# Sentry SSO with Meraki Dashboard

**(This Article is under construction)**

**(This integration has not been released yet)**

## Contents



## Setup Sentry Keys

Before you are able to create a Single Sign On configuration on Meraki, you will need to setup some Keys if you haven't previously. Please see a separate article: HowToCreateKeysOnCmi. You will need the certificate from the View Keys menu option of Swivel Sentry. Download the Cert file and save it with the .crt extension name.

## Enable SAML SSO in Meraki Dashboard

In Meraki Dashboard menu, go to Organization > Settings > SAML Configuration, enable SAML SSO and click "Add a SAML Idp"


**SAML SSO** = select "SAML SSO enabled"

**X.509 cert SHA1 fingerprint** = open the saved certificate from sentry and get the fingerprint/thumbprint from the Details. The fingerprint needs to have colons on every two characters. ex: 00:11:22:33:44...

**SLO logout URL (optional)** = set the logout url: https://<FQDN_OF_SENTRY_SERVER>:8443/sentry/singlelogout

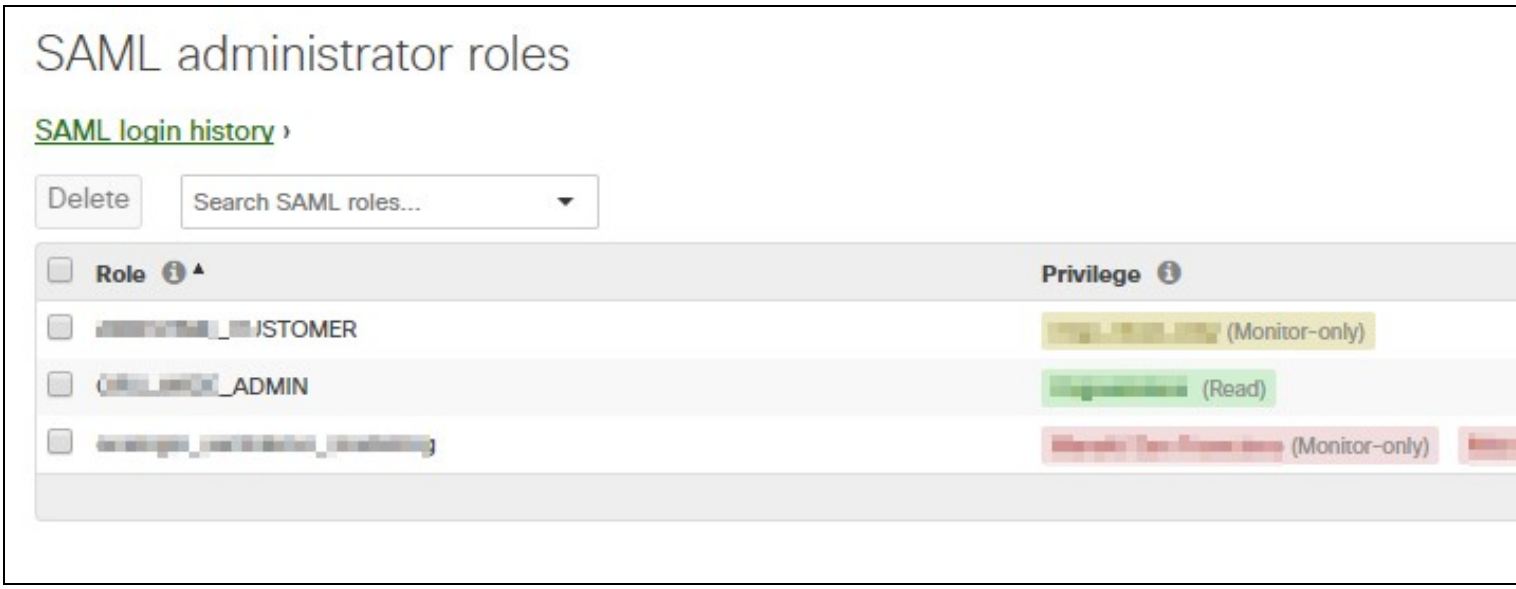
### Add SAML administrator roles

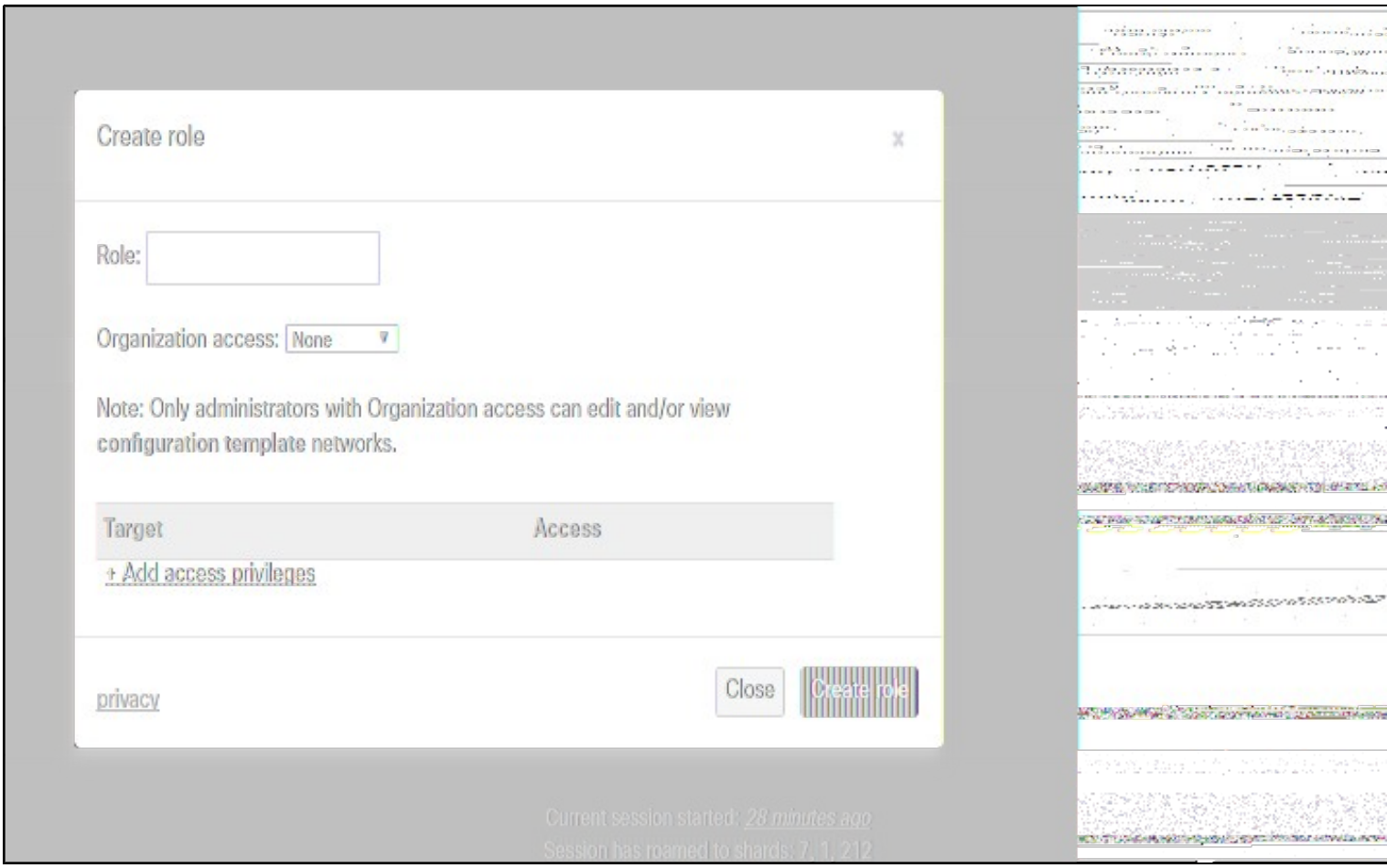
Go to Organization > Administrators > SAML administrator roles

This section is used to assign permissions to user groups in Dashboard. When SAML users log-in, they will be granted whatever permissions have been assigned to the 'role' attribute included in the SAML token provided by the IdP.

You can create roles based on the username or other attributes of the user.

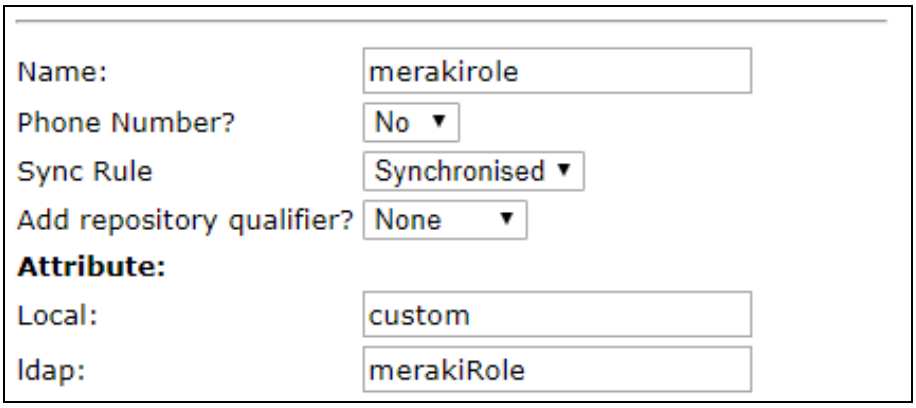
To create a new role, click Add SAML role and specify the role.




## Setup additional role attribute in Swivel Core (if needed)

If you want to use specific roles for the Meraki User roles, you can create the attribute in Swivel Core > Repository > Attributes




## Setup Sentry Application

You can select Application Images in the left hand menu to upload the Meraki Dashboard logo. (Optional)


Open the Sentry SSO administration page and Click Applications in the left hand menu. To add a new Application definition for Meraki, click the SAML - Other select button.


**Name** = Meraki (Arbitrary name for the application)

**Image** = the meraki logo

**Points** = the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application

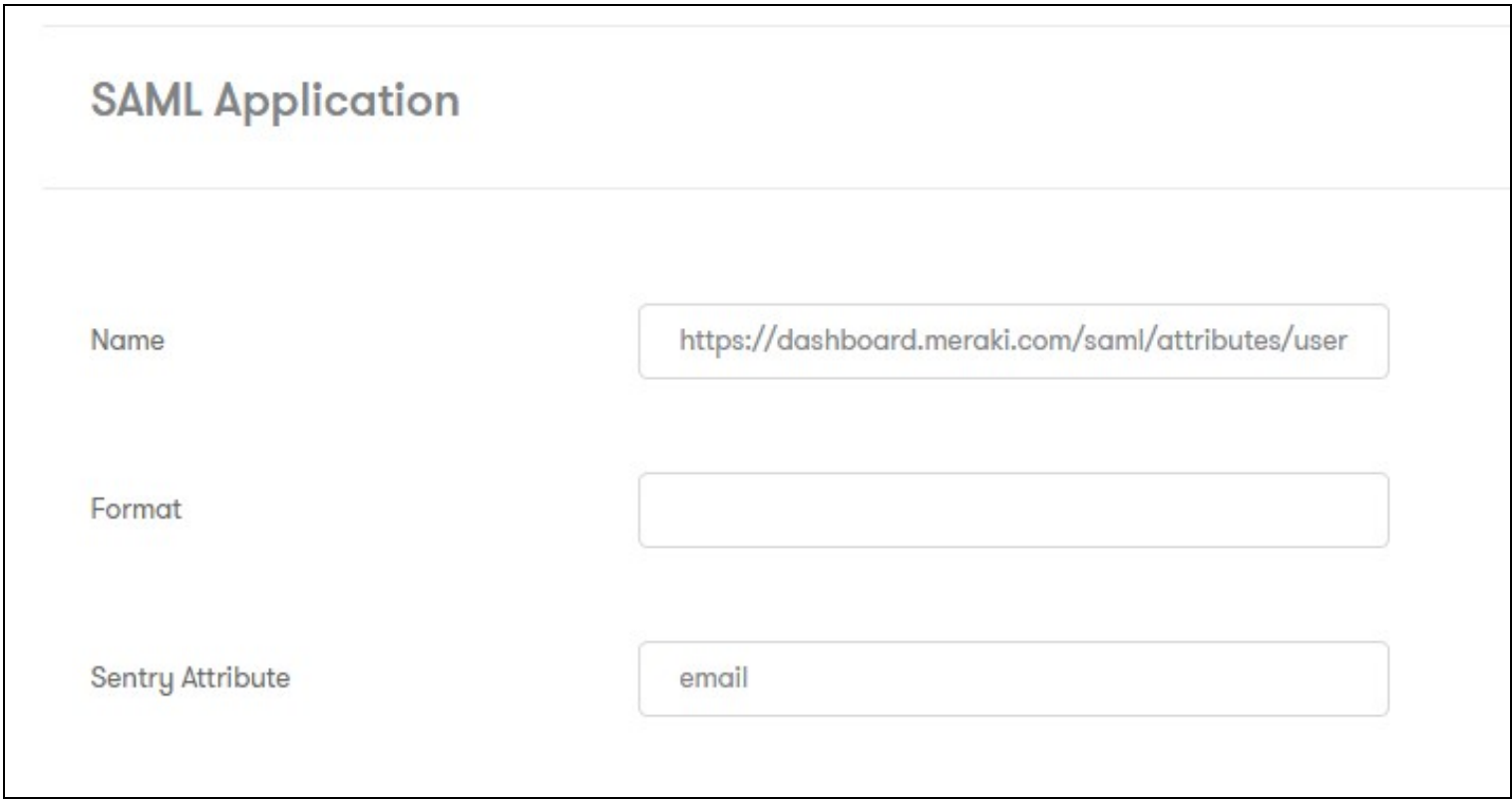
**Portal URL** = the Meraki Dashboard **Consumer URL** that is given when enabling SAML SSO

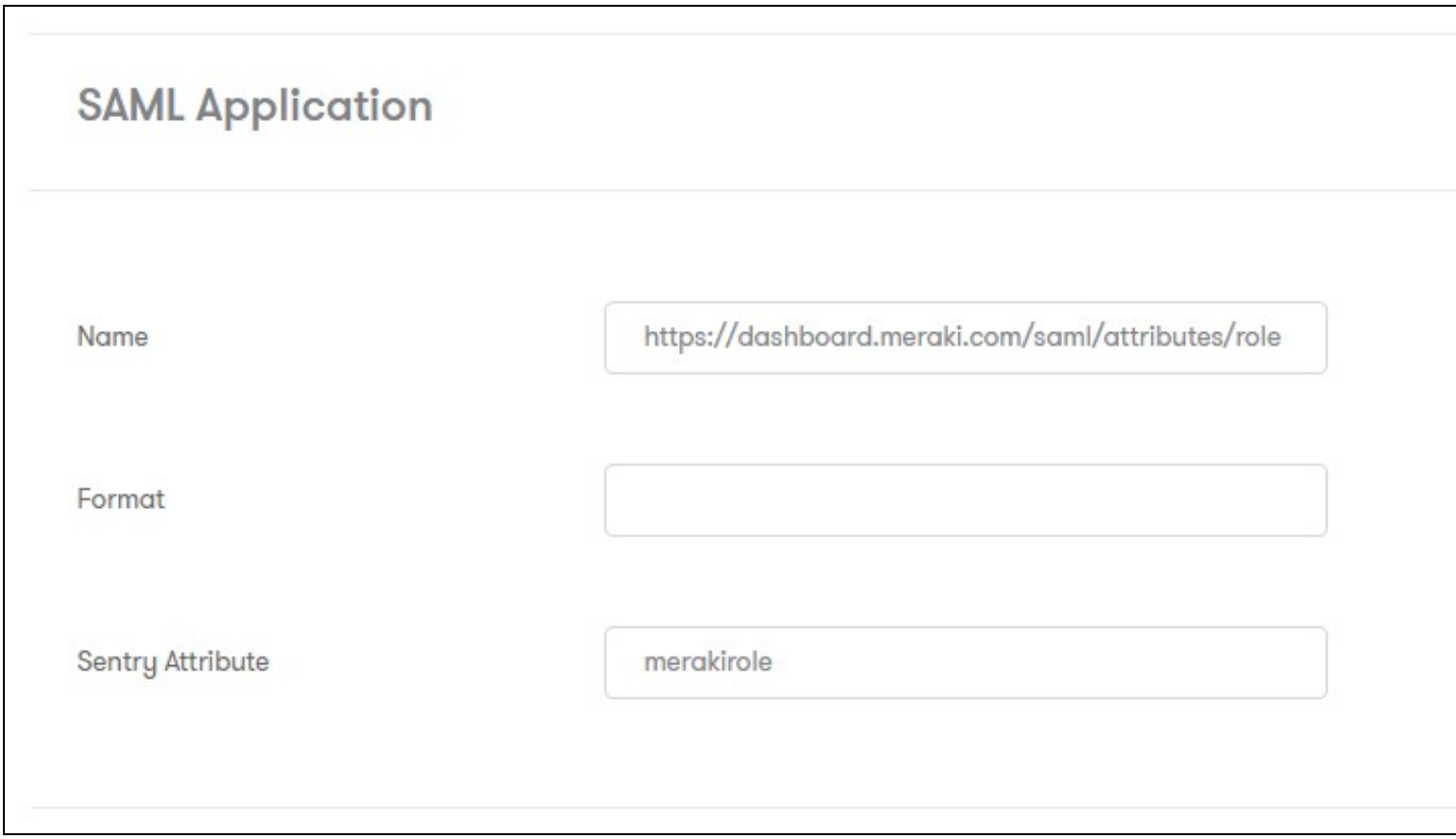
**Entity ID** = https://dashboard.meraki.com

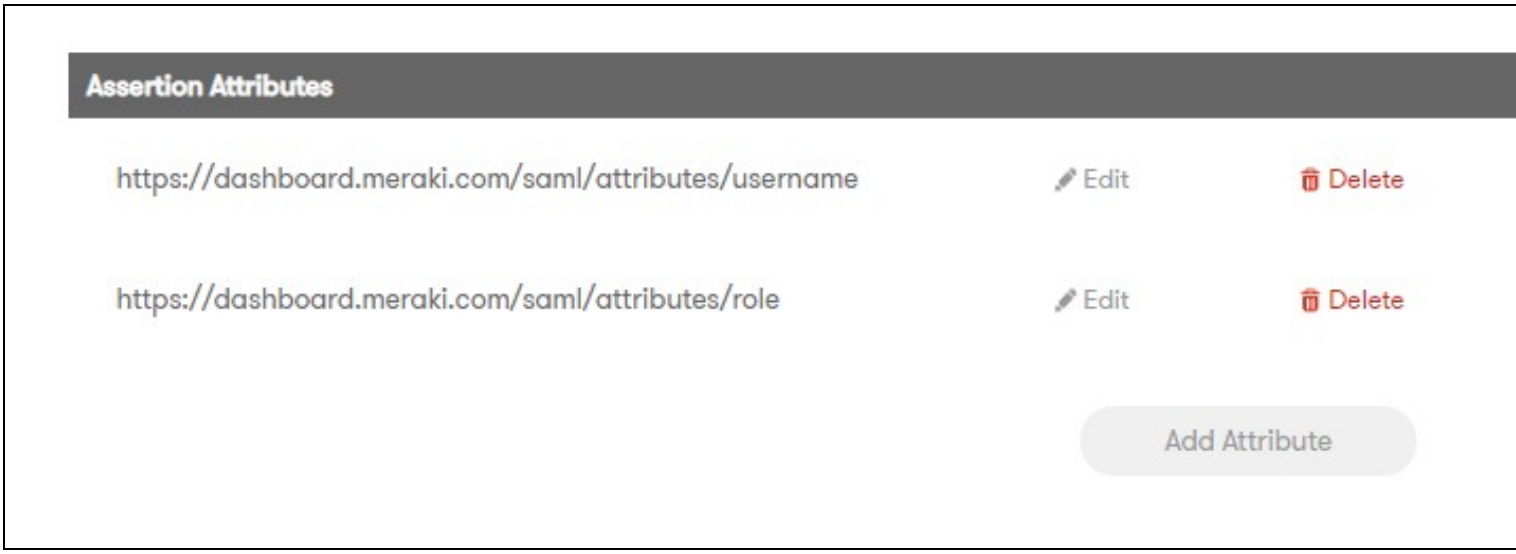
**Federated ID** = email (That needs to match with the attributed defined on Swivel Core)

Save and click edit to be able to add SAML Assertion Attributes to the application. Add the two attributes required by Meraki:

https://dashboard.meraki.com/saml/attributes/username and https://dashboard.meraki.com/saml/attributes/role



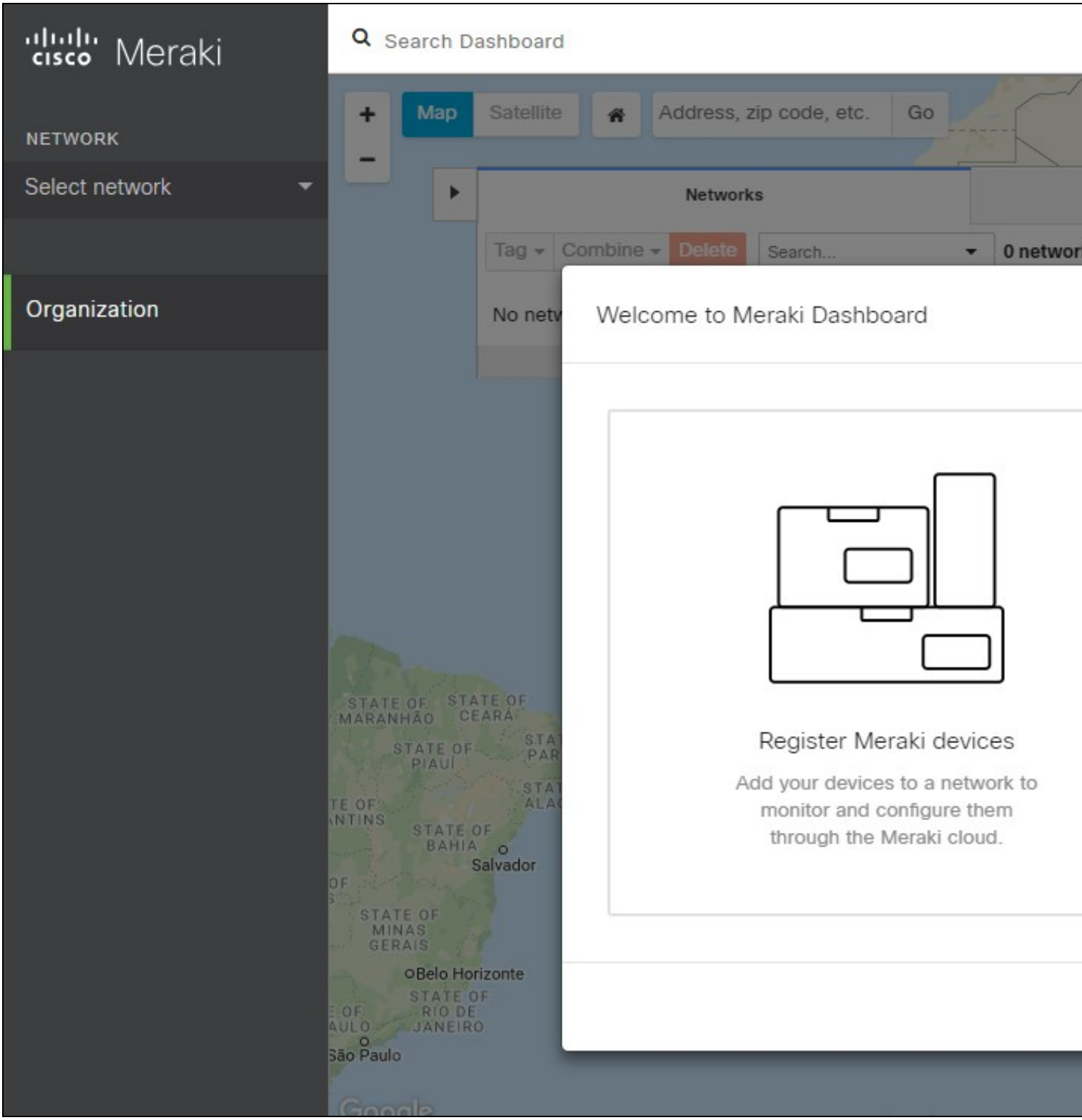



### Testing authentication to Meraki Dashboard via Swivel Sentry

In the Sentry Start Page, select Meraki Dashboard and login.

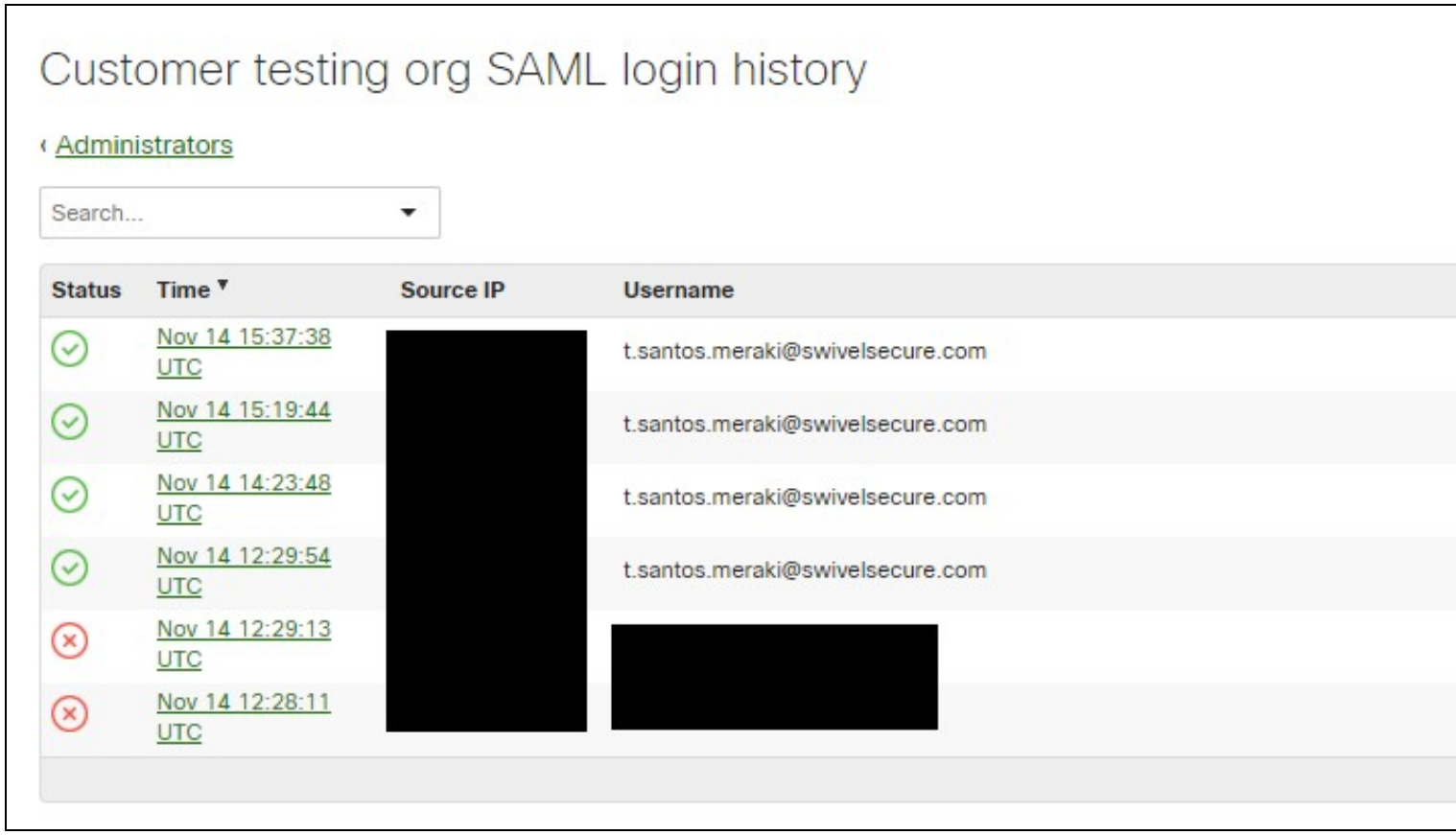

If the login is successful, you will login to the Meraki Dashboard and will see on the top right the username that was specified in the user attribute




## Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel Sentry has a View Log menu item which provides details about the SAML assertion and response received from Meraki and can be useful for comparison with the Meraki SAML Assertion Validator output;
- Meraki has a SAML login history which can provide diagnostics about the latest SAML authentication attempt. This can be particularly useful for verifying the SAML Attributes and various elements within the SAML assertion that takes place between the Swivel Sentry and Meraki. To get to the SAML Login history in Meraki select Organization -> Administrators -> SAML login history.


It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the Sentry logging or Meraki login history shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
  - Can Sentry find the Certificate locally, is it the correct one?
  - Has the correct Certificate Fingerprint been set in Meraki?
- Attributes mismatch.
  - Has the Role been created in Meraki Dashboard?
  - Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?