Use IDP Federation to enforce zero trust policies on all SaaS Applications integrated with OneLogin

Use federation capabilities in OneLogin to enforce CSE Policies on your SaaS applications

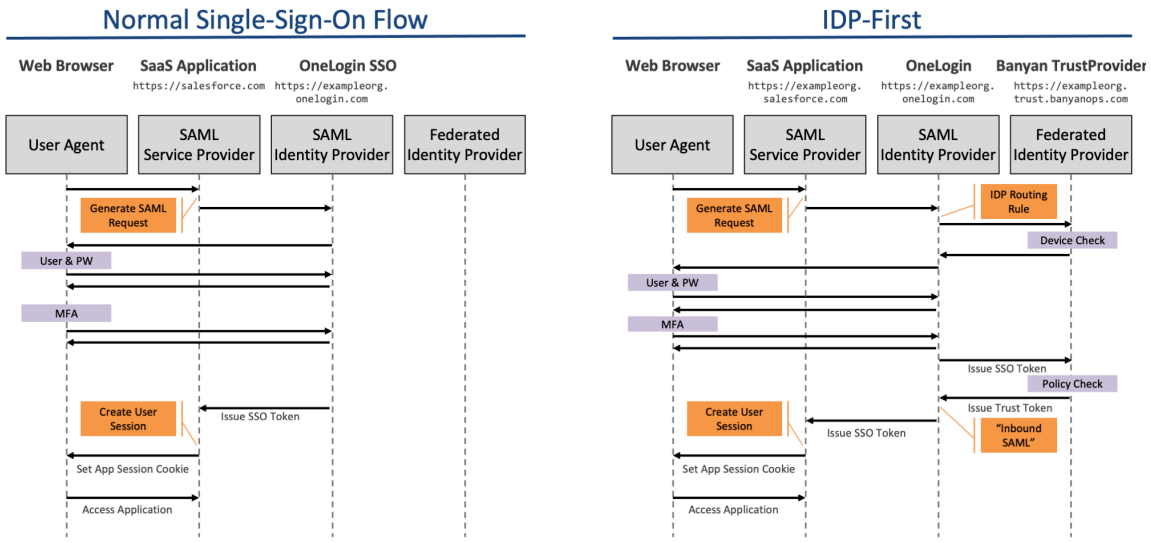
Updated on

ON THIS PAGE:

Overview

This guide details the steps required to set up OneLogin and CSE TrustProvider to enable device registration and authentication for any SaaS application. Additionally, this guide covers how to add policy enforcement in CSE TrustProvider at the SaaS application level.

How it Works



In the IDP-first authentication flow, you configure your OneLogin to federate authentication requests to CSE's TrustProvider component. CSE TrustProvider federates right back to OneLogin for user authentication but, because CSE is now in the authentication flow, it is able to enforce Zero Trust security policy.

CSE supports two types of IDP-first authentication flows for OneLogin:

1. Service Provider-initiated - End users launch the SaaS application directly.

- 1.1 SaaS application redirects the user to OneLogin with Special Query parameter for Application and Trusted IDP
- 1.2 User is redirected to OneLogin
- 1.3 OneLogin selects the CSE Trusted IDP
- 1.4 User is redirected to Trust Provider
- 1.5 Trust Provider validates the certificate
- 1.6 Trust Provider is redirected the user to OneLogin for authentication (SAML Connector)
- 1.7 User enters credentials and OneLogin posts the SAML Response to Trust Provider
- 1.8 Trust Provider exchanges the access token and issues the token to OneLogin
- 1.9 OneLogin redirects the user to Application Portal

2. Identity Provider-initiated - End users launch the SaaS application from the OneLogin catalog.

- 2.1 User logs in to OneLogin
- 2.2 User is redirected to application catalog
- 2.3 User clicks on SaaS Application (Proxy App)
- 2.4 Proxy Application routes the user to Trust Provider with Application Redirect URL and Group Id as SAML Assertion Claims
- 2.5 Trust Provider verifies the device certificate and applies Policy
- 2.6 On success, user is redirected to application redirect URL

> OneLogin currently cannot redirect the end user back to intended SaaS application. The end user must click the SaaS application again from OneLogin Portal.

Prerequisites

Before proceeding with the setup steps below, please ensure you have:

- A OneLogin account with Admin privileges
- Integrated CSE with OneLogin to create a directory of users that can access your Services
- A CSE Organization and a configured CSE Trust Provider
- A role and policy tailored for your organization's needs
- A SaaS application for testing (such as Slack)

Setup

At a high level, configuring OneLogin IdP federation to CSE can be broken out into three phases:

Phase 1. Configure CSE as a OneLogin Trusted IDP

This phase establishes trust between OneLogin and CSE's TrustProvider.

Step	Description
1	Configure OneLogin Trusted IdP
2	Configure CSE IDP-routed Service
3	Update OneLogin Trusted IdP Configuration
4	Configure SaaS Application SSO

Phase 2. Configure SP-initiated Access

This phase sets up all apps federated with OneLogin to use CSE TrustProvider for ZeroTrust policy checks.

Step	Description
5	Configure OneLogin SaaS Application

Phase 3. Configure IdP-initiated Access

> Phase 3 is only required if your end users will launch the SaaS application from the OneLogin application catalog.

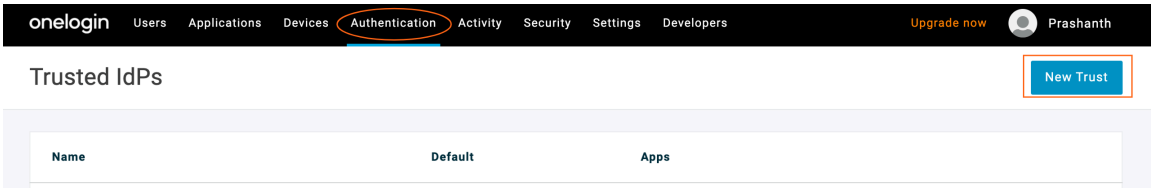
This phase sets up applications launched from the OneLogin catalog to use CSE TrustProvider for ZeroTrust policy checks.

Step	Description
6	Assign Users to Application
7	Configure Proxy SaaS Application
8	Disable Original Application from OneLogin Catalog

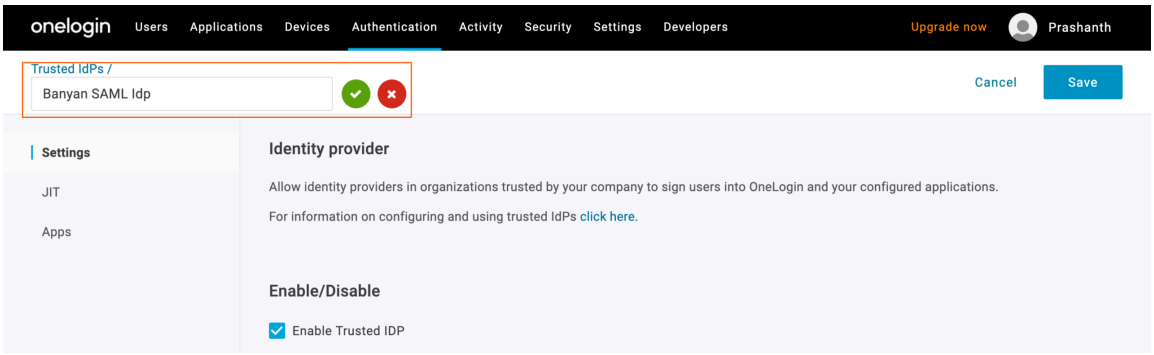
Phase 1. Configure CSE as a OneLogin Trusted IDP

Step 1. Configure OneLogin Trusted IdP

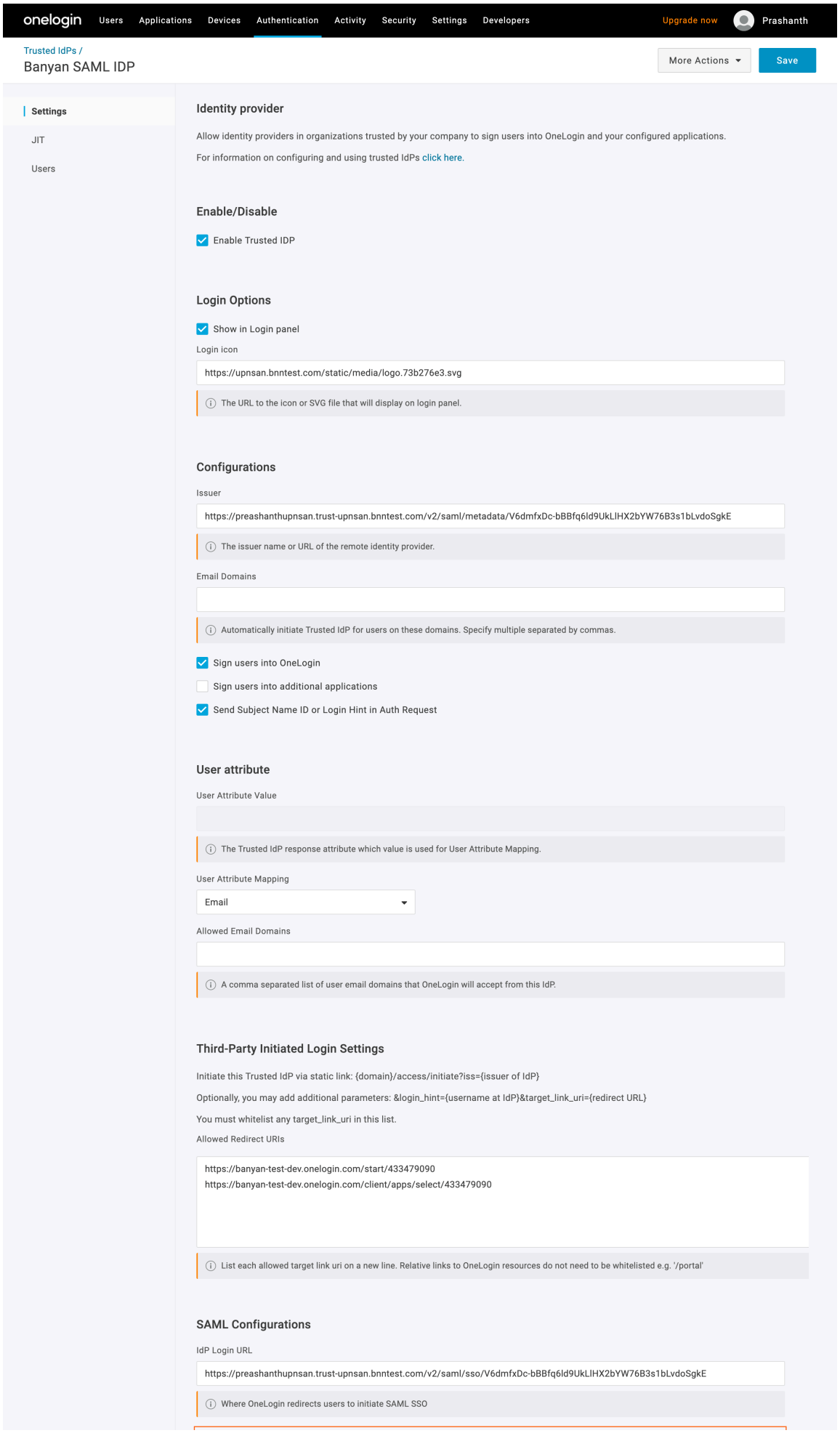
1.1 In the OneLogin Admin Portal, navigate to **Authentication** > **Trusted Idps** and then click **New Trust**.

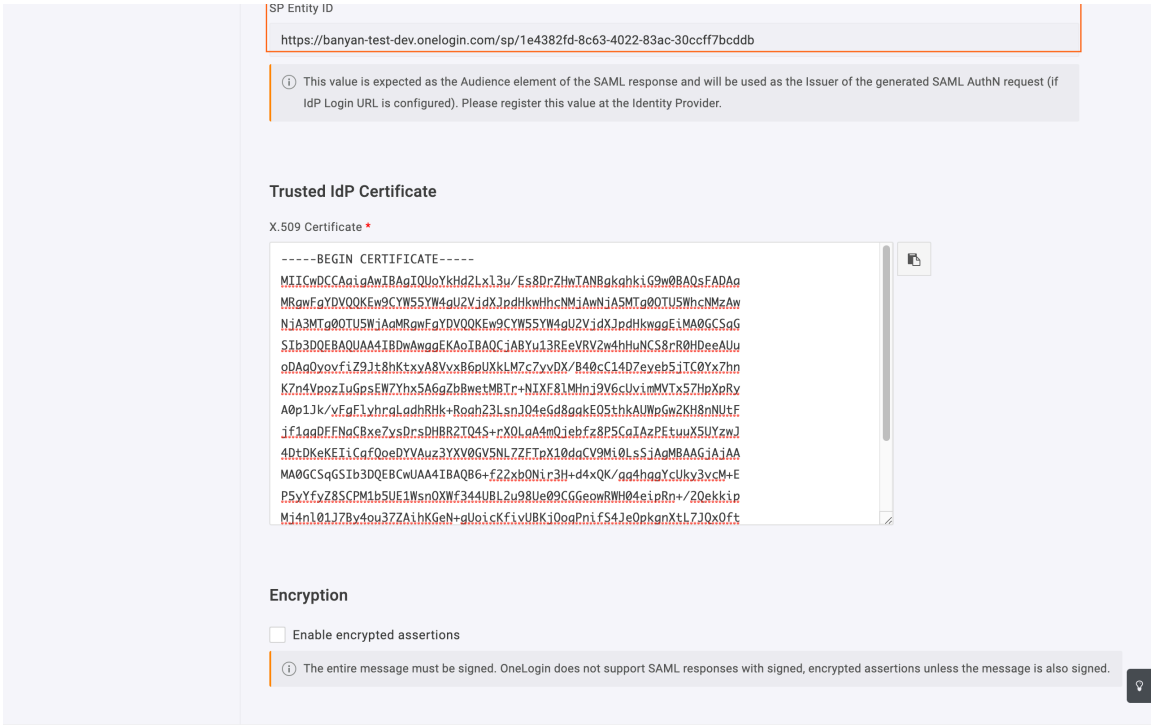


1.2 Enter the Trust Provider name “CSE SAML Idp” and then click the green checkmark.



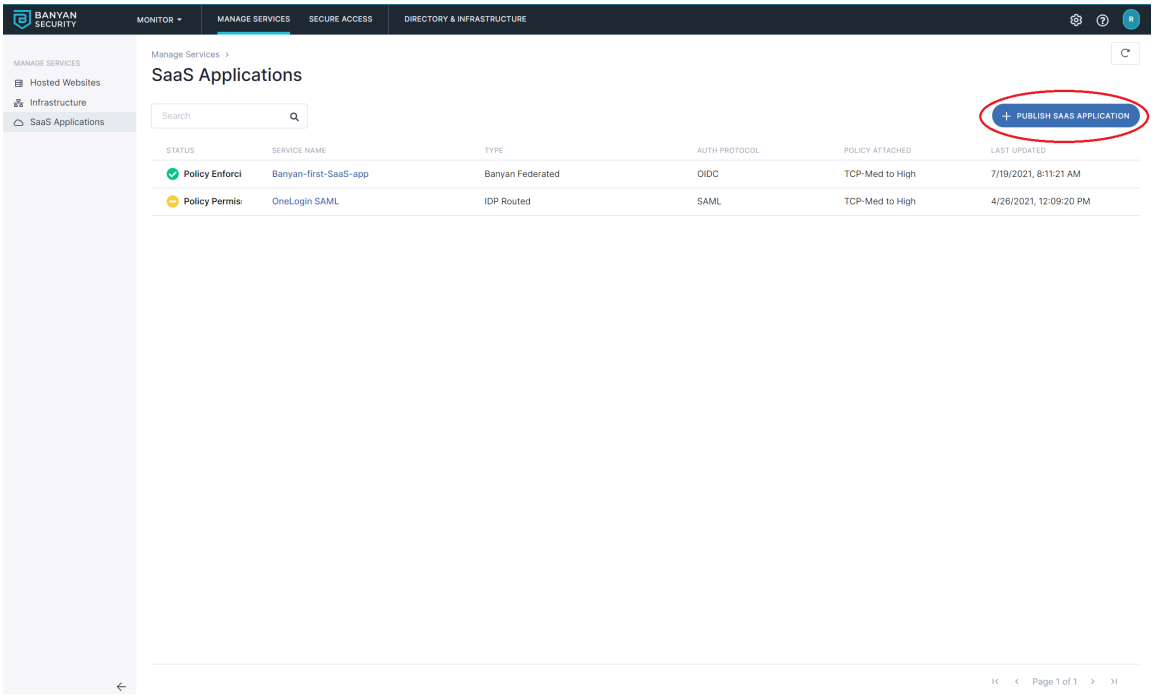
1.3 Navigate to the **Settings** tab and then copy the **SP Entity Id**, which you will use in the steps below.


onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Upgrade now
Prashanth
Trusted IdPs /
Banyan SAML IDP
More Actions
Save
Settings
JIT
Users
Identity provider
Allow identity providers in organizations trusted by your company to sign users into OneLogin and your configured applications.
For information on configuring and using trusted IdPs click here.
Enable/Disable
Enable Trusted IDP
Login Options
Show in Login panel
Login icon
https://upnsan.bnntest.com/static/media/logo.73b276e3.svg
The URL to the icon or SVG file that will display on login panel.
Configurations
Issuer
https://preashanthupnsan.trust-upnsan.bnntest.com/v2/saml/metadata/V6dmfxDc-bBBfq6ld9UkLlHX2bYW76B3s1bLvdoSgkE
The issuer name or URL of the remote identity provider.
Email Domains
Automatically initiate Trusted IdP for users on these domains. Specify multiple separated by commas.
Sign users into OneLogin
Sign users into additional applications
Send Subject Name ID or Login Hint in Auth Request
User attribute
User Attribute Value
The Trusted IdP response attribute which value is used for User Attribute Mapping.
User Attribute Mapping
Email
Allowed Email Domains
A comma separated list of user email domains that OneLogin will accept from this IdP.
Third-Party Initiated Login Settings
Initiate this Trusted IdP via static link: {domain}/access/initiate?iss={issuer of IdP}
Optionally, you may add additional parameters: &login_hint={username at IdP}&target_link_uri={redirect URL}
You must whitelist any target_link_uri in this list.
Allowed Redirect URIs
https://banyan-test-dev.onelogin.com/start/433479090
https://banyan-test-dev.onelogin.com/client/apps/select/433479090
List each allowed target link uri on a new line. Relative links to OneLogin resources do not need to be whitelisted e.g. '/portal'
SAML Configurations
IdP Login URL
https://preashanthupnsan.trust-upnsan.bnntest.com/v2/saml/sso/V6dmfxDc-bBBfq6ld9UkLlHX2bYW76B3s1bLvdoSgkE
Where OneLogin redirects users to initiate SAML SSO

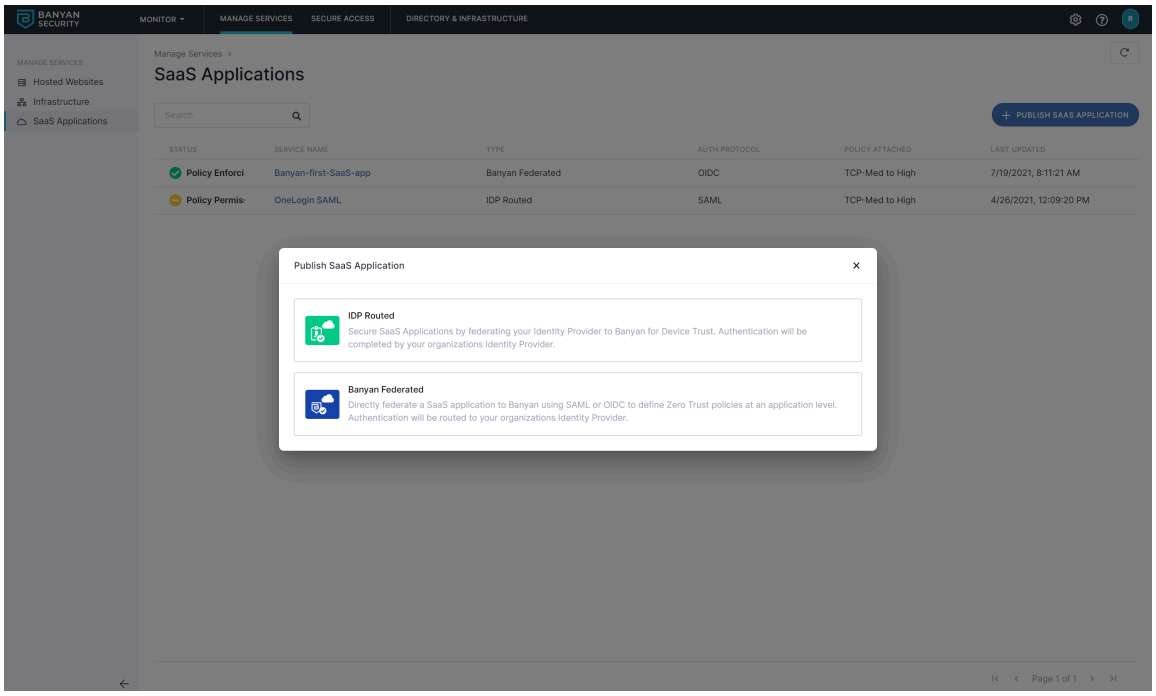


Step 2. Configure CSE IDP-routed Service

2.1 In the CSE Command Center, navigate to **Manage Services** > **SaaS Applications** and then click **+ PUBLISH SAAS APPLICATION**.

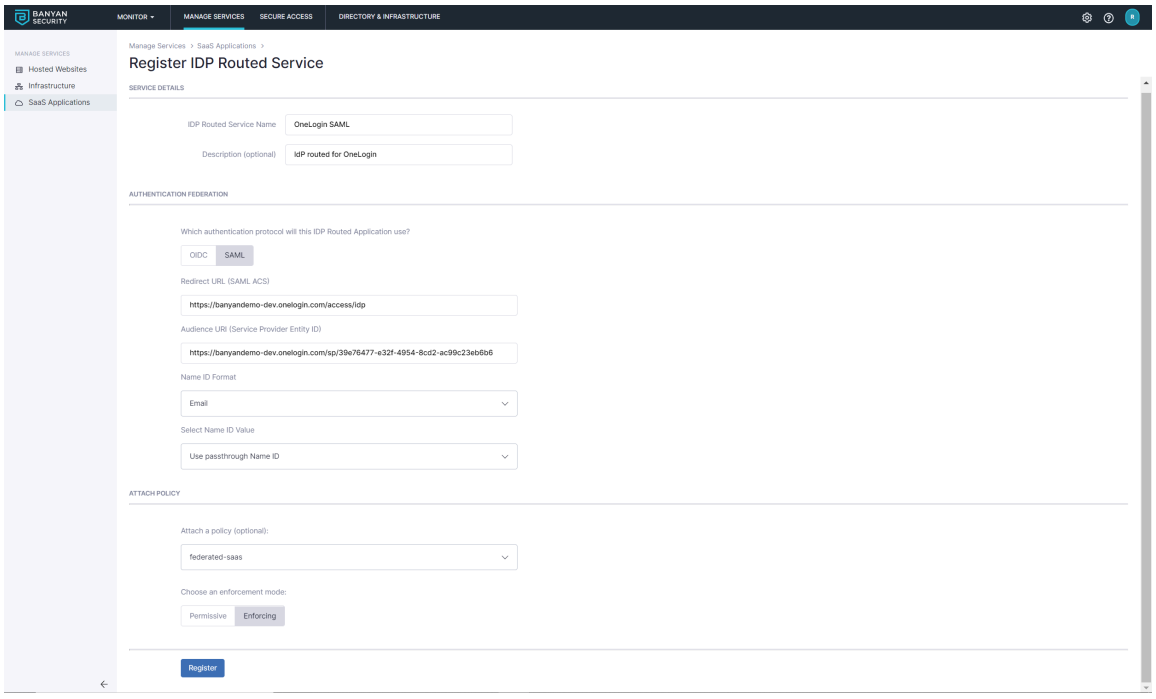


2.2 Select IDP Routed to route OneLogin to CSE



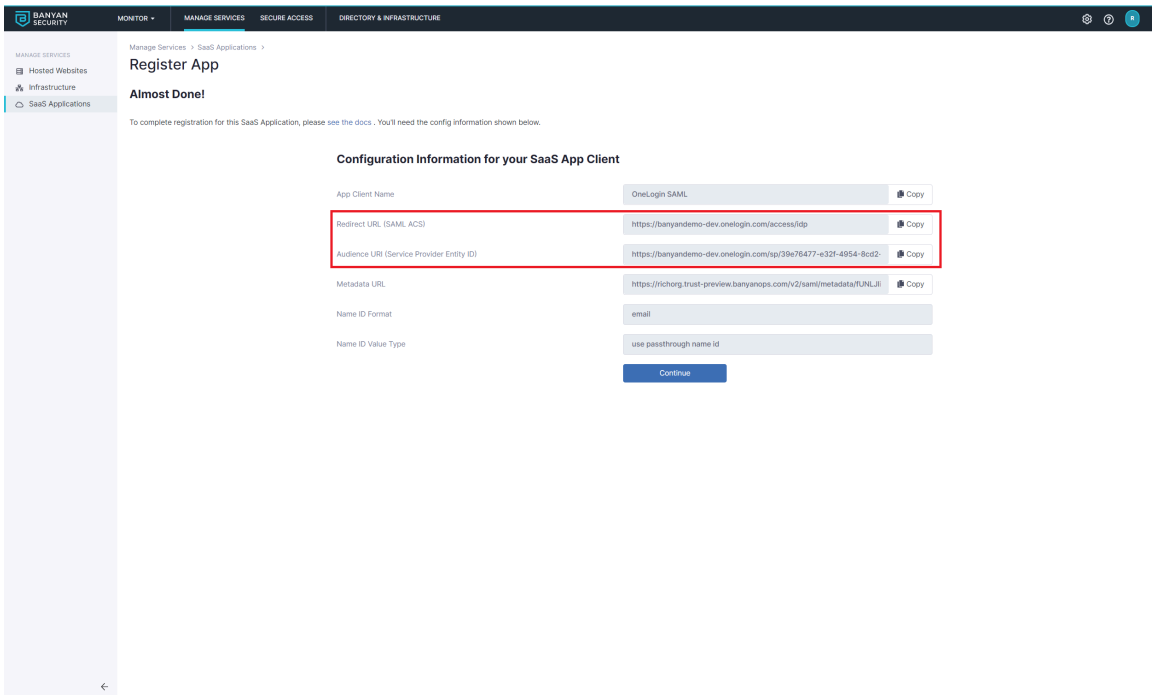
2.3 Enter the service details shown below.

- Enter a **IDP Routed Service Name** (such as “OneLoginSAML”) and **Description**
- Set the authentication protocol to **SAML**
- For **Redirect URL (SAML ACS)**, enter `https://(OneLogin Tenant ID).onelogin.com/access/idp`
- For **Audience URI (Service Provider Entity ID)**, enter the OneLogin Trusted IDP SP Entity ID (copied in step 1.3)
- Set **Name ID Format** to **Email**
- Set **Name ID Value** to **Legacy compatibility mode**
- Attach an applicable policy

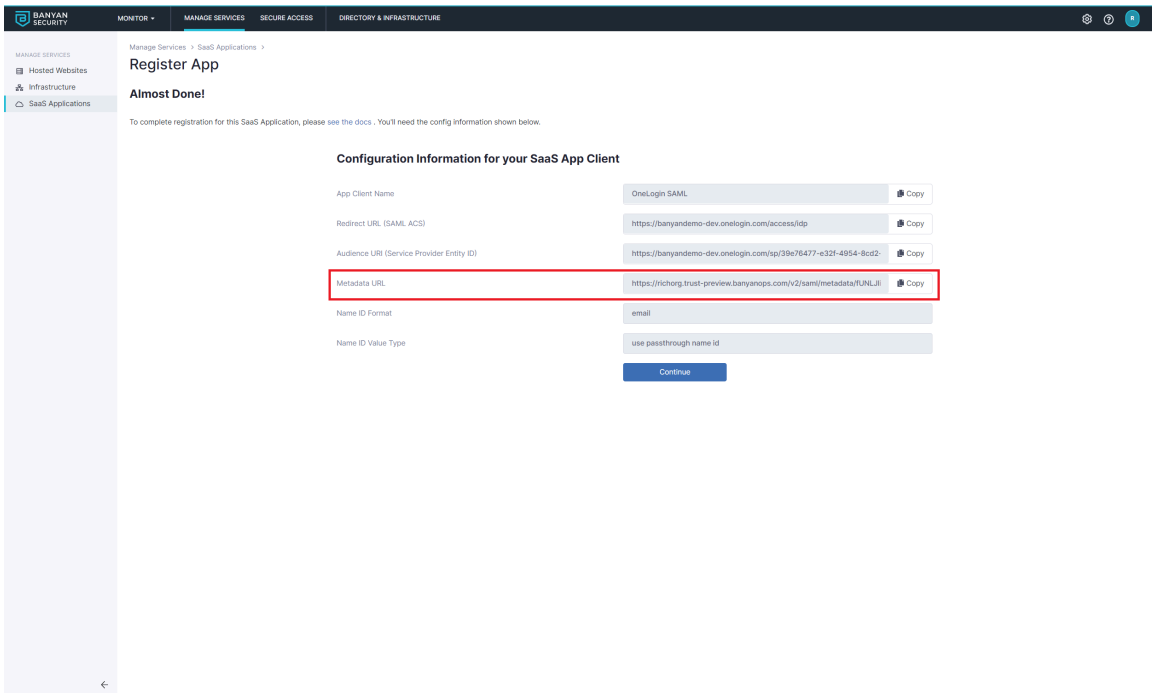


2.4 Register.

2.5 Make note of the SaaS app Client configuration values shown in the Command Center, as you will use them in Step 4.1.



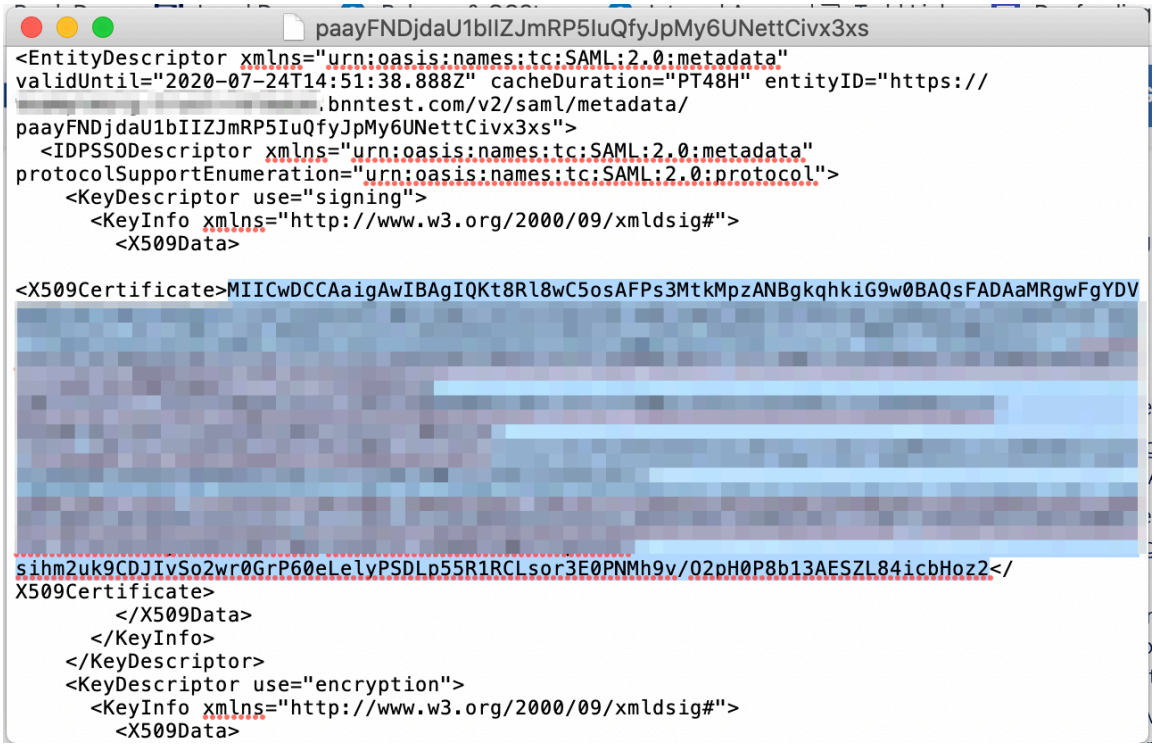
2.6 Also, copy the **Metadata URL**, paste it in your browser search bar and then press enter to download the xml file. You will use the information in this file to configure SSO in OneLogin.



Step 3. Prepare your CSE-registered App Details for OneLogin

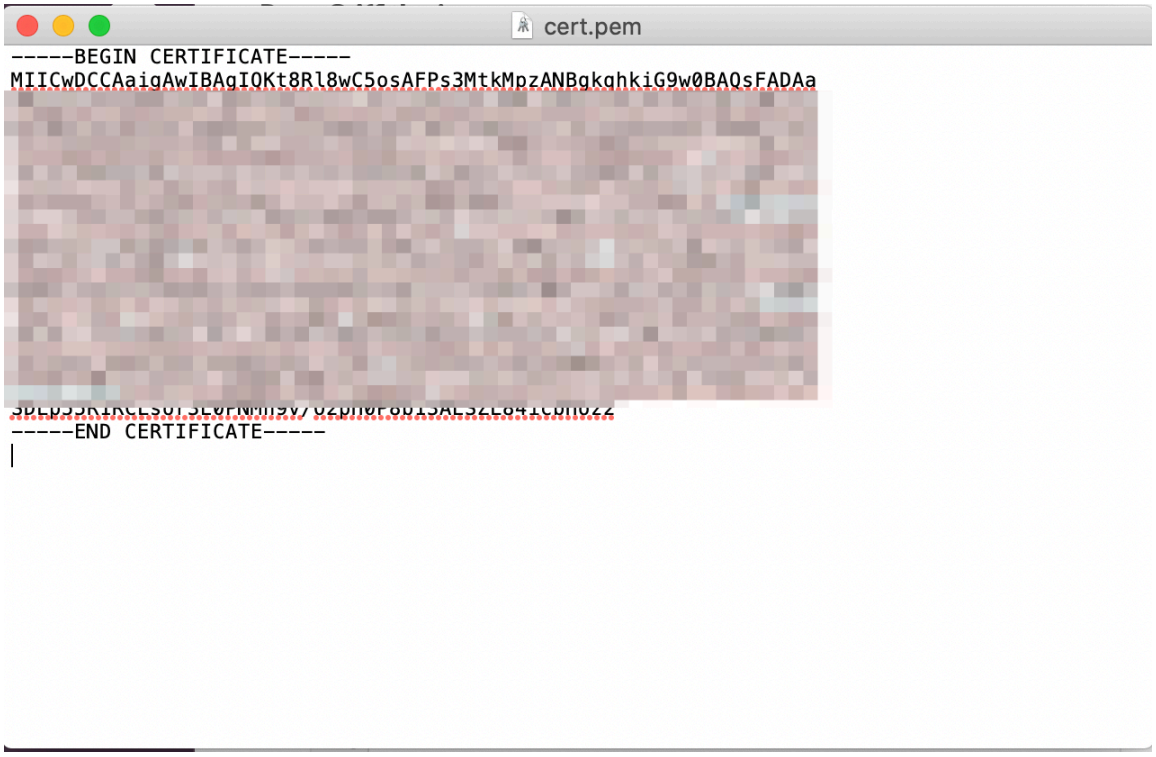
3.1 Open the metadata xml file downloaded in Step 2.5 in your preferred text editor.

3.2 Locate and copy the `X509Certificate` string, and then paste it in a separate, new text editor file.

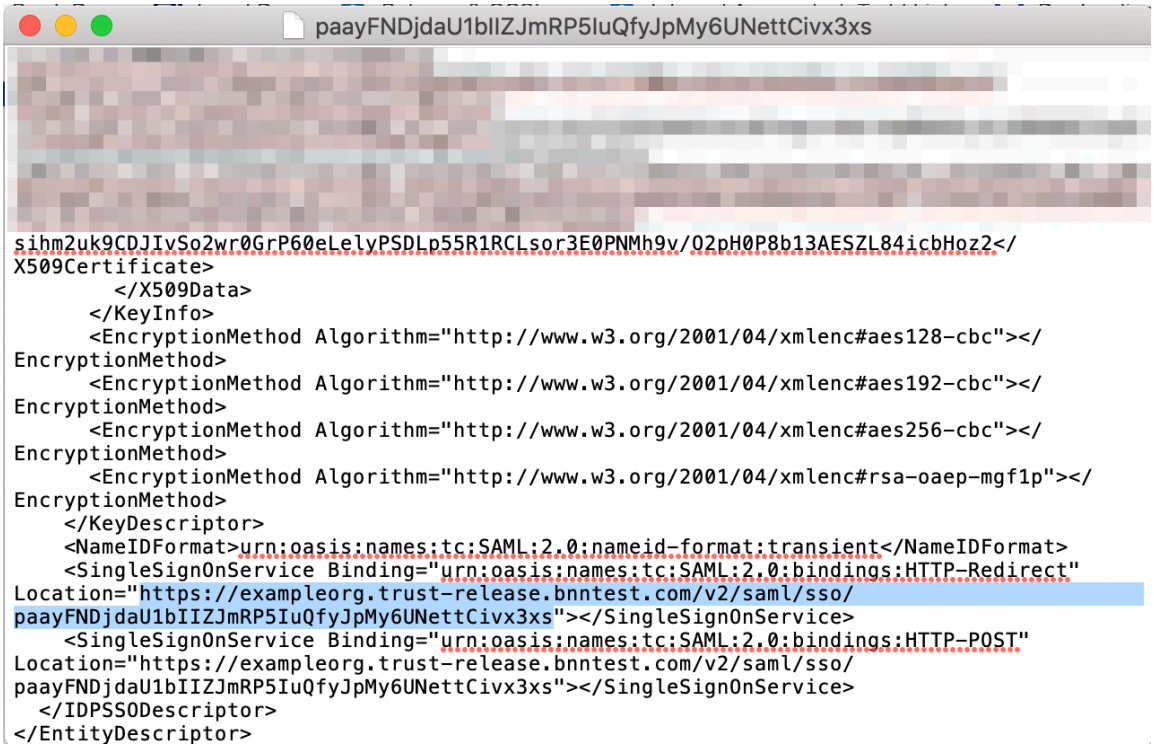


3.3 Format the string and then save it as a pem file. You will upload this file in Step 4.1.

- Ensure you add the header (`-----BEGIN CERTIFICATE-----`) to the first line.
- Ensure you add the footer (`-----END CERTIFICATE-----`) to the last line.
- Ensure you add line breaks so that each line is no longer than 64 characters max.
- The formatted pem file should look like the example below:



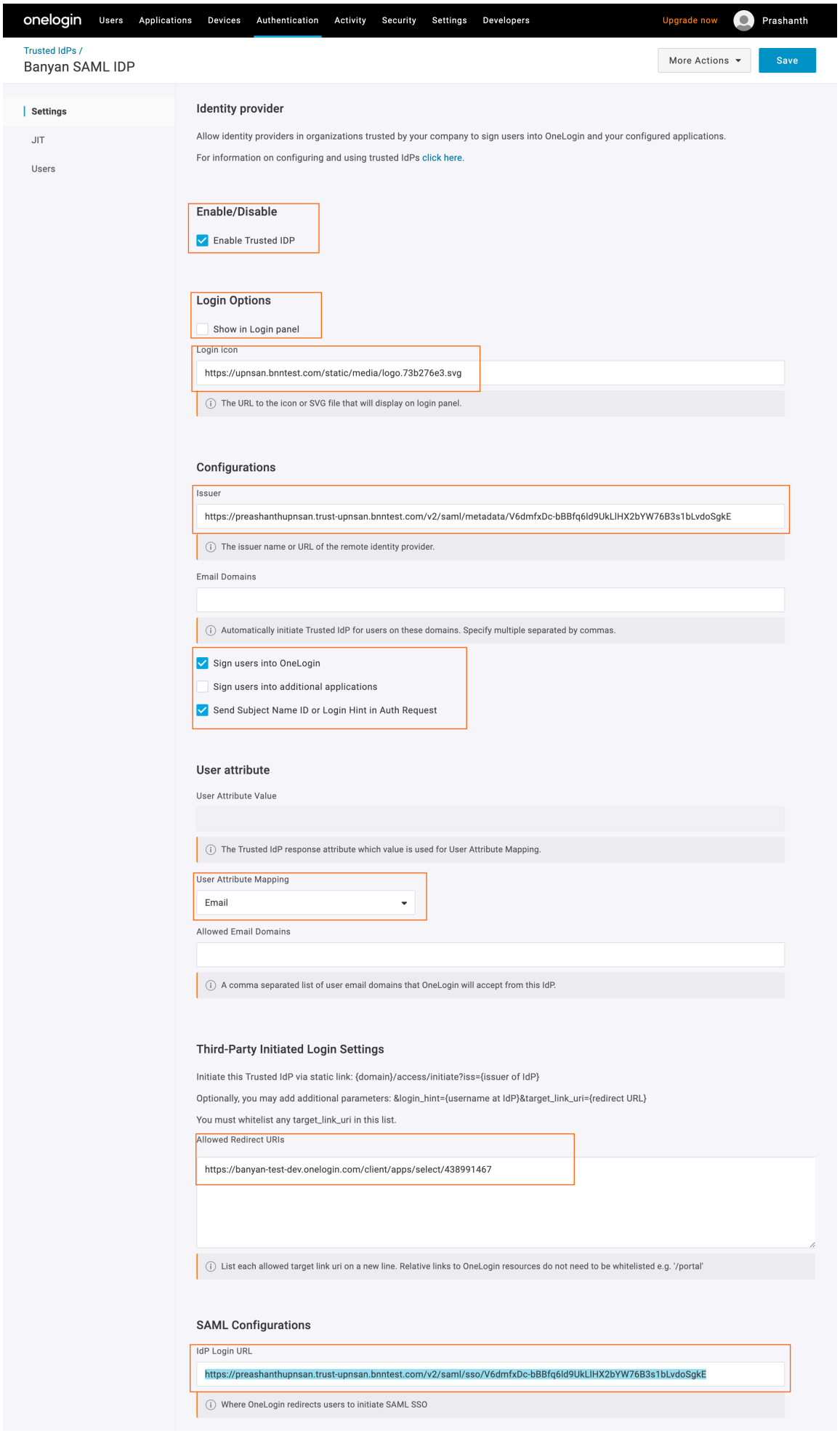
3.4 Also in the downloaded metadata xml file, locate and take note of the `<SingleSignOnService Location>` string. You will enter this value in Step 4.1.

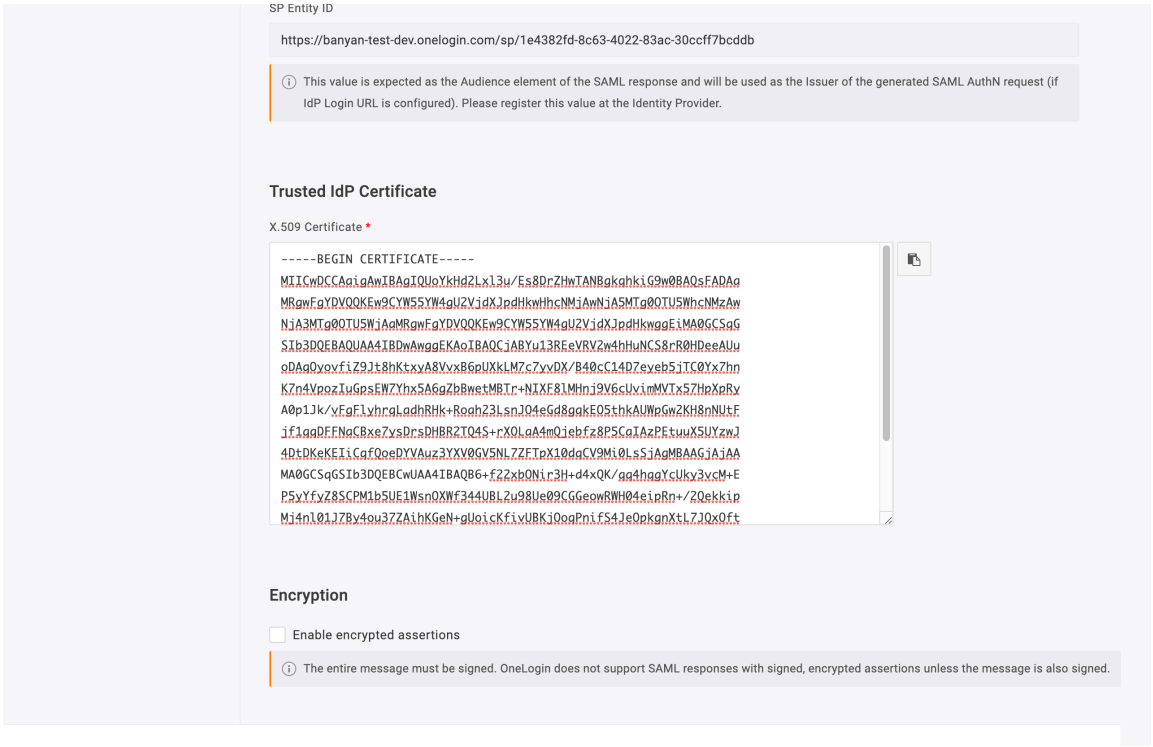


Step 4. Update OneLogin Trusted IdP Configuration

4.1 Navigate to **Settings** and then update following fields:

- **Login Options**
  - **Show in Login Panel** - Unchecked
  - **Login Icon** - Enter the CSE Logo URL (`https://upnsan.bnntest.com/static/media/logo.73b276e3.svg`)
- **Configurations**
  - **Issuer** - Enter the CSE SaaS Application Metadata Url (noted in step 2.6)
  - **Sign users into OneLogin** - Checked
  - **Sign users into additional applications** - Unchecked
  - **Send Subject Name Id or Login Hint in Auth Request** - Checked
- **User Attribute**
  - **User Attribute Mapping** - set to **Email**
- **SAML Configurations**
  - **Idp Login Url** - Get SingleSignOnService Url from CSE SaaS Application metadata Url (noted in step 3.4)
- **Enable/Disable**
  - **Enable Trusted IDP** - Checked
- Paste X.509 Certificate in the relevant box


onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Upgrade now
Prashanth
Trusted IdPs /
Banyan SAML IDP
More Actions
Save
Settings
JIT
Users
Identity provider
Allow identity providers in organizations trusted by your company to sign users into OneLogin and your configured applications.
For information on configuring and using trusted IdPs click here.
Enable/Disable
Enable Trusted IDP
Login Options
Show in Login panel
Login icon
https://upnsan.bnntest.com/static/media/logo.73b276e3.svg
The URL to the icon or SVG file that will display on login panel.
Configurations
Issuer
https://preashanthupnsan.trust-upnsan.bnntest.com/v2/saml/metadata/V6dmfxDc-bBBfq6ld9UkLlHX2bYW76B3s1bLvdoSgkE
The issuer name or URL of the remote identity provider.
Email Domains
Automatically initiate Trusted IdP for users on these domains. Specify multiple separated by commas.
Sign users into OneLogin
Sign users into additional applications
Send Subject Name ID or Login Hint in Auth Request
User attribute
User Attribute Value
The Trusted IdP response attribute which value is used for User Attribute Mapping.
User Attribute Mapping
Email
Allowed Email Domains
A comma separated list of user email domains that OneLogin will accept from this IdP.
Third-Party Initiated Login Settings
Initiate this Trusted IdP via static link: {domain}/access/initiate?iss={issuer of IdP}
Optionally, you may add additional parameters: &login_hint={username at IdP}&target_link_uri={redirect URL}
You must whitelist any target_link_uri in this list.
Allowed Redirect URIs
https://banyan-test-dev.onelogin.com/client/apps/select/438991467
List each allowed target link uri on a new line. Relative links to OneLogin resources do not need to be whitelisted e.g. '/portal'
SAML Configurations
IdP Login URL
https://preashanthupnsan.trust-upnsan.bnntest.com/v2/saml/sso/V6dmfxDc-bBBfq6ld9UkLlHX2bYW76B3s1bLvdoSgkE
Where OneLogin redirects users to initiate SAML SSO



4.2 Click **Save**.

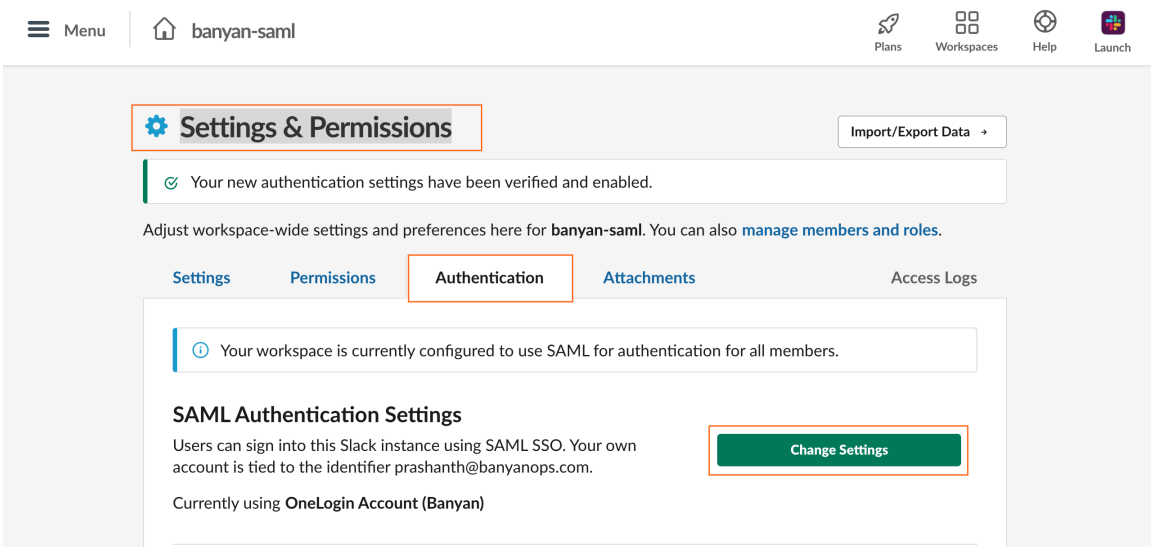
Phase 2. Configure SP-initiated Access

Step 5. Configure SaaS Application SSO

This step uses Slack as an example.

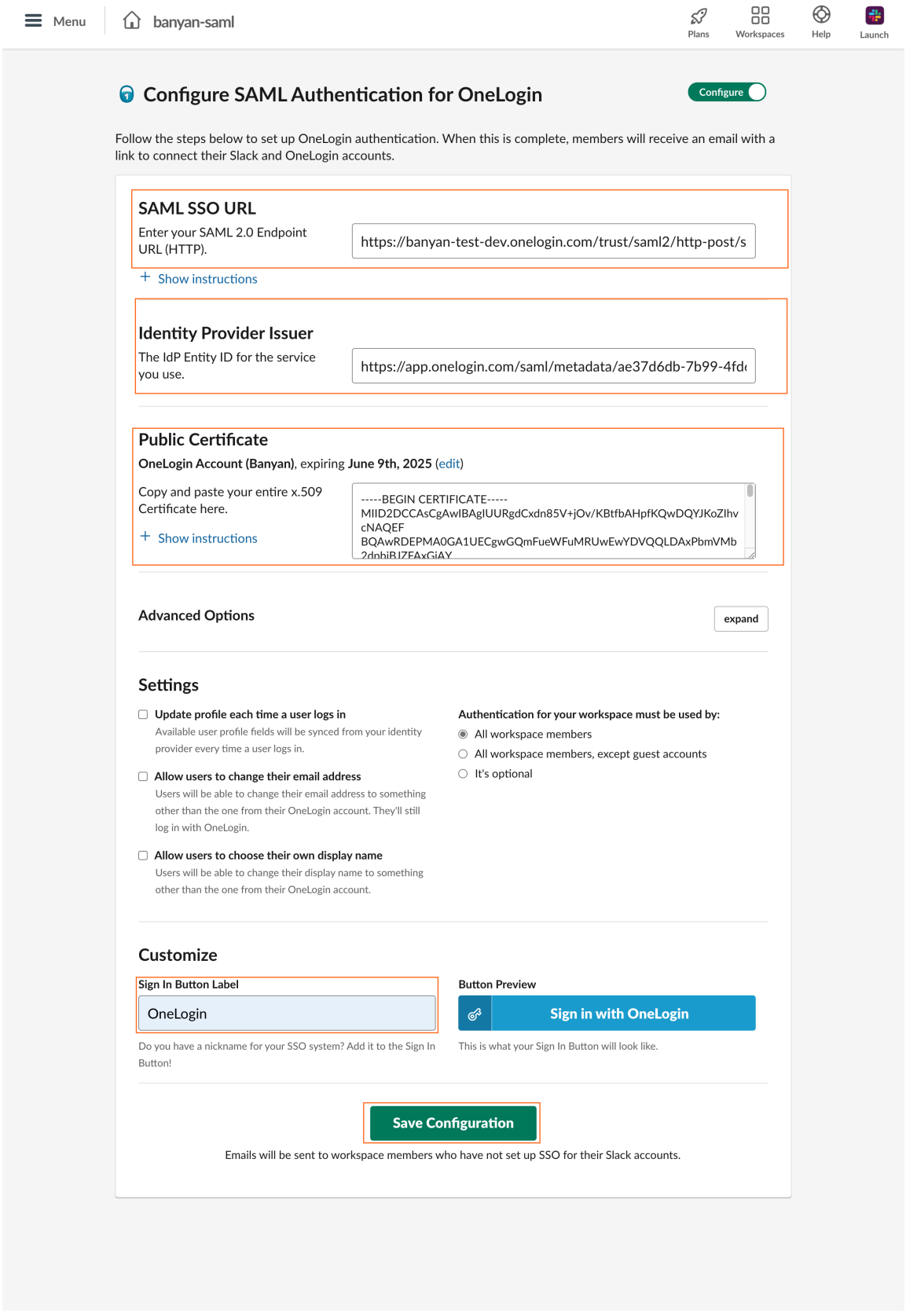
5.1 Log in to the Slack Admin Portal and then navigate to **Settings & Permissions**.

5.2 Select the **Authentication** tab and then click **Change/Add Settings** for SAML Authentication Settings.



5.3 Update the fields accordingly:

- **SAML SSO URL** - Enter the SAML 2.0 Endpoint from OneLogin SaaS (Slack) Application SSO settings (from step 4.2) using the format `{domain}/access/initiate?iss={issuer of IdP}`
  - issuer = Found in Trusted IDP > Settings > Configurations > Issuer URL
  - &target_link_uri={redirect URL} Found in applications > SSO > SAML 2.0 Endpoint (HTTP)
- **Identity Provider Issuer** - Enter the Issuer Url from OneLogin SaaS (Slack) Application SSO settings (from step 4.1)
- **Public Certificate** - Enter the certificate from OneLogin SaaS (Slack) Application SSO settings (from step 4.2)
- **Sign In Button Label** - Enter “OneLogin”

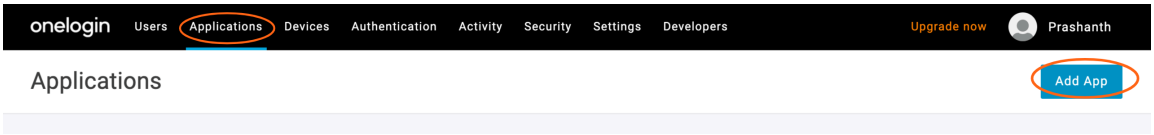


5.4 Click **Save Configuration** to verify and complete SSO setup.

Phase 3. Configure IdP-initiated Access

Step 6. Configure Proxy SaaS Application

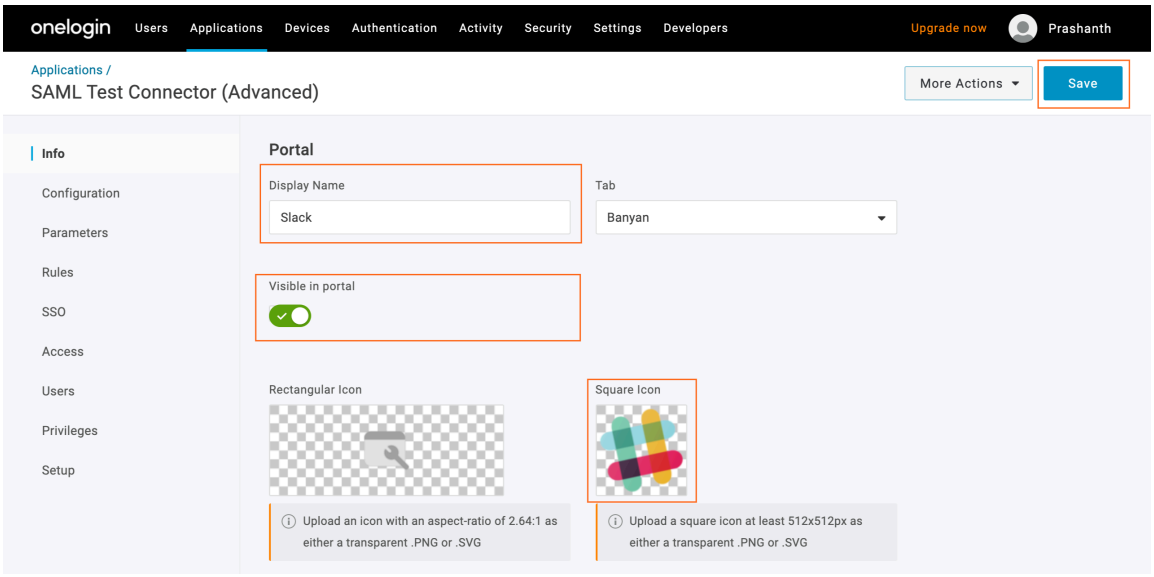
6.1 In OneLogin, navigate to **Applications** and then select **Add App**.



6.2 Search for “SAML Test Connector”, select **SAML Custom Connector (Advanced)**, and then click `Save`.

6.3 Navigate to the **Info** tab and then update the following fields:

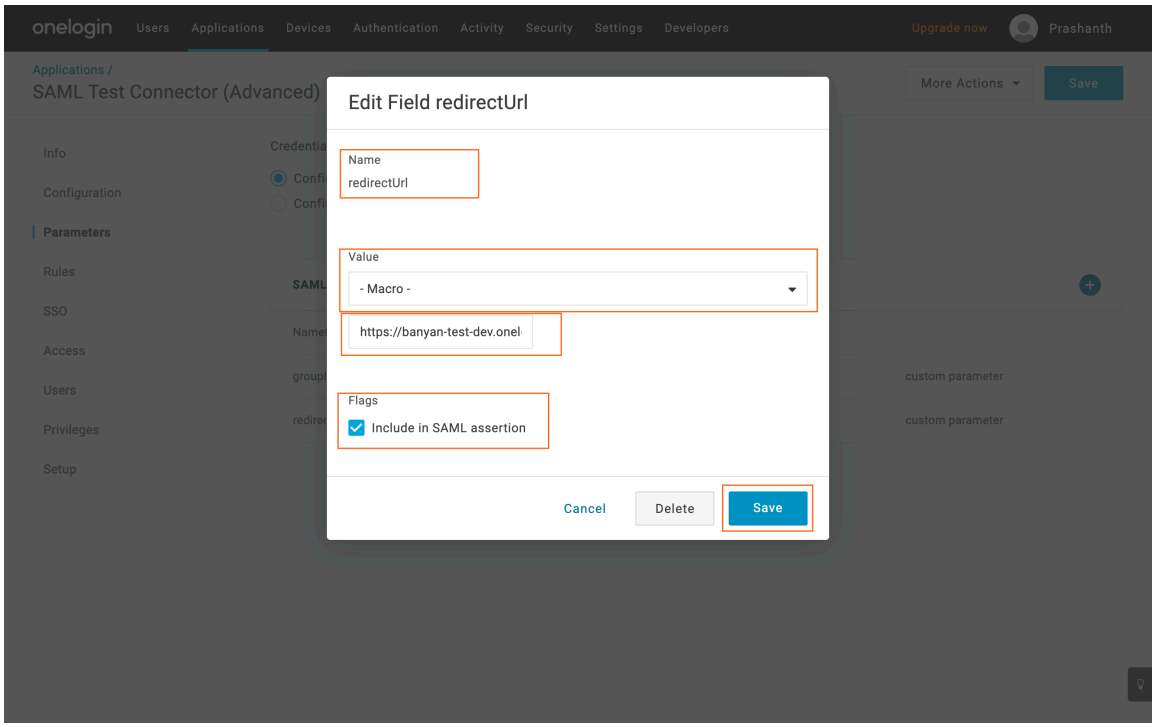
- **Display Name** - Enter the app name (such as “Slack”)
- **Visible in portal** - Checked/enabled
- **Square Icon** - Upload the app logo icon (such as the Slack logo icon)



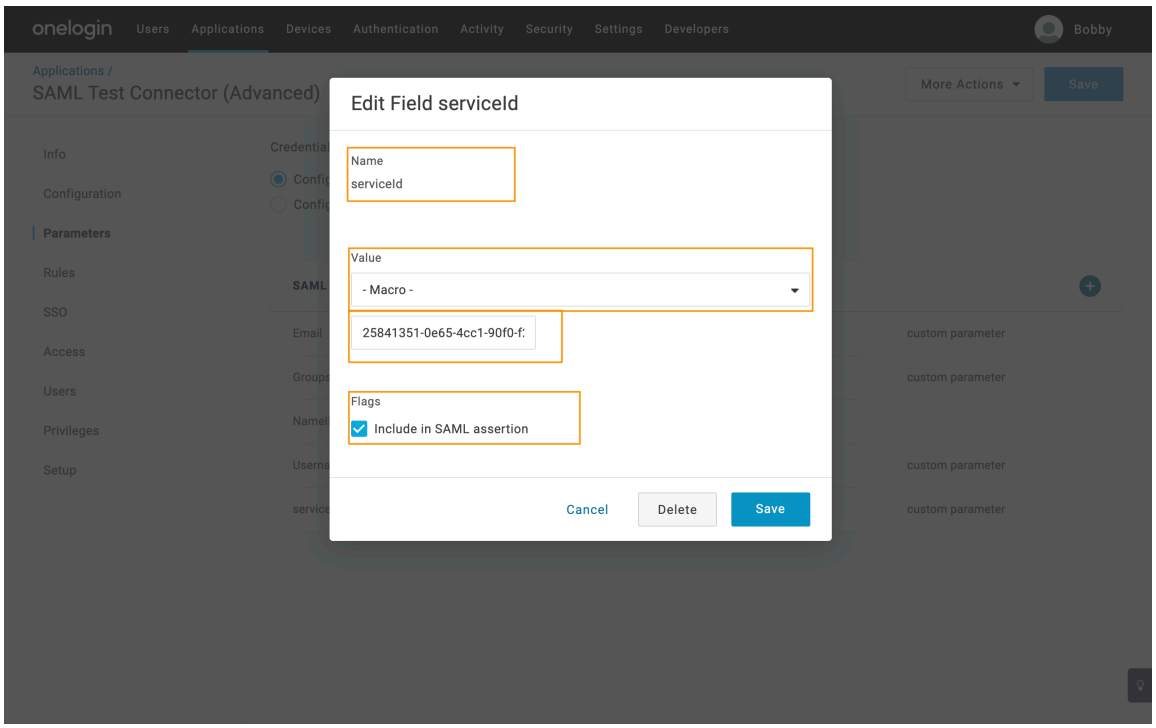
6.4 Save.

6.5 Navigate to the **Parameters** tab and then add `redirect url` and `serviceId`.

- To add `redirectUrl`, select the Plus icon and enter:
  - **Name** - Enter “redirectUrl”, then click **Save**
  - **Value** - Select **Macro** and then enter the application’s SAML 2.0 Endpoint (HTTP) URL
  - **Flags** - Check the **Include in SAML assertion** checkbox



- To add `serviceId`, selec the Plus icon and enter:
  - **Name** - Enter `serviceId`, then click **Save**
  - **Value** - Select **Macro** and then enter your SaaS Application ID from the CSE Command Center.
  - **Flags** - Check the **Include in SAML assertion** checkbox

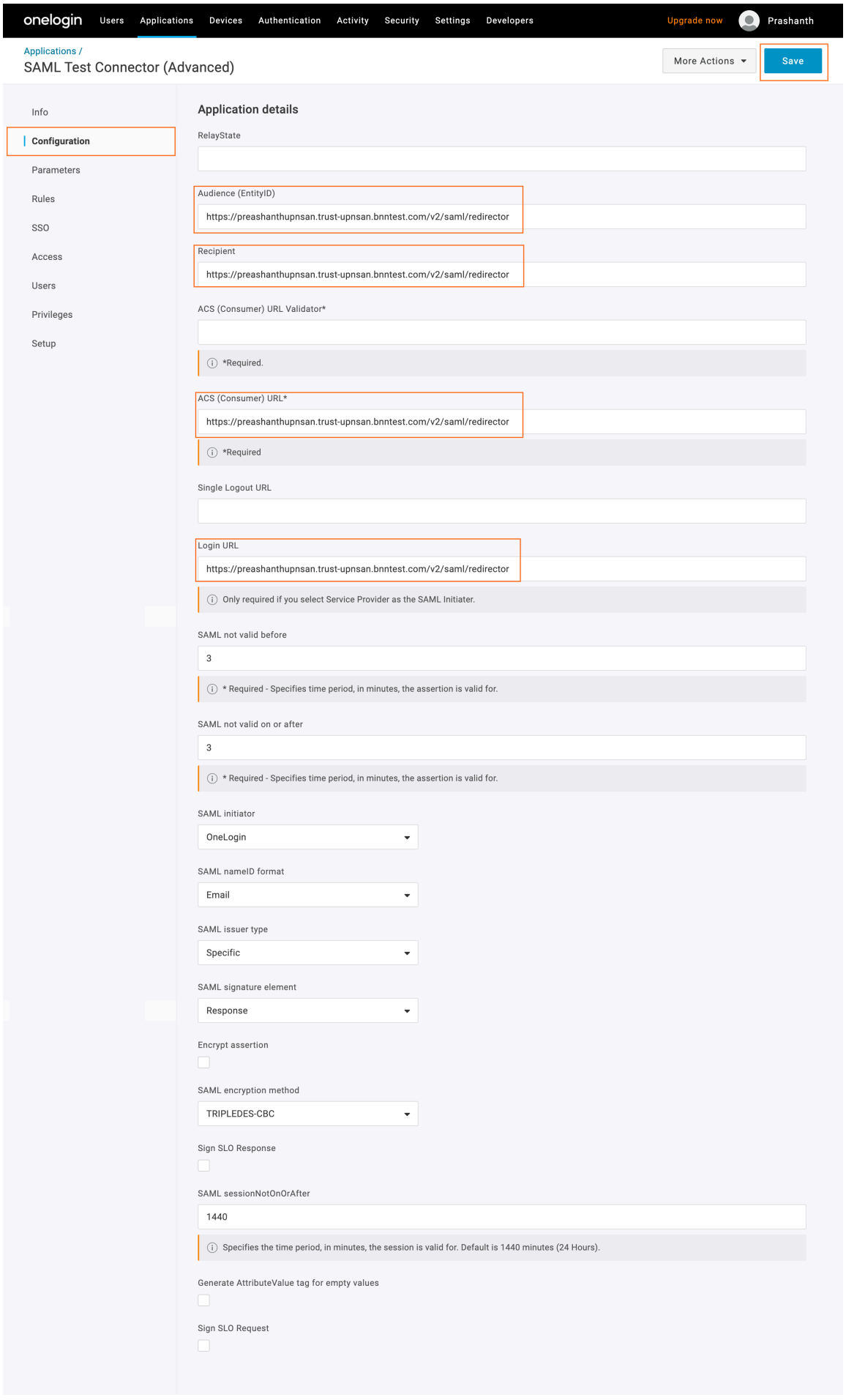


6.6 Save, and then select **Save** again to update the parameters.

6.7 Navigate to the **Configuration** tab and enter the **SAML Proxy URL** from the IDP Routed App in the Command Center.

- **Audience (EntityID)**

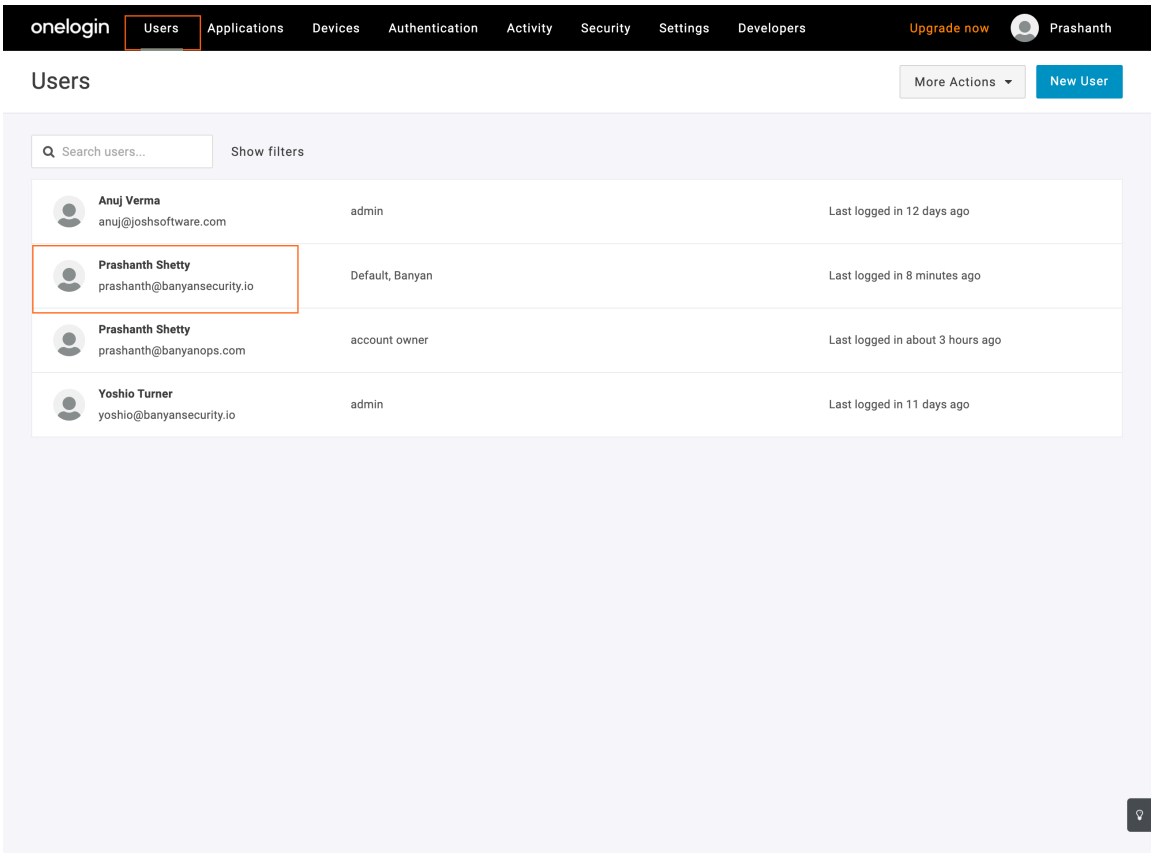
- **Recipient**
- **ACS (Consumer) Url**
- **Login Url**


onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Upgrade now
Prashanth
Applications /
SAML Test Connector (Advanced)
More Actions
Save
Info
Configuration
Parameters
Rules
SSO
Access
Users
Privileges
Setup
Application details
RelayState
Audience (EntityID)
https://preashanthupnsan.trust-upnsan.bnntest.com/v2/saml/redirector
Recipient
https://preashanthupnsan.trust-upnsan.bnntest.com/v2/saml/redirector
ACS (Consumer) URL Validator*
*Required.
ACS (Consumer) URL*
https://preashanthupnsan.trust-upnsan.bnntest.com/v2/saml/redirector
*Required
Single Logout URL
Login URL
https://preashanthupnsan.trust-upnsan.bnntest.com/v2/saml/redirector
Only required if you select Service Provider as the SAML Initiater.
SAML not valid before
3
* Required - Specifies time period, in minutes, the assertion is valid for.
SAML not valid on or after
3
* Required - Specifies time period, in minutes, the assertion is valid for.
SAML initiator
OneLogin
SAML nameID format
Email
SAML issuer type
Specific
SAML signature element
Response
Encrypt assertion
SAML encryption method
TRIPLEDES-CBC
Sign SLO Response
SAML sessionNotOnOrAfter
1440
Specifies the time period, in minutes, the session is valid for. Default is 1440 minutes (24 Hours).
Generate AttributeValue tag for empty values
Sign SLO Request

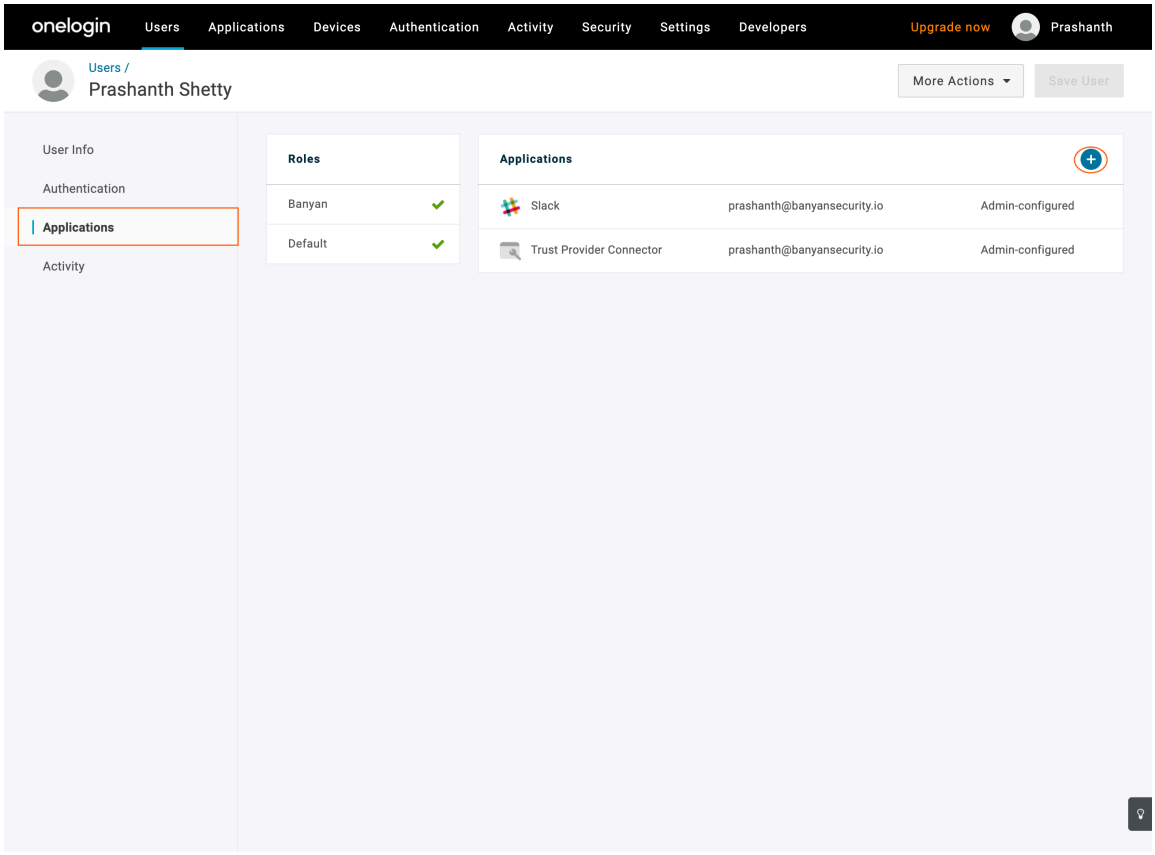
6.8 Save.

Step 7. Assign Users to Application

7.1 In OneLogin, navigate to **Users** and then select a User.



7.2 Navigate to the **Applications** tab and then click the plus icon (+) to add a new Application.

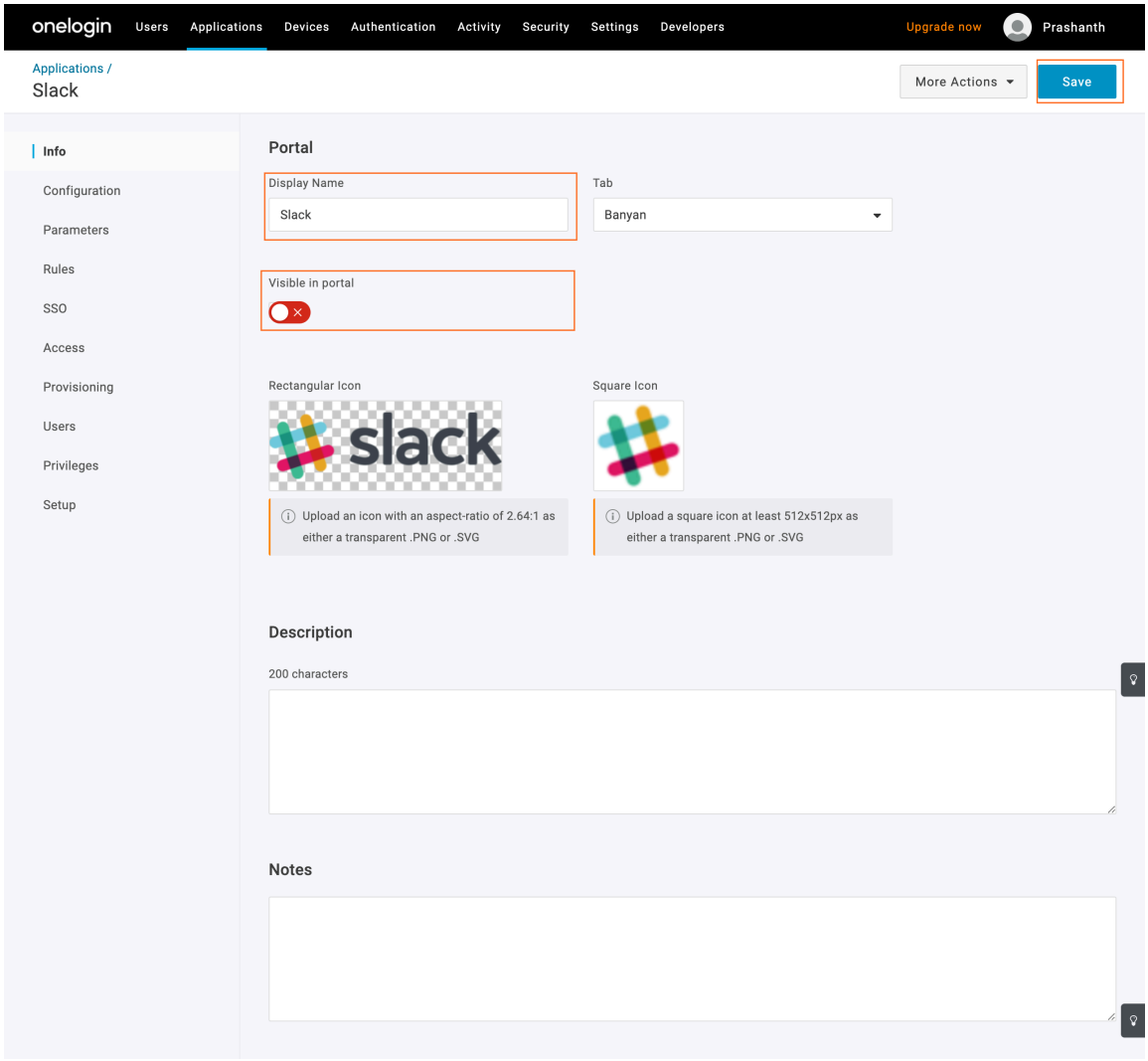


7.3 Add Slack and Slack proxy application to the user.

7.4 Click **Save User**.

Step 8. Disable Original Application from OneLogin Catalog

8.1 Navigate to **Info** and then disable **Visible in portal**.



Enabling Passwordless

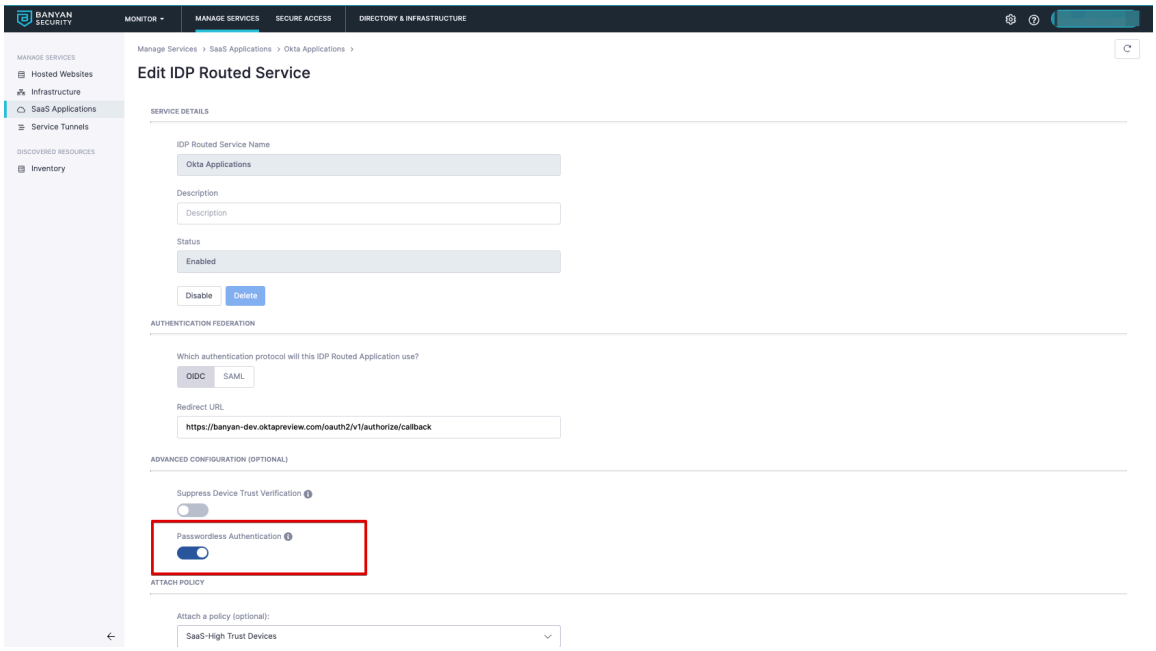
> Passwordless is recommended to provide an optimal user experience when accessing applications on CSE registered devices. If Passwordless is not enabled, end users will default to OneLogin's authentication methods.

Passwordless authentication with CSE leverages the fact that the trusted Device Certificate includes the user's email address in the `UserPrincipalName` SAN extension field.

When passwordless is enabled, the device certificate that is presented during device trust will be used to extract the user who is attempting to authenticate. The identified user will be issued a TrustToken without requiring username and password. The user will then proceed with OneLogin's authentication configurations for the user selected application such as adding MFA.

6.1 Edit the existing CSE IDP Routed Service for OneLogin (**Step 2.3**)

6.2 Enable **Passwordless Authentication**



SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

Concepts

Components

Release Notes

Guides

Quick Start Guides

Solutions

Feature Guides

API Guide