

envi



# SINGLE-SIGN ON

Configuration Guide



# Table of Contents

<b>Introduction</b> .....	<b>2</b>
<b>Obtaining Envi SAML metadata</b> .....	<b>3</b>
<b>Identity Provider configuration</b> .....	<b>4</b>
Automatic configuration.....	4
Manual configuration.....	5
Post configuration steps .....	6
<b>Envi configuration</b> .....	<b>7</b>
Automatic Configuration .....	7
Manual Configuration .....	8
Envi Users Configuration .....	9

## Introduction

Single sign-on providers make it easy to manage application logins and permissions. The SSO integration allows you to effectively manage access to Envi using a secure and scalable identity management system.

Your SSO provider prevents common weak points in the authentication experience, including username and password login or password reset requests. You do not need to manually renew or worry about weak login credentials that cause security issues and enforce session timeouts and require users to sign in again after these time-outs. It also provides a familiar login experience across your applications.

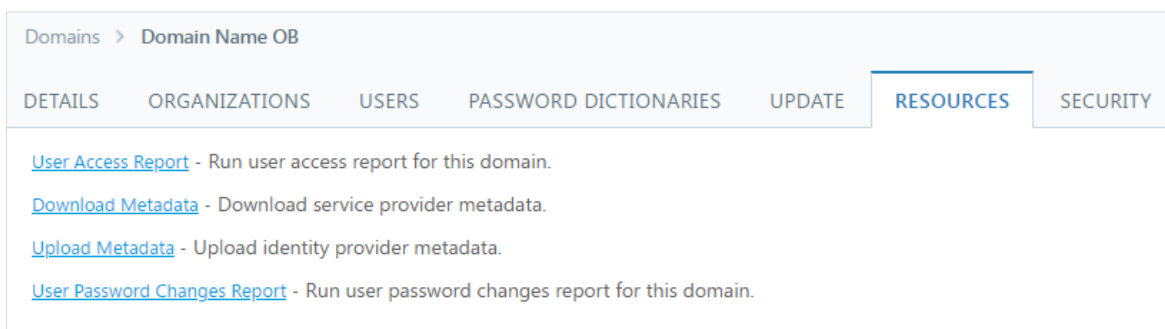
This step-by-step guide explains how to set up single sign-on to your Envi account with the SSO providers.

## Obtaining Envi SAML metadata

To configure your Identity Provider (IdP) for successful connection with Envi, you need to have the SAML metadata file.

In the Envi application set up the following domain and user configurations:

1. Sign in to the Envi application.
2. Go to the **Domain List**, and then select the domain you need.
3. Go to the **Resources** tab, and then click the **Download Metadata** link.



The screenshot shows the 'Resources' tab selected in the Envi application. The breadcrumb navigation is 'Domains > Domain Name OB'. The tabs are 'DETAILS', 'ORGANIZATIONS', 'USERS', 'PASSWORD DICTIONARIES', 'UPDATE', 'RESOURCES', and 'SECURITY'. The 'RESOURCES' tab is active and contains the following links:

- [User Access Report](#) - Run user access report for this domain.
- [Download Metadata](#) - Download service provider metadata.
- [Upload Metadata](#) - Upload identity provider metadata.
- [User Password Changes Report](#) - Run user password changes report for this domain.

As a result, you will get the Envi SAML metadata file.

# Identity Provider configuration

The SAML metadata file ([Obtaining Envi SAML metadata](#)) contains all information you need to configure Service Provider (SP) connection on IdP side, either in automatic or manual way.

## Automatic configuration

Some IdPs support automatic configuration of connections based on the SAML metadata file.

1. Sign in to your IdP as an administrator and create new instance of the SAML based connection (other possible names: **SP connection**, **SAML connector**, **SAML application**, etc.).
2. Go to the **SSO configuration** step and select the create from metadata file option. Follow further instructions and complete configuration.

When configuration is completed, navigate to the section that describes included outgoing claims and configure one for Name ID:

1. Select **Name ID** as a claim type
2. Select **Email Address** as a value.

## Manual configuration

If your IdP doesn't support automatic configuration, you can configure it manually using information provided in Envi SAML metadata file. For that, you need the following information:

1. **Audience** (other possible names: **Identifier**, **EntityID**, **Audience Restriction**, **Audience URI**, **SP Entity ID**)—Described as a value of the **entityID** attribute by the following path: **EntityDescriptor** > **entityID**:

```
<EntityDescriptor ID="_c990ba84-8alf-4430-bcf4-436f1e1074c0" entityID="https://host-name/Account" cacheDuration="P1D"
```

2. **ACS (Consumer) URL** (other possible names: **Single Sign On URL**, **Reply URL**)—Described as a value of the **Location** attribute by the following path: **EntityDescriptor** > **SPSSODescriptor** > **AssertionConsumerService** (with HTTPPOST binding) > **Location**:

```
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <KeyDescriptor>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Data>
        <X509Certificate>MIID1TCCAn2gAwIBAgIJPXT0UCrVX1RMA0GCSqGSIb3DQEBCwUAMGExCzAJBgNVBAYTA1VBMQ0wCwYDVQQIDARMDm12MQ0wCwYDVQOH
      </X509Data>
    </KeyInfo>
  </KeyDescriptor>
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://host-name/Account/Logout" />
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://host-name/Account/Logout" />
  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://host-name/Account/Acs" index="0"
  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://host-name/Account/Acs" index="1"
  <AttributeConsumingService index="0" isDefault="false">
    <ServiceName xml:lang="en"/>
    <RequestedAttribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" isRequired="true"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Name ID" />
    <RequestedAttribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" isRequired="false"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Email" />
  </AttributeConsumingService>
</SPSSODescriptor>
```

3. **Envi certificate public key in PEM format**—Described as a value of the X509Certificate element by the following path: **SPSSODescriptor** > **KeyDescriptor** > **KeyInfo** > **X509Data** > **X509Certificate**:

```
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <KeyDescriptor>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Data>
        <X509Certificate>MIID1TCCAn2gAwIBAgIJPXT0UCrVX1RMA0GCSqGSIb3DQEBCwUAMGExCzAJBgNVBAYTA1VBMQ0wCwYDVQQIDARMDm12MQ0wCwYDVQOH
      </X509Data>
    </KeyInfo>
  </KeyDescriptor>
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://
```

**Note:** Public key is provided as a single string value. Depending on your IdP, it may expect different format of the key (with headers). In this case, you need to convert the **X.509 certificate single string** value to the **X.509 certificate with header** value. For example, you can use the [SAML online tool](#) for conversion.

4. **SAML nameID format** (other possible names: **Name ID Format**)—Need to be set to **Email** or **EmailAddress**.
5. **ACS (Consumer) URL Validator** (other possible names: **Recipient**, **Recipient URL**, **Destination URL**)—Populate these additional required fields with the same value as **Audience** (the **entityID** value from metadata file).

If your IdP doesn't provide a setting for Name ID Format while creating the connection, you need to navigate to the section that describes included outgoing claims and configure one for **Name ID**:

1. Select **Name ID** as a claim type
2. Select **Email Address** as a value.

## Post configuration steps

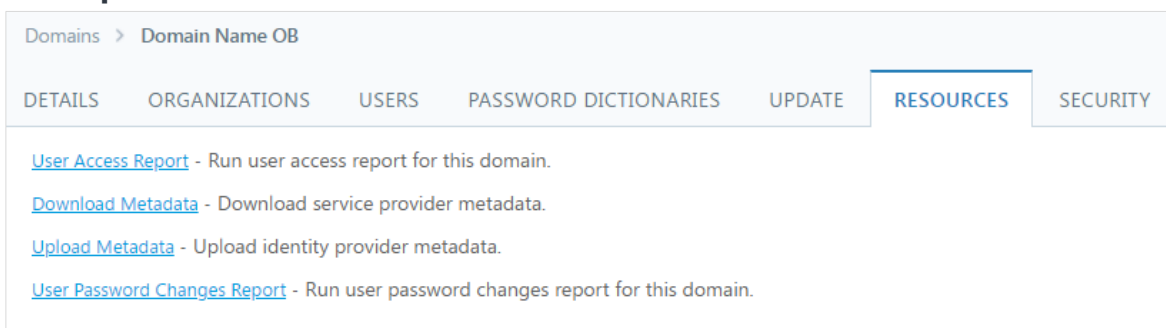
For correct setup of the SP side (Envi) you need to get metadata information about IdP configuration. If your IdP supports such possibility, you just need to copy IdP's metadata URL or download IdP's metadata file and configure Envi with it. If your IdP doesn't support such possibility, you will need to perform manual configuration of Envi SAML connection settings.

# Envi configuration

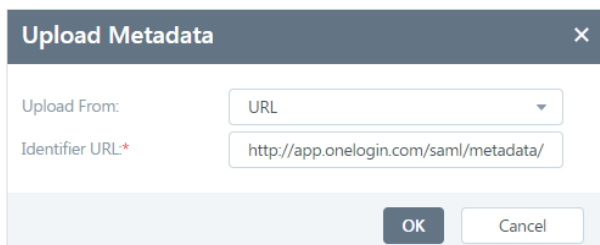
In case you have the IdP SAML metadata file or URL of the location, you can configure Envi domain automatically. Otherwise, you will need to perform manual configuration based on information available from your IdP.

## Automatic Configuration

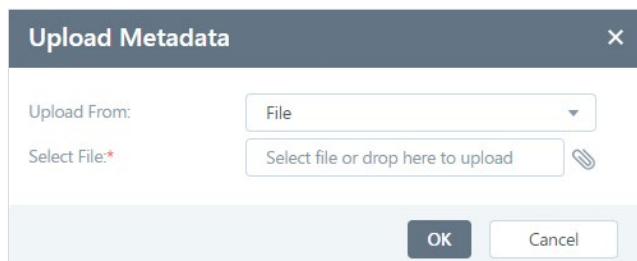
1. Sign in to the Envi application.
2. Go to the **Domain** list, and then select the domain you need.
3. On the **Domain Details** page, go to the **Resources** tab.
4. Click **Upload Metadata** link.



5. If you have the URL address (link) to the IdP metadata file, select **URL** as a value for the **Upload From** dropdown list. Specify URL to the IdP metadata location in the **Identifier URL** field, and then click the **OK** button.

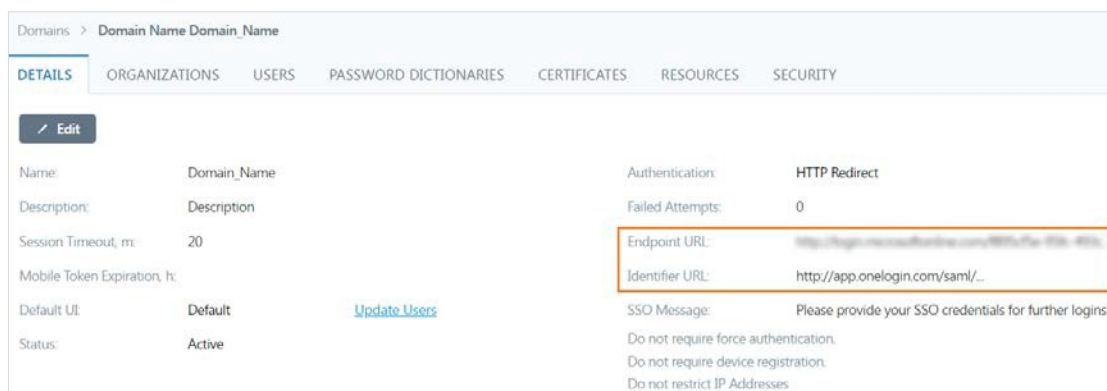


6. If you have IdP metadata saved as a file, select **File** as value for the **Upload From** dropdown list. Specify path to the IdP metadata location in the **Select File** field, and then click **OK** button.





7. Make sure that **Endpoint URL** and **Identifier URL** are populated with the new values.



## Manual Configuration

For manual configuration of the SAML connection on the Envi side, you will need the following information:

1. URL of the endpoint to which Envi should send the SAML request. You can find this information on the **Details** page of Envi connection configuration on IdP side. Usually, it is called SAML 2.0 Endpoint (HTTP).
2. **IdP Identifier**—Value that represents identifier of current IdP. Usually, it is called **Issuer URL**, **Identifier URL**, or **SAML Issuer ID**.
3. IdP certificate used for SAML assertion signing (public key only).
4. IdP certificate used for SAML assertion encryption (public key only).

Perform the following steps for the manual configuration of Envi domain:

1. Sign in to the Envi application.
2. Go to the **Domain** list, and then select the domain you need.
3. Click the **Edit** button.
4. Make sure that the **Authentication** type is set to **HTTP Redirect**.
5. Specify **SAML 2.0 Endpoint** in the **Endpoint URL** field.
6. Specify IdP Identifier in the **Identifier URL** field.
7. Click the **Update** button.

- In the bottom section of the **Details** tab, click the **Add Certificate** button.

- Specify name for the signing certificate and location of the signing certificate file. Click the **Save** button.
- Repeat the 7-9 steps for the certificate used for encryption.

## Envi Users Configuration

While creating user, select the needed domain with the HTTP Redirect type of authentication. In the **SSO User Name** field enter the username from the IdP.

Attribute	Value
User Name:	UserName@xx.com
First Name:	FirstName
Last Name:	LastName
Title:	Title
Email Address:	<a href="mailto:Email@xx.com">Email@xx.com</a>
Phone:	Phone
Phone Ext.:	Phone Ext.
Fax:	Fax
Time Zone:	(UTC+13:00) Samoa
Default UI:	Envi HTML v.2
Status:	Active
User Type:	User
Domain:	Domain_Name
Default Organization:	UVZ
Role:	None
Org User Type:	Interface
Session Timeout:	201
Report Format:	PDF
Email Format:	Plain Text
SSO User Name:	SSO User Name

Now, user can sign in to the Envi application using SSO with configured IdP.