

Configuring Cisco Meraki

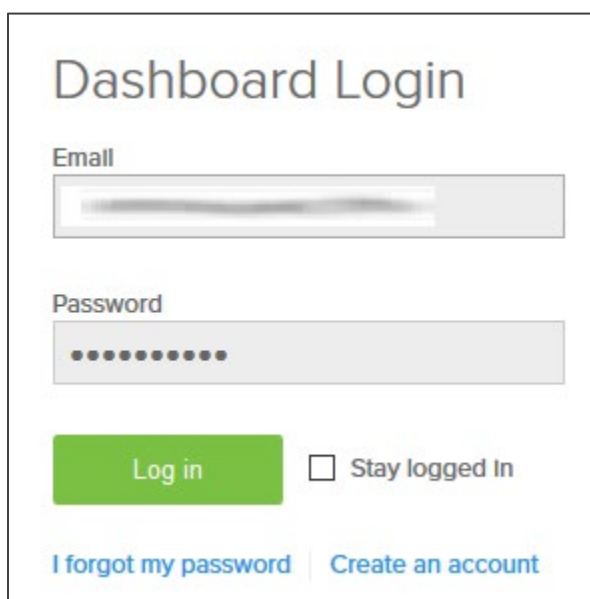
Configuring Cisco Meraki for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Cisco Meraki by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure Cisco Meraki for SSO by using SAML:

1. In a browser, type <https://meraki.cisco.com/> and press **Enter**.
2. Type your Cisco Meraki admin account credentials (**Email** and **Password**) and click **Log in**.



Dashboard Login

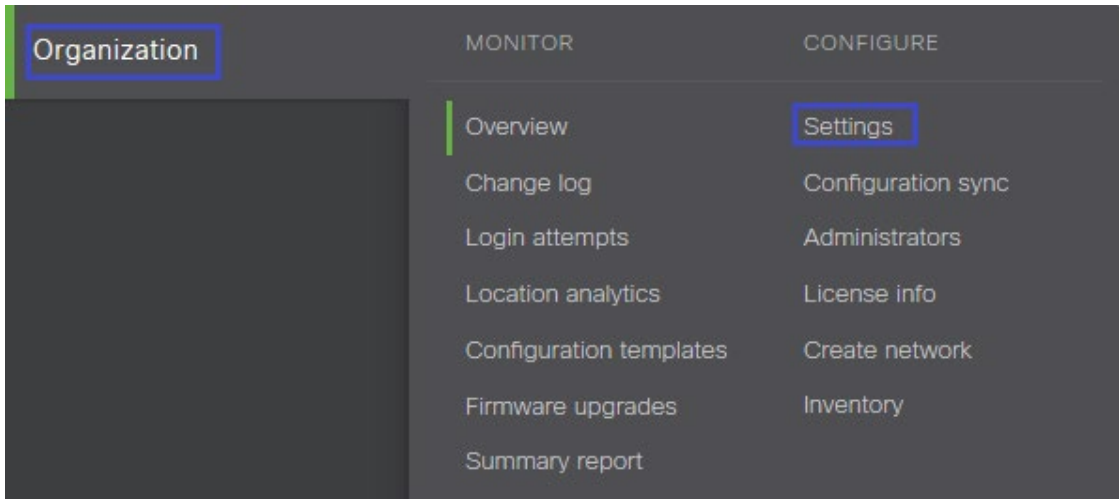
Email

Password

Stay logged in

[Log in](#) [I forgot my password](#) [Create an account](#)

3. In the left panel, navigate to **Organization** > **CONFIGURE**, and select **Settings**.



4. In the **SAML Configuration** section, select **SAML SSO enabled** from the drop-down menu of **SAML SSO** and enter the values for the following fields.

Field Name	Description
Consumer URL	Consumer URL
X.509 cert SHA1 fingerprint	Copy and paste the IdP certificate fingerprint from the https://www.samltool.com/fingerprint.php link, select SHA1 Algorithm and CALCULATE FINGERPRINT

SAML Configuration

SAML SSO ⓘ SAML SSO enabled ▾

Consumer URL ⓘ **https://n240.meraki.com/saml/login/**

X.509 cert SHA1 fingerprint ⓘ

SLO logout URL (optional) ⓘ

[Add a SAML IdP](#)

5. In the **Dashboard API access** section, select the **Enable access to the Cisco Meraki Dashboard API** check box.

Dashboard API access

API Access ⓘ Enable access to the Cisco Meraki Dashboard API

After enabling the API here, go to your [profile](#) to generate an API key. The API will return 404 for requests with a missing or incorrect API key.

Delete this organization

You can delete this organization only if it has no networks, users, licenses, or devices claimed in its inventory.

Delete organization

Save Changes or [cancel](#).

6. Finally, click **Save Changes**.