envi

Duo Azure AD

Integration Guide

Table of Contents

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 **Azure AD** connection with your **Envi** account.

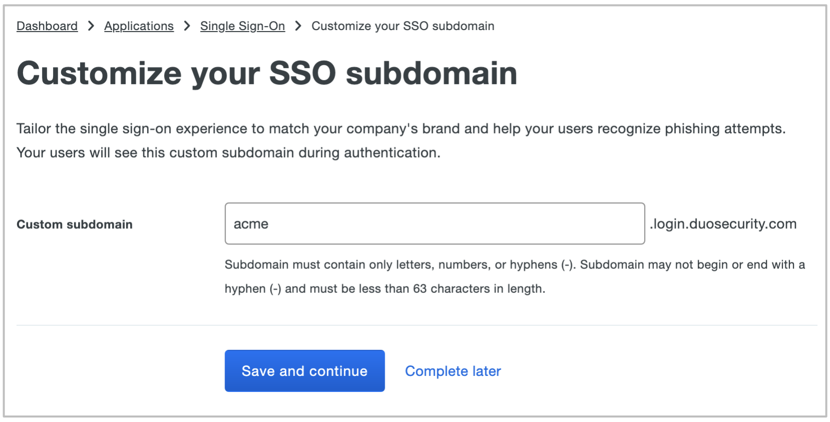
Duo Single Sign-On and Azure AD Configuration

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**. For example, if you enter **acme**, users will see **acme.login.duosecurity.com** in the URL.

    b. Select **Save and continue** to use the desired subdomain or select **Complete later** to skip this step for now.



Dashboard > Applications > Single Sign-On > Customize your SSO subdomain

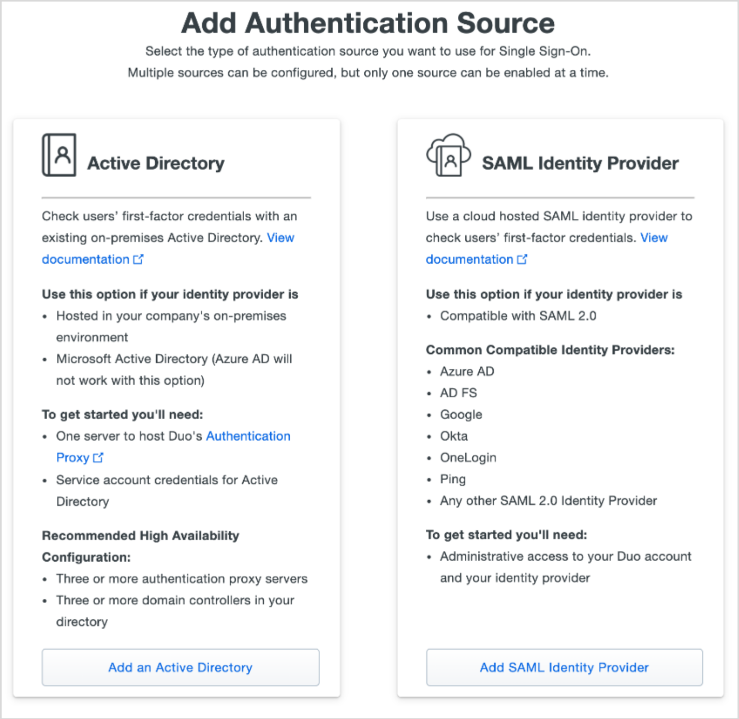
Customize your SSO subdomain

Tailor the single sign-on experience to match your company's brand and help your users recognize phishing attempts. Your users will see this custom subdomain during authentication.

Custom subdomain: acme .login.duosecurity.com

Subdomain must contain only letters, numbers, or hyphens (-). Subdomain may not begin or end with a hyphen (-) and must be less than 63 characters in length.

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



Add Authentication Source

Select the type of authentication source you want to use for Single Sign-On.
Multiple sources can be configured, but only one source can be enabled at a time.

Active Directory

Check users' first-factor credentials with an existing on-premises Active Directory. View documentation

Use this option if your identity provider is
- Hosted in your company's on-premises environment
- Microsoft Active Directory (Azure AD will not work with this option)

To get started you'll need:
- One server to host Duo's Authentication Proxy
- Service account credentials for Active Directory

Recommended High Availability Configuration:
- Three or more authentication proxy servers
- Three or more domain controllers in your directory

SAML Identity Provider

Use a cloud hosted SAML identity provider to check users' first-factor credentials. View documentation

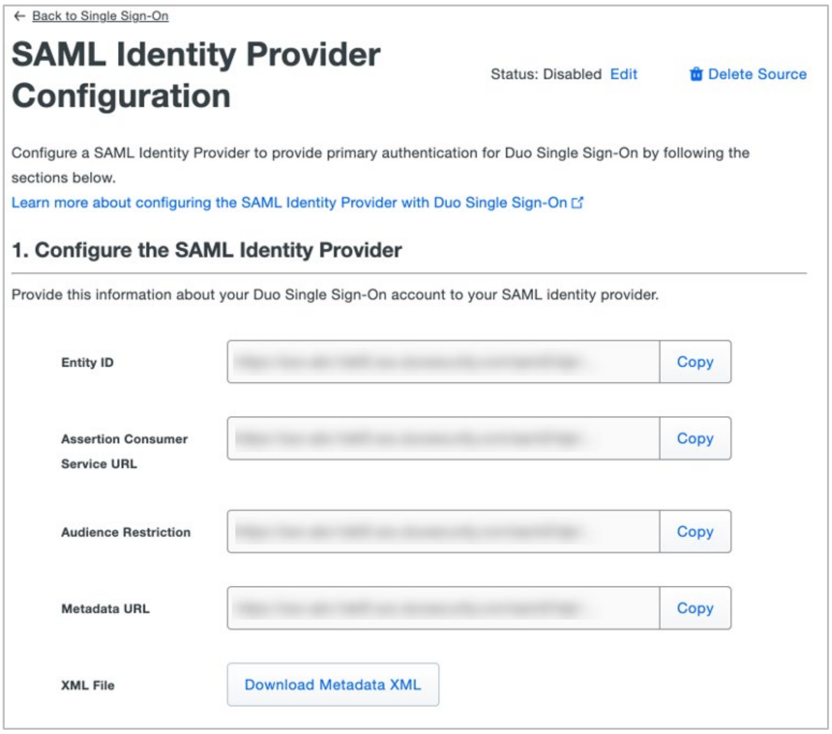
Use this option if your identity provider is
- Compatible with SAML 2.0

Common Compatible Identity Providers:
- Azure AD
- AD FS
- Google
- Okta
- OneLogin
- Ping
- Any other SAML 2.0 Identity Provider

To get started you'll need:
- Administrative access to your Duo account and your identity provider

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 Copy

Assertion Consumer Service URL Copy

Audience Restriction Copy

Metadata URL Copy

XML File Download Metadata XML

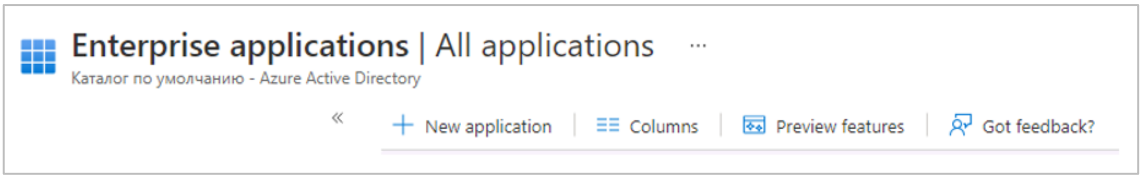
Azure AD Identity Provider Configuration

To configure **Azure AD IdP**, perform the following steps:

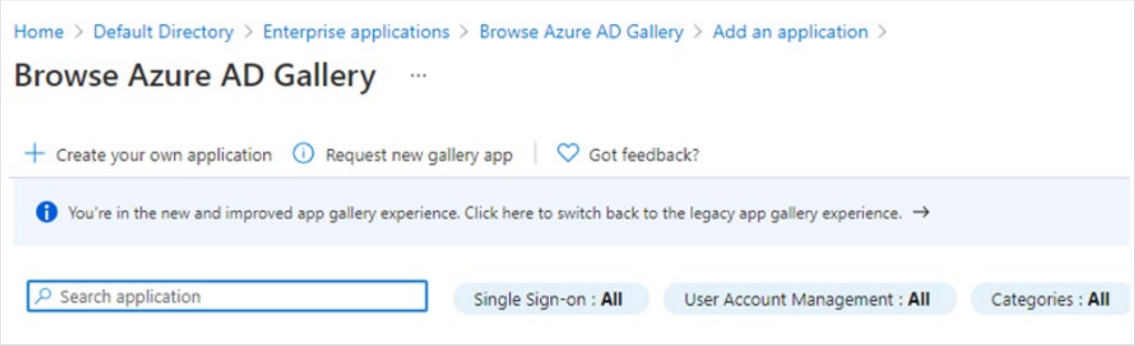
1. Sign in to your [Microsoft Azure administrative portal.]()

   Note: If you're already using an **SSO** configuration for **Envi**, then open it up and you can skip steps 3-5.

2. Go to the menu and select **Azure Active Directory**.
3. On the **Enterprise Applications** page, select **+New application**.


Enterprise applications | All applications
Каталог по умолчанию - Azure Active Directory
New application
Columns
Preview features
Got feedback?

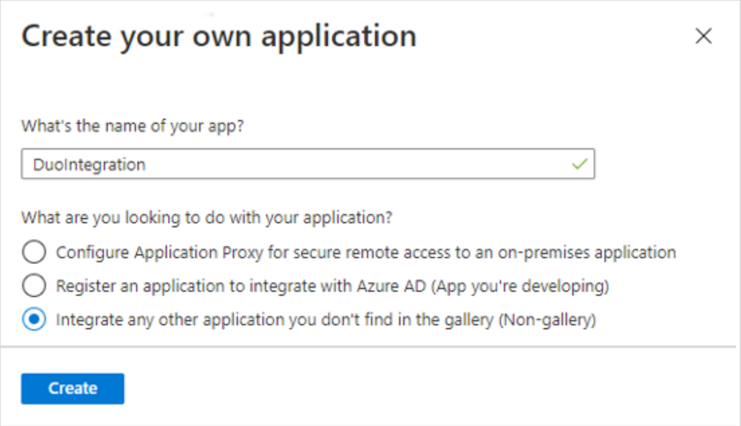
4. On the **Browse Azure AD Gallery** page, select **+Create your own application**.


Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Add an application >
Browse Azure AD Gallery
Create your own application
Request new gallery app
Got feedback?
Search application

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

Single Sign-on : **All** User Account Management : **All** Categories : **All**

5. On the **Create your own application** page, enter a name for the new application, then select **Integrate any other application you don't find in the gallery (Non-gallery)**, and **Create**.



What's the name of your app?

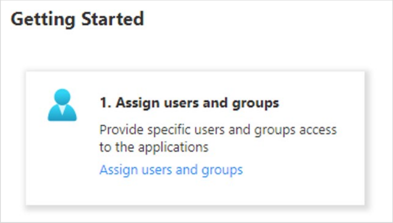
DuoIntegration ✓

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

6. If the application is new, you need to assign users and groups that will use the application. To do that, perform the following steps:

   a. On the **Overview** page, under **Getting Started**, select **Assign users and groups**.

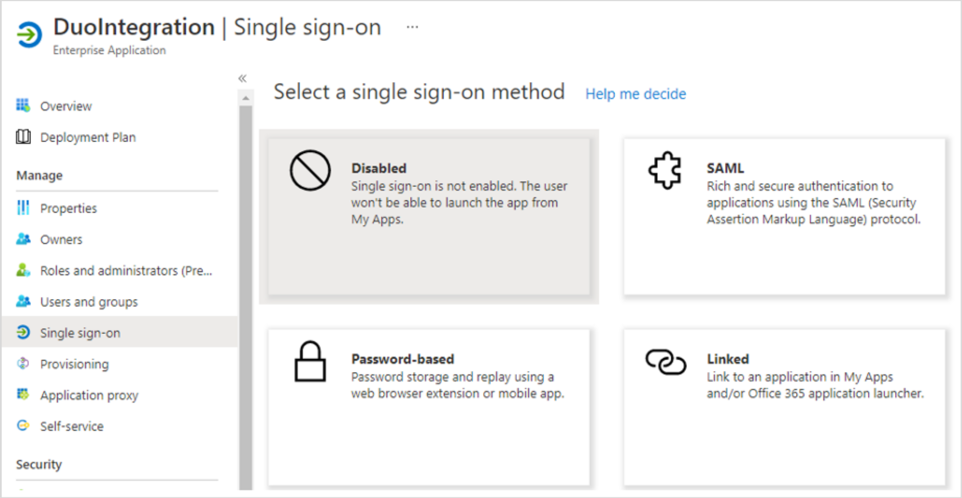


Provide specific users and groups access to the applications

b. Select **+Add users/group** and start selecting users and groups that should have access to sign in with **Azure** to **Duo Single Sign-On.**

c. After you have selected users and groups, select **Assign** at the bottom of the page.

7. In the menu, go to the **Manage** section and select **Single sign-on**, on the **Select a single sign-on method** page, select **SAML**.



Select a single sign-on method Help me decide

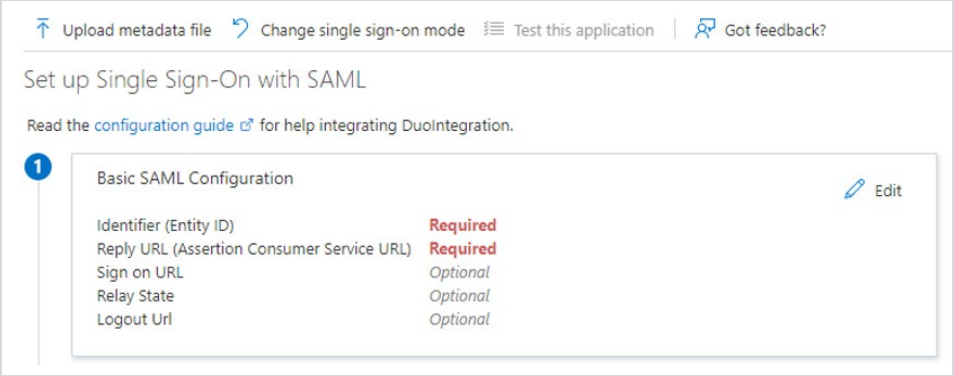
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

8. On the **Set up Single Sign-On with SAML** page, select **Edit** in the **Basic SAML Configuration** section.



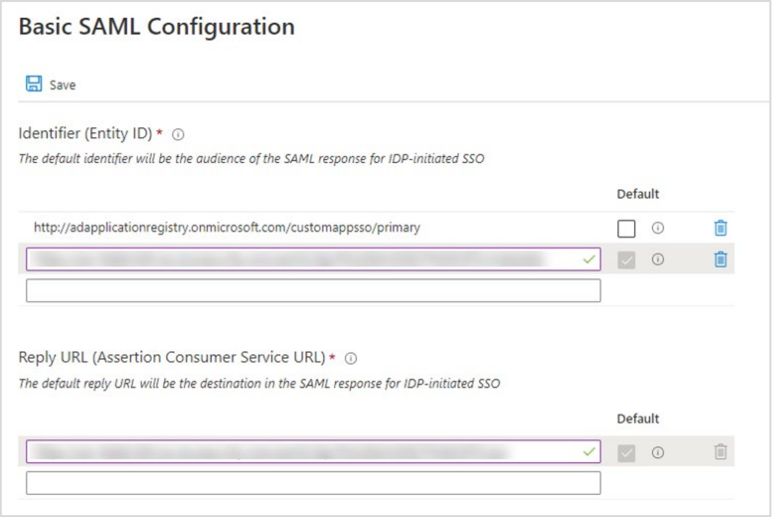
Set up Single Sign-On with SAML

Read the configuration guide for help integrating DuoIntegration.

Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

9. On the **Basic SAML Configuration** page, perform the following steps:
   a. In the **Identifier (Entity ID)** box, enter **Entity ID** obtained from **Duo Admin Panel** (the Duo Single Sign-On and Azure AD Configuration section, step 6).
   b. In the **Reply URL (Assertion Consumer Service URL)** box, enter **Assertion Consumer Service URL** obtained from **Duo Admin Panel** (step 6).
   c. Leave other boxes as is by default.
   d. Select **Save**.



Basic SAML Configuration

Save

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

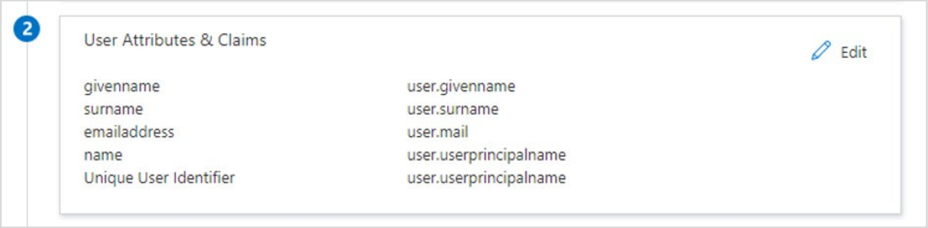
	Default		
http://adapplicationregistry.onmicrosoft.com/customappsso/primary	□	ⓘ	🗑
[redacted] ✓	☑	ⓘ	🗑

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default		
[redacted] ✓	☑	ⓘ	🗑

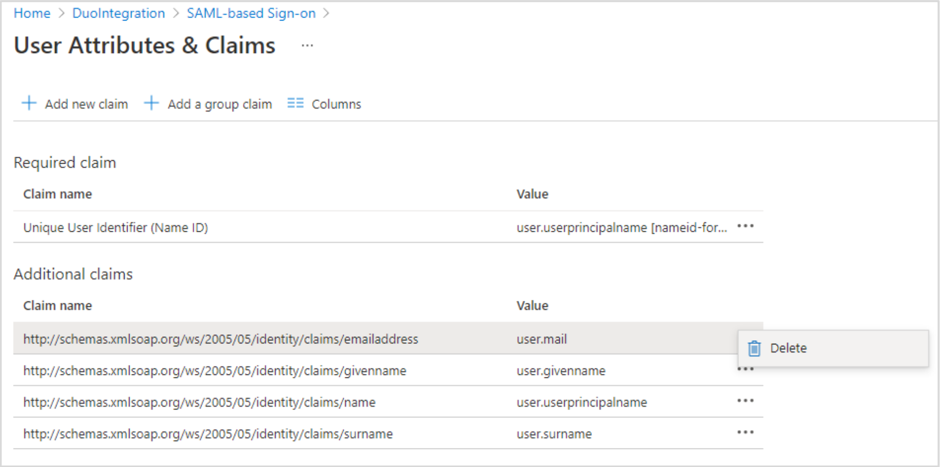
10. On the **Set up Single Sign-On with SAML** page, in the **User Attributes & Claims** section, select **Edit**.



User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

11. In **Additional Claims**, select the ellipsis icon (**...**) and then **Delete**. Perform the same action in each row and delete all four default claims.



User Attributes & Claims ...

Required claim

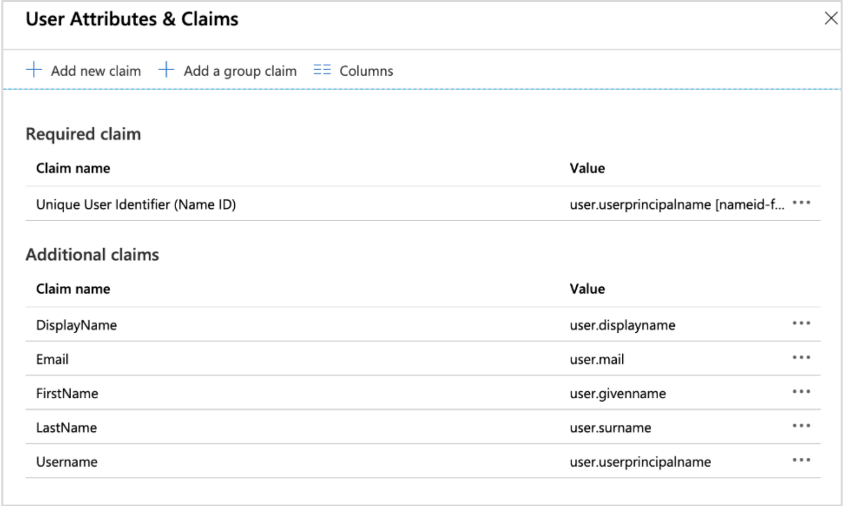
Claim name	Value	
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...	•••

Additional claims

Claim name	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail	🗑 Delete
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	•••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	•••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname	•••

12. Go to the top of the page and select **+Add new claim**. Add the five additional claims (the **Additional claims** column on the screenshot):

- **DisplayName**
- **Email**
- **FirstName**
- **LastName**
- **Username**



Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-f...

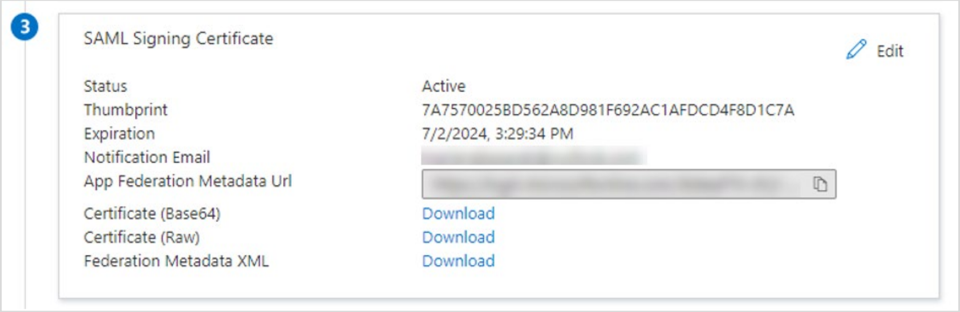
Additional claims

Claim name	Value
DisplayName	user.displayname
Email	user.mail
FirstName	user.givenname
LastName	user.surname
Username	user.userprincipalname

13. Once you have added all five claims, select the **X** button (top right-hand side of the page).

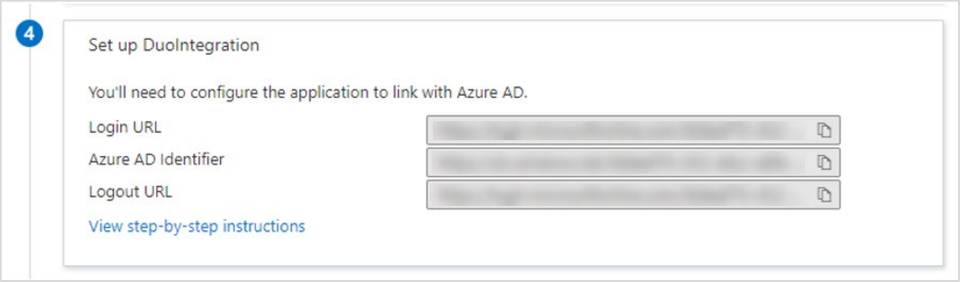
Note: Duo Single Sign-On is not configured yet, so do **NOT** select **Test** because it will fail.

14. On the **Set up Single Sign-On with SAML** page, in **SAML Signing Certificate**, select **Download** next to **Certificate (Base64)**. Keep this file for later use.



Status	Active
Thumbprint	7A7570025BD562A8D981F692AC1AFDCD4F8D1C7A
Expiration	7/2/2024, 3:29:34 PM
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

15. In **Set up YourAppName**, you will find metadata information that you need to provide for **Duo Single Sign-On**.



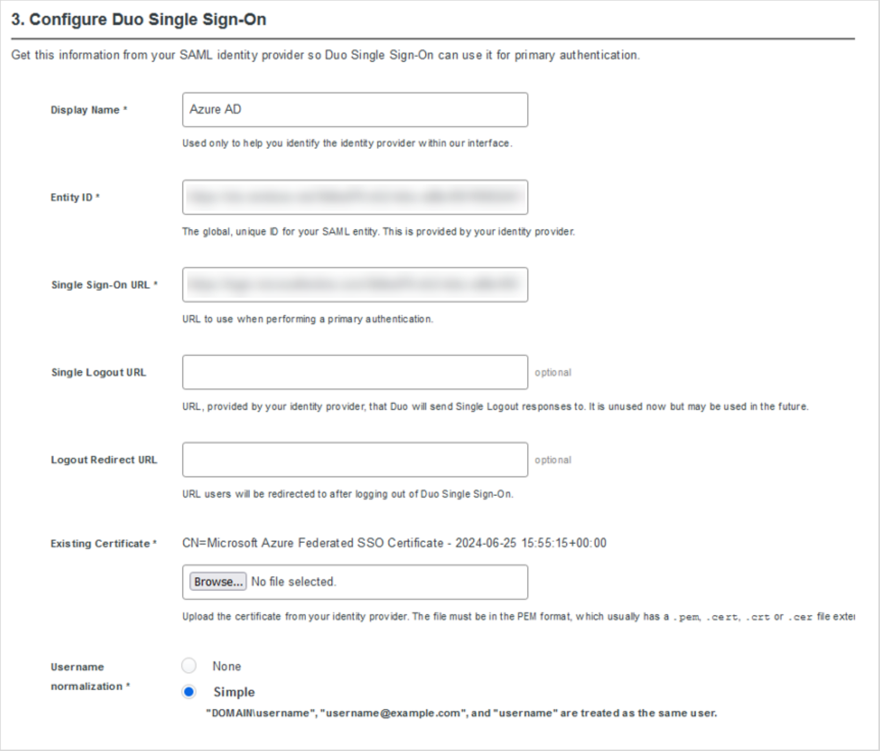
You'll need to configure the application to link with Azure AD.

Login URL	[redacted]
Azure AD Identifier	[redacted]
Logout URL	[redacted]

View step-by-step instructions

16. Go back to **Duo Admin Panel** (the Duo Single Sign-On and Azure AD Configuration section, step 6), move through 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 a name that helps you easily identify the identity provider.
    b. In the **Entity ID** box, enter **Azure AD Identifier** from **Azure** (the Azure AD Identity Provider Configuration section, step 15)
    c. In the **Single Sign-On URL** box, enter **Login URL** from **Azure** (step 15).
    d. Leave the **Single Logout URL** and **Logout Redirect URL** boxes empty.
    e. In the **Certificate** section, upload the certificate that you downloaded (step 15).
    f. In **Username normalization**, set **Simple**.
    g. **Save** the changes.



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 *: Azure AD

Used only to help you identify the identity provider within our interface.

Entity ID *: [redacted]

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

Single Sign-On URL *: [redacted]

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 *: CN=Microsoft Azure Federated SSO Certificate - 2024-06-25 15:55:15+00:00

Browse... No file selected.

Upload the certificate from your identity provider. The file must be in the PEM format, which usually has a `.pem`, `.cert`, `.crt` or `.cer` file exte

Username normalization *: ○ None ● **Simple**

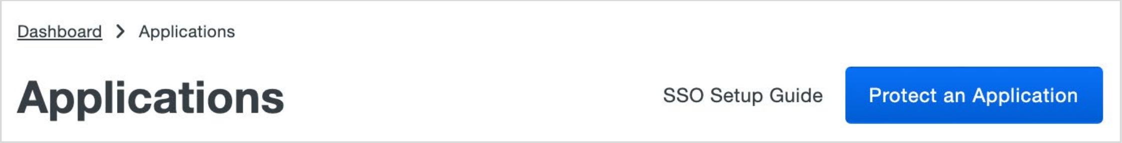
"DOMAIN\username", "username@example.com", and "username" are treated as the same user.

Now, the **Duo Single Sign-On** configuration is complete.

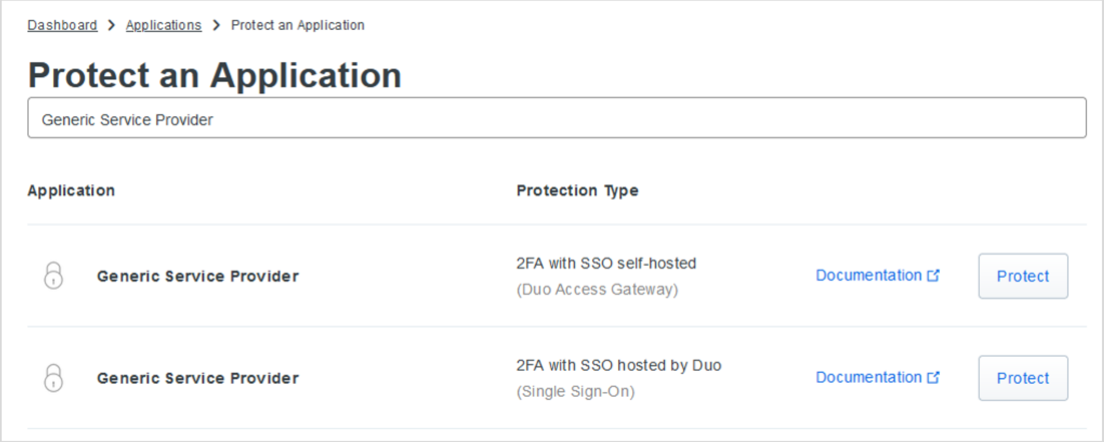
Create a Cloud Application in Duo

Once you have completed the **Duo Single Sign-On** configuration, let us proceed with the creation of 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.

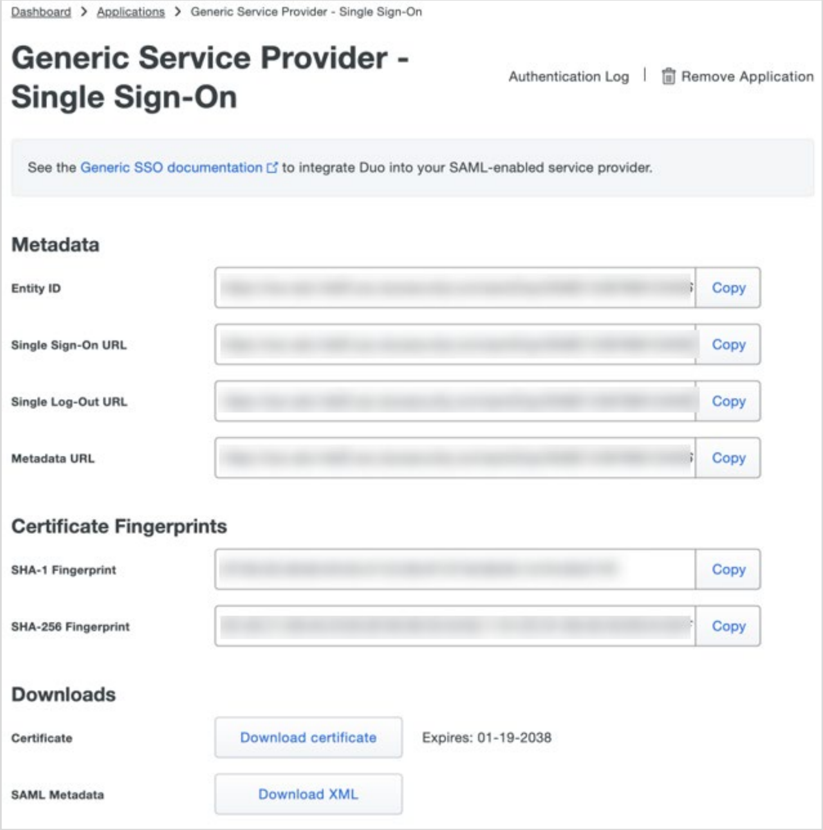


4. Select **Protect** to start configuring **Generic Service Provider**.
5. The **Protect an Application** page lists different types of services you can protect with **Duo**. The **Protection Type** column indicates how **Duo** protects a specific application. In the search box, enter **Generic Service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



Application	Protection Type		
Generic Service Provider	2FA with SSO self-hosted (Duo Access Gateway)	Documentation	Protect
Generic Service Provider	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect

6. Then, you will be redirected to the details page of an application to protect.
   In **Metadata**, you can get **SAML** identity provider information about **Duo Single Sign-On** to provide it 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.



Dashboard > Applications > Generic Service Provider - Single Sign-On

Generic Service Provider - Single Sign-On

See the Generic SSO documentation to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID

Single Sign-On URL

Single Log-Out URL

Metadata URL

Certificate Fingerprints

SHA-1 Fingerprint

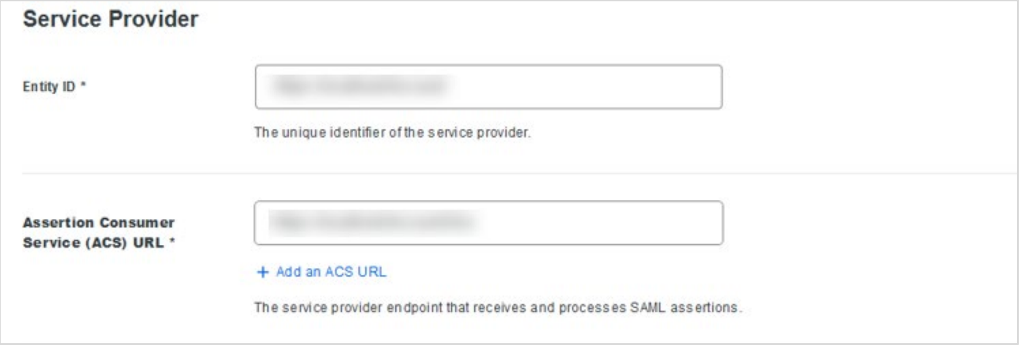
SHA-256 Fingerprint

Downloads

Certificate — Expires: 01-19-2038

SAML Metadata

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.



Service Provider

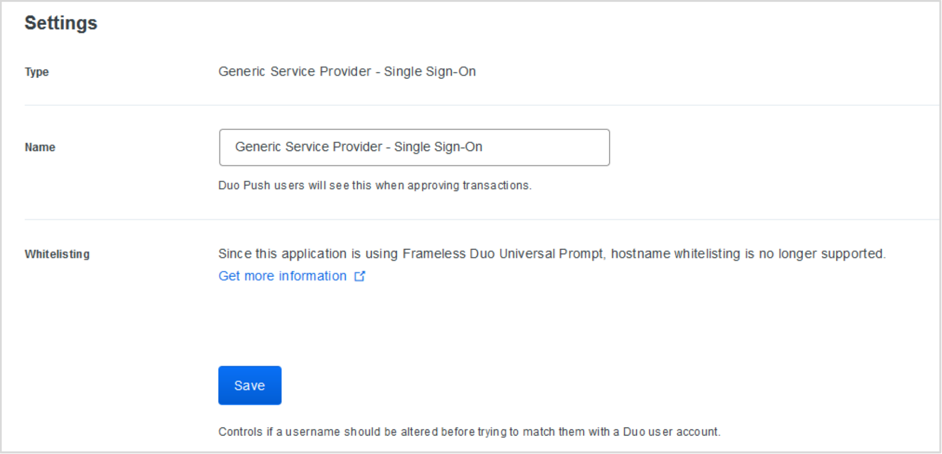
Entity ID *

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

The service provider endpoint that receives and processes SAML assertions.

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



Settings

Type: Generic Service Provider - Single Sign-On

Name: Generic Service Provider - Single Sign-On

Duo Push users will see this when approving transactions.

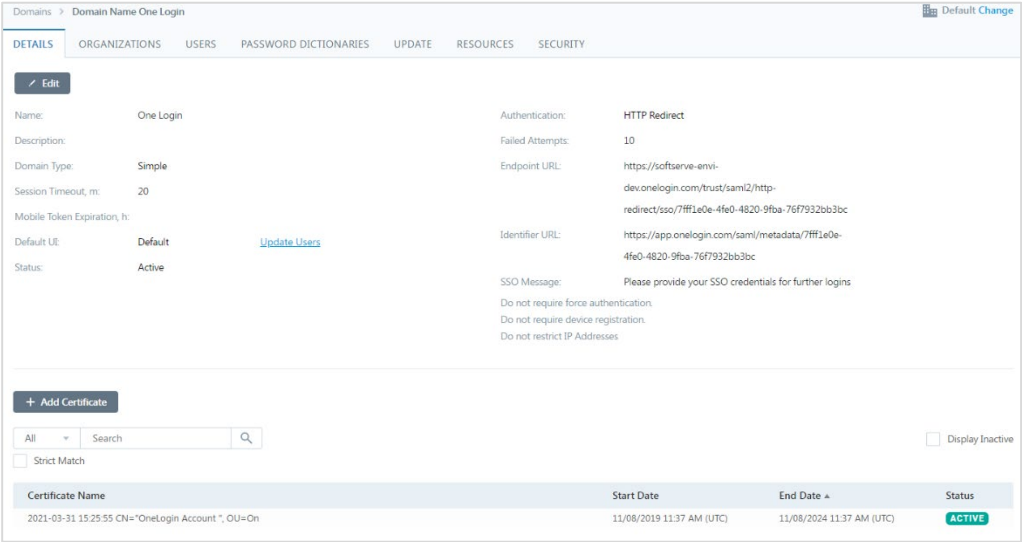
Whitelisting: Since this application is using Frameless Duo Universal Prompt, hostname whitelisting is no longer supported.
Get more information

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 **Azure AD** 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.

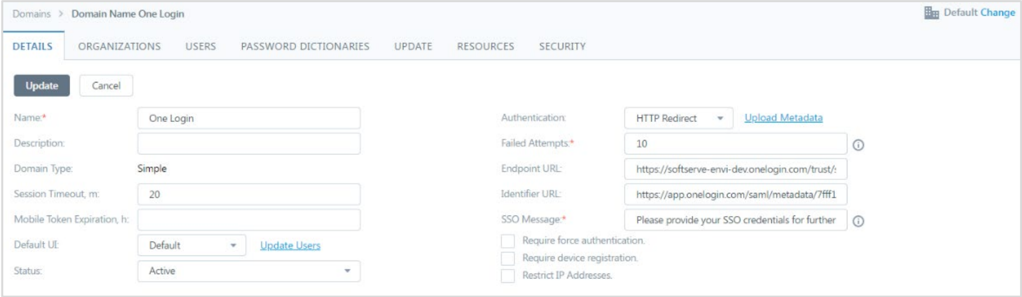


Name: One Login
Description:
Domain Type: Simple
Session Timeout, m: 20
Mobile Token Expiration, h:
Default UI: Default
Status: Active

Authentication: HTTP Redirect
Failed Attempts: 10
Endpoint URL: https://softserve-envi-dev.onelogin.com/trust/saml2/http-redirect/sso/7fff1e0e-4fe0-4820-9fba-76f7932bb3bc
Identifier URL: https://app.onelogin.com/saml/metadata/7fff1e0e-4fe0-4820-9fba-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

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**.

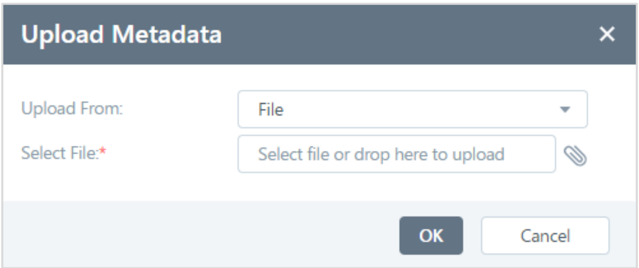


Name:* One Login
Description:
Domain Type: Simple
Session Timeout, m: 20
Mobile Token Expiration, h:
Default UI: Default
Status: Active

Authentication: HTTP Redirect
Failed Attempts:* 10
Endpoint URL: https://softserve-envi-dev.onelogin.com/trust/:
Identifier URL: https://app.onelogin.com/saml/metadata/7fff1
SSO Message:* Please provide your SSO credentials for further
□ Require force authentication.
□ Require device registration.
□ Restrict IP Addresses.

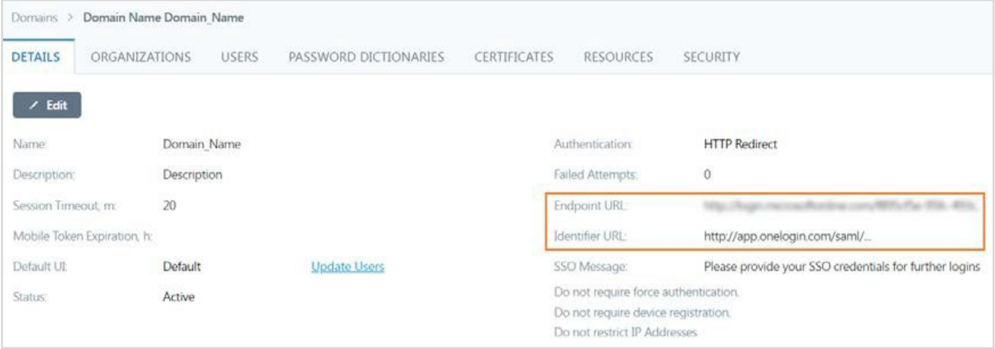
4. In the **Upload Metadata** pop-up, perform the following steps:

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

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

Name: Domain_Name

Description: Description

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default Update Users

Status: Active

Authentication: HTTP Redirect

Failed Attempts: 0

Endpoint URL: [redacted]

Identifier URL: http://app.onelogin.com/saml/...

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

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