

SSO against Cisco Duo Identity Provider

This article describes how to configure Cisco Duo to enable Imagicle users to login to web portal, gadgets and Attendant Console with Single Sign-on based on SAML protocol.

Prerequisites

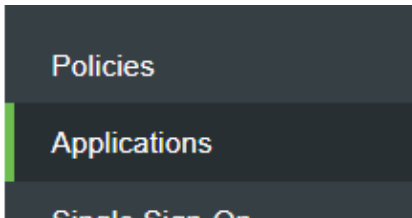
In order to successfully configure your Cisco Duo, you should have the following data:

- **User Pool ID**
- **Redirect URI**

More details are available [here](#).

Procedure

1. Login to your DUO admin portal
2. Select **Applications** item from the left menu panel



3. Click on "**Protect an Application**"
4. Enter "**generic**" in the search box
5. Hit "**Protect**" button, included in "**2FA with SSO hosted by Duo**" protection type
6. In "Service Provider" section, please enter the **User Pool ID** in the "Entity ID" field. See below:

Service Provider

Entity ID *

urn:amazon:cognito:sp:eu-central-1_ocxxxxxx

The unique identifier of the service provider.

7. In the "Assertion Consumer Service (ACS) URL" field, please enter the **Redirect URI**. See below:

Assertion Consumer Service (ACS) URL *

https://sso.acme.imagicle.cloud/saml2/idpresponse

+ Add an ACS URL

The service provider endpoint that receives and processes SAML assertions.

8. In "SAML Response" section, enter the **NameID format** corresponding to an email address. See below:

SAML Response

NameID format *

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

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

9. In **Nameid attribute**, please select "**Email Address**". See below:

NameID attribute *

✖ <Email Address> |

NameID is a SAML attribute that identifies the user. Enter in an IdP attribute or attribute based on the IdP. There are five preconfigured attributes: <Email Addr

10. In "Settings" section, enter the **Name** "Imagicle SSO" to identify Imagicle applications. See below:

Settings

Type

Generic Service Provider - Single Sign-On

Name

Imagicle SSO

Duo Push users will see this when approving transactions.

11. Hit "**Save**"

12. Click on "**Download XML**" button:

Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

SAML Metadata

[Download XML](#)

13. Please send downloaded file to **Imagicle Team** to complete the SSO federation.