

Home > Public Applications > OneLogin >

# 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

How it Works

Prerequisites

Setup

Phase 1. Configure CSE as a OneLogin Trusted IDP

Phase 2. Configure SP-initiated Access

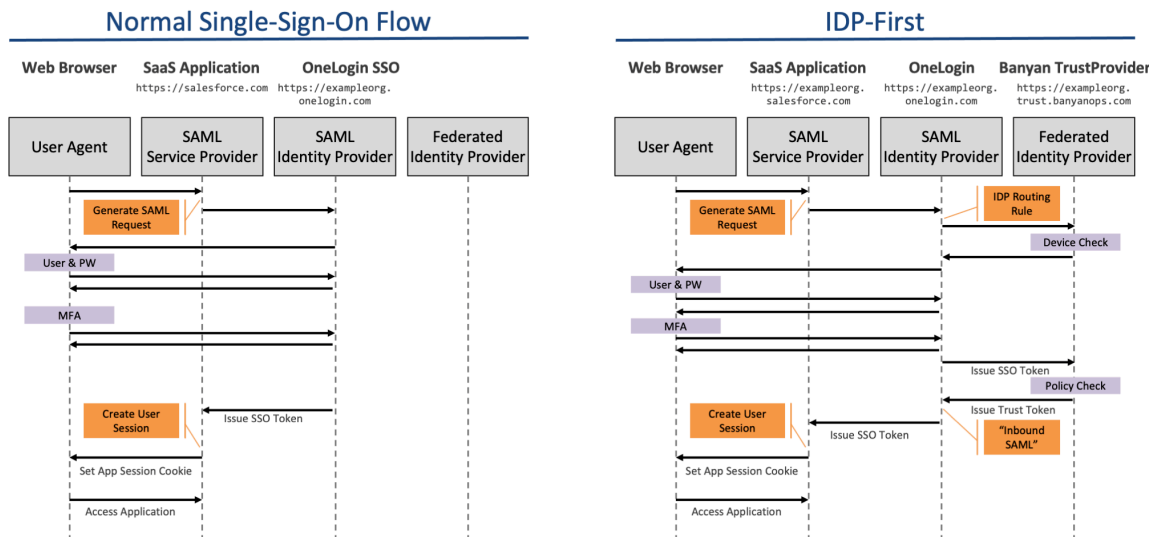
Phase 3. Configure IdP-initiated Access

Enabling Passwordless

## 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.

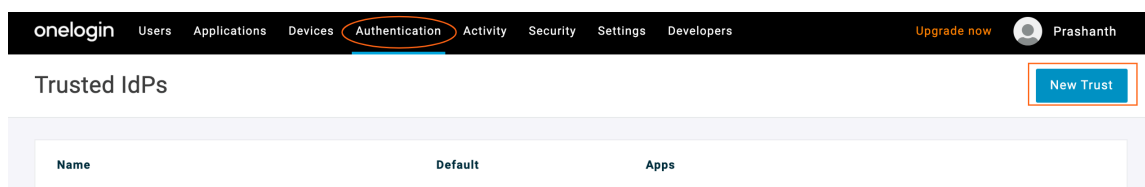
This phase sets up applications launched from the OneLogin catalog to use CSE TrustProvider for ZeroTrust policy checks.

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

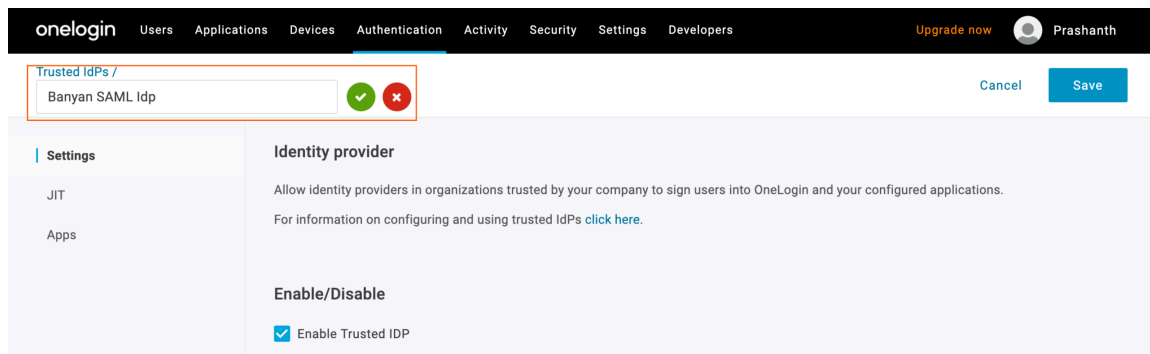
## Phase 1. Configure CSE as a OneLogin Trusted IDP #

### 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.



The screenshot shows the OneLogin interface. At the top, the navigation bar includes 'onelogin', 'Users', 'Applications', 'Devices', 'Authentication', 'Activity', 'Security', 'Settings', and 'Developers'. The user 'Prashanth' is logged in. The 'Trusted IdPs' section is highlighted, showing a list with 'Banyan SAML Idp' and a green checkmark icon. Below this, the 'Settings' tab is active, displaying the 'Identity provider' configuration. The 'Enable/Disable' section has the 'Enable Trusted IDP' checkbox checked.

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

**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

① The URL to the icon or SVG file that will display on login panel.

#### Configurations

Issuer

① The issuer name or URL of the remote identity provider.

Email Domains

① 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

① The Trusted IDP response attribute which value is used for User Attribute Mapping.

User Attribute Mapping

Allowed Email Domains

① 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



① 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

① Where OneLogin redirects users to initiate SAML SSO

SP Entity ID  
<https://banyan-test-dev.onelogin.com/sp/1e4382fd-8c63-4022-83ac-30ccff7bcddb>

① This value is expected as the Audience element of the SAML response and will be used as the Issuer of the generated SAML AuthN request (if IdP Login URL is configured). Please register this value at the Identity Provider.

**Trusted IdP Certificate**

X.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIICwDCAgIgaAwIBAgIQUoYkHdZLxL3u/Es8DrZhwTANBkqhkiG9w0BAQsFADAa
MRgwFgYDVQQKEw9CYW55YW4gU2VidXJpdHkwdHcnMjAwNjA5MTg0TU5hcnMzAw
NjA3MTg0TU5hcnMzAwMRgwFgYDVQQKEw9CYW55YW4gU2VidXJpdHkwdHcnMzAw
SIB3DQEBBAQAA4IBDwAwggEKAoIBAQCjABYu13REeVRVZn4hHuNCS8rR0HDeeAUu
oDAgOyovfiZ9Jt8hktxyA8Vvx86pUXkLM7c7yvDX/B40cC14D7eyeb5jTC0YxZhp
K7n4VpozTuGpsEW7Yhx5A6gZbBwetMBTr+NIxF81Mhnj9V6cUvImMVTx5Z7hpXpRy
A0p1jk/vFgF1vhrqLadhRHK+RoahZ3LsnJ04eGd8gaKE05thkAUWpGzKH8nNUTf
jf1aaDFFNacBxe7ysDrsDHBRTQ4S+rXOLa4mQiebFz8P5caAzPEtuuX5UYzwJ
4DtDKeKEIiCqfQoeDYAuZ3YXV0GVSNL7ZFTpX10dqCV9Mi0LSjAgMBAAGjAIAA
MA0GCSqGSIb3DQEBCAUAA4IBAQB6+fZ2xbONir3H+d4xQK/gg4hggYcUky3vcM+E
P5yYfz85CPM1b5UE1Wsn0XWf344UblZu98Ue09CGGeowRWH04eipRn+/ZQekkiP
Mj4n101J7By4ou37ZAIhKGeN+gUoiKfiVURKjQoqPni.f54Je0pkanXtL7JQxOfT
-----
```

**Encryption**

Enable encrypted assertions

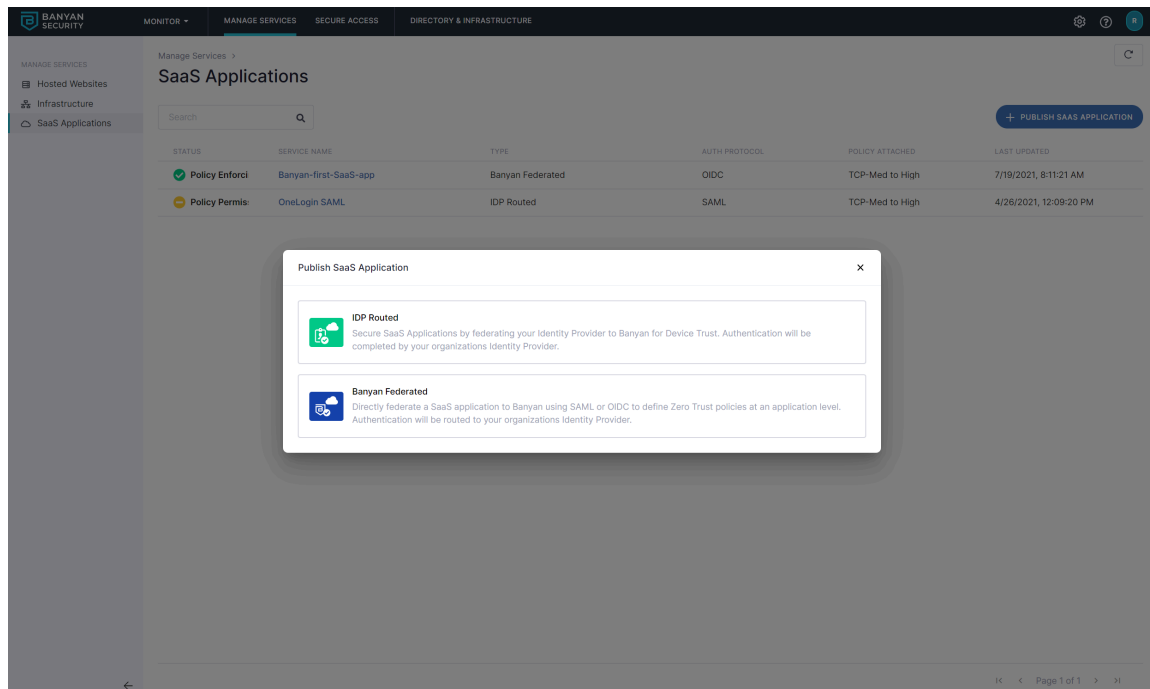
① The entire message must be signed. OneLogin does not support SAML responses with signed, encrypted assertions unless the message is also signed.

## 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**.

STATUS	SERVICE NAME	TYPE	AUTH PROTOCOL	POLICY ATTACHED	LAST UPDATED
<span style="color: green;">✔</span> Policy Enforci	Banyan-first-SaaS-app	Banyan Federated	OIDC	TCP-Med to High	7/19/2021, 8:11:21 AM
<span style="color: orange;">⚠</span> Policy Permis	OneLogin SAML	IDP Routed	SAML	TCP-Med to High	4/26/2021, 12:09:20 PM

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

**Register IDP Routed Service**

**SERVICE DETAILS**

IDP Routed Service Name:

Description (optional):

**AUTHENTICATION FEDERATION**

Which authentication protocol will this IDP Routed Application use?

OIDC  SAML

Redirect URL (SAML ACS):

Audience URI (Service Provider Entity ID):

Name ID Format:

Select Name ID Value:

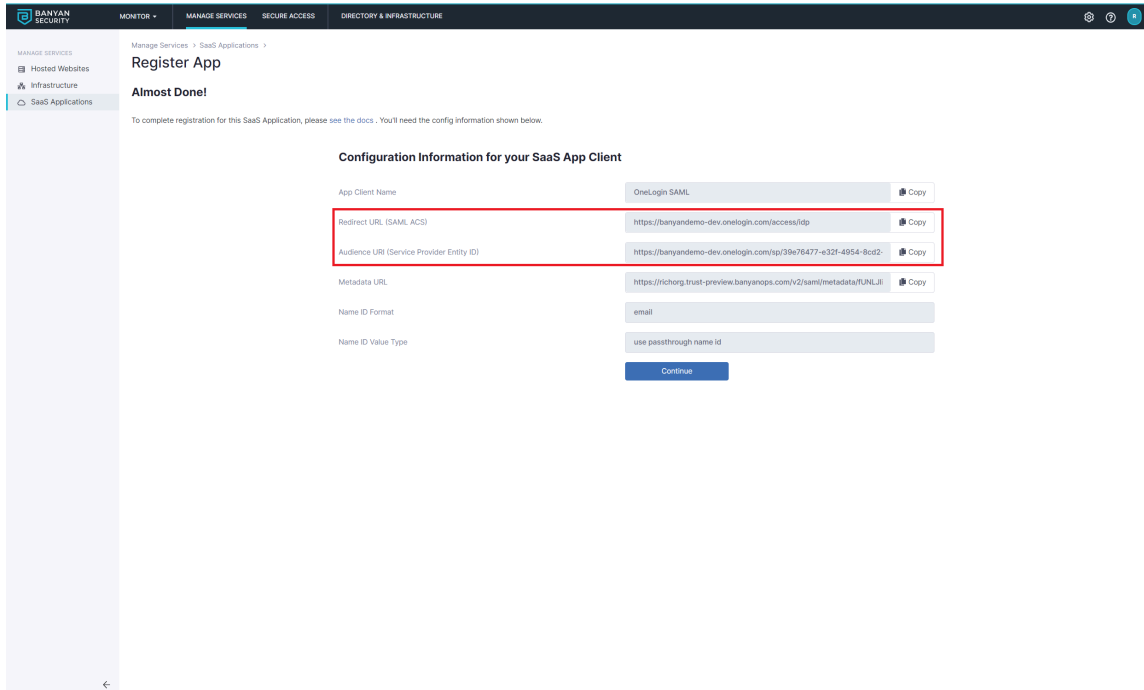
**ATTACH POLICY**

Attach a policy (optional):

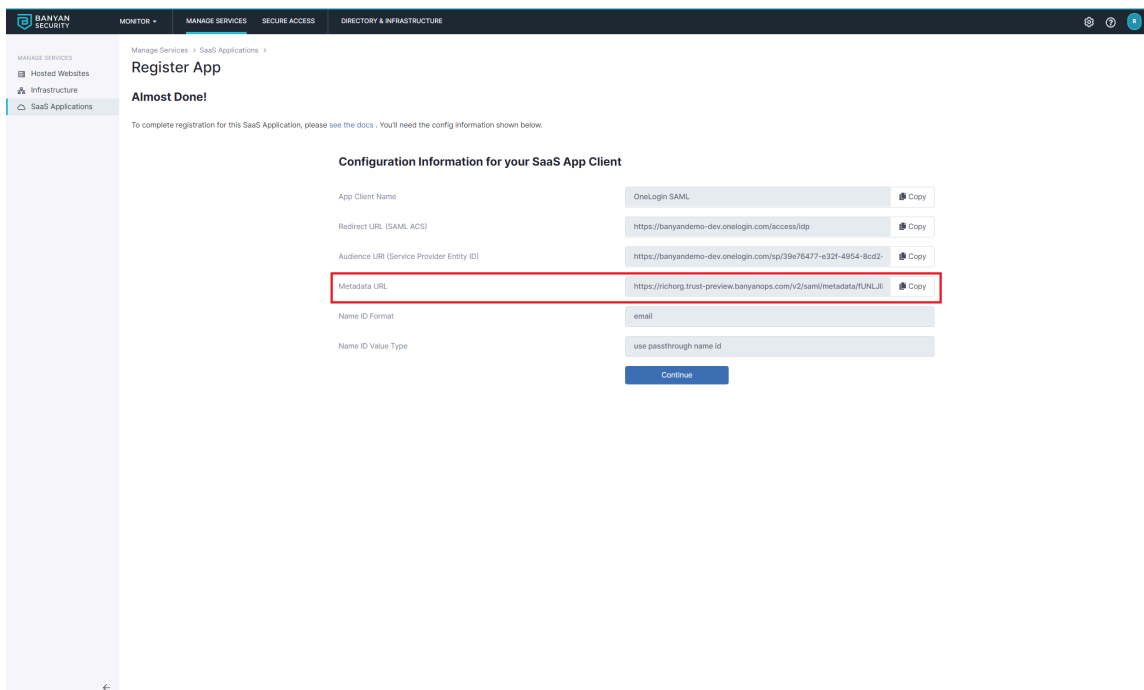
Choose an enforcement mode:  Permissive  Enforcing

## 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.



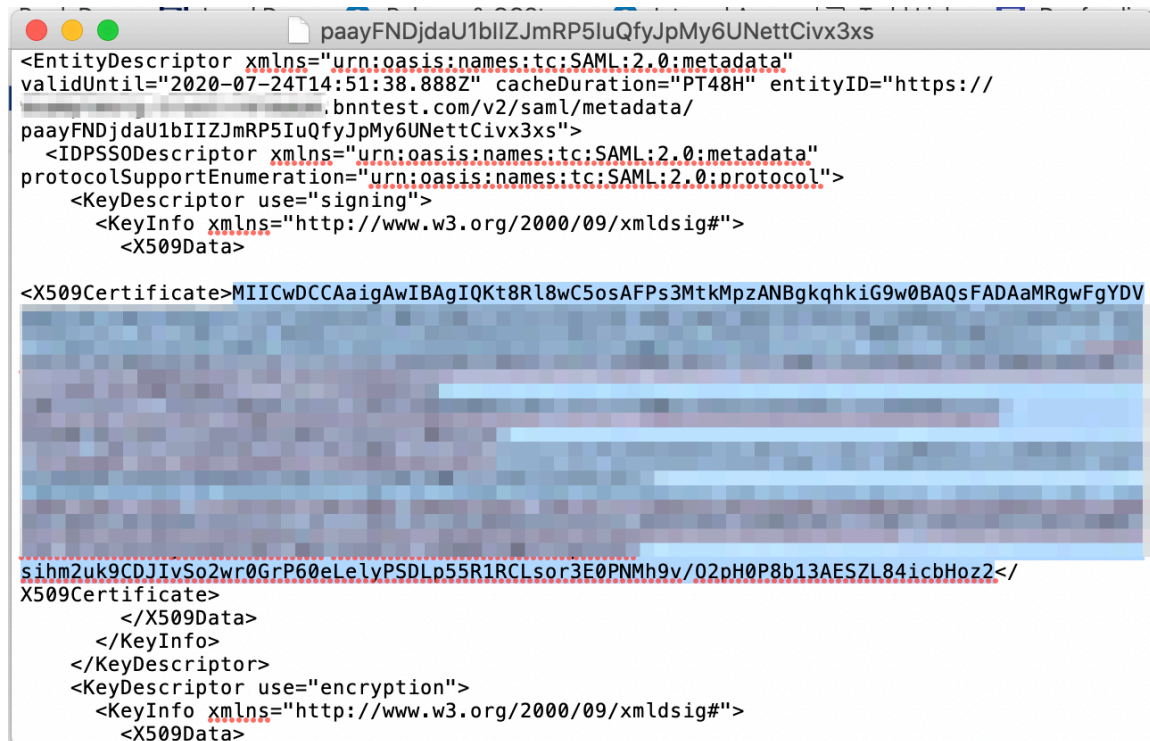
2.6 Also, copy the **Metadata URL**, paste it in your browser search bar and then press enter to download the xml file. You will use the information in this file to configure SSO in OneLogin.



## 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.



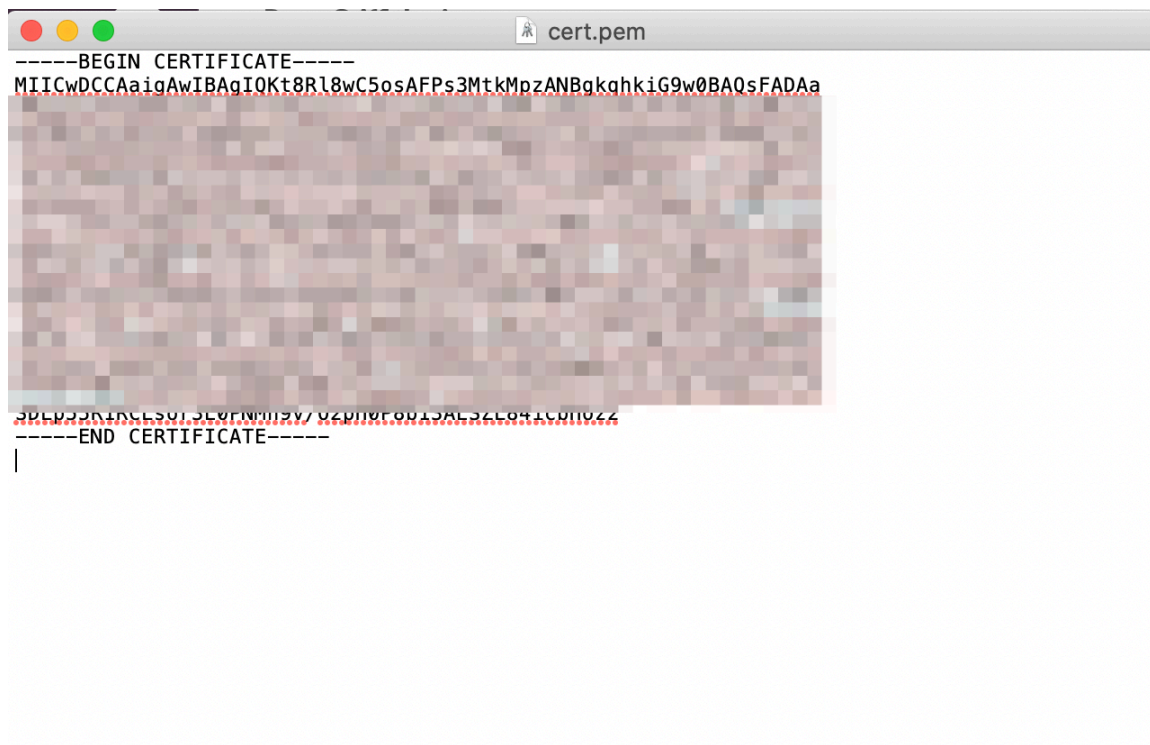
```

paayFNDjdaU1bIIIZJmRP5IuQfyJpMy6UNettCivx3xs
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
validUntil="2020-07-24T14:51:38.888Z" cacheDuration="PT48H" entityID="https://
.bnnstest.com/v2/saml/metadata/
paayFNDjdaU1bIIIZJmRP5IuQfyJpMy6UNettCivx3xs">
  <IDPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
<X509Certificate>MIICwDCCAaigAwIBAgIQKt8Rl8wC5osAFPs3MtkMpzANBgkqhkiG9w0BAQsFADAaMRgwFgYDV
[Redacted]
sihm2uk9CDJivSo2wr0GrP60eLelyPSDLp55R1RCLsor3E0PNMh9v/02pH0P8b13AESZL84icbHoz2</
X509Certificate>
  </X509Data>
</KeyInfo>
</KeyDescriptor>
<KeyDescriptor use="encryption">
  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <X509Data>

```

### 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:

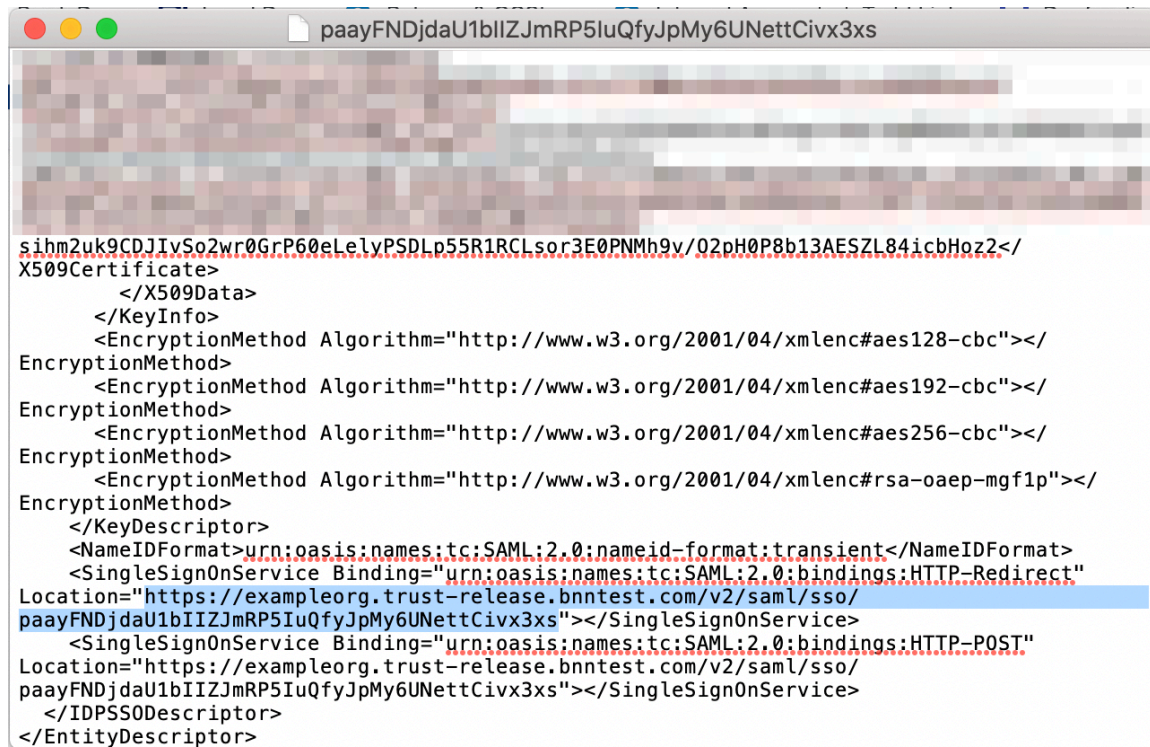


```

cert.pem
-----BEGIN CERTIFICATE-----
MIICwDCCAaigAwIBAgIQKt8Rl8wC5osAFPs3MtkMpzANBgkqhkiG9w0BAQsFADAa
[Redacted]
-----END CERTIFICATE-----

```

**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.



```

sihm2uk9CDJIVSo2wr0GrP60eLelyPSDLp55R1RCLsor3E0PNMh9v/02pH0P8b13AESZL84icbHoz2</
X509Certificate>
  </X509Data>
  </KeyInfo>
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></
EncryptionMethod>
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes192-cbc"></
EncryptionMethod>
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"></
EncryptionMethod>
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"></
EncryptionMethod>
  </KeyDescriptor>
  <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://exampleorg.trust-release.bnntest.com/v2/saml/sso/
paayFNDjdaU1bIIJmRP5IuQfyJpMy6UNettCivx3xs"></SingleSignOnService>
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://exampleorg.trust-release.bnntest.com/v2/saml/sso/
paayFNDjdaU1bIIJmRP5IuQfyJpMy6UNettCivx3xs"></SingleSignOnService>
</IDPSSODescriptor>
</EntityDescriptor>

```

## 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

① The URL to the icon or SVG file that will display on login panel.

### Configurations

Issuer

① The issuer name or URL of the remote identity provider.

Email Domains

① 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

① The Trusted IDP response attribute which value is used for User Attribute Mapping.

User Attribute Mapping

Allowed Email Domains

① 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

① 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

① Where OneLogin redirects users to initiate SAML SSO

SP Entity ID

https://banyan-test-dev.onelogin.com/sp/1e4382fd-8c63-4022-83ac-30ccff7bcddb

This value is expected as the Audience element of the SAML response and will be used as the Issuer of the generated SAML AuthN request (if IdP Login URL is configured). Please register this value at the Identity Provider.

**Trusted IdP Certificate**

X.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIICwDCSAqiGAWIABAgTQOoYkHdZLxL3u/Es8DrZhwTANBkakahkiG9w0BAQsFADAa
MRgwFgYDVQKKEw9CYW55YW4gU2VidXJpdHkwHhcnMjAwNjA5MTa0TU5hcnMzAw
NjA3MTg0TU5WjAqMRgwFgYDVQKKEw9CYW55YW4gU2VidXJpdHkwGgEiMA0GCsAg
SIB3DQEBBAQUAA4IBDwAwggEKAoIBAQcjABYuI3REeVRVZn4hHuNCS8rR0HDesAUu
oDAgOyovfiZ9Jt8hktxyA8Vvx86pUXkLM7c7yvDX/B40cC14D7eyeb5jTC0YxZhp
K7n4VpozTuGpsEWZyh5A6gZbBwetMBTr+NXf81Mhnj9V6cUvimMVTx5Z7hpXpRy
A0p1Jk/vFgF1vhrqLadhRHk+RoahZ3LsnJ04eGd8gkE05thkAUWpGw2KH8nNUTf
jf1aaDFFNacBxe7ysDrSDHBR2TQ45+rXOLa4mQjebfz8P5caIAzPEtuuX5UYzwJ
4dTDKeKEiCqfQoeDYAuZ3YXV0GV5NL7ZFTpX10dqCV9Mi0Ls5jAgMBAAGjAIAA
MA0GCsAgSIB3DQEBcwAA4IBAQB6+fZ2xbONir3H+d4xQK/gg4hggYcUky3vcM+E
P5yYfyz85CPM1b5UE1Wsn0XWf344UBLZu98Ue09CGGeowRHH04eipRn+/ZQekkiP
Mj4n101J7By4ou37ZAihkGeN+gUoiCKfiVURKjQoaPni.f54Je0pkanXtL7JQx0ft
```

**Encryption**

Enable encrypted assertions

The entire message must be signed. OneLogin does not support SAML responses with signed, encrypted assertions unless the message is also signed.

4.2 Click **Save**.

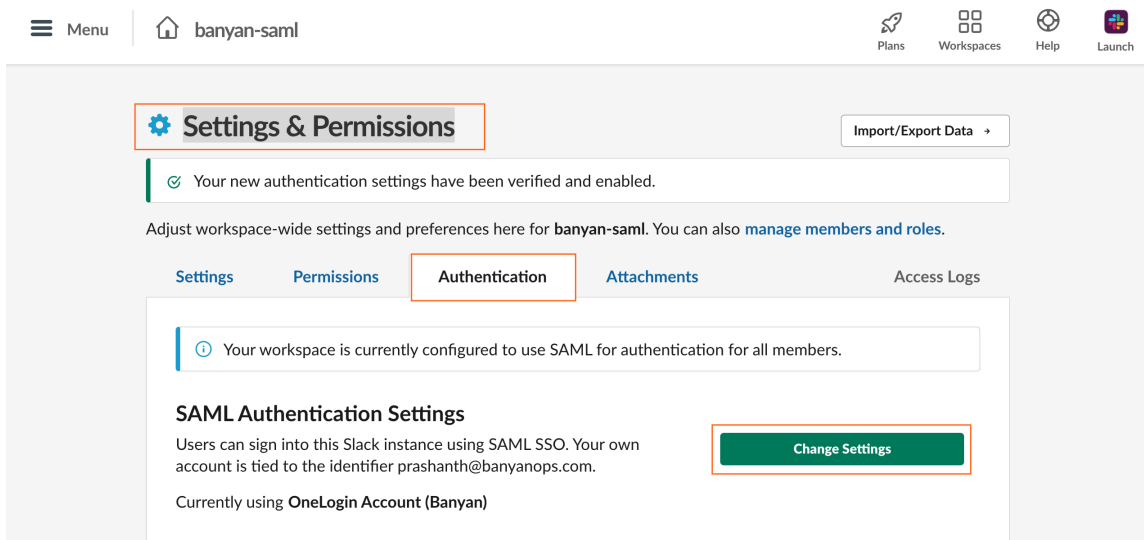
## Phase 2. Configure SP-initiated Access #

### 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"

### Configure SAML Authentication for OneLogin

Configure

Follow the steps below to set up OneLogin authentication. When this is complete, members will receive an email with a link to connect their Slack and OneLogin accounts.

#### SAML SSO URL

Enter your SAML 2.0 Endpoint URL (HTTP).

https://banyan-test-dev.onelogin.com/trust/saml2/http-post/s

+ Show instructions

#### Identity Provider Issuer

The IdP Entity ID for the service you use.

https://app.onelogin.com/saml/metadata/ae37d6db-7b99-4fd

#### Public Certificate

OneLogin Account (Banyan), expiring June 9th, 2025 (edit)

Copy and paste your entire x.509 Certificate here.

-----BEGIN CERTIFICATE-----
MIID2DCCA5CgAwIBAgIUURgdCxdn85V+jOv/KBtfbAHpfKQwDQYJKoZIhvcNAQEF
BQAwRDEPMA0GA1UECgwGQmFueWZlZmVudWwMRUwEwYDVQLDAXPbmVmb
2dohRlZFAxGiAY

+ Show instructions

#### Advanced Options

expand

#### Settings

- Update profile each time a user logs in
Allow users to change their email address
Allow users to choose their own display name
Authentication for your workspace must be used by:
All workspace members
All workspace members, except guest accounts
It's optional

#### Customize

##### Sign In Button Label

OneLogin

##### Button Preview



Do you have a nickname for your SSO system? Add it to the Sign In Button!

This is what your Sign In Button will look like.

Save Configuration

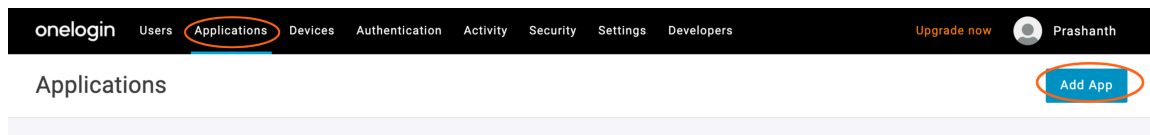
Emails will be sent to workspace members who have not set up SSO for their Slack accounts.

5.4 Click Save Configuration to verify and complete SSO setup.

## Phase 3. Configure IdP-initiated Access #

### Step 6. Configure Proxy SaaS Application

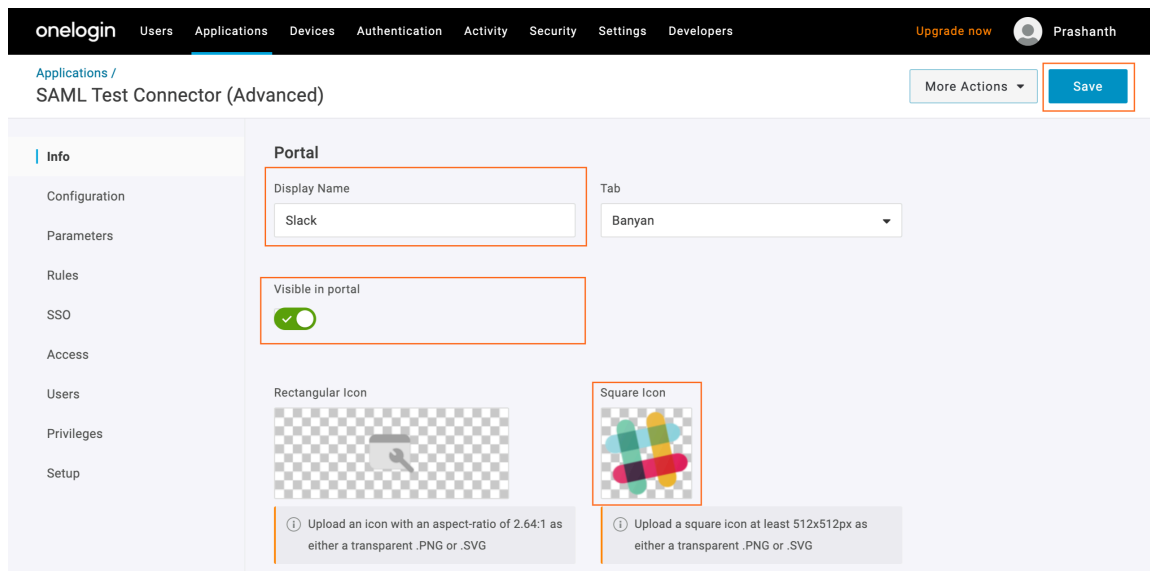
## 6.1 In OneLogin, navigate to **Applications** and then select **Add App**.



## 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:

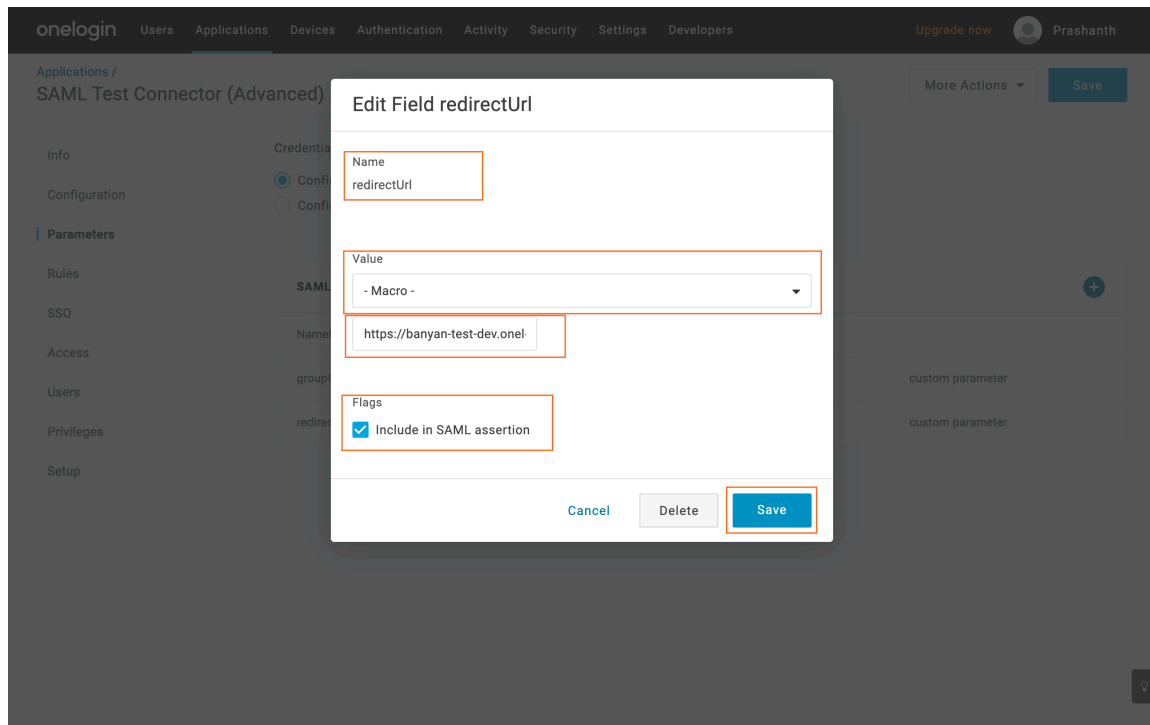
- **Display Name** - Enter the app name (such as "Slack")
- **Visible in portal** - Checked/enabled
- **Square Icon** - Upload the app logo icon (such as the [Slack logo icon](#))



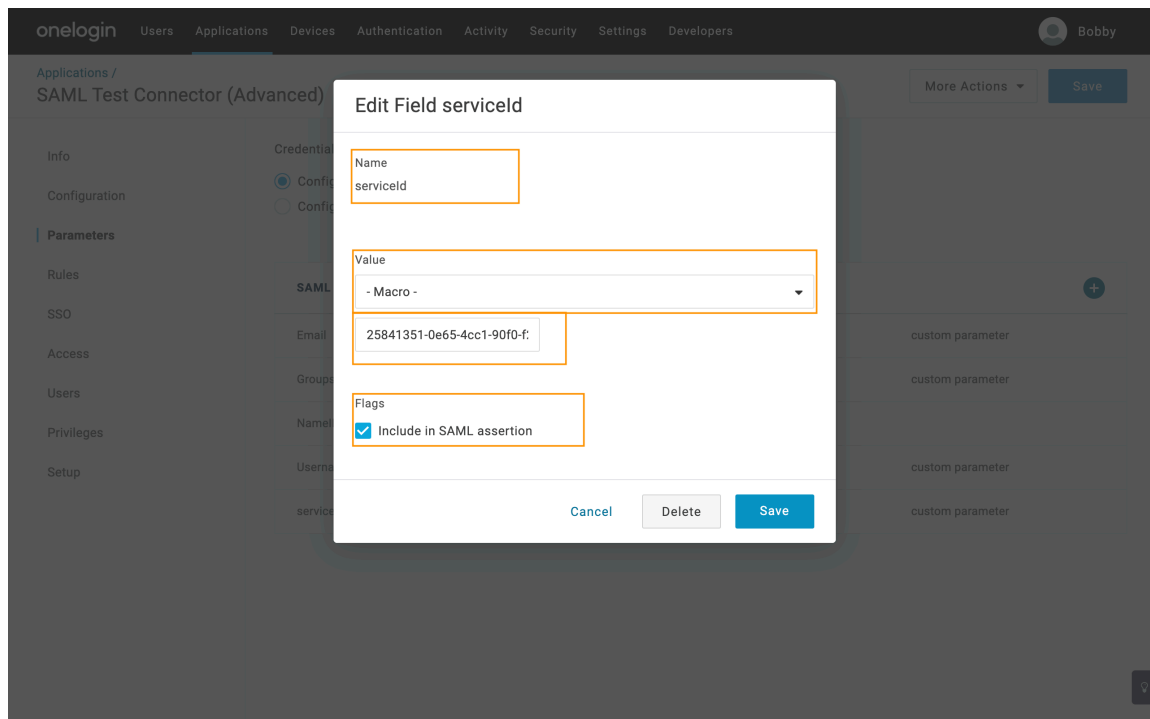
## 6.4 Save.

## 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**, select 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 Initiator.

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).

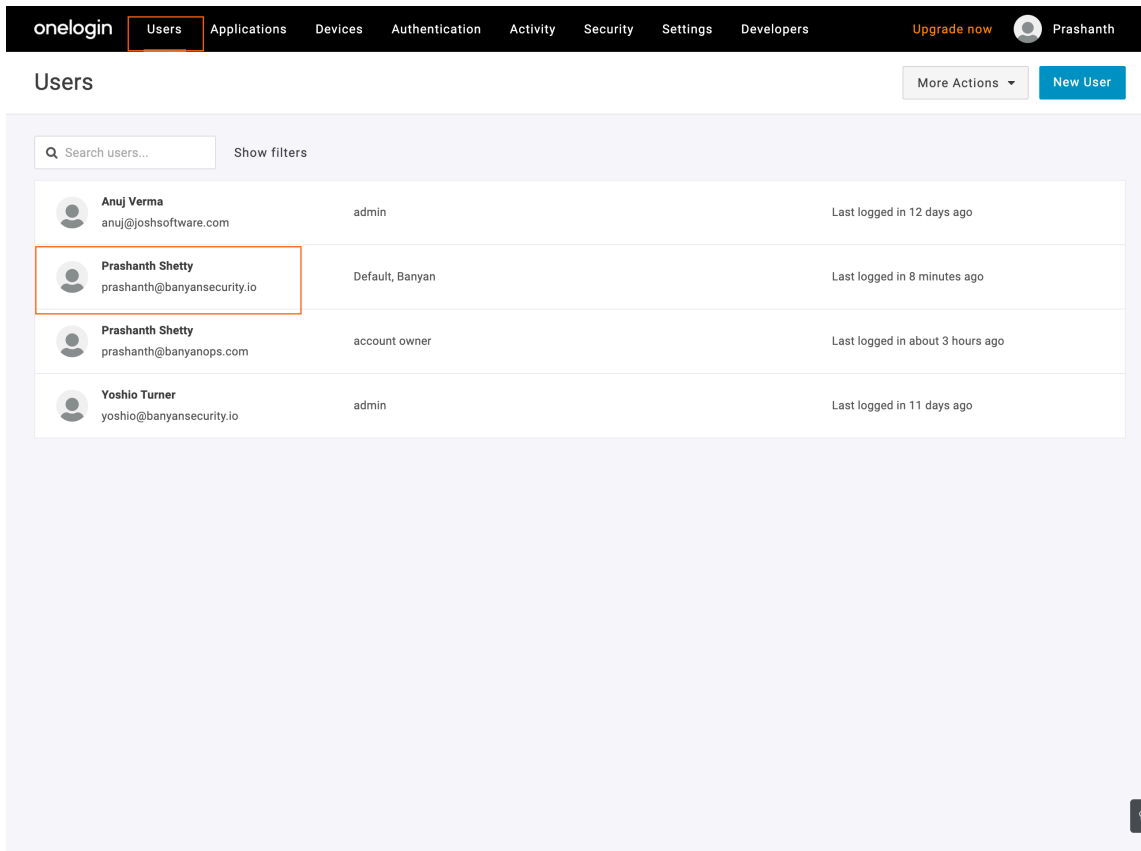
Generate AttributeValue tag for empty values

Sign SLO Request

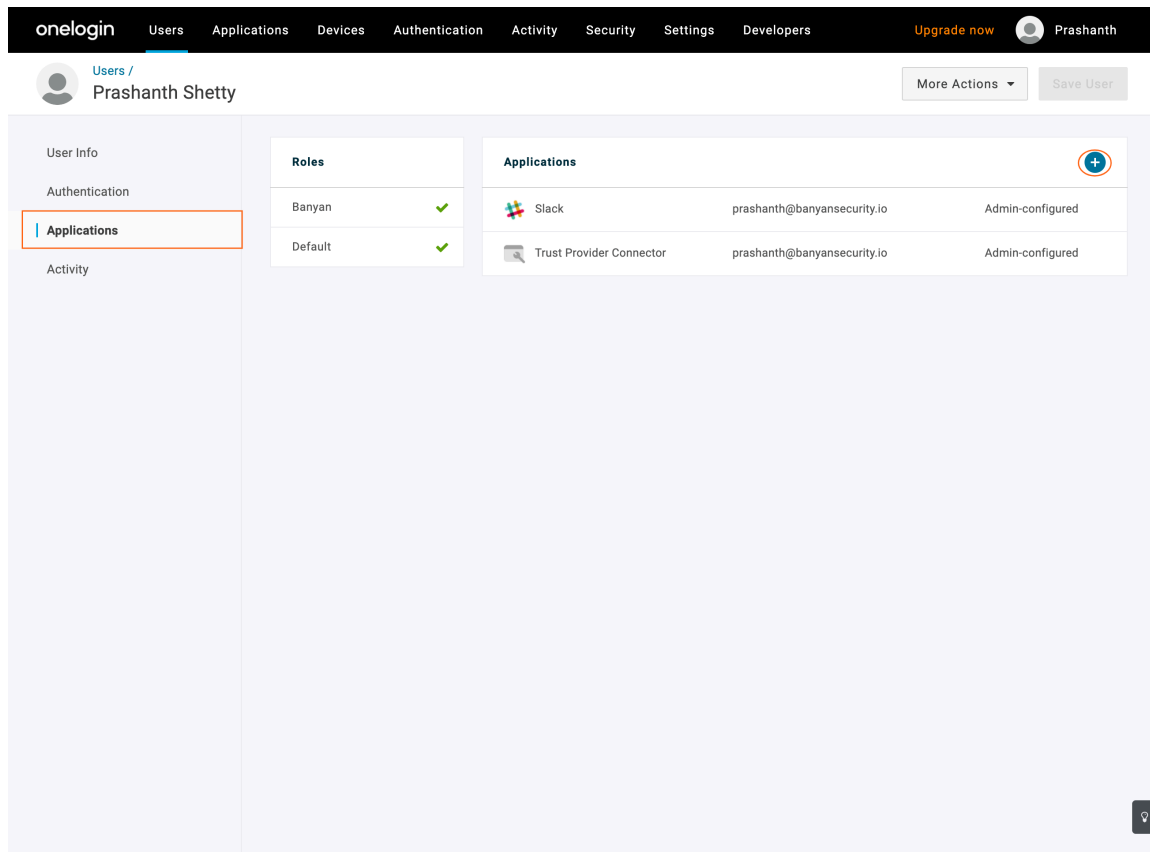
## 6.8 Save.

## 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.



The screenshot shows the OneLogin user management interface for user Prashanth Shetty. The 'Applications' tab is selected and highlighted with an orange border. The interface displays the following information:

Roles	Applications
Banyan ✓	Slack prashanth@banyansecurity.io Admin-configured
Default ✓	Trust Provider Connector prashanth@banyansecurity.io Admin-configured

**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**.

The screenshot shows the OneLogin configuration interface for a Slack application. The top navigation bar includes 'onelogin', 'Users', 'Applications', 'Devices', 'Authentication', 'Activity', 'Security', 'Settings', and 'Developers'. The user 'Prashanth' is logged in. The main content area is titled 'Applications / Slack' and includes a 'More Actions' dropdown and a 'Save' button. A left sidebar lists various configuration categories: Info, Configuration, Parameters, Rules, SSO, Access, Provisioning, Users, Privileges, and Setup. The 'Portal' section is active, displaying a 'Display Name' field with 'Slack' and a 'Tab' dropdown with 'Banyan'. Below this is a 'Visible in portal' toggle switch, which is currently turned off. Two icon upload options are provided: 'Rectangular Icon' and 'Square Icon', each with a placeholder image of the Slack logo and specific upload instructions regarding aspect ratio and file format. The 'Description' and 'Notes' sections are empty text areas.

## 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

The screenshot shows the 'Edit IDP Routed Service' configuration page in the SonicWall Cloud Secure Edge interface. The page is divided into several sections:

- SERVICE DETAILS:** Includes fields for 'IDP Routed Service Name' (Okta Applications), 'Description', and 'Status' (Enabled). There are 'Disable' and 'Delete' buttons.
- AUTHENTICATION FEDERATION:** A section titled 'Which authentication protocol will this IDP Routed Application use?' with radio buttons for 'OIDC' (selected) and 'SAML'. Below it is a 'Redirect URL' field containing 'https://banyan-dev.oktapreview.com/oauth2/v1/authorize/callback'.
- ADVANCED CONFIGURATION (OPTIONAL):** Contains two toggle switches: 'Suppress Device Trust Verification' (disabled) and 'Passwordless Authentication' (enabled). The 'Passwordless Authentication' toggle is highlighted with a red rectangular box.
- ATTACH POLICY:** A dropdown menu labeled 'Attach a policy (optional):' with 'SaaS-High Trust Devices' selected.



© 2026. All rights reserved.

Site generated at YYYYMMDD

Links

[Concepts](#)

[Components](#)

[Release Notes](#)

Guides

[Quick Start Guides](#)

[Solutions](#)

[Feature Guides](#)

[API Guide](#)