

CyberArk (SAML) Setup Guide

The following document outlines the steps required to **manually** onboard an organization to start connecting to Lasso's toolchain via CyberArk using the SAML protocol.

Once integrated, users stored in an organization's CyberArk will be able to use their organizations' email and be granted tokens to communicate with Lasso.

Let's get started!

1. Configure External IdP in CyberArk

CyberArk requires defining Lasso as an **External Identity Provider**, including setting routing rules so that login attempts from the customer's domain are correctly redirected to Lasso's SAML endpoint.

Step 1 - Create an External Identity Provider:

- a. Log in to **CyberArk Identity Administration** with an administrator account.
- b. Navigate to: **Settings** → **Users** → **External Identity Providers**.
- c. Click **Add** to create a new SAML identity provider.
- d. Enter a clear and descriptive name (e.g. **"Lasso SAML"**).

Step 1.1 - Configure Routing Rules:

- a. Go to the **Routing Rules** tab.
- b. Under **Federation Domains**, click **Add**.
- c. Enter the customer's email domain, for example: "example.com"
- d. Important notes:
 - The value must match the domain portion of the user's email (after the @).
 - Do not include the "@" symbol.
 - No trailing spaces.
 - If the customer uses multiple domains, add each one separately.

- Click **Save** to complete step 1.

These routing rules determine when CyberArk will redirect users to the external SAML flow. If a domain is missing or incorrect, federation will fail and users will not be redirected properly.

After completing this step, the customer can proceed to configuring SAML metadata, certificates, and attribute mappings.

2. Create a Lasso-specific application and define it with the following parameters

Assertion Consumer Service (ACS) URL -

```
https://lasso-security.auth.us-east-1.amazonaws.com/saml2/idpresponse
```

Audience URL -

```
urn:amazon:cognito:sp:us-east-1_29GgFPYsf
```

User pool ID -

```
us-east-1_29GgFPYsf
```

3. Provide us with the **metadata URL** certificate URL. In the customer's portal, the certificate resembles the following:

← Back to Web Apps > 3 of 6

Lasso Security

Type: Web - SAML + Provisioning Status: Deployed

Application Configuration Help Actions

Settings

Trust

SAML Response

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

App Gateway

Workflow

Changelog

Additional Attributes

Trust

Learn more

Identity Provider Configuration

Configure your IDP Entity ID / Issuer and Signing Certificate, if needed. Your SAML Service Provider will require you to send IDP Configuration values in a certain method. Choose the method, then follow the instructions.

☒ Metadata

☐ Manual Configuration

Metadata

IDP Entity ID / Issuer and Signing Certificate do not need to be edited in most cases. If you need to edit them, edit them first then proceed to the configuration method required by Service Provider.

> IDP Entity ID / Issuer ⓘ

> Signing Certificate ⓘ

> Single Sign On URL ⓘ

URL [Copy URL](#)

File [Download Metadata File](#)

XML [Copy XML](#)

Service Provider Configuration

Select the configuration method specified by Service Provider, and then follow the instructions.

☐ Metadata

☒ Manual Configuration

Manual Configuration

Fill out the form below with information given by your Service Provider. Be sure to save your work when done.

SP Entity ID / Issuer / Audience ⓘ

[Save](#) [Cancel](#)

4. Ensure the following user attribute mapping exists and resembles the following:

← Back to Web Apps > 3 of 6

Lasso Security

Type: Web - SAML + Provisioning Status: Deployed

Settings

Trust

SAML Response

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

App Gateway

Workflow

Changelog

Additional Attributes

SAML Response

Learn more

Attributes

Click the Add button below to map attributes from your source directory to SAML attributes that should be included in the SAML response for this application.

[Add](#)

	Attribute Name	Attribute Value
☐	email	LoginUser.Email
☐	firstname	LoginUser.FirstName
☐	lastname	LoginUser.LastName

and you should be redirected to the proper CyberArk.

Congrats!

You have successfully configured SAML for your desired company!