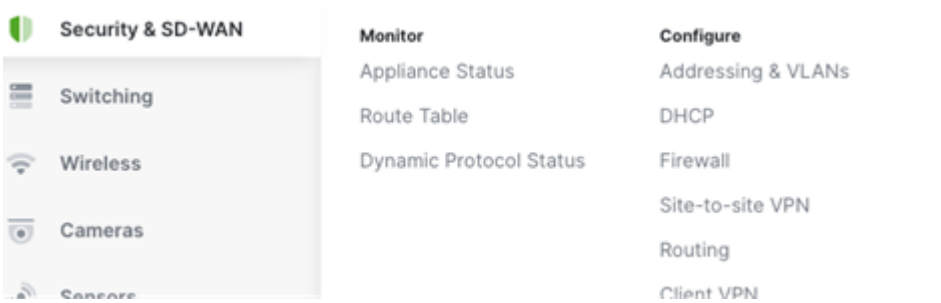


3. Create a new **Policy Object Group**.
4. Add a test IP to this group.
5. In the **Object label** field, type **Test**.
6. Click **Create group**.

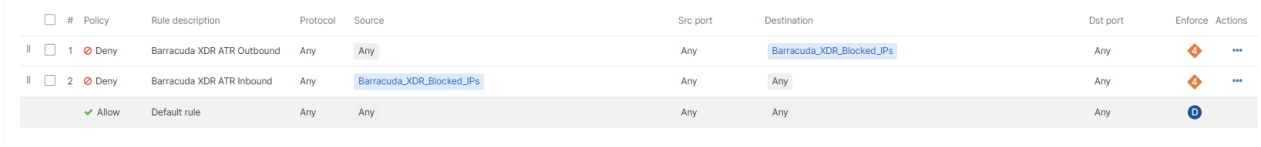


7. In **Group name**, type **Barracuda_XDR_Blocked_IPs**.

8. Click **Next**.
9. Navigate to the appropriate network.
10. Under **Security & SD-WAN**, select **Firewall**.

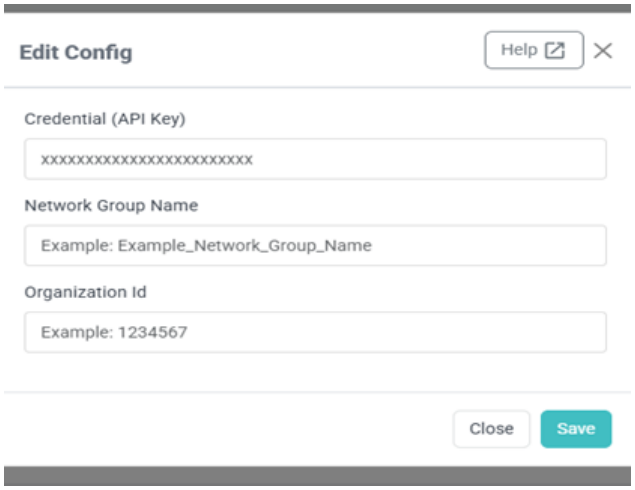


11. Create a new *IPv4 Layer 3 Outbound Rule*. Set the following parameters:
    - **Policy:** *Deny*
    - **Rule Description:** `Barracuda XDR ATR Outbound`
    - **Protocol:** *Any*
    - **Source:** *Any*
    - **Src Port:** *Any*
    - **Destination:** *Type the name of the Policy Object Group you created in the previous procedure.*
    - **Dst Port:** *Any*
12. Create another *IPv4 Layer 3 Outbound Rule*. Set the following parameters:
    - **Policy:** Deny
    - **Rule Description:** `Barracuda XDR ATR Inbound`
    - **Protocol:** Any
    - **Source:***Type the name of the Policy Object Group you created in the previous procedure.*
    - **Src Port:** *Any*
    - **Destination:** *Any*
    - **Dst Port:** *Any*
13. Select **Finish Editing**.
14. Click **Save** at the bottom of the screen.



To configure XDR Dashboard

1. In **Barracuda XDR Dashboard**, click **ATR Settings** > **Firewalls.**
2. In the **Firewalls** table, click the **Meraki Firewall** row.
3. Click **Edit Config**.
4. In the **Edit Config** dialog box, enter the following:
    - **Credential (API Key)**
    - **Network Group Name**
    - **Organization ID**



5. Click **Save**.

If you need to edit the configuration at any time, follow the Editing XDR ATR Settings for a Firewall procedure.

Figures

1. ORGSettings.png
2. APIKEy.png
3. StoreAPIKey.png
4. ORGID.png
5. OrgMenu.png
6. CreatePolicy.png
7. CreatePolicy2.png
8. SelectFirewall.png
9. FinishEditing1.png
10. EditConfig1.png