Setting up SOAR for Cisco Meraki Firewall

https://campus.barracuda.com/doc/104367524/

The documentation below outlines the requirements for the Barracuda XDR Automated Threat Response. All action items listed under the Customer Requirements must be completed and provided to the Barracuda XDR team to set up the integration. All required data will need to be uploaded to the Customer Security Dashboard in the SOAR Settings > Firewalls section. Please note that these instructions are only for customers using a Cisco Meraki Firewall.

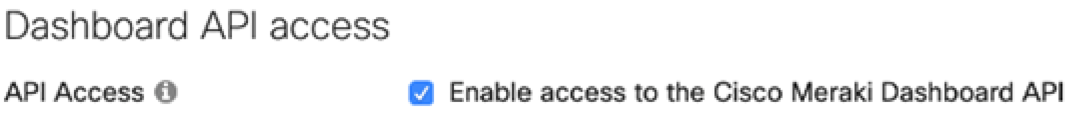
To set up SOAR for Cisco Meraki Firewall, do the following:

- To enable API Access and generate an API Key from the Meraki Dashboard
- To send the Organization ID and the Network ID to the Barracuda XDR team
- To create a Network Group Policy Name
- 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, you must first enable the API for your organization.

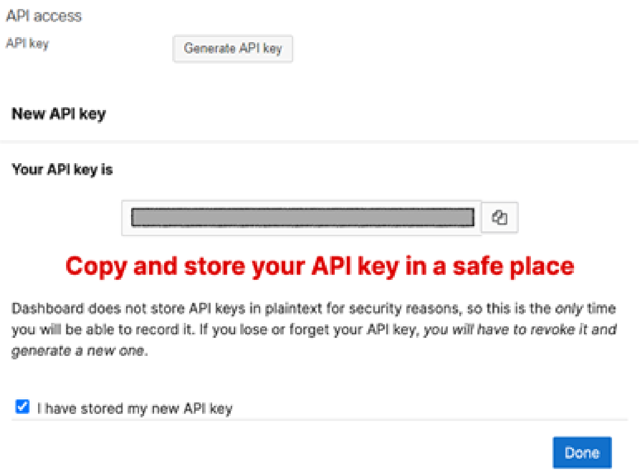
1. Log in to the Meraki dashboard: https://dashboard.meraki.com.
2. Navigate to **Organization** > **Settings**.
3. Ensure the API Access is set to **Enable access to the Cisco Meraki Dashboard API**.



Dashboard API access

API Access ☑ Enable access to the Cisco Meraki Dashboard API

4. After enabling the API, navigate to the profile page by clicking on your account email address in the upper right. Then click **My profile**.
5. Scroll down to **API Access** to generate the API key.
6. Copy, then store the API key in a safe place. Click **Done**.
7. Send this API Key to the Barracuda XDR team.



API access

API key

New API key

Your API key is

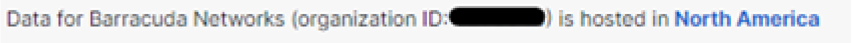
[redacted]

Copy and store your API key in a safe place

Dashboard does not store API keys in plaintext for security reasons, so this is the *only* time you will be able to record it. If you lose or forget your API key, *you will have to revoke it and generate a new one.*

☑ I have stored my new API key

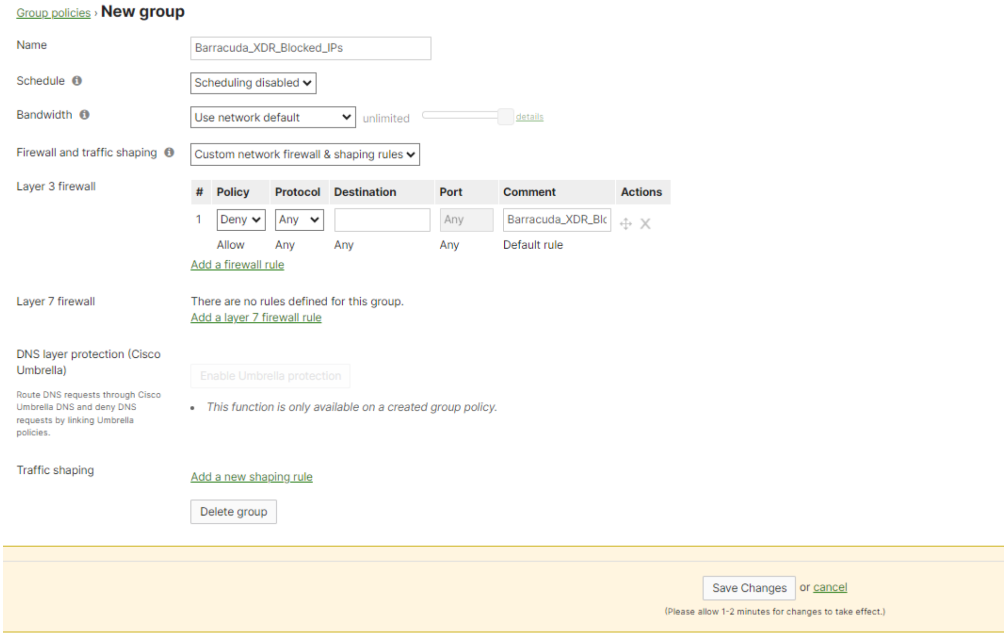
To send the Organization ID and the Network ID to the Barracuda XDR team

1. From the Meraki dashboard, from the bottom of the page, copy the **Organization ID**.
   
   Data for Barracuda Networks (organization ID:[redacted]) is hosted in North America
2. From the Meraki dashboard, copy the ID of the network.
   For more information on finding the network ID, see the Meraki documentation.
3. Send both IDs to the Barracuda XDR team.

To create a Network Group Policy Name

Name the **Network Group Policy** “Barracuda_XDR_Blocked_IPs”. Give the **Network Group Policy ID** to the Barracuda XDR team. Barracuda XDR uses the Group Policy to automatically blocking IPs on the firewall.

1. In the Meraki dashboard, navigate to **Network-wide** > **Configure** > **Group policies**.
2. Click **Add a group** to create a new policy.
3. Do the following:
   1. In **Name**, type `Barracuda_XDR_Blocked_IPs`.
   2. In **Schedule**, select **Scheduling disabled**.
   3. In **Bandwidth**, select **Use network default**.
   4. In **Firewall and traffic shaping**, select **Custom network & shaping rules**.



Group policies › **New group**

Name	Barracuda_XDR_Blocked_IPs
Schedule	Scheduling disabled
Bandwidth	Use network default · unlimited · details
Firewall and traffic shaping	Custom network firewall & shaping rules

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	Any		Any	Barracuda_XDR_Blc	✣ ✕
	Allow	Any	Any	Any	Default rule	

Add a firewall rule

Layer 7 firewall

There are no rules defined for this group.
Add a layer 7 firewall rule

DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Enable Umbrella protection

- *This function is only available on a created group policy.*

Traffic shaping

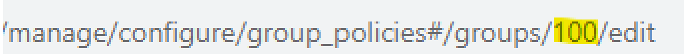
Add a new shaping rule

Delete group

Save Changes or cancel

(Please allow 1-2 minutes for changes to take effect.)

4. Click **Save Changes**.
5. Copy the **Group Policy ID** from the URL at the top of the **Group Policies** page.



'manage/configure/group_policies#/groups/100/edit

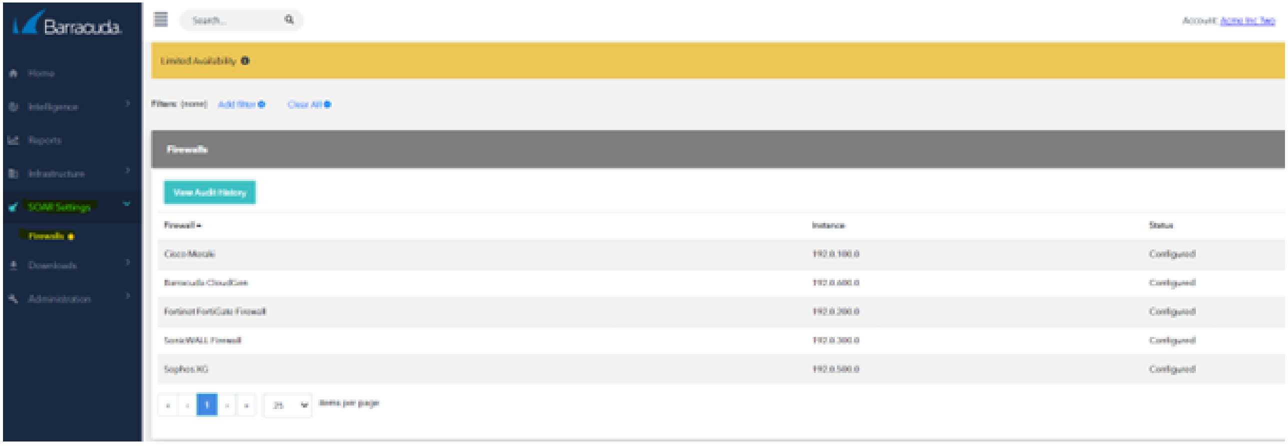
6. Send the **Network Group Policy Name** and **Network Group Policy ID** to the Barracuda XDR team.

To ensure the IP address can make inbound connections to the firewall

- 44.209.49.222 is the static address of Barracuda XDR's SOAR platform Barracuda XDR authenticates from this IP to remediate threats. Ensure that 44.209.49.222 can make inbound connections to the firewall.

To configure the Barracuda XDR Dashboard

1. In **Barracuda XDR Dashboard**, click **SOAR Settings** > **Firewalls.**

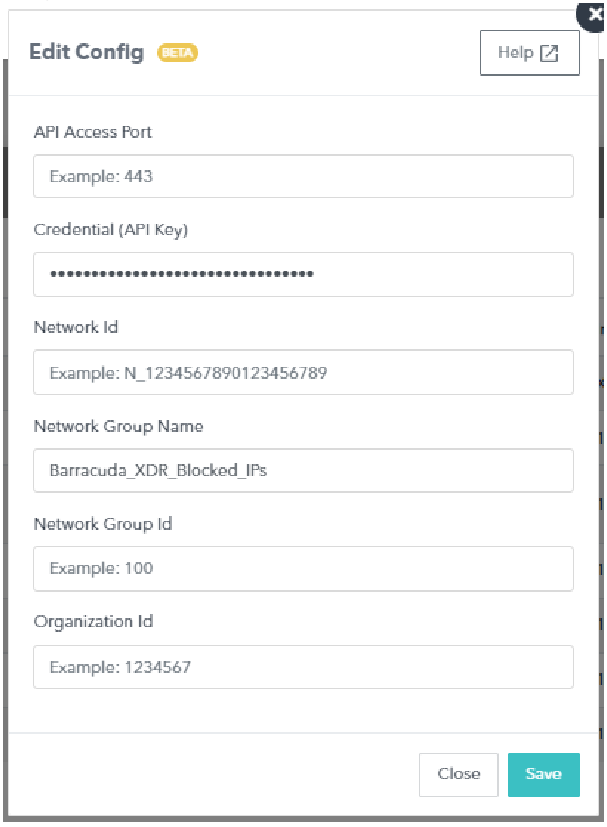


Firewalls

Firewall ▴	Instance	Status
Cisco Meraki	192.0.100.0	Configured
Barracuda CloudGen	192.0.600.0	Configured
Fortinet FortiGate Firewall	192.0.200.0	Configured
SonicWALL Firewall	192.0.300.0	Configured
Sophos XG	192.0.500.0	Configured

2. Click **Config**.
3. In the **Edit Config** dialog box, enter the following:

- **API Access Port**
- **External IP**
- **Network ID**
- **Network Group Name**
- **Network Group ID**
- **Organization ID**



Edit Config BETA

API Access Port: Example: 443

Credential (API Key): ••••••••••••••••••••••••••••••••

Network Id: Example: N_1234567890123456789

Network Group Name: Barracuda_XDR_Blocked_IPs

Network Group Id: Example: 100

Organization Id: Example: 1234567

4. Click **Save**.

Figures