



# Duo OneLogin

## Integration Guide



# Table of Contents

<b>Introduction.....</b>	<b>2</b>
<b>Duo Single Sign-On and OneLogin Configuration.....</b>	<b>3</b>
OneLogin Identity Provider Configuration.....	5
<b>Create a Cloud Application in Duo.....</b>	<b>8</b>
<b>Envi Configuration .....</b>	<b>11</b>

# Introduction

**Duo** multi-factor authentication adds an additional security layer between **Envi** and any **SAML 2.0** identity provider.

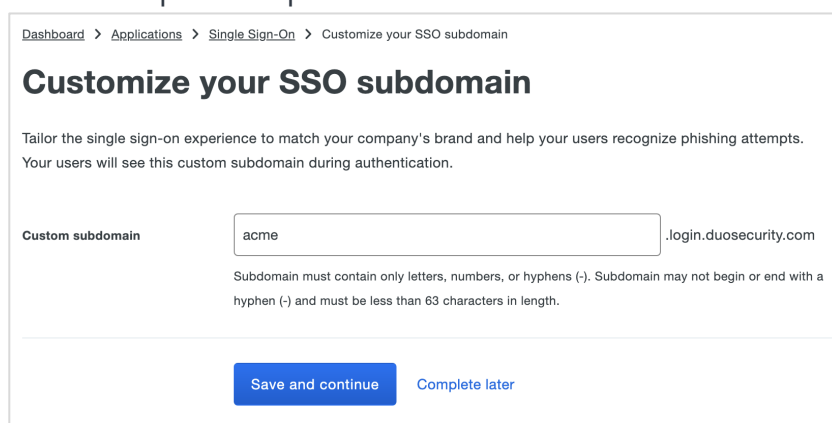
**Duo** protects your applications by using a second source of validation, like a phone or token, to verify user identity before granting access.

This step-by-step guide explains how to configure **Duo Single Sign-On** and **OneLogin** connection with your **Envi** account.

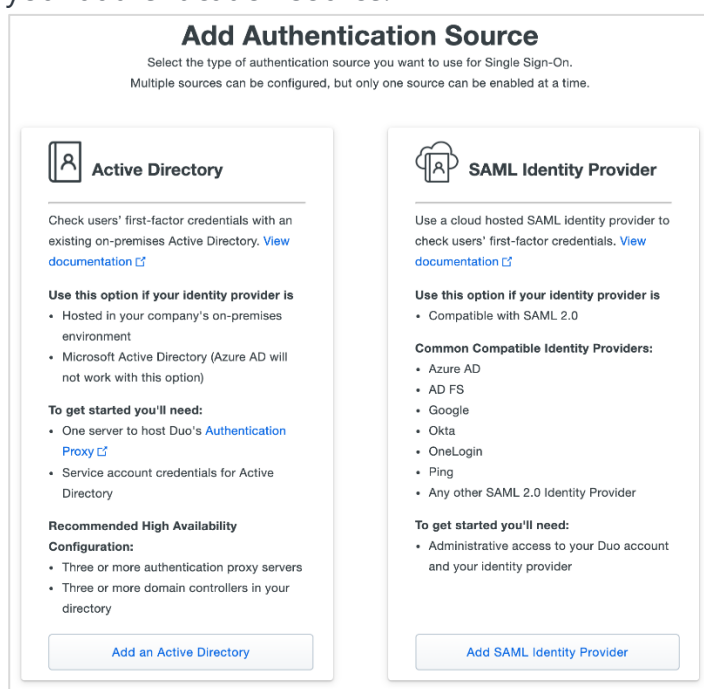
# Duo Single Sign-On and OneLogin Configuration

To add the **Duo MFA** layer to the **SAML 2.0** connection with your identity provider, perform the following steps:

1. Sign in to [Duo Admin Panel](#).
2. In the main menu, select **Single Sign-On**.
3. On the **Single Sign-On** page, review the information. If you agree to the terms, select the checkbox, and select **Activate and Start Setup**.
4. On the **Customize your SSO subdomain** page, perform the following steps:
  - a. Specify a subdomain you would like your users to see while signing in to **Duo Single Sign-On**.
  - b. For example, if you enter **acme**, users will see **acme.login.duosecurity.com** in the URL. Select **Save and continue** to use the desired subdomain or **Complete later** to skip this step for now.



5. On the **Add Authentication Source** page, select **Add SAML Identity Provider** as your authentication source.



6. Go to the **Single Sign-On Configuration** page and proceed to the section **1. Configure your SAML Identity Provider**. Here, you can either select **Download Metadata XML** or **Copy** the data from the provided boxes.

**Note:** You will need the **Duo Single Sign-On** metadata information to provide it for your **SAML Identity Provider** and to configure **Duo Single Sign-On** as a service provider.

[← Back to Single Sign-On](#)

## SAML Identity Provider Configuration

Status: Disabled
[Edit](#)
[Delete Source](#)

Configure a SAML Identity Provider to provide primary authentication for Duo Single Sign-On by following the sections below.

[Learn more about configuring the SAML Identity Provider with Duo Single Sign-On](#)

### 1. Configure the SAML Identity Provider

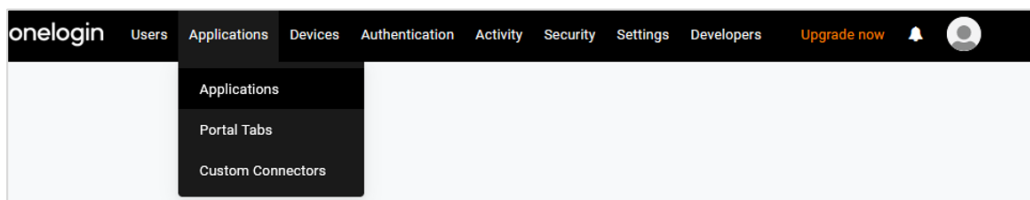
Provide this information about your Duo Single Sign-On account to your SAML identity provider.

Entity ID	<input type="text"/>	<a href="#">Copy</a>
Assertion Consumer Service URL	<input type="text"/>	<a href="#">Copy</a>
Audience Restriction	<input type="text"/>	<a href="#">Copy</a>
Metadata URL	<input type="text"/>	<a href="#">Copy</a>
XML File	<a href="#">Download Metadata XML</a>	

# OneLogin Identity Provider Configuration

To configure **OneLogin IdP**, perform the following steps:

1. Sign in to [OneLogin](#) as an administrator.
2. On the **Applications** tab, select **Applications** and an application you are using for **SAML SSO** with **Envi**.



3. Go to the **Configuration** menu item, clear the prefilled information, and enter new data from **SAML Identity Provider Configuration** (the [Duo Single Sign-On and OneLogin Configuration](#) section, step 6):
  - a. In the **Audience (EntityID)** box, enter **Entity ID** from **Duo**.
  - b. In the **Recipient, ACS (Consumer) URL Validator** and **ACS (Consumer) URL** boxes, enter **Assertion Consumer Service URL** from **Duo**.

- c. Move through to **SAML nameID** format and set **Unspecified**.

4. Go to the **Parameters** menu item and set values in the following **SAML** boxes:

- **DisplayName**
- **Email**
- **FirstName**
- **LastName**
- **NameID value**
- **Username**

SAML Test Connector (Advanced) Field	Value	
DisplayName	- Macro -	custom parameter
Email	Email	custom parameter
FirstName	First Name	custom parameter
LastName	Last Name	custom parameter
NameID value	Email	
Username	Username	custom parameter

**Note:** For the **DisplayName** box, use the **Macro** and **{firstname} {lastname}** values.

Edit Field DisplayName

Name  
DisplayName

Value  
- Macro -  
{firstname} {lastname}

Flags  
☒ Include in SAML assertion

Cancel Delete Save

5. **Save** your changes.
6. Go to the **SSO** menu item and copy the information from the **Issuer URL** and **SAML 2.0 Endpoint (HTTP)** boxes.

**Note:** To view details of your certificate, select **View Details** under **X.509 Certificate**. You will need this information later.

Info  
Configuration  
Parameters  
Rules  
**SSO**  
Access  
Users  
Privileges  
Setup

### Enable SAML2.0

Sign on method  
SAML2.0

X.509 Certificate  
Standard Strength Certificate (2048-bit)  
[Change](#) [View Details](#)

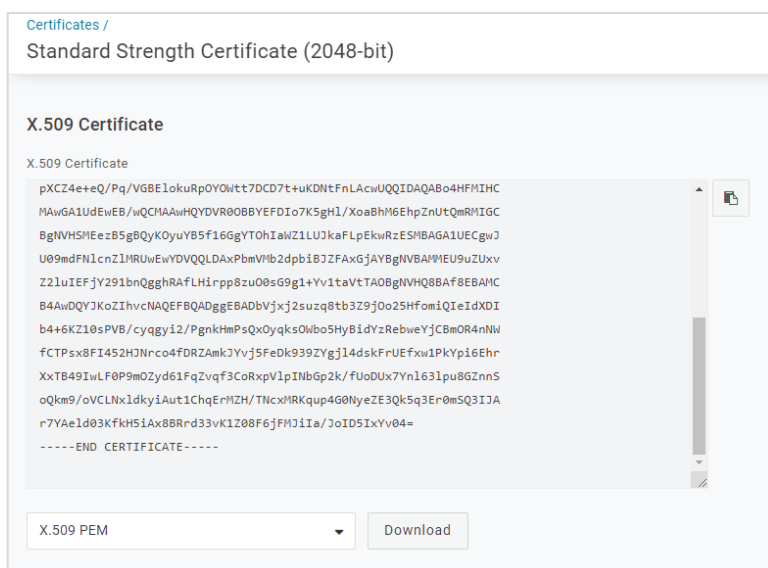
SAML Signature Algorithm  
SHA-1

Issuer URL

SAML 2.0 Endpoint (HTTP)

7. Move through to the bottom of the **Certificate Details** page and select **Download**.

**Note:** The certificate will be downloaded in the **PEM** format.



8. Return to **Duo** and proceed with the configuration of the **Duo Single Sign-On Authentication Source**. Go to the **Single Sign-On Configuration** page to the section **3. Configure Duo Single Sign-On**, and perform the following steps:
  - a. In the **Display Name** box, enter your **IdP** name.
  - b. In the **Entity ID** box, enter **Issuer URL** (the [OneLogin Identity Provider Configuration](#) section, step 6).
  - c. In the **Single Sign-On URL** box, enter **SAML 2.0 Endpoint (HTTP)** (step 6).
  - d. In the **Existing Certificate** box, select **Browse** and upload your certificate from **IdP**. (step 7).
  - e. Select **Save**.

### 3. Configure Duo Single Sign-On

Get this information from your SAML identity provider so Duo Single Sign-On can use it for primary authentication.

**Display Name \***   
Used only to help you identify the identity provider within our interface.

**Entity ID \***   
The global, unique ID for your SAML entity. This is provided by your identity provider.

**Single Sign-On URL \***   
URL to use when performing a primary authentication.

**Single Logout URL**  optional  
URL, provided by your identity provider, that Duo will send Single Logout responses to. It is unused now but may be used in the future.

**Logout Redirect URL**  optional  
URL users will be redirected to after logging out of Duo Single Sign-On.

**Existing Certificate \***  No file selected.



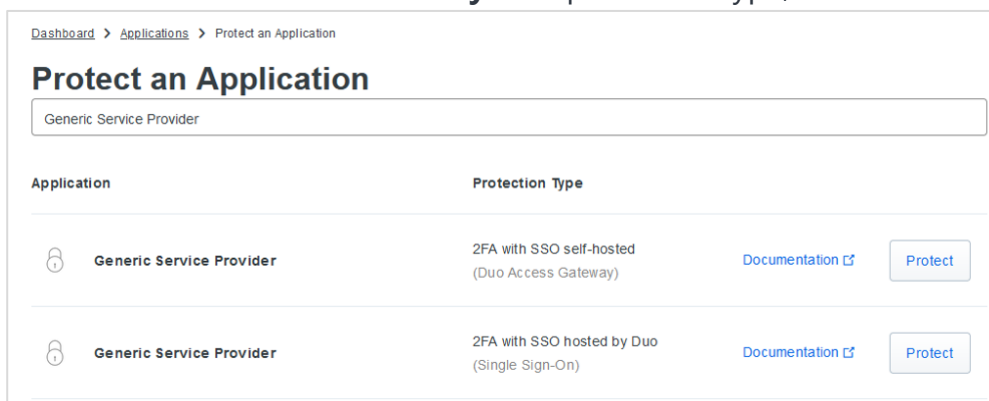
# Create a Cloud Application in Duo

After you have completed the previous part of the configuration, let us move to the next steps of creating the service provider application in **Duo**:

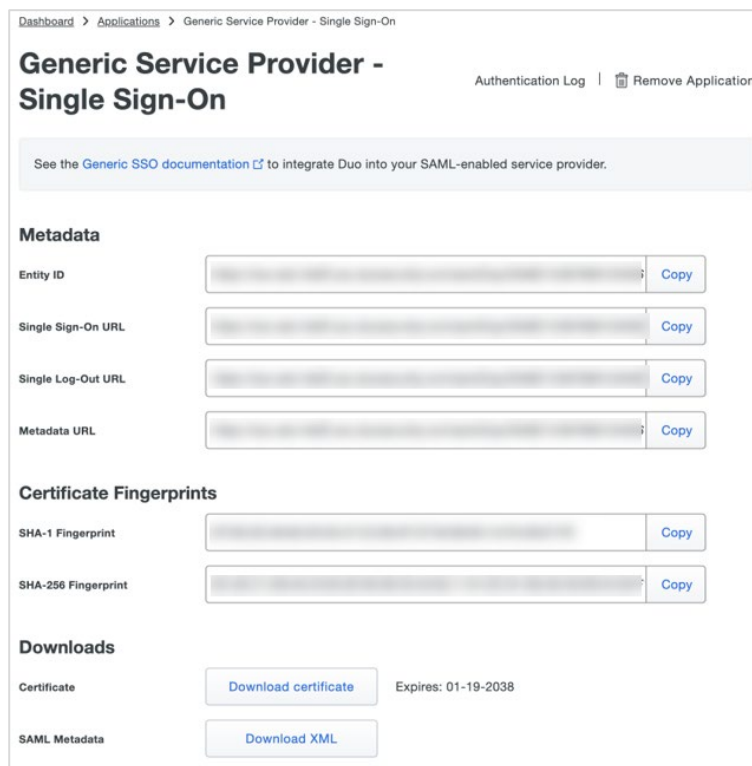
1. Sign in to [Duo Admin Panel](#).
2. In the main menu, select **Applications**.
3. Select **Protect an Application** and find **Generic Service Provider** with the **2FA** with **SSO** protection type hosted by **Duo (Single Sign-On)** in the applications list.



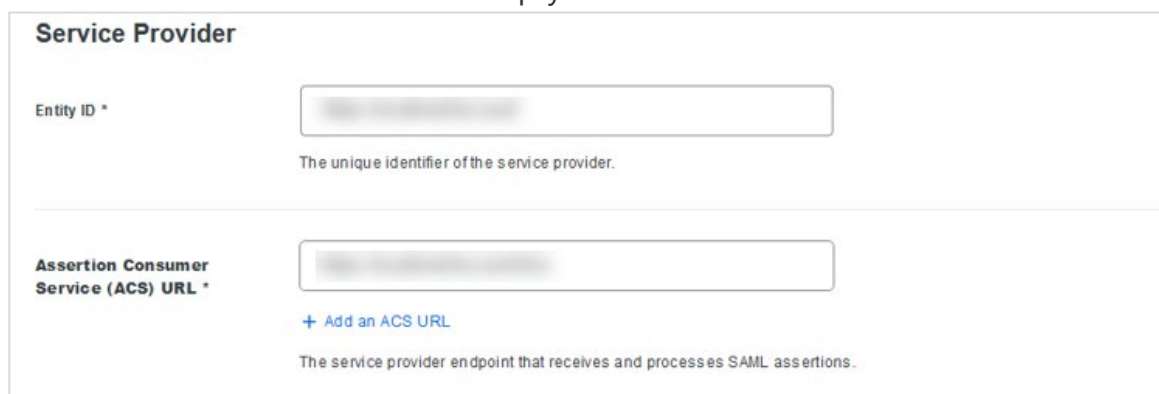
4. Select **Protect** to start configuring **Generic Service Provider**.
5. The **Protect an Application** page lists different types of services you can protect with **Duo**. The **Protection Type** column indicates how **Duo** protects a specific application. In the search box, enter **Generic Service Provider**, then select the item with the **2FA with SSO hosted by Duo** protection type, and select **Protect**.



6. You will be redirected to the details page of an application to protect. In **Metadata**, you can get the **SAML** identity provider information about **Duo Single Sign-On** for your service provider. In **Downloads**, select either **Download XML** or **Copy** the data from the boxes. This metadata information will be used for the **Envi** configuration later.



7. Go to **Service Provider** and fill in the information about the **Envi** application:
  - a. In the **Entity ID** box, enter the base URL of the **Envi** application + **/Account** (for example, `https://envi_domain_name/Account`).
  - b. In the **Assertion Consumer Service (ACS) URL** box, enter the base URL of the **Envi** application + **/Account/Acs** (for example, `https://envi_domain_name/Account/Acs`).
  - c. Leave other boxes in this section empty.



8. Go to **Settings**, then enter the application **Name** and select **Save**.

Settings

Type

Generic Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

Whitelisting

Since this application is using Frameless Duo Universal Prompt, hostname whitelisting is no longer supported.

[Get more information](#)

Save

Controls if a username should be altered before trying to match them with a Duo user account.

# Envi Configuration

To synchronize **Duo Single Sign-On** and **OneLogin** connection with your **Envi** account, perform the following steps:

1. Sing in to the **Envi** application.
2. Go to **My Profile > My Domain > Details** tab. Then, in the **Certificates** section deactivate all existing active certificates.

Domains > Domain Name One Login

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE RESOURCES SECURITY

[Edit](#)

Name: One Login

Description:

Domain Type: Simple

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect

Failed Attempts: 10

Endpoint URL: https://softserve-envi-dev.onelogin.com/trust/saml2/http-redirect/sso/7ff1e0e-4fe0-4820-9ba-76f7932bb3bc

Identifier URL: https://app.onelogin.com/saml/metadata/7ff1e0e-4fe0-4820-9ba-76f7932bb3bc

SSO Message: Please provide your SSO credentials for further logins

Do not require force authentication.

Do not require device registration.

Do not restrict IP Addresses

[+ Add Certificate](#)

All Search

☐ Strict Match

☐ Display Inactive

Certificate Name	Start Date	End Date	Status
2021-03-31 15:25:55 CN="OneLogin Account", OU=On	11/08/2019 11:37 AM (UTC)	11/08/2024 11:37 AM (UTC)	ACTIVE

3. Select **Edit** and then **Upload metadata**.

Domains > Domain Name One Login

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE RESOURCES SECURITY

[Update](#) [Cancel](#)

Name\*: One Login

Description:

Domain Type: Simple

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect [Upload Metadata](#)

Failed Attempts\*: 10

Endpoint URL: https://softserve-envi-dev.onelogin.com/trust/h

Identifier URL: https://app.onelogin.com/saml/metadata/7ff1

SSO Message\*: Please provide your SSO credentials for further

☐ Require force authentication.

☐ Require device registration.

☐ Restrict IP Addresses.

4. In the **Upload Metadata** pop-up, perform the following steps:
  - a. In the **Upload From** dropdown, select **File**.
  - b. In the **Select File** box, enter the path to the **Duo** metadata file location (the [Create a Cloud Application in Duo](#) section, step 6).
  - c. Select **OK**.

**Upload Metadata** ✕

Upload From: File

Select File\*: Select file or drop here to upload

[OK](#) [Cancel](#)

**Note:** Make sure that both **Endpoint URL** and **Identifier URL** are populated with the new values and **Certificates** section is populated with new certificates.

Domains > Domain Name Domain\_Name

[DETAILS](#)
[ORGANIZATIONS](#)
[USERS](#)
[PASSWORD DICTIONARIES](#)
[CERTIFICATES](#)
[RESOURCES](#)
[SECURITY](#)

[Edit](#)

Name:	Domain_Name	Authentication:	HTTP Redirect
Description:	Description	Failed Attempts:	0
Session Timeout, m:	20	Endpoint URL:	http://login.microsoftonline.com/885512e1-456d-405b-856b-405b-405b
Mobile Token Expiration, h:		Identifier URL:	http://app.onelogin.com/saml/...
Default UI:	Default	SSO Message:	Please provide your SSO credentials for further logins
Status:	Active	Do not require force authentication:	
		Do not require device registration:	
		Do not restrict IP Addresses:	

[Update Users](#)

Now, you can sign in to the **Envi** application using **Duo OneLogin**.