Configure SAML for Security Management Appliance with Duo and Azure

Contents

Introduction

This document describes how to integrate Duo with Security Management Appliance (SMA) and Azure for Security Assertion Markup Language (SAML) authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- An active Azure account: You must have an Azure subscription and access to the Azure AD console to set up the integration with Duo (Free License)
- A SAML-supported Service Provider (SP): You must have an application or system that supports SAML authentication and is configured to work with Azure AD as the identity provider.
- Configuration information: You must have specific configuration information for your SP and Duo, such as SAML entity IDs, SAML response URL, and SAML security key.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco SMA
- Azure Cloud
- Duo

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

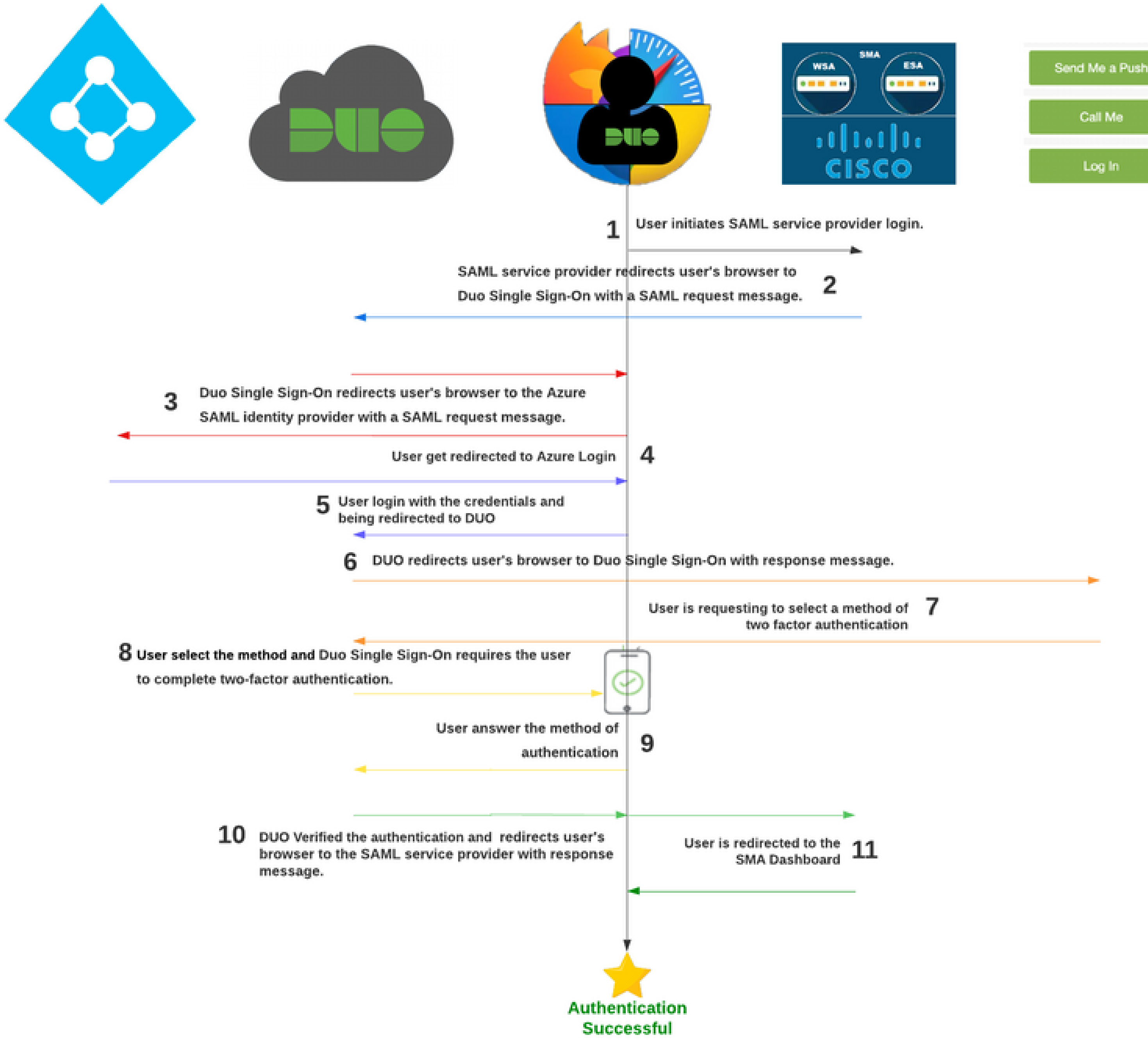
Background Information

Duo is a two-factor authentication service provider that adds a layer of security to SAML authentication.

In a typical scenario, Azure acts as the Identity Provider (IdP) and an external service, such as a web application or information system, acts as the Security SMA.

The flow of SAML authentication with Duo and Azure would look like this:

1. A user attempts to access the Security SMA and is redirected to Azure to log in.
2. Azure requests user authentication and uses Duo to verify the users identity through a second authentication factor (Call, SMS, Hardware Token, WebAuth).
3. Once authenticated, Azure sends a SAML response to the SMA which includes authorization information and assertions about the user.
4. The SMA validates the SAML response and, if valid, allows the user to access the protected resource.
5. In summary, SAML with Duo and Azure enables secure and centralized user authentication across different systems and platforms, use a combination of password authentication and two-factor authentication to increase security.


SMA
WSA
ESA
CISCO
Send Me a Push
Call Me
Log In
1 User initiates SAML service provider login.
SAML service provider redirects user's browser to Duo Single Sign-On with a SAML request message. 2
3 Duo Single Sign-On redirects user's browser to the Azure SAML identity provider with a SAML request message.
User get redirected to Azure Login 4
5 User login with the credentials and being redirected to DUO
6 DUO redirects user's browser to Duo Single Sign-On with response message.
User is requesting to select a method of two factor authentication 7
8 User select the method and Duo Single Sign-On requires the user to complete two-factor authentication.
User answer the method of authentication 9
10 DUO Verified the authentication and redirects user's browser to the SAML service provider with response message.
User is redirected to the SMA Dashboard 11
Authentication Successful

Important Observations

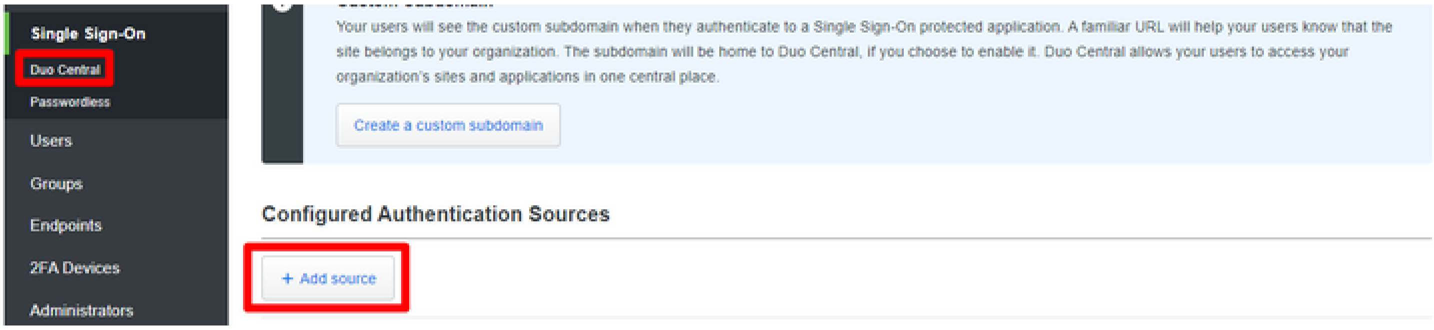
- SAML is a security standard that enables user authentication and authorization across different systems and platforms.
- IdP is the Identity that stores all the information of the users to permit the authentication (that means Duo has all the user information to confirm and approve a request for authentication).
- SP In simple words, it is the application.

Note: This only works with Azure as a SAML authentication source.

Configure

1. Configure Single Sign-on

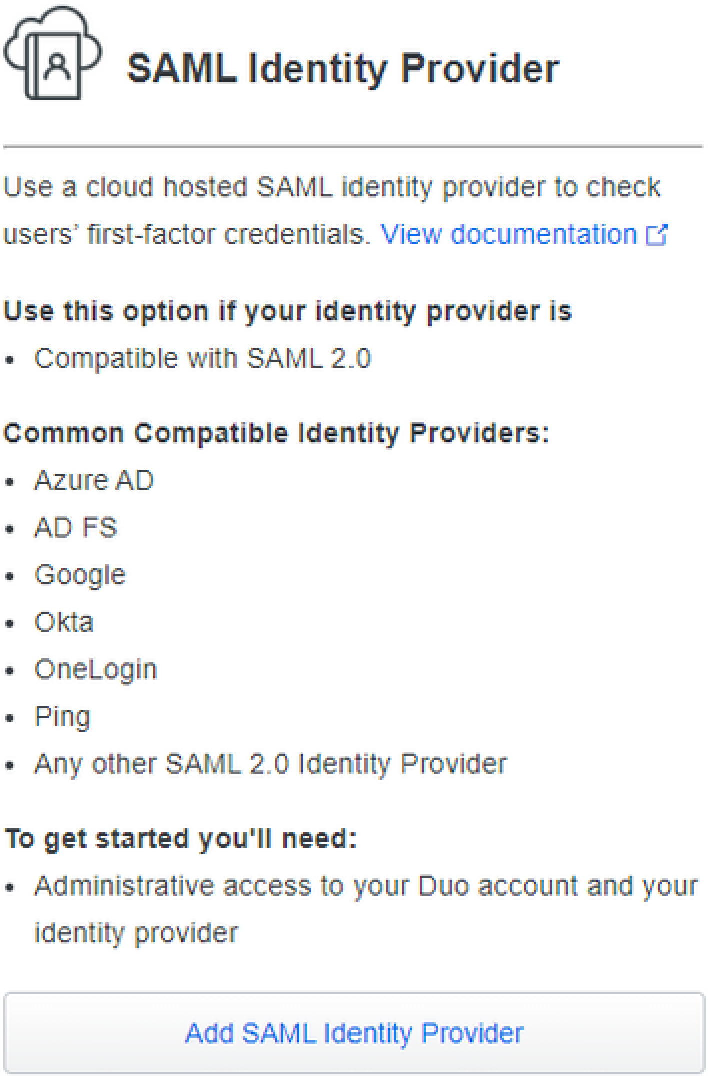
Navigate in the admin portal to **Single Sign-on** > **Duo Central** > **Add source**.



Your users will see the custom subdomain when they authenticate to a Single Sign-On protected application. A familiar URL will help your users know that the site belongs to your organization. The subdomain will be home to Duo Central, if you choose to enable it. Duo Central allows your users to access your organization's sites and applications in one central place.

Configured Authentication Sources

And select Add SAML Identity Provider as shown in the image.



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:

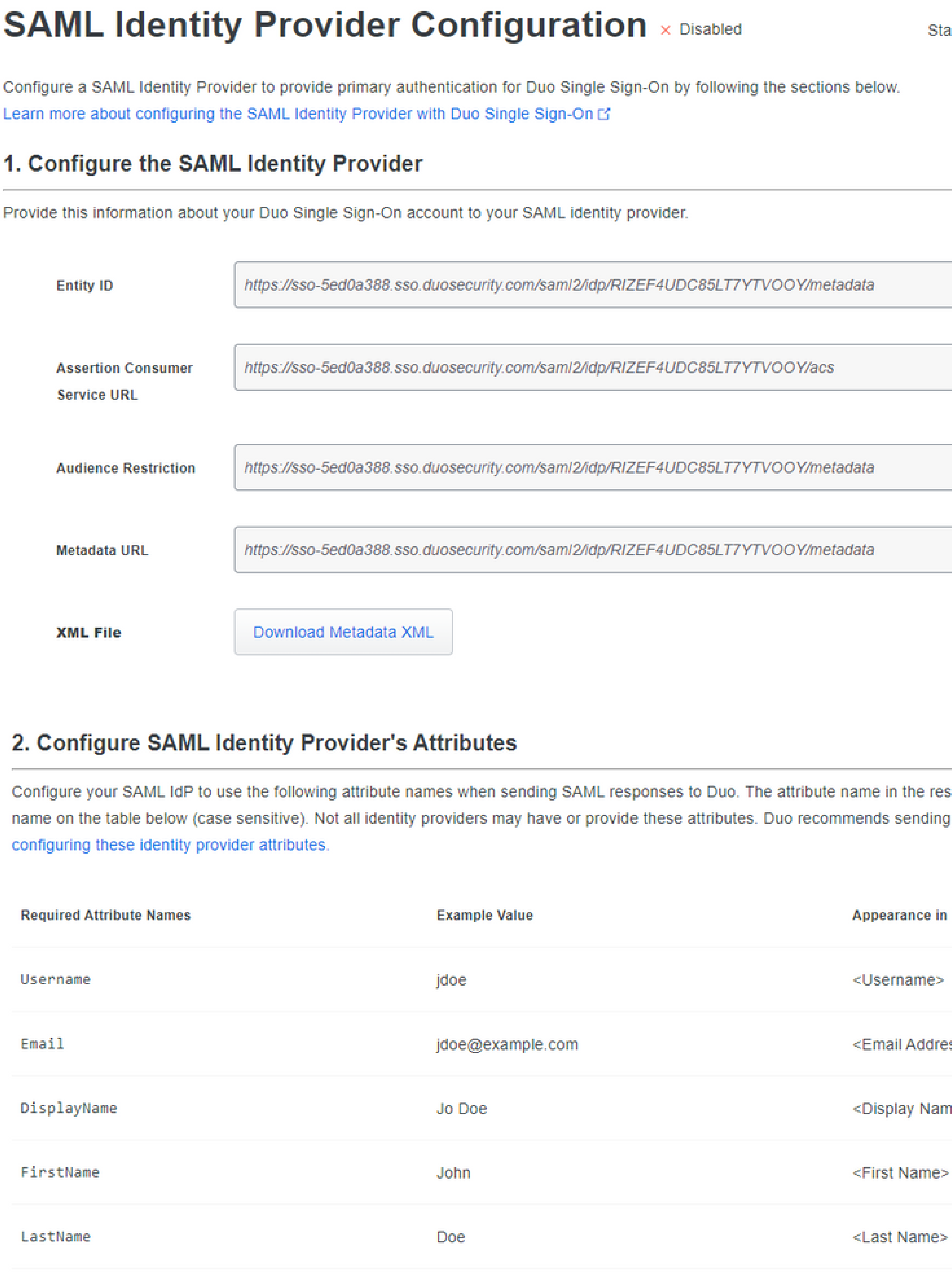
- Azure AD
- AD FS
- Google
- Okta
- OneLogin
- Ping
- Any other SAML 2.0 Identity Provider

To get started you'll need:

- Administrative access to your Duo account and your identity provider

Here in this part, you find all the information which you need to integrate Duo with Azure to integrate with your SMA.

Maintain the information in other windows to use in the integration meanwhile, you configure the parameters in Azure.



SAML Identity Provider Configuration

× Disabled

Sta

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

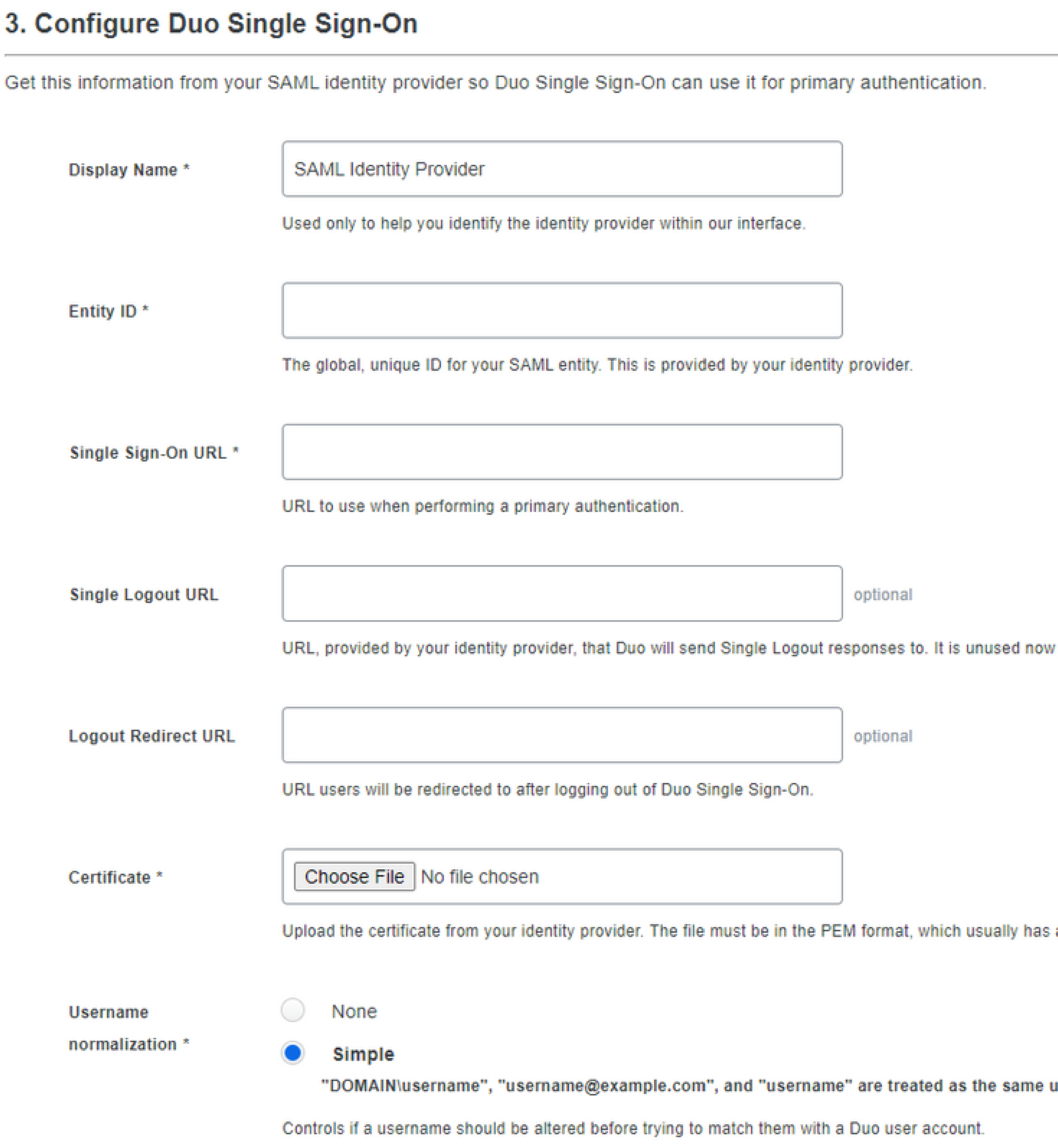
Provide this information about your Duo Single Sign-On account to your SAML identity provider.

Entity ID	*https://sso-5ed0a388.sso.duosecurity.com/saml2/idp/RIZEF4UDC85LT7YTVOOY/metadata*
Assertion Consumer Service URL	*https://sso-5ed0a388.sso.duosecurity.com/saml2/idp/RIZEF4UDC85LT7YTVOOY/acs*
Audience Restriction	*https://sso-5ed0a388.sso.duosecurity.com/saml2/idp/RIZEF4UDC85LT7YTVOOY/metadata*
Metadata URL	*https://sso-5ed0a388.sso.duosecurity.com/saml2/idp/RIZEF4UDC85LT7YTVOOY/metadata*
XML File	Download Metadata XML

2. Configure SAML Identity Provider's Attributes

Configure your SAML IdP to use the following attribute names when sending SAML responses to Duo. The attribute name in the res
name on the table below (case sensitive). Not all identity providers may have or provide these attributes. Duo recommends sending
configuring these identity provider attributes.

Required Attribute Names	Example Value	Appearance in
`Username`	jdoe	<Username>
`Email`	jdoe@example.com	<Email Addres
`DisplayName`	Jo Doe	<Display Nam
`FirstName`	John	<First Name>
`LastName`	Doe	<Last Name>



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 * SAML Identity Provider

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

Logout Redirect URL optional

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

Certificate * Choose File No file chosen

Upload the certificate from your identity provider. The file must be in the PEM format, which usually has a

Username normalization *

○ None

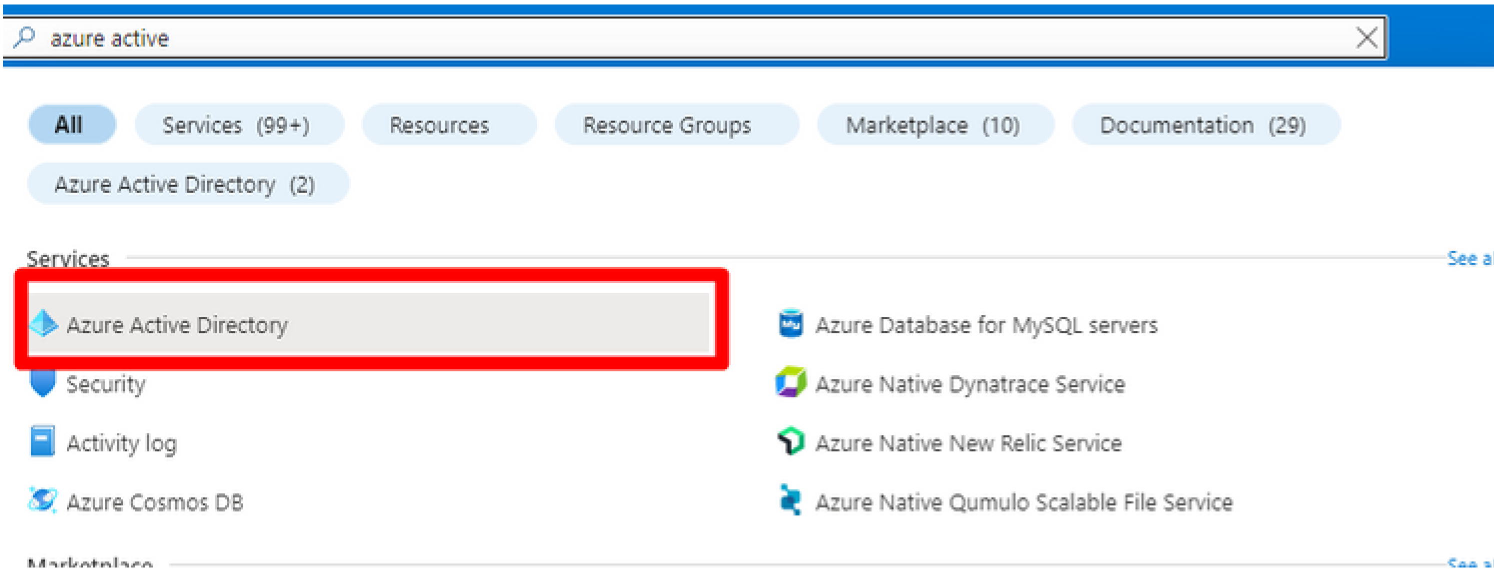
● Simple

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

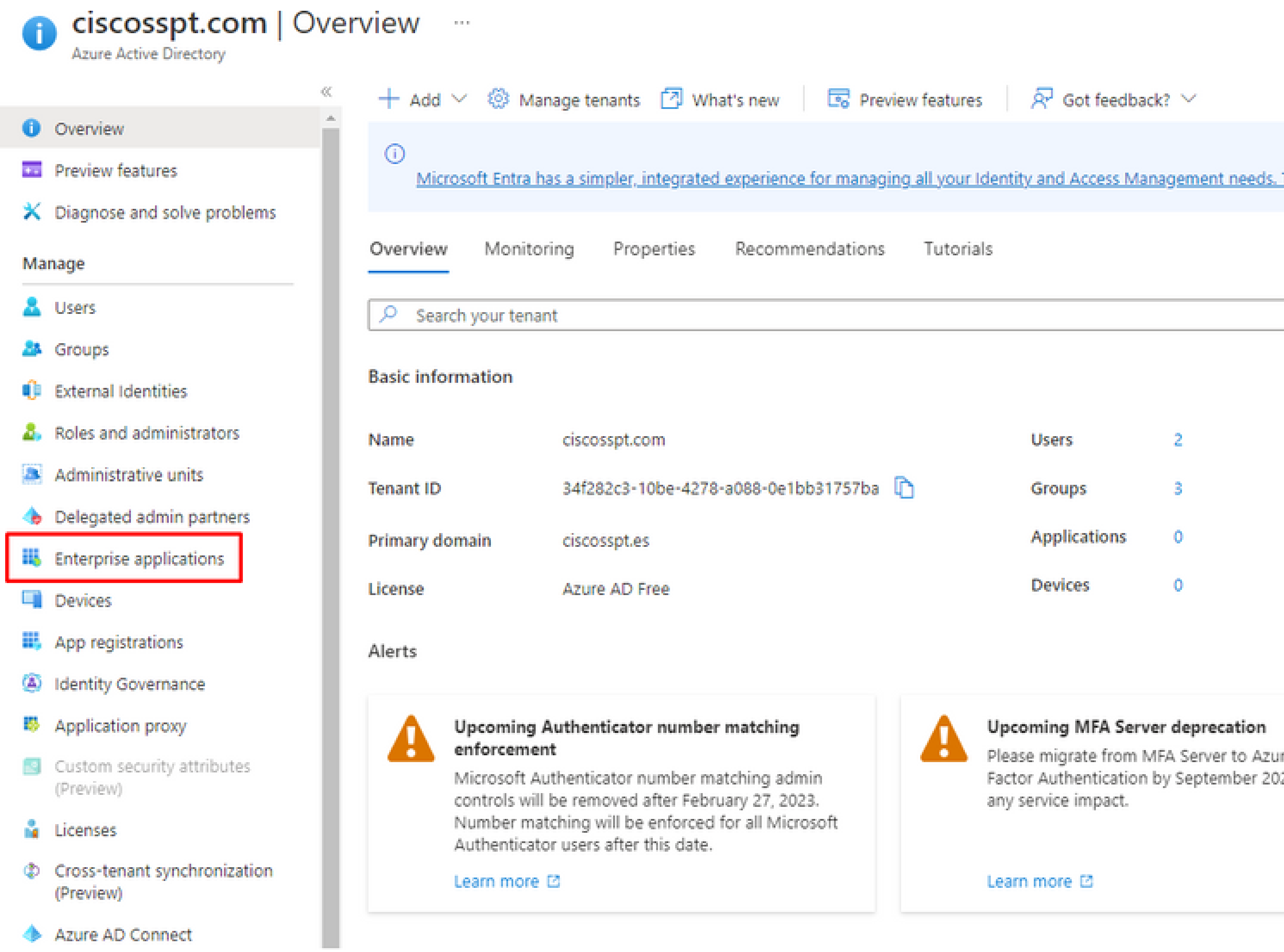
Controls if a username should be altered before trying to match them with a Duo user account.

Now, after you check what information you have in the SAML Azure integration (Duo Admin Portal) part you need to log under the Azure portal [https://portal.azure.com/.](https://portal.azure.com/)

Search for Azure Active Directory in the search bar at the top as shown in the image.



Navigate to **Enterprise Applications** as shown in the image.



Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs.

Basic information

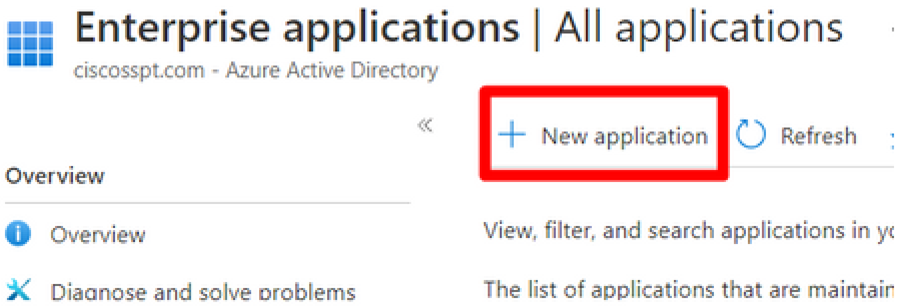
Name	ciscosspt.com	Users	2
Tenant ID	34f282c3-10be-4278-a088-0e1bb31757ba	Groups	3
Primary domain	ciscosspt.es	Applications	0
License	Azure AD Free	Devices	0

Alerts

Upcoming Authenticator number matching enforcement
Microsoft Authenticator number matching admin controls will be removed after February 27, 2023. Number matching will be enforced for all Microsoft Authenticator users after this date.
Learn more

Upcoming MFA Server deprecation
Please migrate from MFA Server to Azur Factor Authentication by September 202 any service impact.
Learn more

Select New Application as shown in the image.



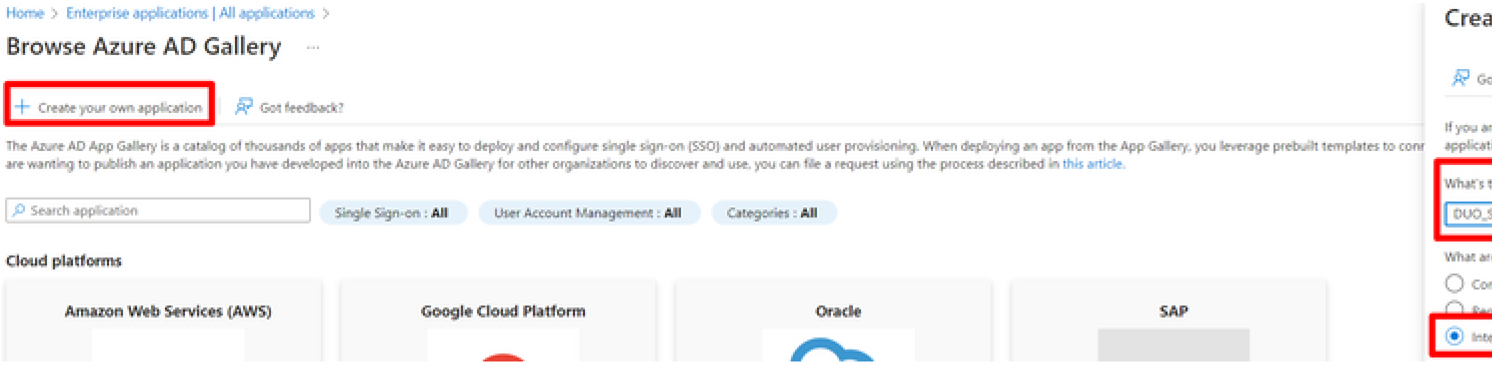
Enterprise applications | All applications

ciscosspt.com - Azure Active Directory

View, filter, and search applications in yo

The list of applications that are maintain

Select Create your own application, choose the name of your app and select Integrate any other application you don't find in the gallery (Non-Gallery)and click Create.



Home > Enterprise applications | All applications >

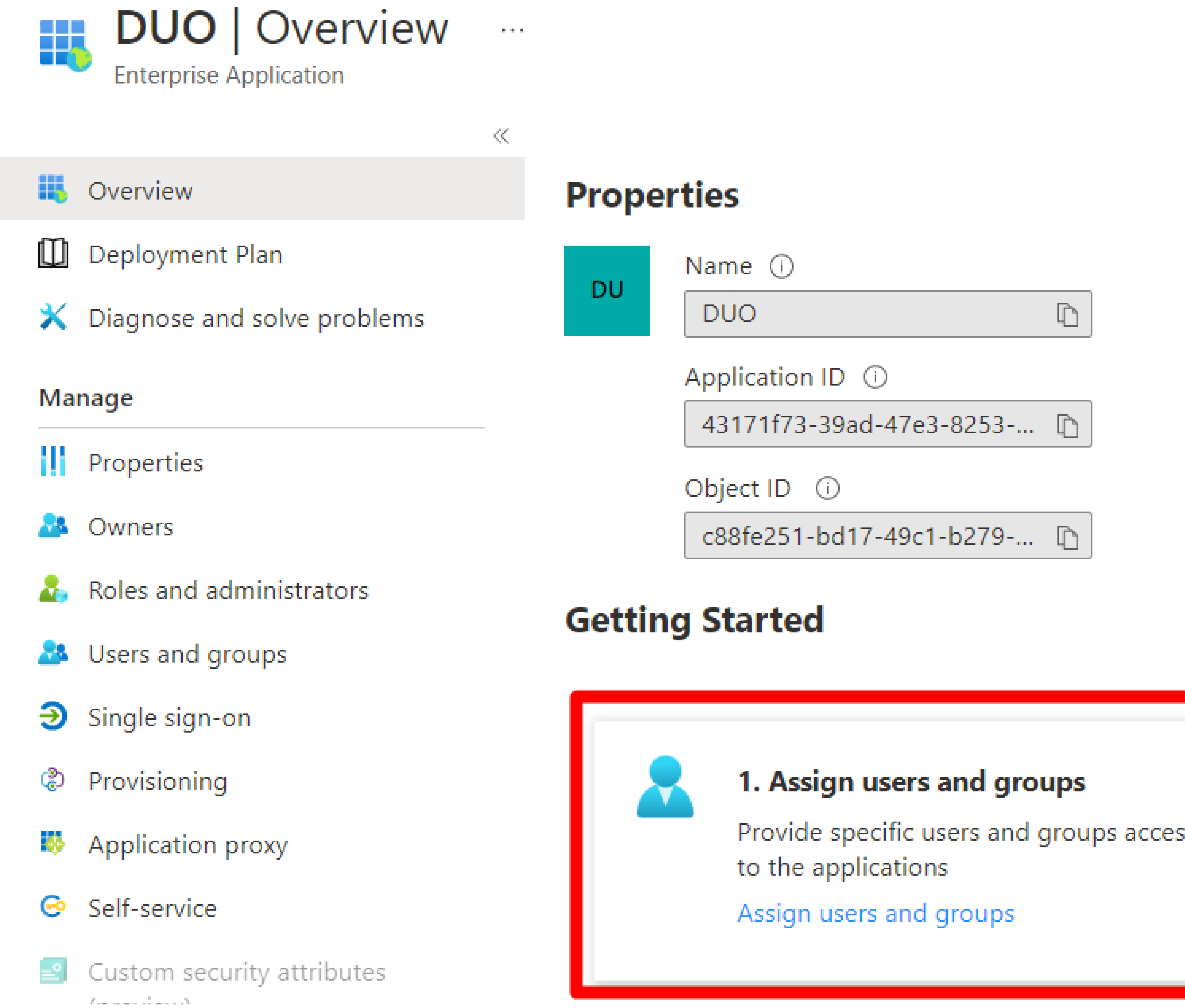
Browse Azure AD Gallery

+ Create your own application
Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to conr are wanting to publish an application you have developed into the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in this article.

Now, add the users. (only the users added here can be used at the time of Single Sign-on (SSO) login).

Select Assign Users and Groups as shown in the image.



DUO | Overview ...

Enterprise Application

Properties

Name: DUO

Application ID: 43171f73-39ad-47e3-8253-...

Object ID: c88fe251-bd17-49c1-b279-...

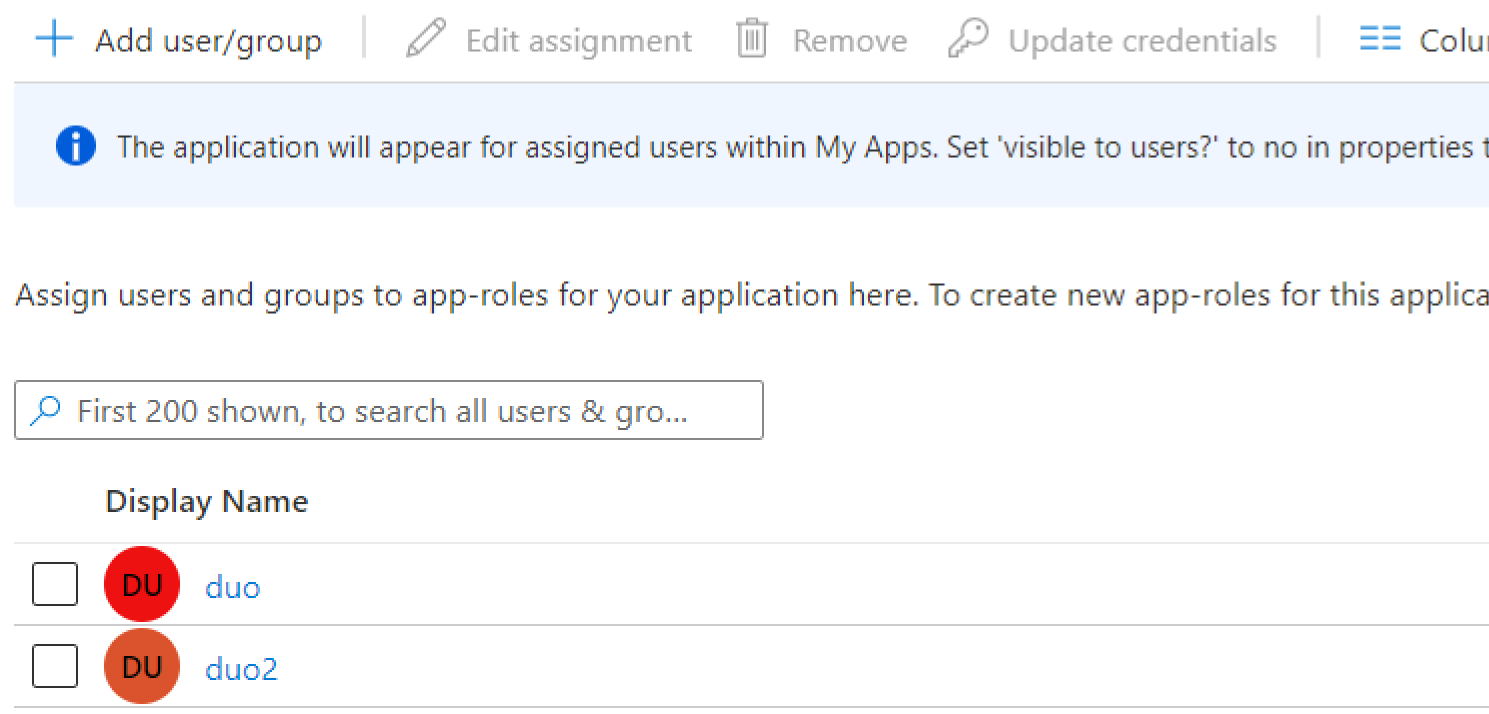
Getting Started

1. Assign users and groups

Provide specific users and groups acces to the applications

Assign users and groups

Select Add user/group as shown in the image.



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties t

Assign users and groups to app-roles for your application here. To create new app-roles for this applica

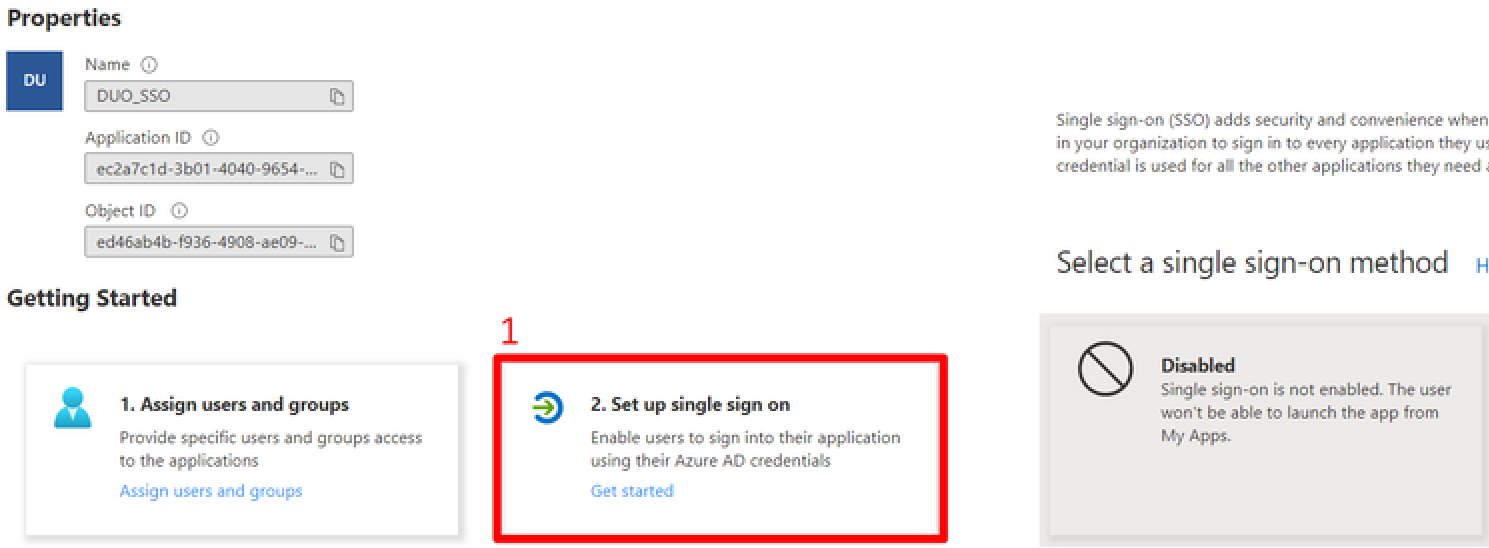
First 200 shown, to search all users & gro...

	Display Name
□ DU	duo
□ DU	duo2

Note: You only can add groups if your AD is licensed, if not then you can use users.

After the users or groups have been added, you start with the SSO Configuration.

- Select **Set Up Single Sign-on**
- Select SAML



Properties

DU

Name: DUO_SSO

Application ID: ec2a7c1d-3b01-4040-9654-...

Object ID: ed46ab4b-f936-4908-ae09-...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

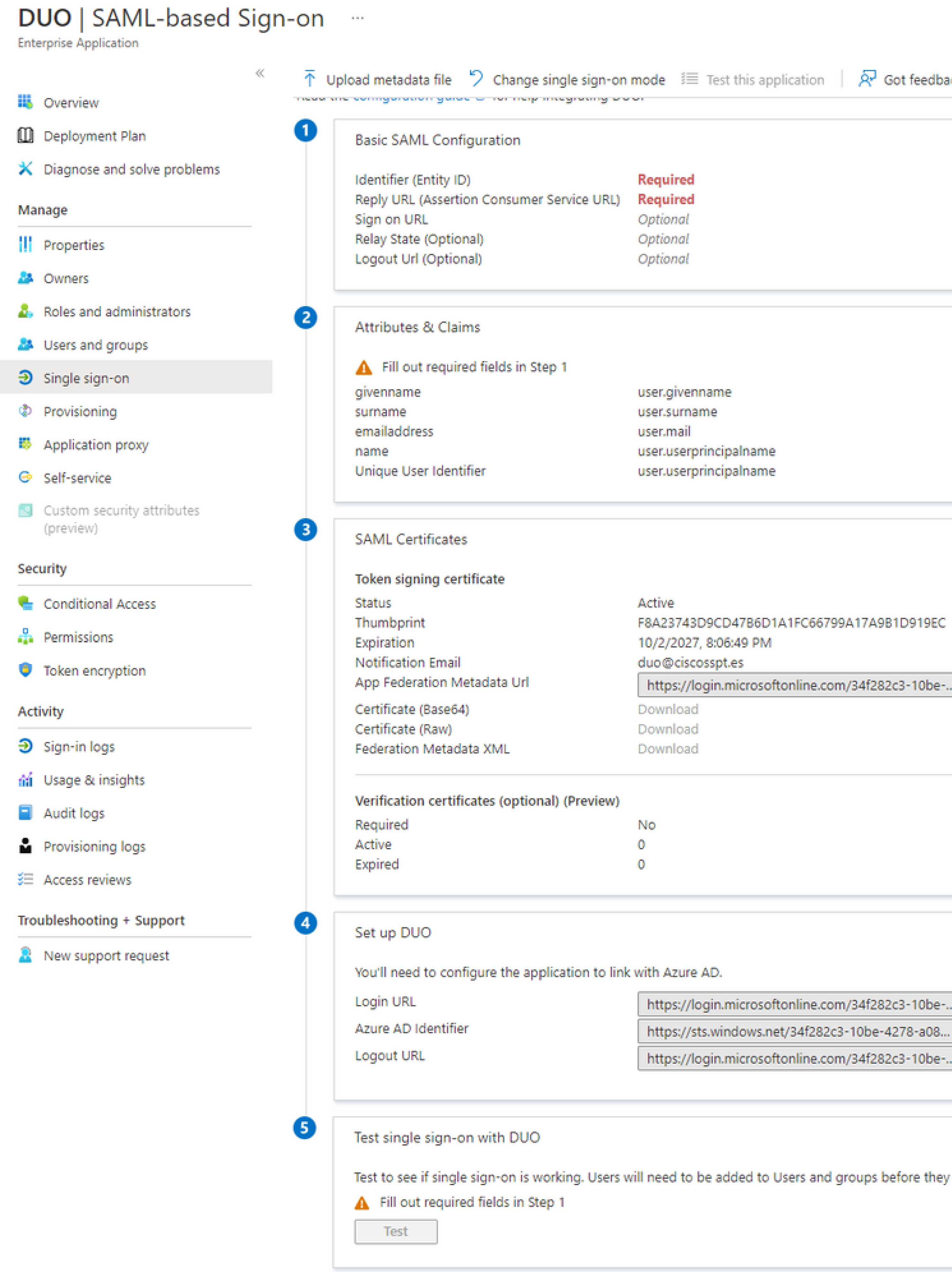
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

Single sign-on (SSO) adds security and convenience when in your organization to sign in to every application they u credential is used for all the other applications they need

Select a single sign-on method

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

After that, you need to configure the Duo SAML-Based Sign-on on Azure with the data of SAML Azure integration in the Duo Admin Portal.



DUO | SAML-based Sign-on ···

Enterprise Application

Basic SAML Configuration

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

Attributes & Claims

⚠ Fill out required fields in Step 1

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

SAML Certificates

Token signing certificate

Status	Active
Thumbprint	F8A23743D9CD47B6D1A1FC66799A17A9B1D919EC
Expiration	10/2/2027, 8:06:49 PM
Notification Email	duo@ciscospt.es
App Federation Metadata Url	https://login.microsoftonline.com/34f282c3-10be-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) (Preview)

Required	No
Active	0
Expired	0

Set up DUO

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

Login URL	https://login.microsoftonline.com/34f282c3-10be-...
Azure AD Identifier	https://sts.windows.net/34f282c3-10be-4278-a08...
Logout URL	https://login.microsoftonline.com/34f282c3-10be-...

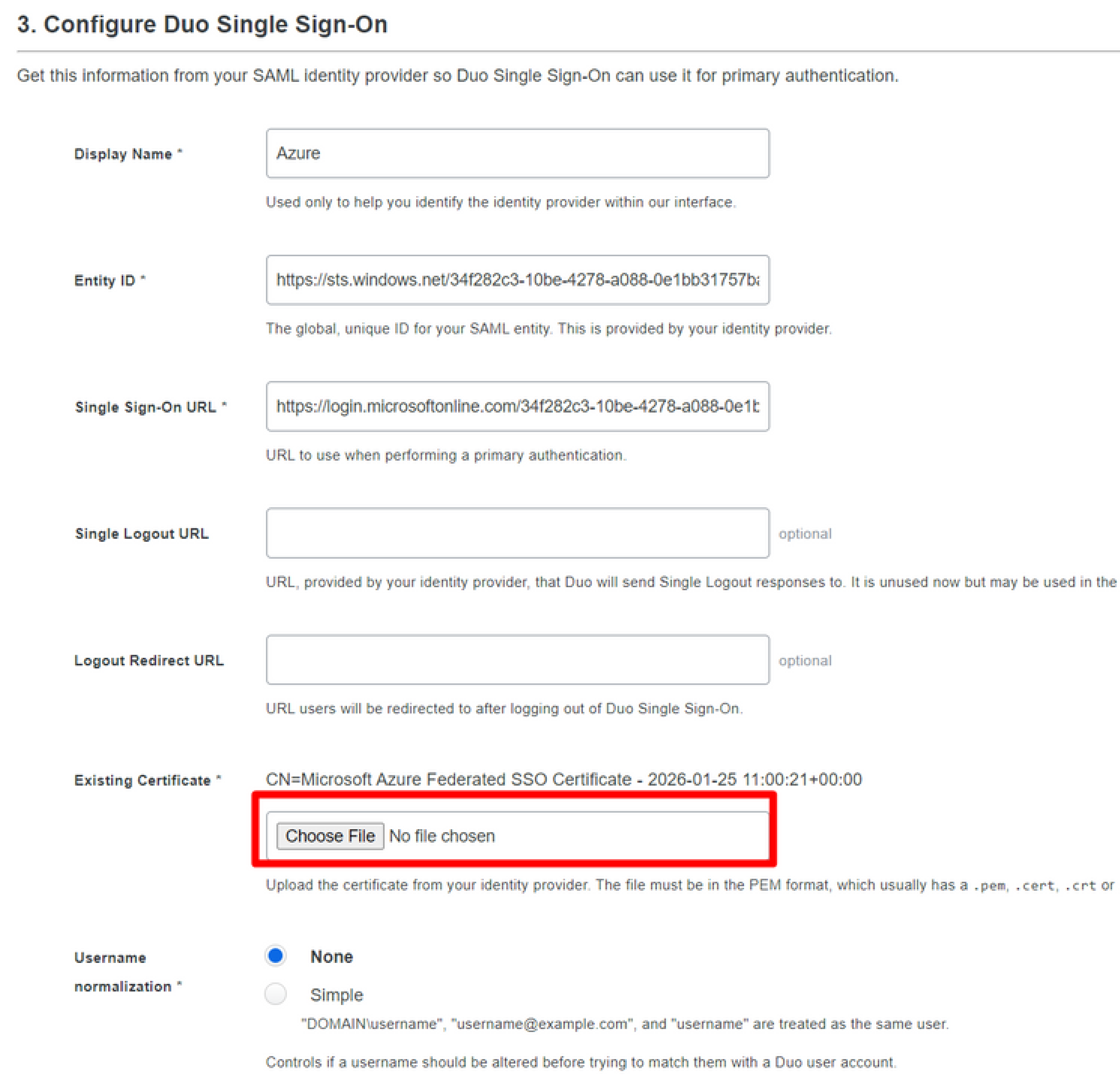
Test single sign-on with DUO

Test to see if single sign-on is working. Users will need to be added to Users and groups before they

⚠ Fill out required fields in Step 1

Select **Edit** under **Basic SAML Configuration** as shown in the image.

and select the certificate which you want to download as shown in the previous image. (this is under your Duo app in the admin panel).



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

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

Entity ID * : https://sts.windows.net/34f282c3-10be-4278-a088-0e1bb31757ba

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

Single Sign-On URL * : https://login.microsoftonline.com/34f282c3-10be-4278-a088-0e1b

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

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 - 2026-01-25 11:00:21+00:00

Choose File No file chosen

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

Username normalization *

● None

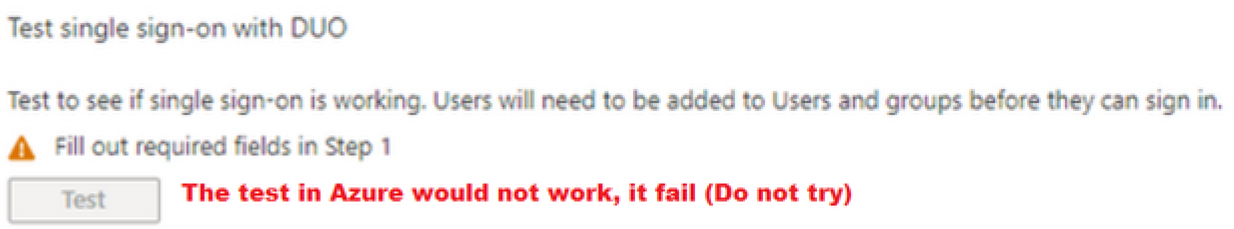
○ Simple

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

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

You have now ended the SAML Configuration between Duo and Azure.

Warning: The test in Azure does not work, it fails (please do not try).



Test single sign-on with DUO

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

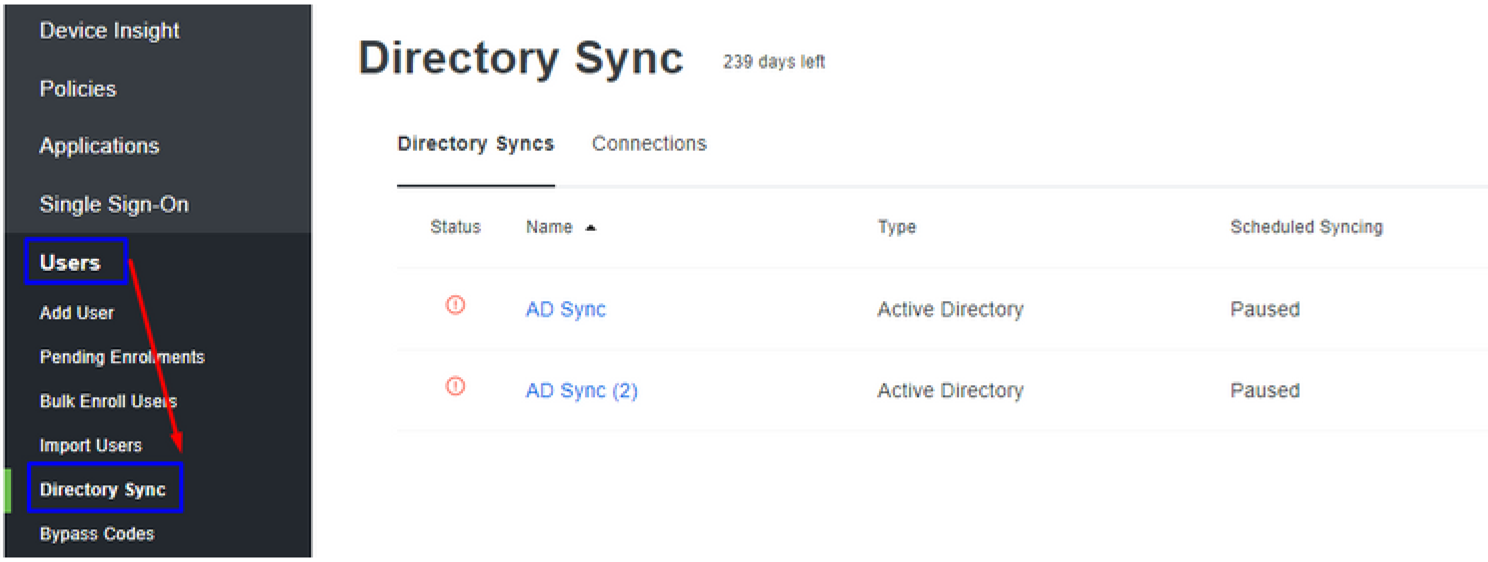
⚠ Fill out required fields in Step 1

The test in Azure would not work, it fail (Do not try)

2. Configure AD Sync to Sync the Users from Azure in Duo (Optional)

This step is optional but helps to Sync the Groups from Azure to Duo. You can skip this step if you do not want to do that.

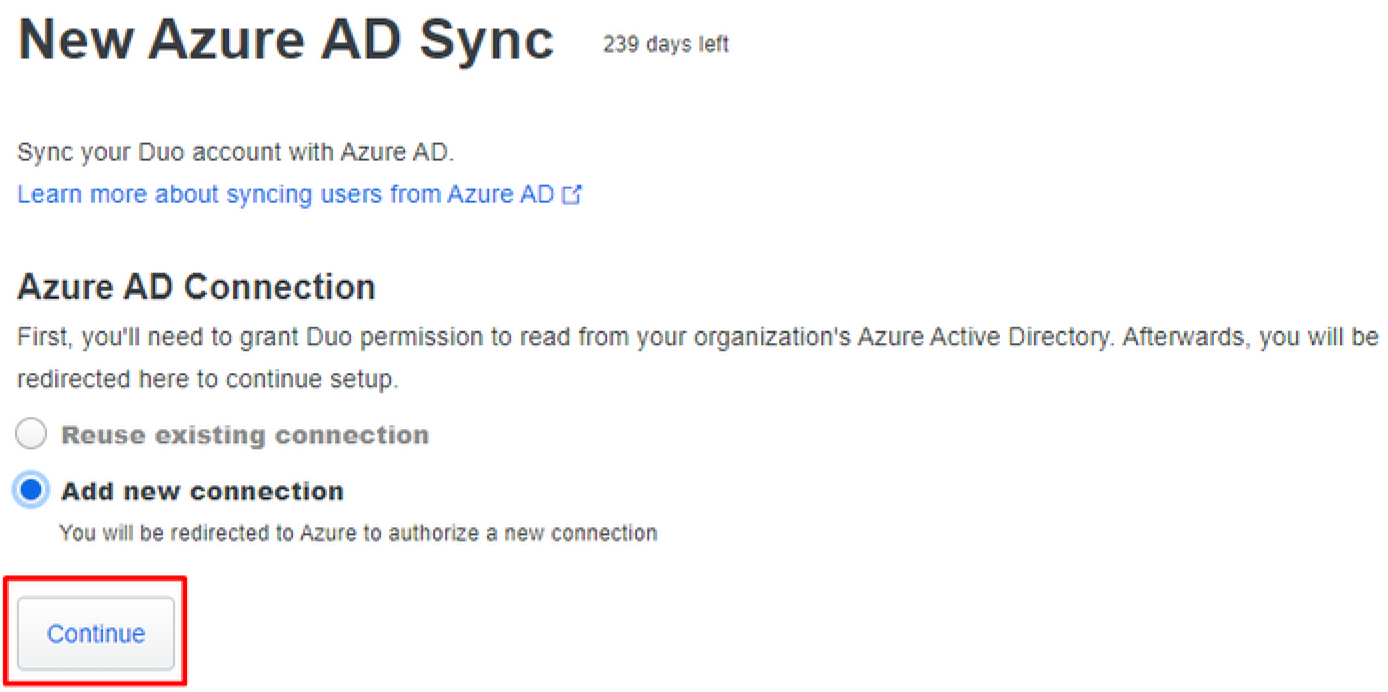
Navigate toUsers > Directory Sync > Add New Sync > Azure AD as shown in the image.



Directory Sync 239 days left

Status	Name ▲	Type	Scheduled Syncing
ⓘ	AD Sync	Active Directory	Paused
ⓘ	AD Sync (2)	Active Directory	Paused

After that, you are redirected to New Azure AD Sync. Choose Add New Connection, and click Continue.



New Azure AD Sync 239 days left

Sync your Duo account with Azure AD.

Learn more about syncing users from Azure AD

Azure AD Connection

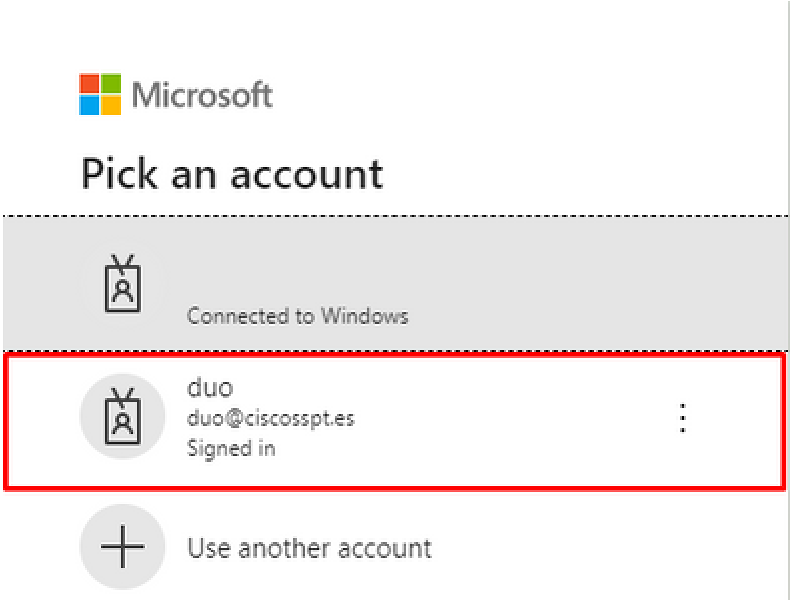
First, you'll need to grant Duo permission to read from your organization's Azure Active Directory. Afterwards, you will be redirected here to continue setup.

○ Reuse existing connection

● Add new connection

You will be redirected to Azure to authorize a new connection

You must need to authenticate in Azure in order to accept the agreements and rights.



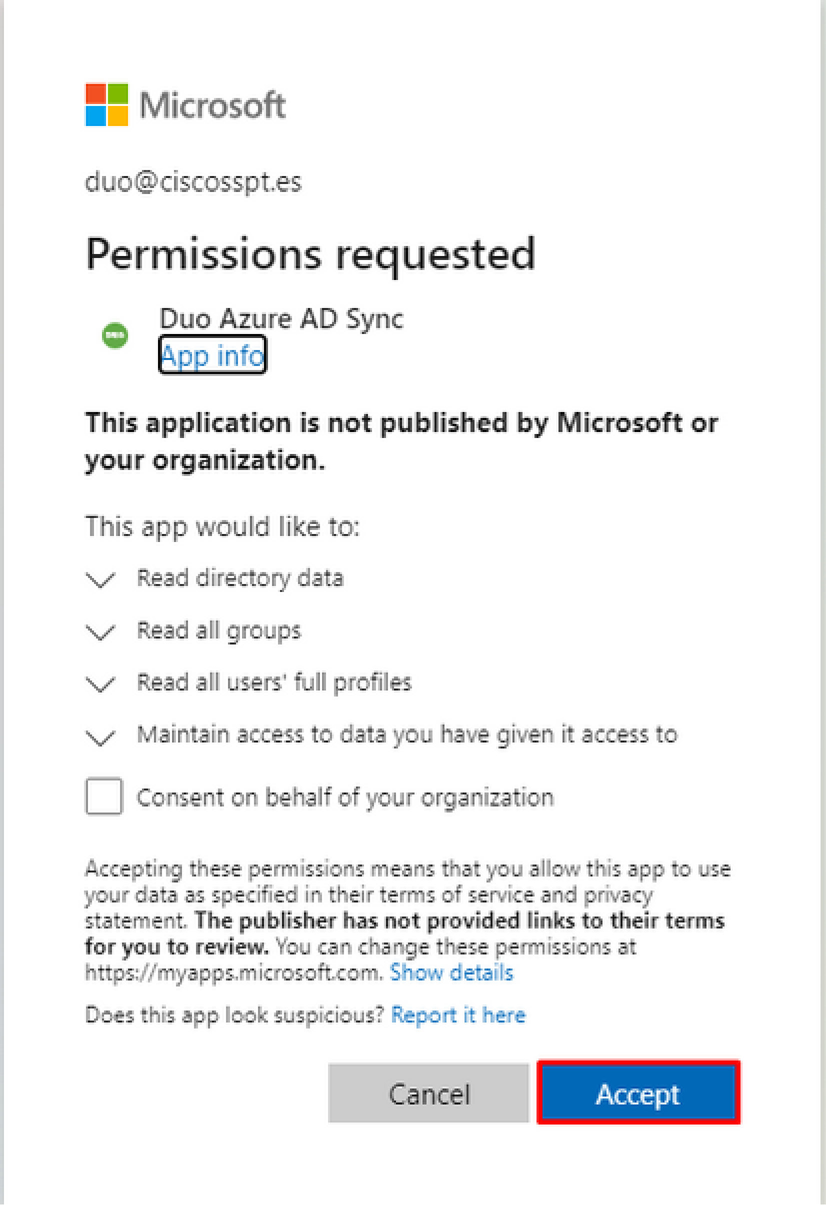
Microsoft

Pick an account

Connected to Windows

duo
duo@ciscosspt.es
Signed in

Use another account



Microsoft

duo@ciscosspt.es

Permissions requested

Duo Azure AD Sync
App info

This application is not published by Microsoft or your organization.

This app would like to:

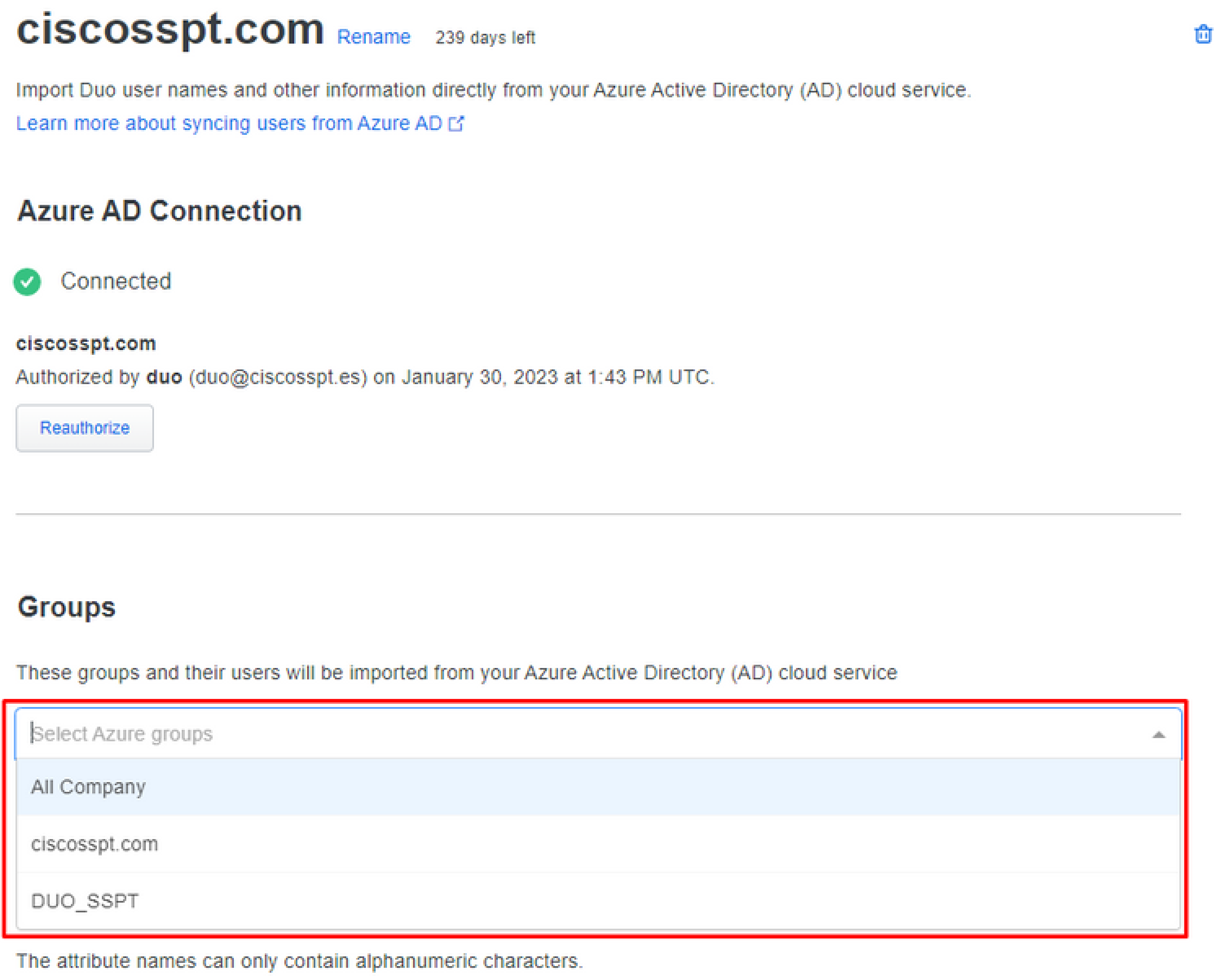
- Read directory data
- Read all groups
- Read all users' full profiles
- Maintain access to data you have given it access to

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Select theGroups which you want to integrate.



ciscosspt.com Rename 239 days left

Import Duo user names and other information directly from your Azure Active Directory (AD) cloud service.
Learn more about syncing users from Azure AD

Azure AD Connection

✓ Connected

ciscosspt.com
Authorized by **duo** (duo@ciscosspt.es) on January 30, 2023 at 1:43 PM UTC.

Reauthorize

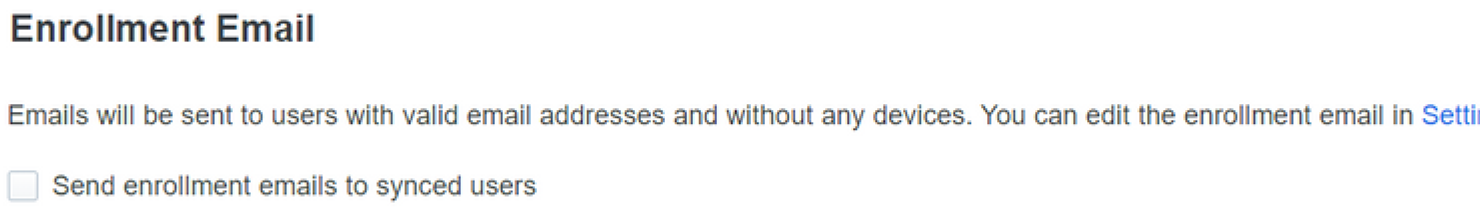
Groups

These groups and their users will be imported from your Azure Active Directory (AD) cloud service

Select Azure groups
- All Company
- ciscosspt.com
- DUO_SSPT

The attribute names can only contain alphanumeric characters.

Before that, you can mark the checkbox to permit you to send the email for enrollment, or wait for the user to log in to the app and be prompted to enroll in Duo.



Enrollment Email

Emails will be sent to users with valid email addresses and without any devices. You can edit the enrollment email in Setti

□ Send enrollment emails to synced users

And choose Save.

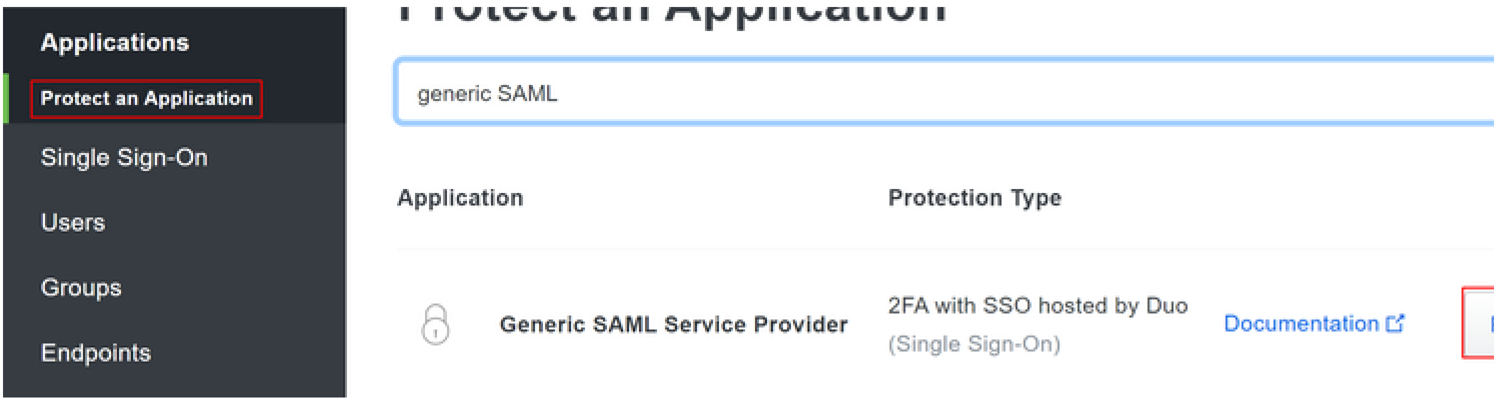
Note: To know more about enrollment and users, you can go to the next link https://duo.com/docs/enrolling-users.

3. Configure Duo Single Sign-on App for the SMA

Please refer to Single Sign-On for Generic SAML Service Providers | Duo Security.

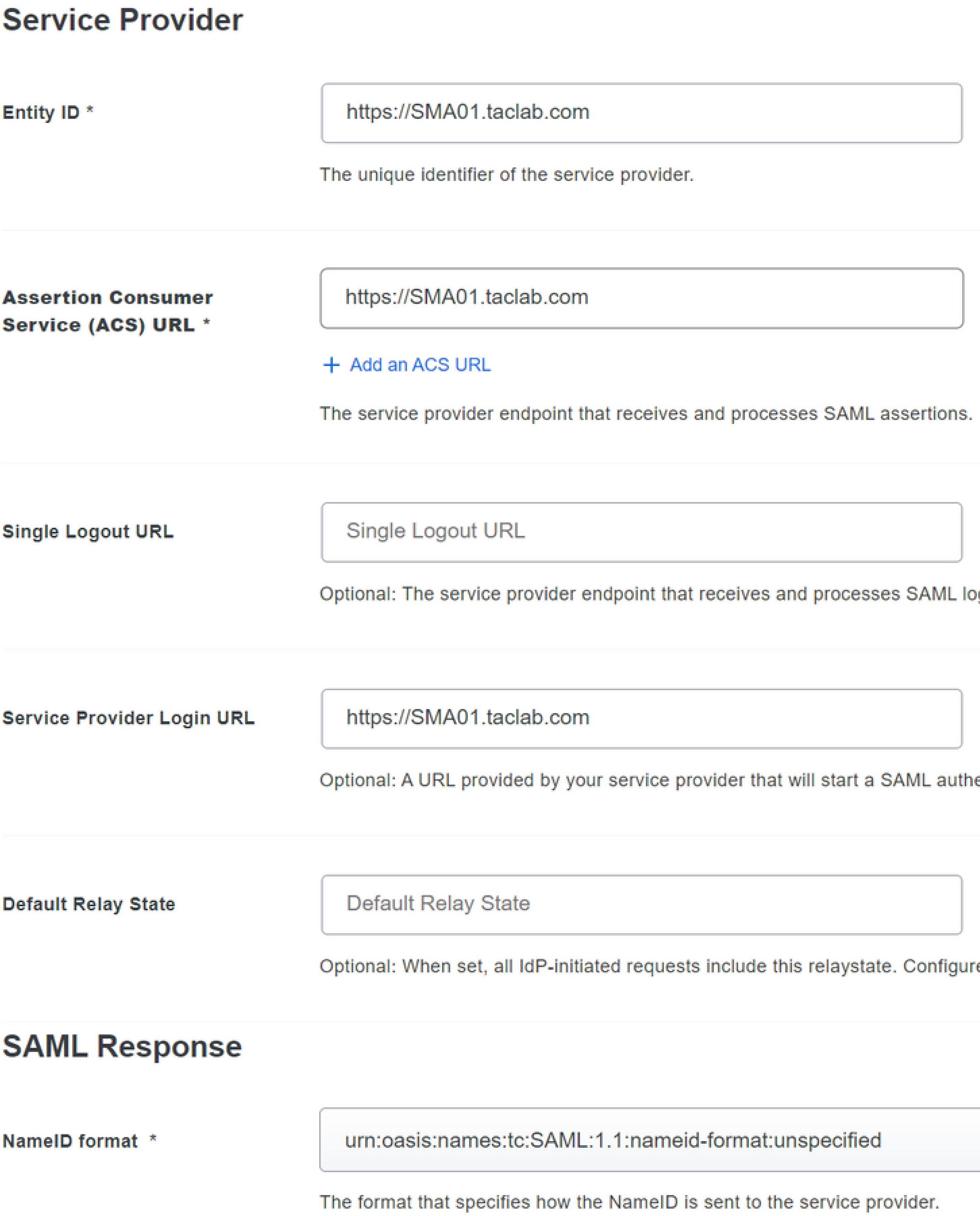
Create the APP in Duo to integrate the SMA.

- Navigate to **Applications** > **Protect an Application**
- Search for Generic SAML Service Provider.
- ChooseProtect.



In this part, you configure some variables for Service Provider and SAML Response that share the SP and the IdP.

You configure the most important part for the IdP to permit the users to authenticate and send the correct parameters in SAML.



Service Provider

Entity ID *: https://SMA01.taclab.com

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *: https://SMA01.taclab.com

The service provider endpoint that receives and processes SAML assertions.

Single Logout URL: Single Logout URL

Optional: The service provider endpoint that receives and processes SAML lo

Service Provider Login URL: https://SMA01.taclab.com

Optional: A URL provided by your service provider that will start a SAML authe

Default Relay State: Default Relay State

Optional: When set, all IdP-initiated requests include this relaystate. Configure

SAML Response

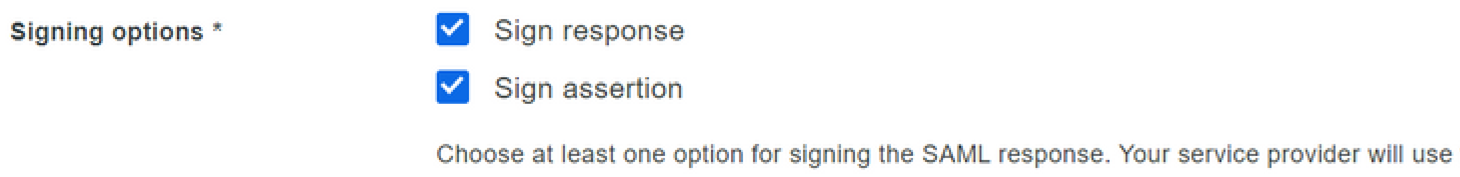
NameID format *: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

The format that specifies how the NameID is sent to the service provider.

- Entity ID: The Service Provider Entity ID is used to uniquely identify a service provider. The format of the Service Provider Entity ID is typically a URI.

- Assertion Consumer: The service provider endpoint that receives and processes SAML assertions. The SAML Assertion Consumer Service (ACS) URL for your application.
- Service Provider Login URL: The location where the SAML assertion is sent with HTTP POST. This is often referred to as the SAML Assertion Consumer Service (ACS) URL for your application.
- Name ID format: Identifies the SAML processing rules and constraints for the assertion subject statement. Use the default value of 'Unspecified' unless the application explicitly requires a specific format.

Sign response and Sign assertion need to be marked on both SMA and Duo.



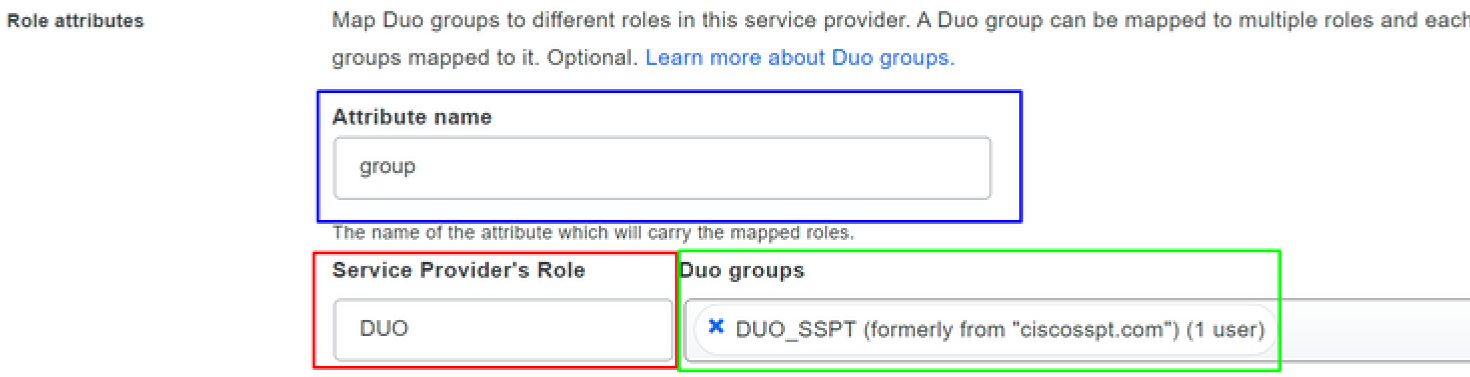
Signing options *

☑ Sign response

☑ Sign assertion

Choose at least one option for signing the SAML response. Your service provider will use

- Attribute Name: The Attribute Name depends on the attributes configured for the Identity Provider. The appliance search for match entries of the Attribute Name in the Group Mapping field, this is optional. If you do not configure it, the appliance search for match entries of all attributes in the Group Mapping field.
- Service Provider Role: Write whatever you want this is only to make the match with the group name in the directory in the SMA.
- Duo Groups: The group integrated to be used under the authentication phase between the SMA and Duo. (remember the groups to be used for the authentication are in Duo not in the SMA).



Role attributes

Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each groups mapped to it. Optional. Learn more about Duo groups.

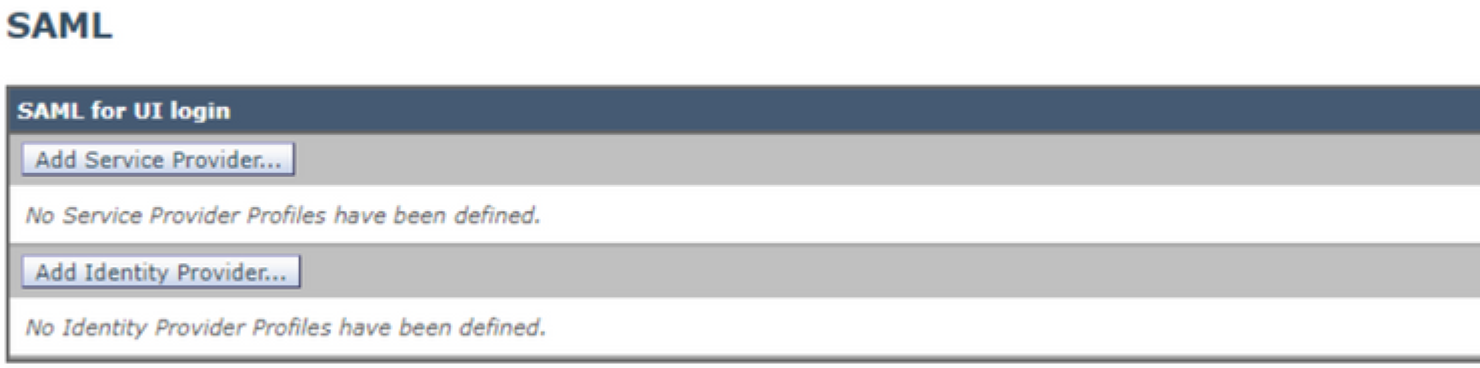
Attribute name: group

The name of the attribute which will carry the mapped roles.

Service Provider's Role	Duo groups
DUO	× DUO_SSPT (formerly from "ciscosspt.com") (1 user)

4. Configure SMA to Use SAML

Navigate to System Administration > SAML as shown in the image.



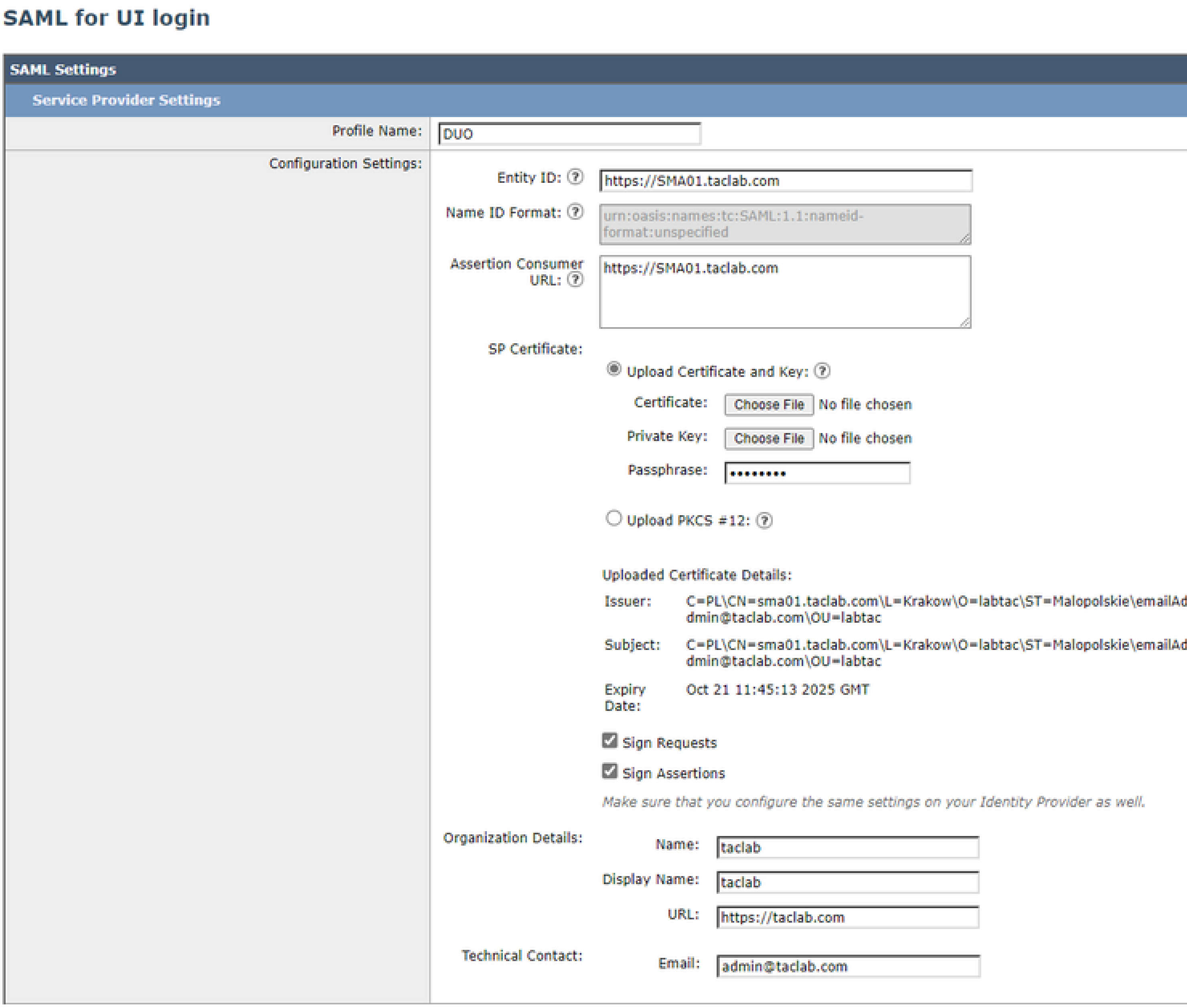
SAML

SAML for UI login

No Service Provider Profiles have been defined.

No Identity Provider Profiles have been defined.

Choose Add Service Provider.



SAML for UI login

SAML Settings

Service Provider Settings

Profile Name: DUO

Configuration Settings:

Entity ID: https://SMA01.taclab.com

Name ID Format: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Assertion Consumer URL: https://SMA01.taclab.com

SP Certificate:

● Upload Certificate and Key:

Certificate: Choose File No file chosen

Private Key: Choose File No file chosen

Passphrase: ••••••••

○ Upload PKCS #12:

Uploaded Certificate Details:

Issuer: C=PL\CN=sma01.taclab.com\L=Krakow\O=labtac\ST=Malopolskie\emailAd
dmin@taclab.com\OU=labtac

Subject: C=PL\CN=sma01.taclab.com\L=Krakow\O=labtac\ST=Malopolskie\emailAd
dmin@taclab.com\OU=labtac

Expiry Date: Oct 21 11:45:13 2025 GMT

☑ Sign Requests

☑ Sign Assertions

Make sure that you configure the same settings on your Identity Provider as well.

Organization Details:

Name: taclab

Display Name: taclab

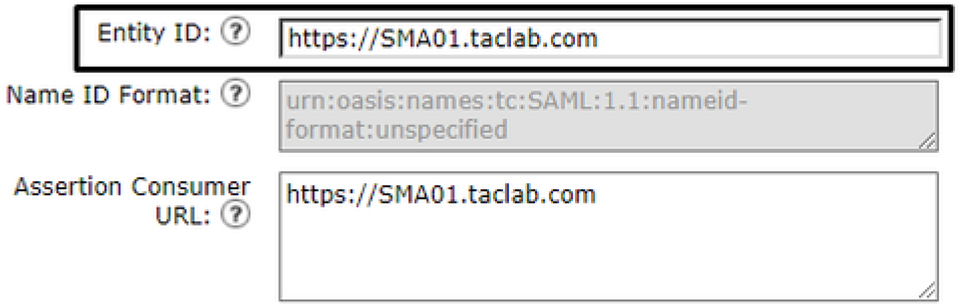
URL: https://taclab.com

Technical Contact:

Email: admin@taclab.com

Note: Remember this parameter needs to be identical in SMA and Duo.

- Entity ID: The Service Provider Entity ID is used to uniquely identify a service provider. The format of the Service Provider Entity ID is typically a URL.

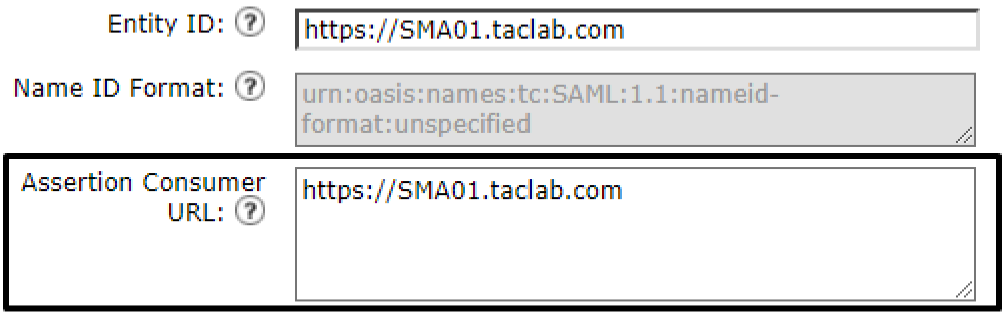


Entity ID: https://SMA01.taclab.com

Name ID Format: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Assertion Consumer URL: https://SMA01.taclab.com

- Assertion Consumer URL: The Assertion Consumer URL is the URL that the Identity Provider must send the SAML assertion after successful authentication. The URL that you use to access the web interface of your SMA must be the same as the Assertion Consumer URL. You need this value while you configure the SMA settings on Duo.

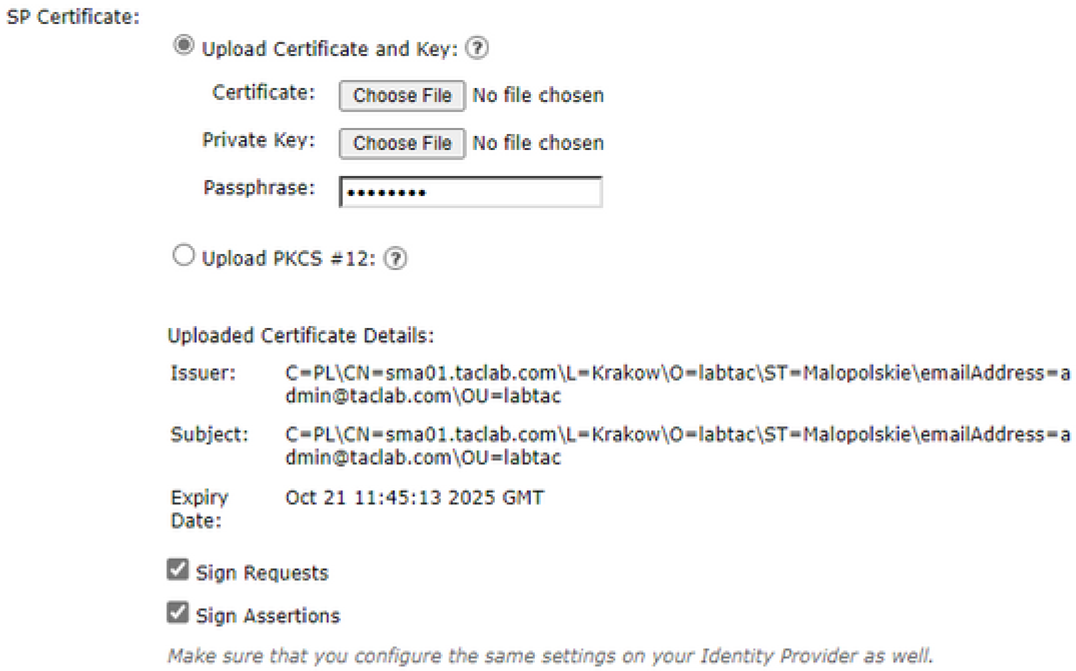


Entity ID: https://SMA01.taclab.com

Name ID Format: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Assertion Consumer URL: https://SMA01.taclab.com

- SP Certificate: That is the certificate for the hostname for which you have configured the assertion consumer URL.



SP Certificate:

● Upload Certificate and Key:

Certificate: Choose File No file chosen

Private Key: Choose File No file chosen

Passphrase: ••••••••

○ Upload PKCS #12:

Uploaded Certificate Details:

Issuer: C=PL\CN=sma01.taclab.com\L=Krakow\O=labtac\ST=Malopolskie\emailAddress=admin@taclab.com\OU=labtac

Subject: C=PL\CN=sma01.taclab.com\L=Krakow\O=labtac\ST=Malopolskie\emailAddress=admin@taclab.com\OU=labtac

Expiry Date: Oct 21 11:45:13 2025 GMT

☑ Sign Requests

☑ Sign Assertions

Make sure that you configure the same settings on your Identity Provider as well.

It would be best if you used openssl on Windows or Linux. If you want to configure a self-signed certificate you can do that with the next step-by-step or you can use your certificate:

1. Create the private key. This helps to enable encryption or decryption.

```
openssl genrsa -out domain.key 2048
```

2. Create a Certificate Signing Request (CSR).

```
openssl req -key domain.key -new -out domain.csr
```

3. Create the self-signed certificate.

```
openssl x509 -signkey domain.key -in domain.csr -req -days 365 -out domain.crt
```

If you want more days, you can change the value after -days .

> **Note**: Remember, by best practices, you must not put more than 5 years for the certificates.

After that, you have the certificate and keys to upload on the SMA in the option **upload certificate and key**.

> **Note**: If you want to upload the certificate in PKCS #12 format, it is possible to create it after Step 3.

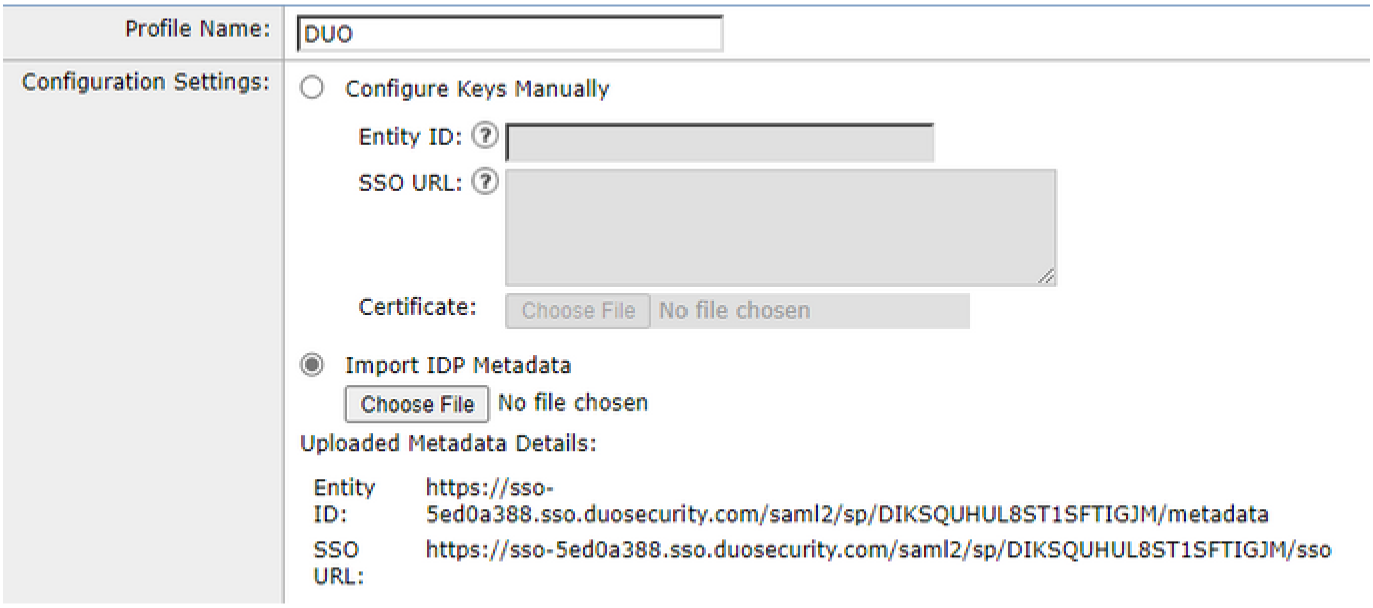
Optional

- From PEM to PKCS#12

```
openssl pkcs12 -inkey domain.key -in domain.crt -export -out domain.pfx
```

For organization details, you can fill it as you want and select submit

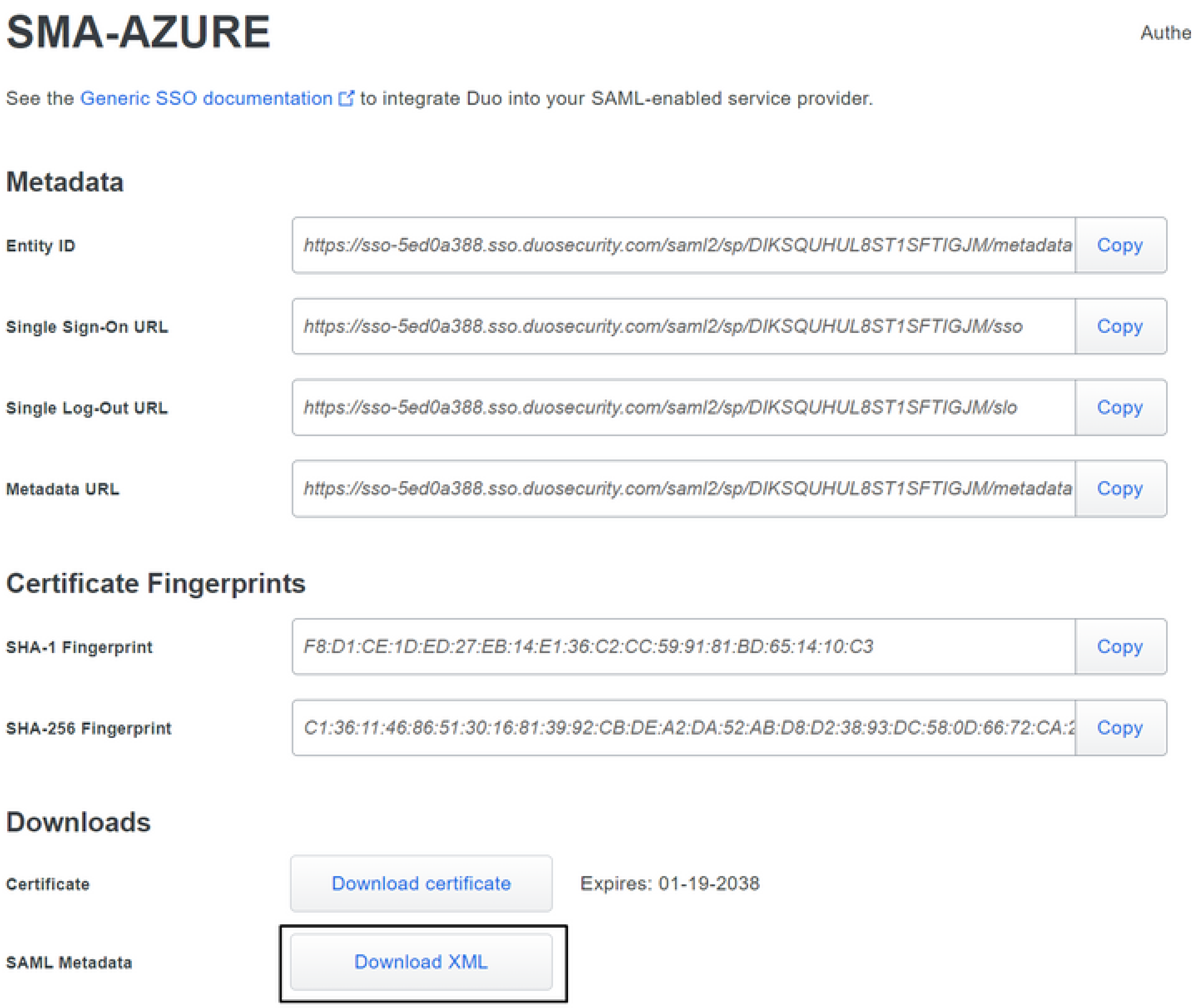
Navigate to**System Administration** > **SAML** > **Add Identity Provider** as shown in the image.



Profile Name:	DUO
Configuration Settings:	○ Configure Keys Manually Entity ID: ? SSO URL: ? Certificate: Choose File No file chosen ● Import IDP Metadata Choose File No file chosen Uploaded Metadata Details: Entity ID: https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIKSQUHUL8ST1SFTIGJM/metadata SSO URL: https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIKSQUHUL8ST1SFTIGJM/sso

In this step, you have two options, you can upload that information manually or via an XML file.

Navigate to your application in Duo and download the IdP metadata file.



SMA-AZURE

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

Metadata

Entity ID	https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIKSQUHUL8ST1SFTIGJM/metadata	Copy
Single Sign-On URL	https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIKSQUHUL8ST1SFTIGJM/sso	Copy
Single Log-Out URL	https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIKSQUHUL8ST1SFTIGJM/slo	Copy
Metadata URL	https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIKSQUHUL8ST1SFTIGJM/metadata	Copy

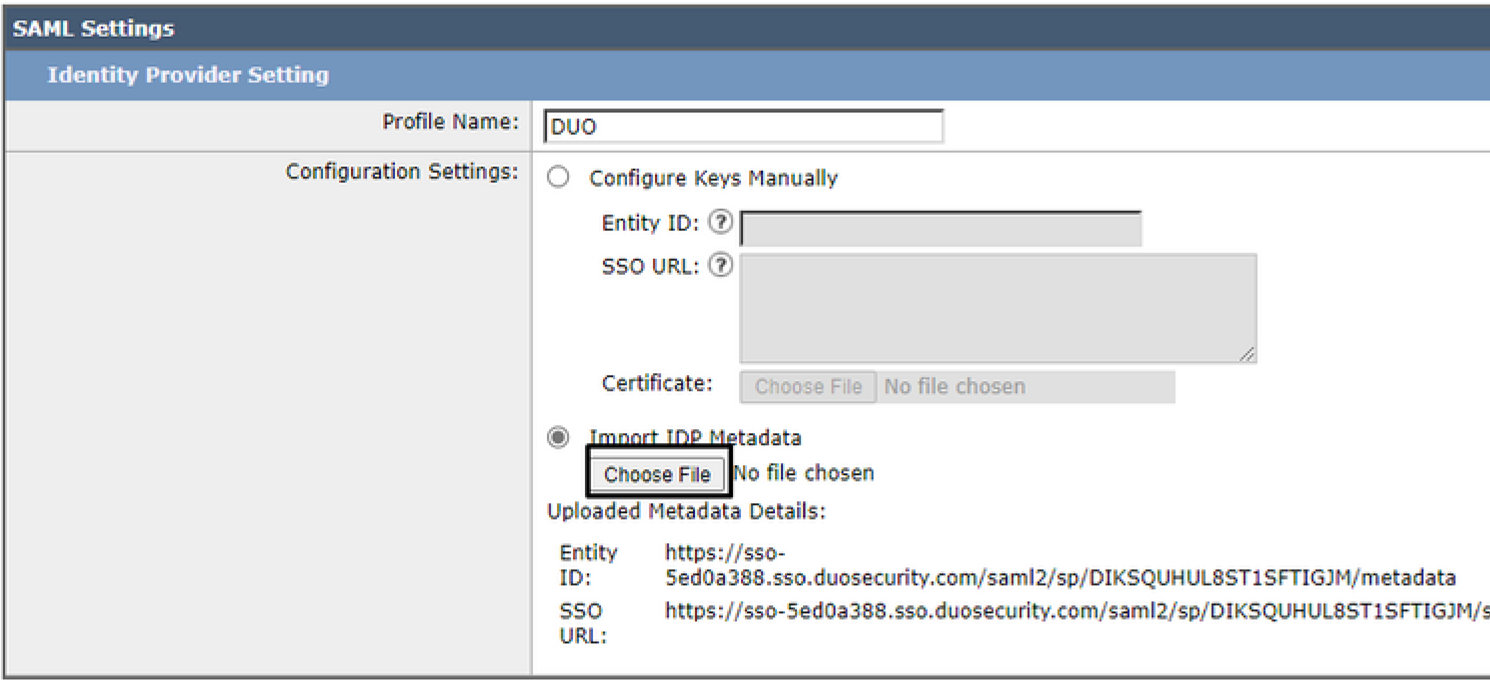
Certificate Fingerprints

SHA-1 Fingerprint	F8:D1:CE:1D:ED:27:EB:14:E1:36:C2:CC:59:91:81:BD:65:14:10:C3	Copy
SHA-256 Fingerprint	C1:36:11:46:86:51:30:16:81:39:92:CB:DE:A2:DA:52:AB:D8:D2:38:93:DC:58:0D:66:72:CA:2	Copy

Downloads

Certificate	Download certificate	Expires: 01-19-2038
SAML Metadata	Download XML	

After you have the file downloaded, you can just upload it in the IdP Metadata option in the SMA.

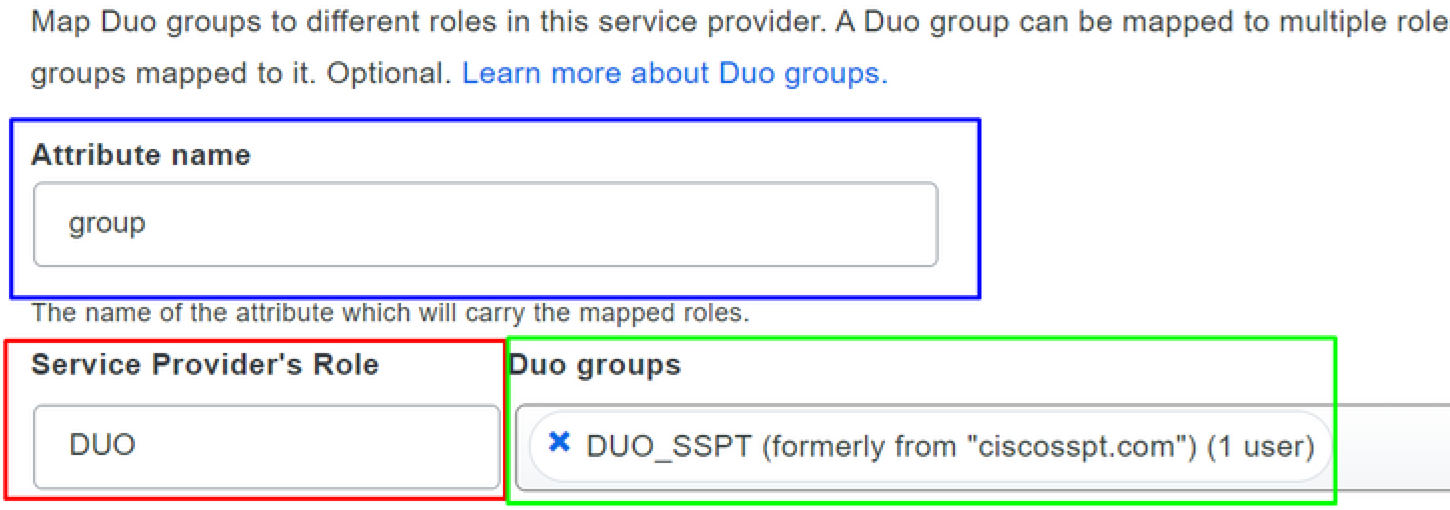


SAML Settings

Identity Provider Setting

Profile Name:	DUO
Configuration Settings:	○ Configure Keys Manually Entity ID: ? SSO URL: ? Certificate: Choose File No file chosen ● Import IDP Metadata Choose File No file chosen Uploaded Metadata Details: Entity ID: https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIKSQUHUL8ST1SFTIGJM/metadata SSO URL: https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIKSQUHUL8ST1SFTIGJM/s

For the final step under the SMA, navigate to **System Administration** > **Users** > **External Authentication** > **SAML**. And configure the next parameters to look the same as the Duo configuration.



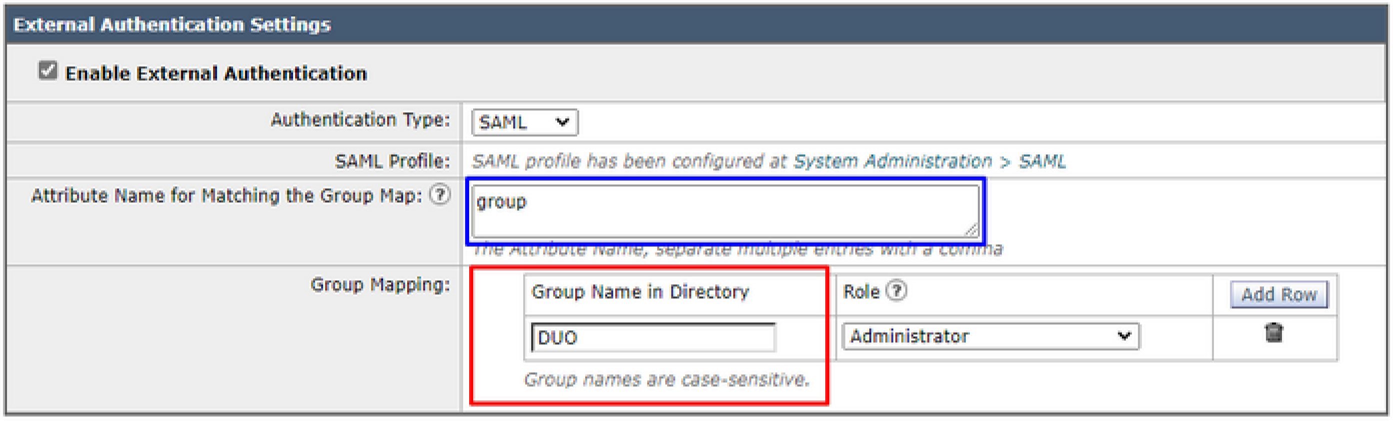
Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple role groups mapped to it. Optional. Learn more about Duo groups.

Attribute name

group

The name of the attribute which will carry the mapped roles.

Service Provider's Role	Duo groups
DUO	✕ DUO_SSPT (formerly from "ciscosspt.com") (1 user)



External Authentication Settings

☑ **Enable External Authentication**

Authentication Type:	SAML
SAML Profile:	*SAML profile has been configured at System Administration > SAML*
Attribute Name for Matching the Group Map: ?	group *The Attribute Name, separate multiple entries with a comma*
Group Mapping:	Group Name in Directory: DUO Role ?: Administrator *Group names are case-sensitive.*

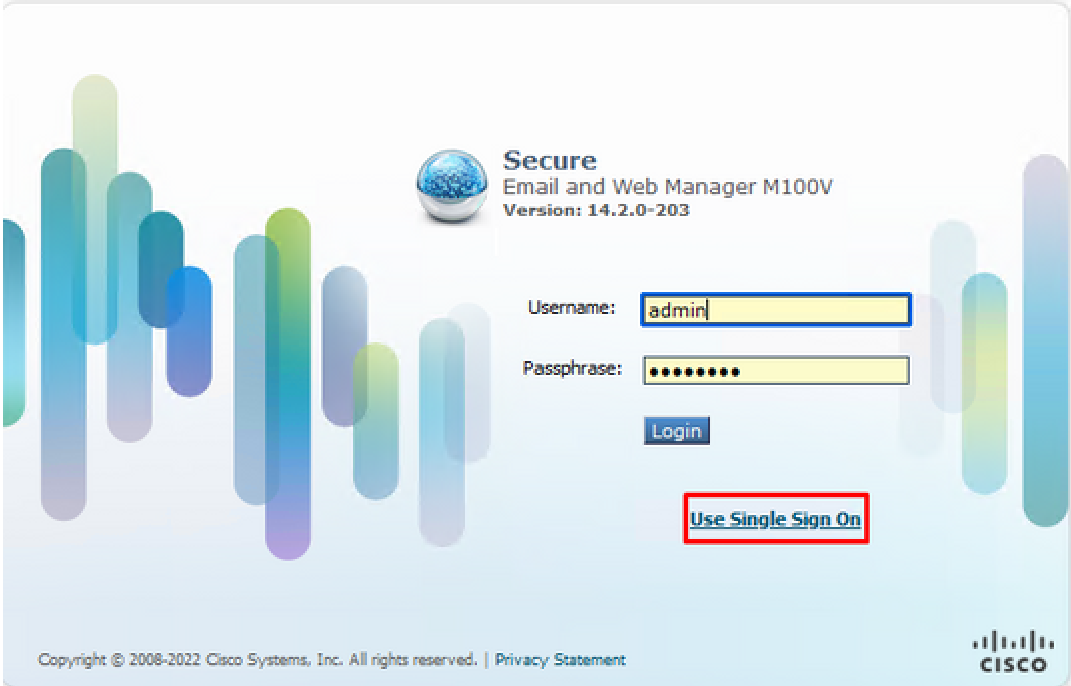
Attribute Name = Attribute Name for Match the Group Map Service Provider Role = Group Mapping

After that, you can commit the changes and confirm if your deployment work as expected!

Verify

Use this section to confirm that your configuration works properly.

In order to test your configuration, select Use Single Sign on as shown in the image.

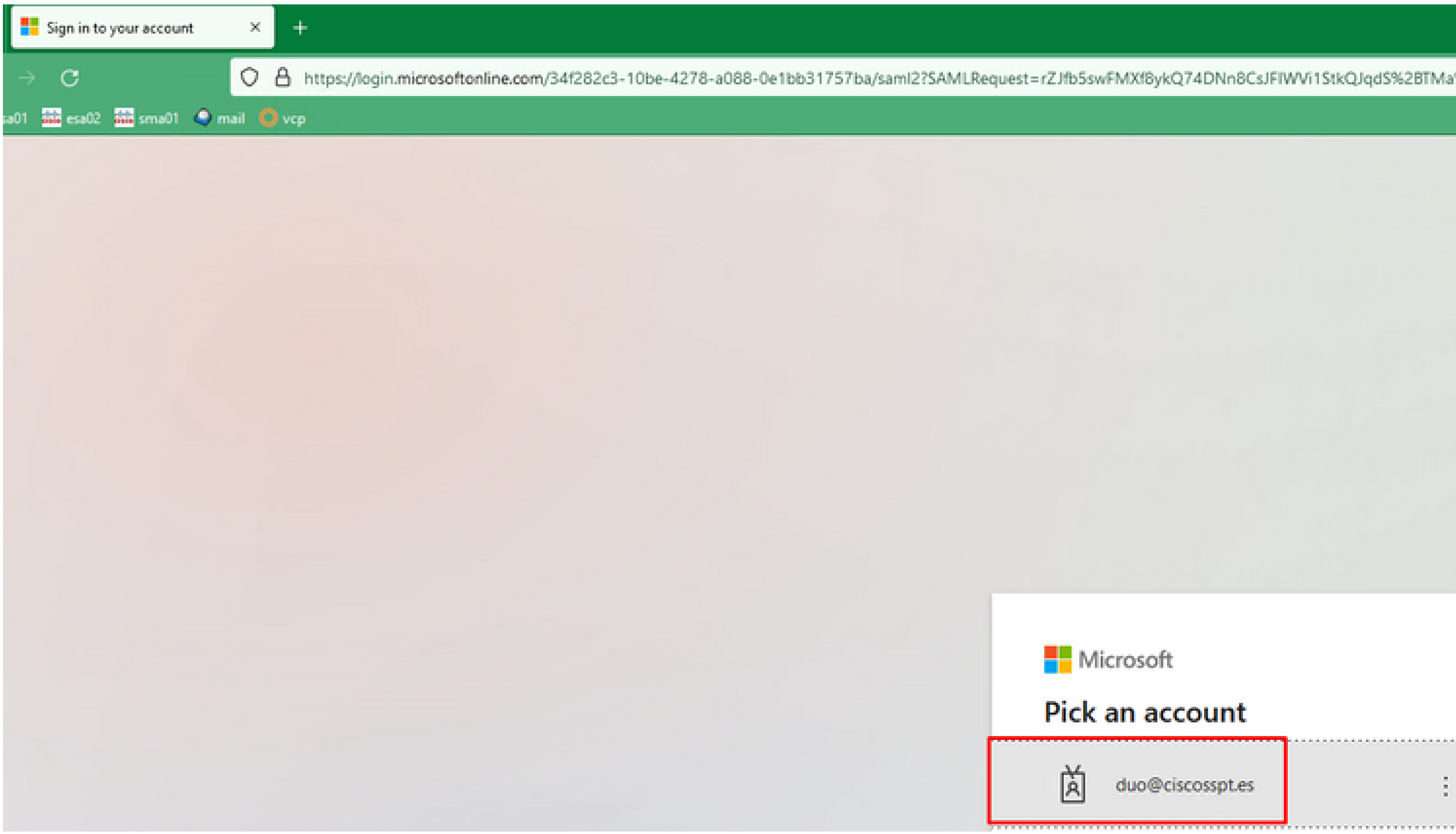


Username: admin

Passphrase: •••••••••

Copyright © 2008-2022 Cisco Systems, Inc. All rights reserved. | Privacy Statement

You are prompted to log in on Microsoft Log in as shown in the image.



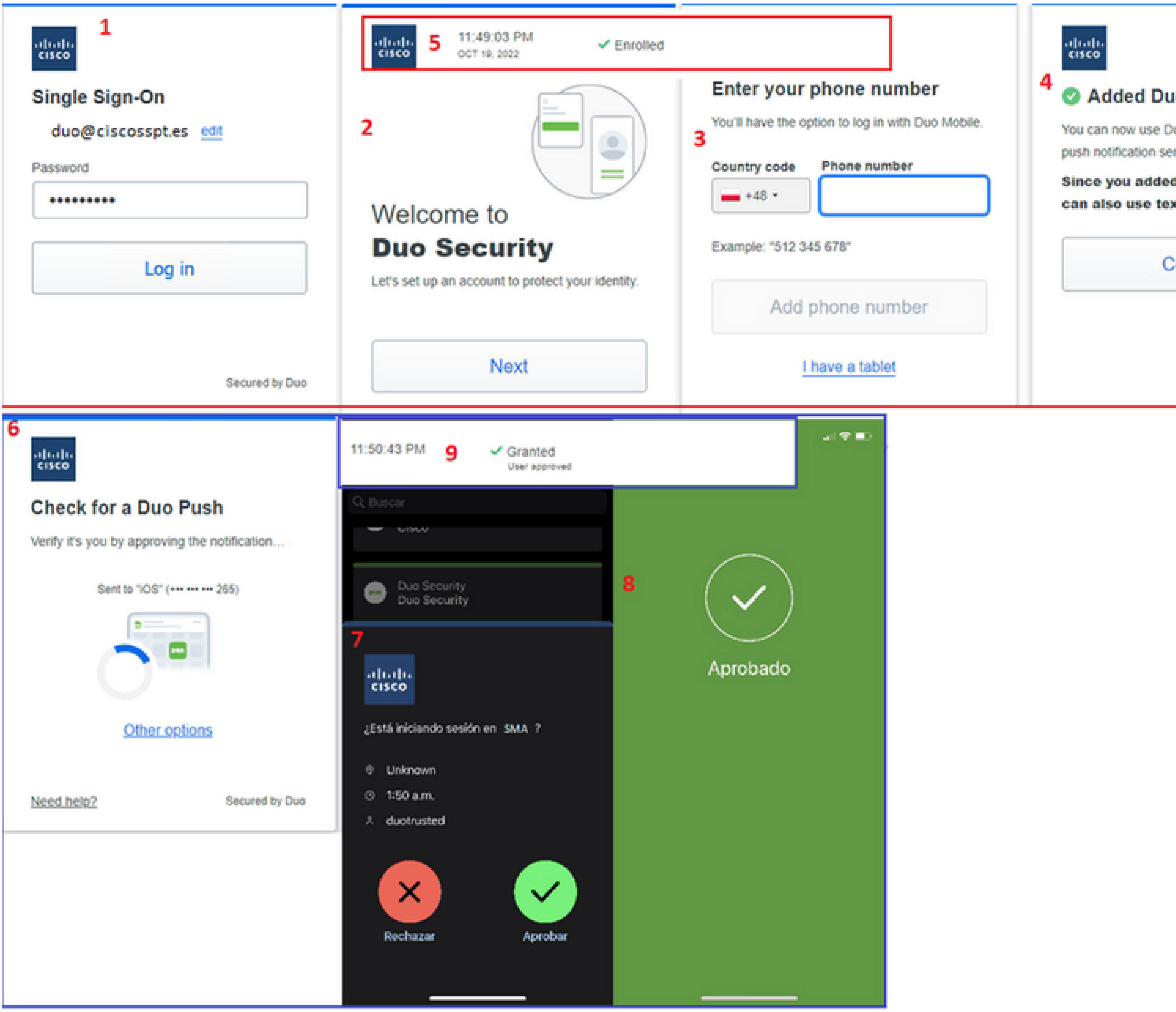
https://login.microsoftonline.com/34f282c3-10be-4278-a088-0e1bb31757ba/saml2?SAMLRequest=rZJfb5swFMXf8ykQ74DNn8CsJFIWVi1StkQJqdS%2BTMa

Pick an account

duo@ciscosspt.es

After that, if you have your user enrolled you must be prompted to configure a username and password in Duo to authenticate, and after that, you need to select the authentication method.

If you do not have your user enrolled and you have the policy configured to enroll an unenrolled user, you are moved to the enrollment process and authentication method after that, like in the next example.



1 Single Sign-On

duo@ciscosspt.es edit

Password

•••••••••

5 11:49:03 PM OCT 19, 2022 ✓ Enrolled

2 Welcome to Duo Security

Let's set up an account to protect your identity.

3 Enter your phone number

You'll have the option to log in with Duo Mobile.

Country code +48

Phone number

Example: "512 345 678"

4 Added Du

You can now use D

push notification se

Since you added

can also use tex

6 Check for a Duo Push

Verify it's you by approving the notification...

Sent to "iOS" (••• ••• ••• 265)

9 11:50:43 PM ✓ Granted User approved

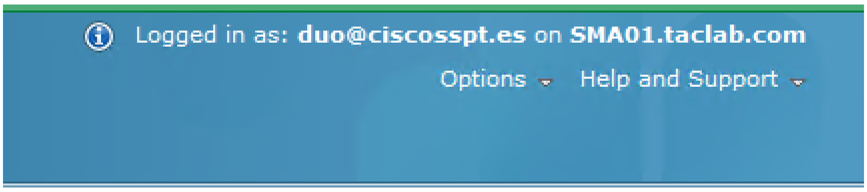
7 ¿Está iniciando sesión en SMA ?

Unknown

1:50 a.m.

duotrusted

If everything was configured and corrected, you have successfully logged in.



Logged in as: **duo@ciscosspt.es** on **SMA01.taclab.com**

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- Duo SSO for SAML Auth with Azure
- **Technical Support & Documentation - Cisco Systems**