RSA SecurID Access SAML Configuration for Cisco Meraki

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

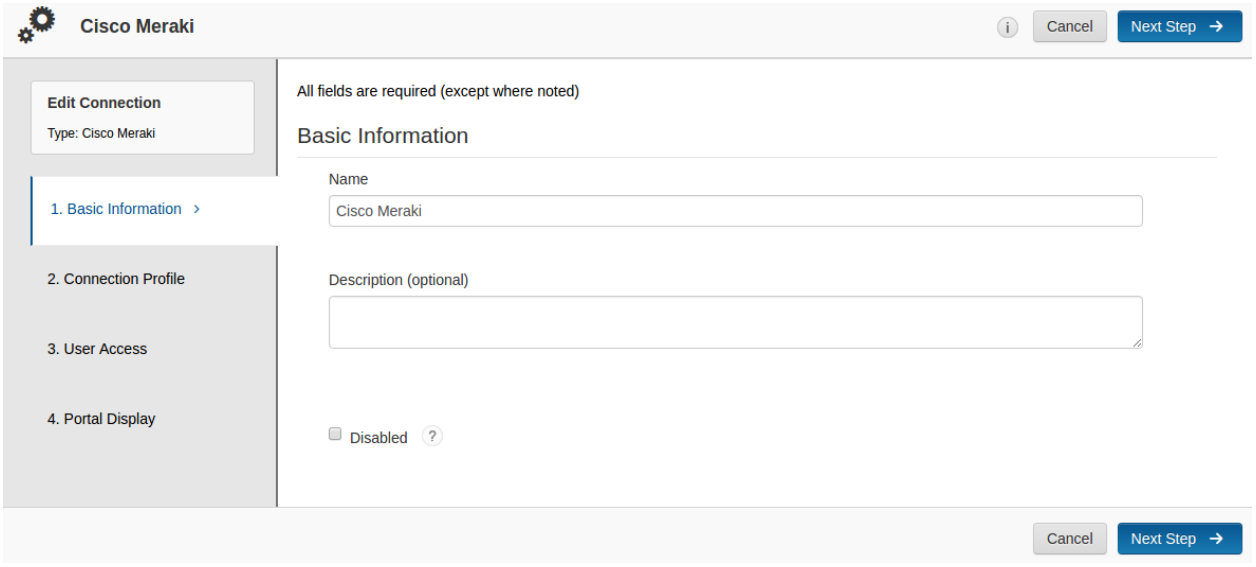
1. Add the Application in RSA SecurID Access
2. Configure Cisco Meraki to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

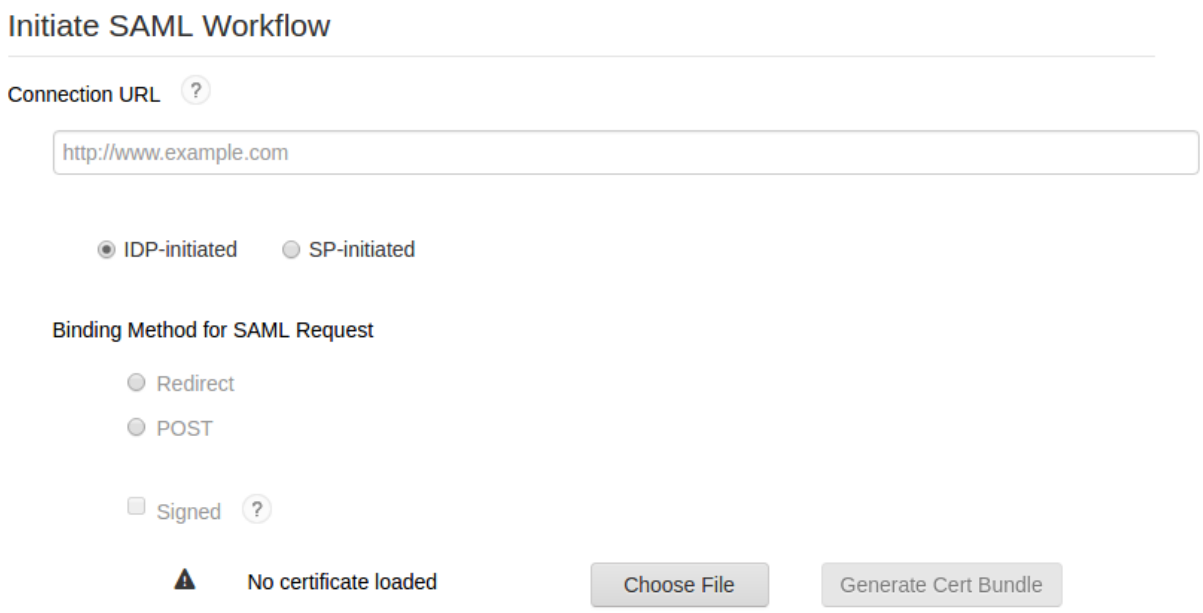
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Cisco Meraki.

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

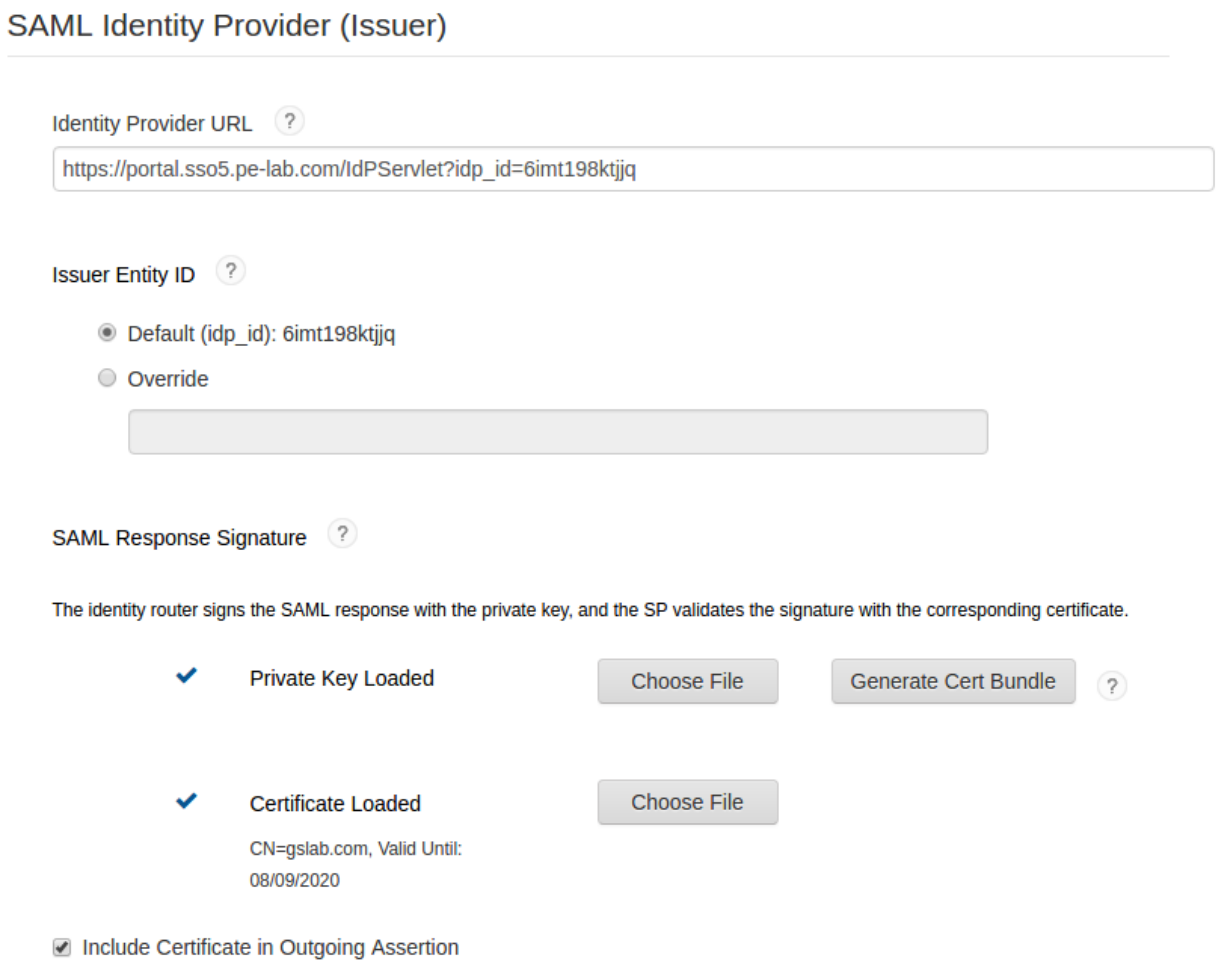


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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

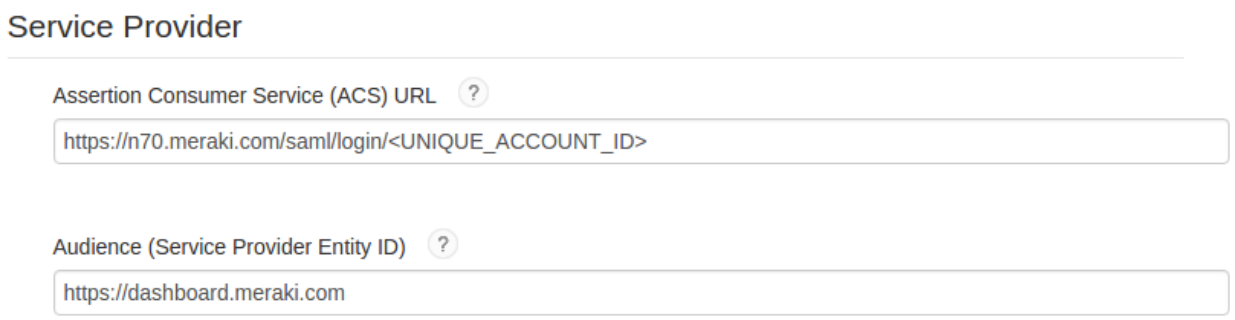


5. Scroll down to **SAML Identity Provider (Issuer)** section.



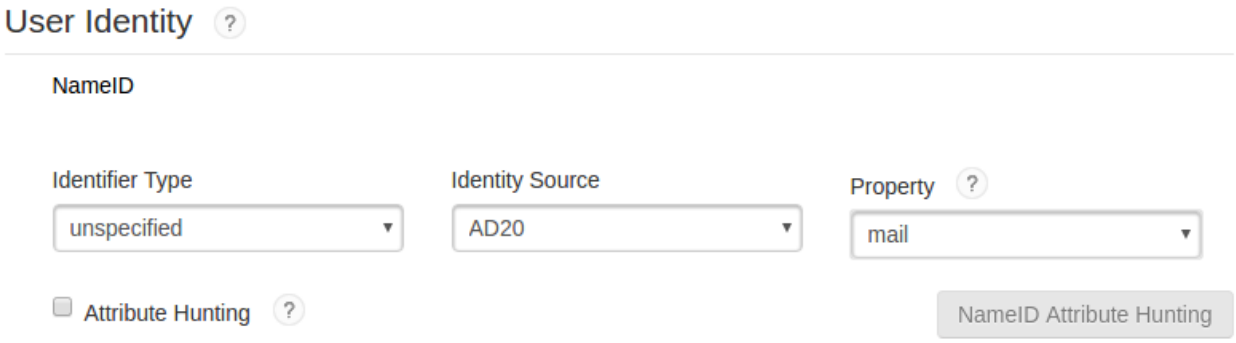
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File**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

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

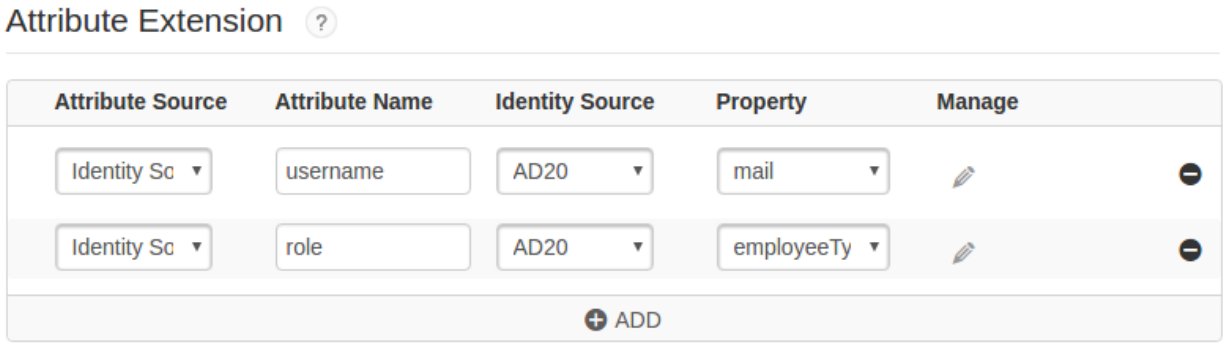


   a. In the **Assertion Consumer Service (ACS) URL** field, replace <UNIQUE_ACCOUNT_ID> value with your organization account value.
   b. In the **Audience (Service Provider Issuer ID)** field, provide the value as per received with service provider metadata.

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.

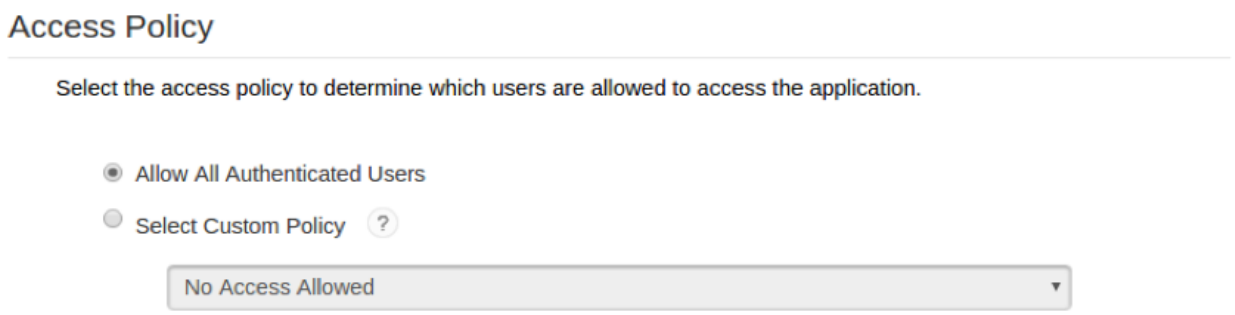


8. Moving next, select **Show Advanced Configuration**. In the **Attribute Extension** section, add **username, role**. These are mandatory provisioning attributes needs to be forwarded at the time of SSO.

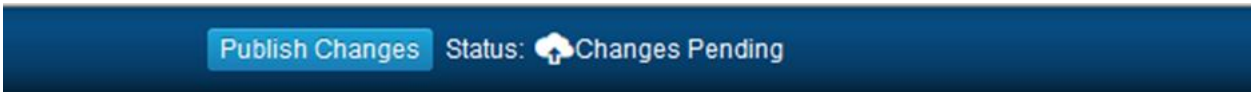


9. Click **Next Step**.

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



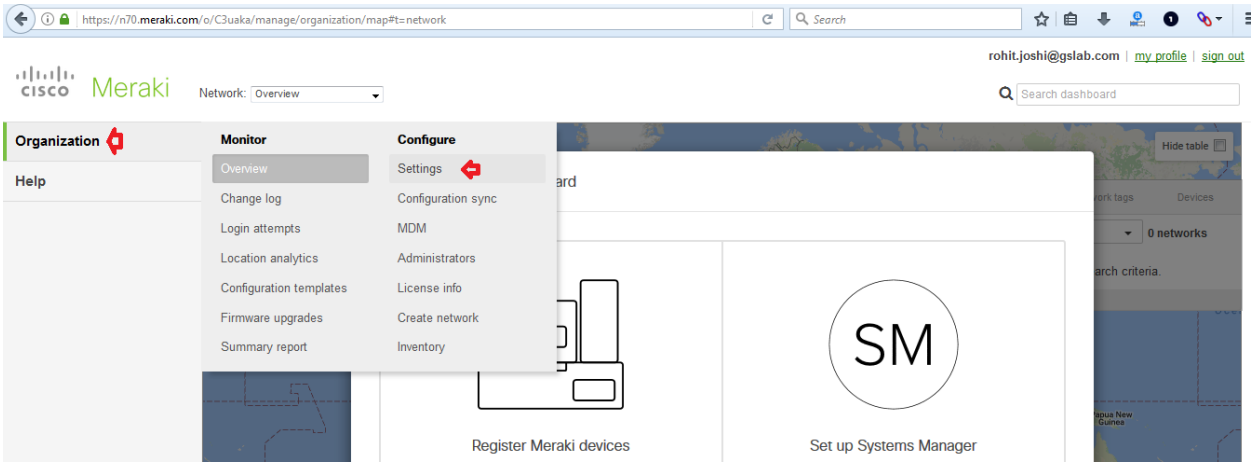
11. Click **Next Step**.
12. On the **Portal Display** page, select **Display in Portal**.
13. Click **Save and Finish**.
14. Click **Publish Changes**. Your application is now enabled for SSO.



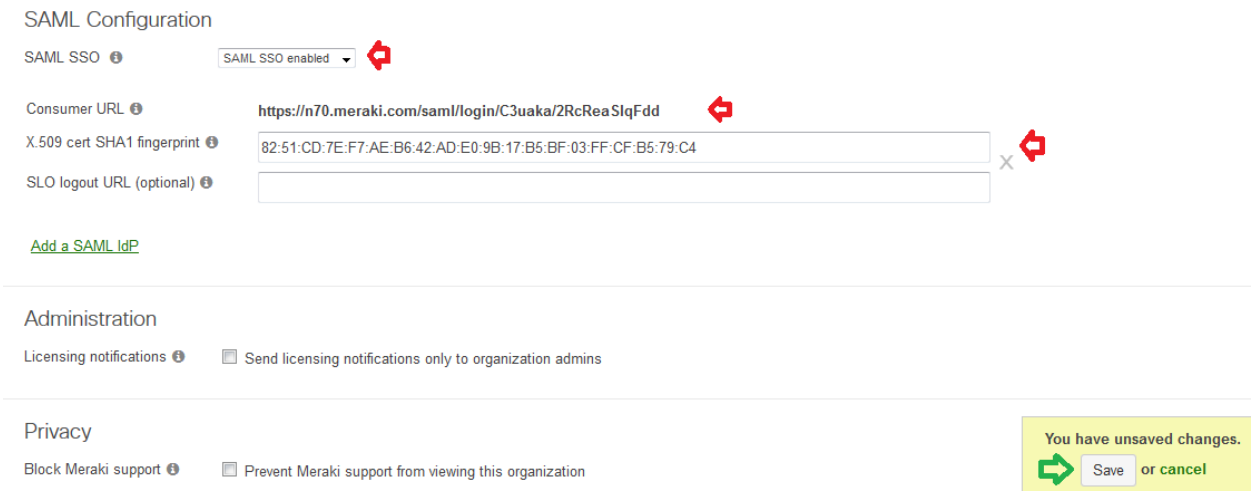
Procedure

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*.

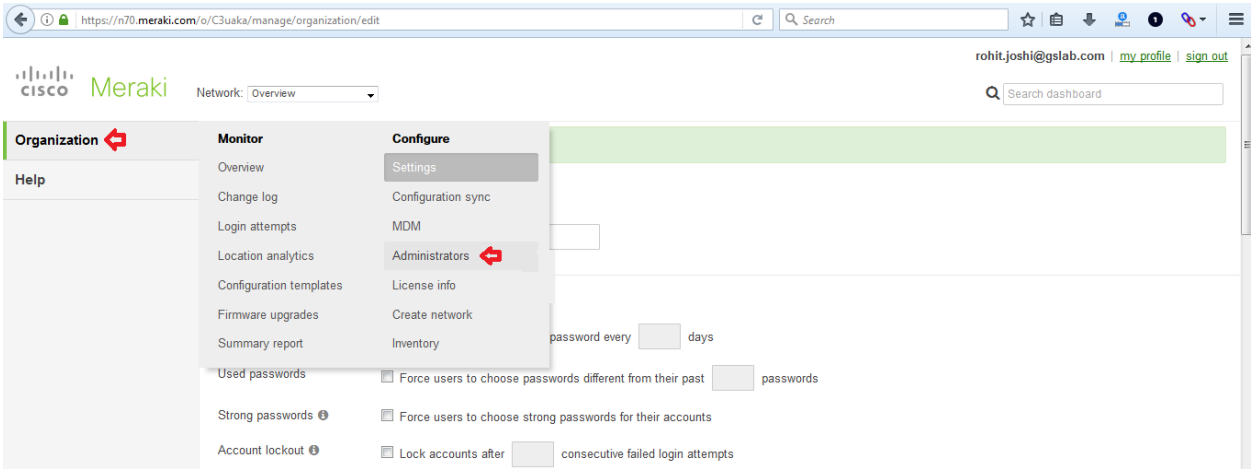


3. Following UI will be displayed. Navigate to *SAML Configuration.*

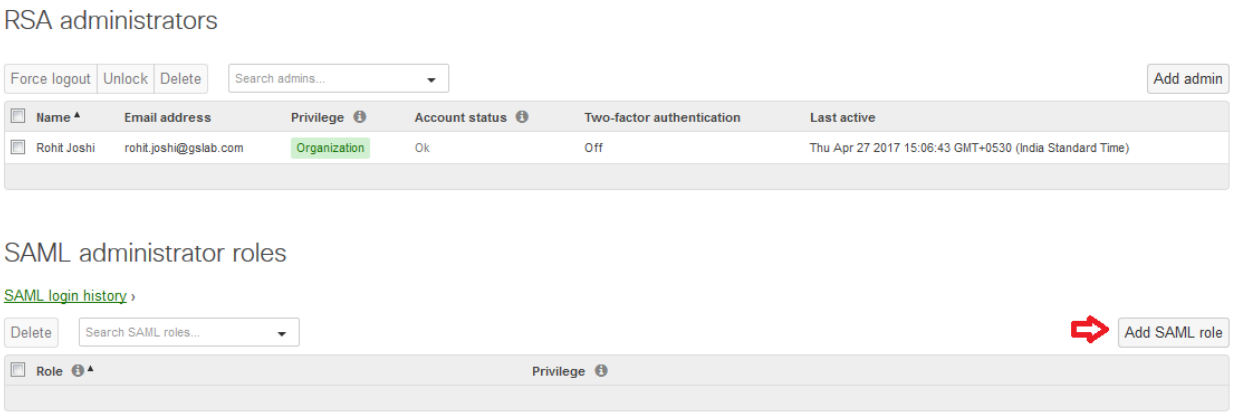


   a. Select **SAML SSO enabled** option in front of **SAML SSO** field.
   b. Make a note the value of **Consumer URL** as it will be handy during IdP side configurations (During fresh SAML configuration this value won't be available. This value gets generated after completion of SAML settings).
   c. **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.

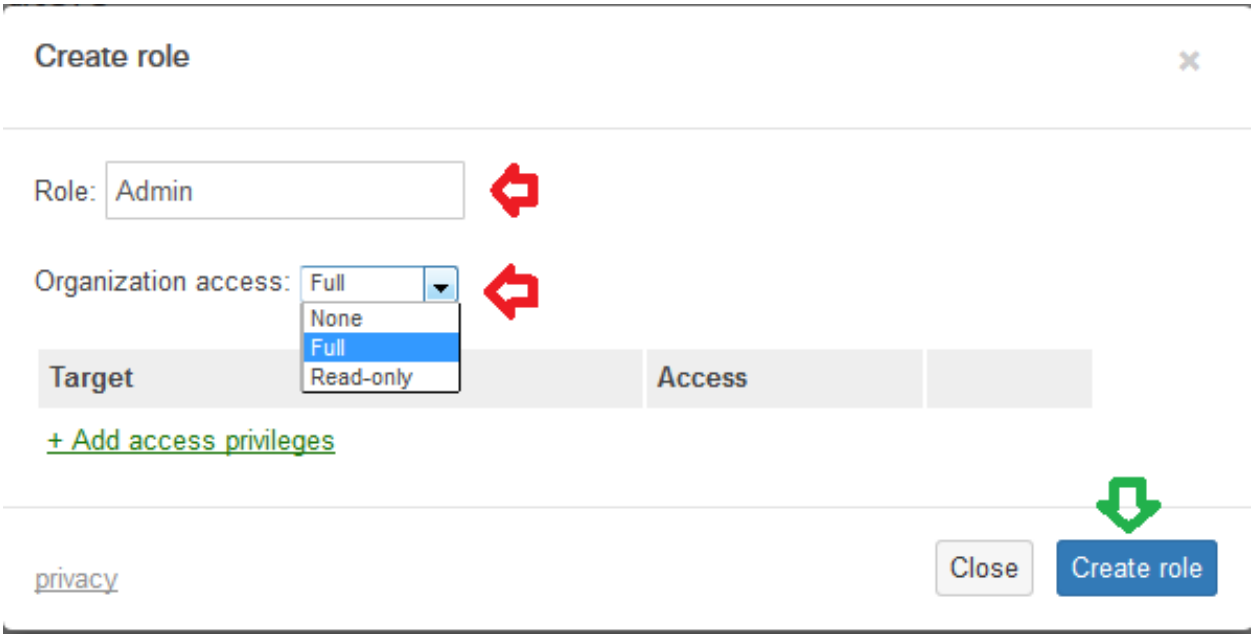
4. Cisco Meraki requires user to manually add role for their organization to identify them correctly during SAML authentication and to grant proper access rights. To do so, again go to home page of the account. Following UI will be displayed. Go to *Organization → Administrators.*



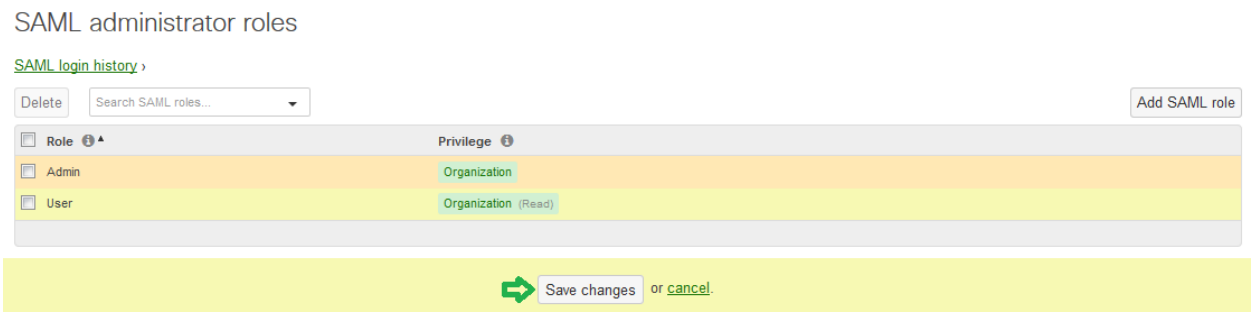
5. Following UI will be displayed. Click on **Add SAML role** button under **SAML administrator roles** option.



6. 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.



7. 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.



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

RJ