

Last Modified: May 02, 2017

Cisco Meraki is a cloud managed IT company. Their solutions include wireless, switching, security, EMM, communications, and security cameras, all centrally managed from the web. Meraki was acquired by Cisco Systems in December of 2012. Cisco Meraki supports auto-provisioning of the user feature.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Cisco Meraki.
- Obtain SP metadata details from the Service Provider.
- Obtain IdP metadata from IDR portal.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

| | |
|-----------------------------------|---|
| SP Login URL | https://account.meraki.com/secure/login/dashboard_login |
| ACS URL | https://n70.meraki.com/saml/login/C3uaka/2RcReaSIqFdd |
| Service Provider Issuer ID | https://dashboard.meraki.com/ |

Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Cisco Meraki to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Cisco Meraki.



Cisco Meraki
SAML Direct



3. On the Basic Information page, specify the application name and click **Next Step**.

The screenshot shows the 'Edit Connection' page for a Cisco Meraki application. The page title is 'Cisco Meraki'. On the left, there is a sidebar with 'Edit Connection' (Type: Cisco Meraki) and a list of steps: 1. Basic Information (selected), 2. Connection Profile, 3. User Access, and 4. Portal Display. The main content area is titled 'Basic Information' and contains the following fields: 'Name' (text input with 'Cisco Meraki'), 'Description (optional)' (text area), and a 'Disabled' checkbox. At the top right and bottom right of the main content area are 'Cancel' and 'Next Step' buttons. A message at the top states 'All fields are required (except where noted)'.

4. Navigate to **Initiate SAML Workflow** section.
 - a. In the **Connection URL** field, keep the field blank as the value is not required.
 - b. Choose **IDP-initiated**.

Note: Cisco Meraki application only supports IdP-initiated SSO scenario as of now.

Initiate SAML Workflow

Connection URL

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

No certificate loaded

Choose File

Generate Cert Bundle

5. Scroll down to **SAML Identity Provider (Issuer)** section.

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): 6imt198ktjjq

Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded

?

Certificate Loaded

CN=gslab.com, Valid Until:
08/09/2020

Include Certificate in Outgoing Assertion

- Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
- Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
- Select **Choose File** and upload the private key.
- Select **Choose File** to import the public signing certificate.
- Select the checkbox for **Include Certificate in Outgoing Assertion**.

6. Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://n70.meraki.com/saml/login/<UNIQUE_ACCOUNT_ID>

Audience (Service Provider Entity ID) ?

https://dashboard.meraki.com

- In the **Assertion Consumer Service (ACS) URL** field, replace <UNIQUE_ACCOUNT_ID> value with your organization account value.
 - In the **Audience (Service Provider Issuer ID)** field, provide the value as per received with service provider metadata.
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

User Identity ?

NameID

Identifier Type

unspecified

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

8. Moving next, select **Show Advanced Configuration**. In the **Attribute Extension** section, add **username, role**. These are mandatory provisioning attributes needs to be forwarded at the time of SSO.

Attribute Extension ?

| Attribute Source | Attribute Name | Identity Source | Property | Manage |
|------------------|----------------|-----------------|------------|--------|
| Identity Sc | username | AD20 | mail | |
| Identity Sc | role | AD20 | employeeTy | |
| + ADD | | | | |

9. Click **Next Step**.

10. On the **User Access** page, select **Allow All Authenticated Users** user policy from the available options.

Access Policy

Select the access policy to determine which users are allowed to access the application.


Allow All Authenticated Users

Select Custom Policy ?

No Access Allowed ▼

11. Click **Next Step**.
12. On the **Portal Display** page, select **Display in Portal**.
13. Click **Save and Finish**.
14. Click **Publish Changes**. Your application is now enabled for SSO.

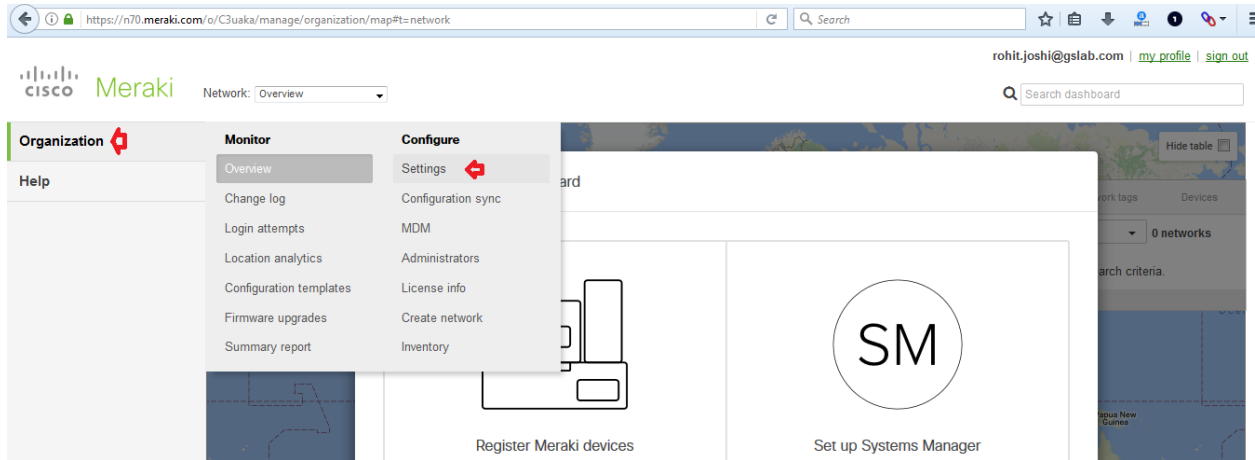
Publish Changes

Status:  Changes Pending

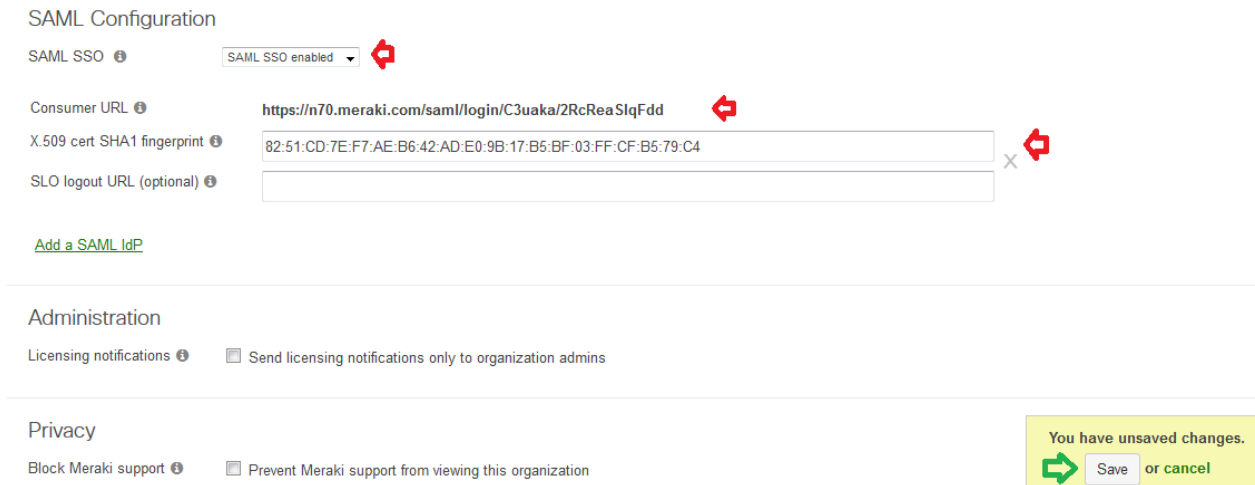
Configure Cisco Meraki to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to your Cisco Meraki application web account.
(https://account.meraki.com/secure/login/dashboard_login)
2. Following UI will be displayed. Go to *Organization* → *Settings*.

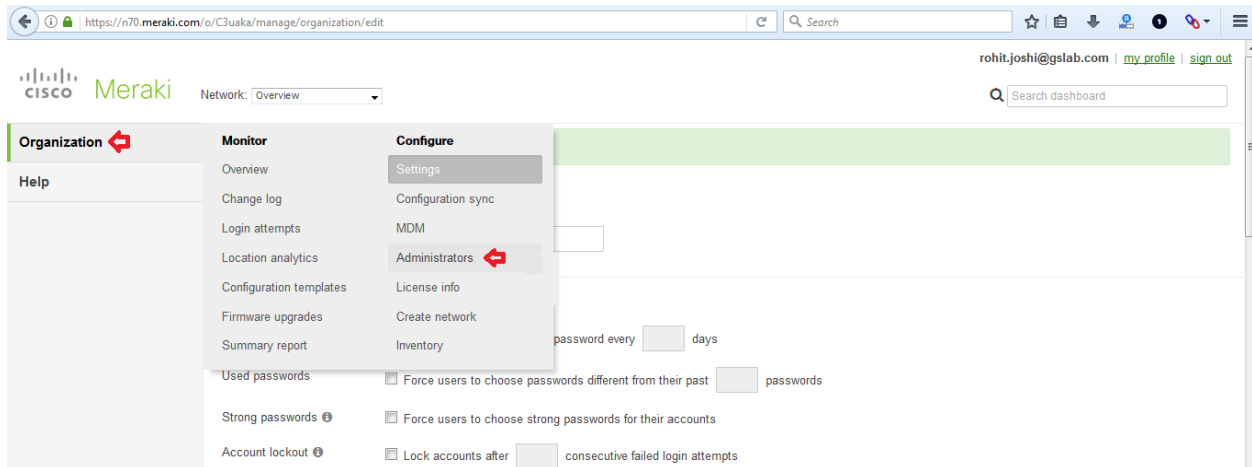


3. Following UI will be displayed. Navigate to *SAML Configuration*.



- a. Select **SAML SSO enabled** option in front of **SAML SSO** field.
- b. Make a note the value of **Consumer URL** as it will be handy during IdP side configurations (During fresh SAML configuration this value won't be available. This value gets generated after completion of SAML settings).
- c. **X.509 cert SHA1 fingerprint** : Paste here SHA1 fingerprint of RSA SecurID Admin's public certificate separated by `:`.
- d. Once sure of settings, click on **Save** button to complete configuration changes.

- Cisco Meraki requires user to manually add role for their organization to identify them correctly during SAML authentication and to grant proper access rights. To do so, again go to home page of the account. Following UI will be displayed. Go to *Organization* → *Administrators*.



- Following UI will be displayed. Click on **Add SAML role** button under **SAML administrator roles** option.

RSA administrators

Force logout | Unlock | Delete | Search admins... | Add admin

| Name | Email address | Privilege | Account status | Two-factor authentication | Last active |
|-------------|-----------------------|--------------|----------------|---------------------------|---|
| Rohit Joshi | rohit.joshi@gslab.com | Organization | Ok | Off | Thu Apr 27 2017 15:06:43 GMT+0530 (India Standard Time) |

SAML administrator roles

SAML login history

Delete | Search SAML roles... | Add SAML role

| Role | Privilege |
|------|-----------|
| | |

- Following pop-up appears. Specify proper **Role** and their **Organization access** rights followed by clicking on **Create role** button.
For ex. You can add **Admin** role with **Full** Organization access.

Create role [X]

Role: [↩]

Organization access: [↩]

| Target | Access |
|--------|--------|
| | |

[+ Add access privileges](#)

[privacy](#) [Close] [Create role]

- Following UI is displayed now which shows the roles and access rights added in last *step* - 6. Click on **Save changes** button once sure of details and roles will get saved for organization.

SAML administrator roles

[SAML login history](#)

Delete Search SAML roles... Add SAML role

| Role | Privilege |
|-------|---------------------|
| Admin | Organization |
| User | Organization (Read) |

[Save changes] or [cancel]

- Your Cisco Meraki account is now enabled for SAML SSO authentication.