

Single Sign-On (SSO)

Brief Overview

The Single Sign-On page in the [Admin Center](#) offers enterprise grade **Self Served SSO** configuration Management, based on the new Authentication Infrastructure.



Use Cases

- Reduce onboarding time
- Enable self served configuration and management
- Replace old proprietary SSO
- Enable Full SSO capabilities
- Enhanced Security and compliance

SSO Glossary

Assertion: Data provided by the IdP that supplies one or more of the following statements to a service provider:

- *Authentication statements* assert that the user specified in the assertion actually did authenticate successfully, and what time they did so.
- *Attribute statements* supply attribute values pertaining to the user. The NameID attribute is required and specifies the username, but other attributes can be manually configured as well.
- *Authorization decision* statements declare that a request to allow the assertion subject to access the specified resource has been granted or denied

Assertion Consumer Service (ACS): The service provider's endpoint (URL) that is responsible for receiving and parsing a SAML assertion. Keep in mind that some service providers use a different term for the ACS. In the Okta SAML template, this is entered in the **Single Sign On URL** field.

Attribute: A set of data about a user, such as username, first name, employee ID, etc

Audience Restriction: A value within the SAML assertion that specifies who (and *only* who) the assertion is intended for. The "audience" will be the service provider and is typically a URL but can technically be formatted as any string of data. If this value is not provided by the SP, try using the ACS

Default Relay State: The URL that users will be directed to after a successful authentication through SAML.

Endpoint: The URL's that are used when Service Providers and Identity Providers communicate to one another.

Entity ID: A globally unique name for an Identity Provider or a Service Provider. A unique Okta Entity ID is generated for each application, and is referred to as the **Identity Provider Issuer** in the Okta application's Setup Instructions.

Identity Provider (IdP): The authority that verifies and asserts a user's identity and access to a requested resource (the "Service Provider")

Metadata: A set of information supplied by the IdP to the SP, and/or vice versa, in xml format.

- SP supplied metadata will typically provide the ACS, the Audience Restriction, the NameID format, and an x.509 certificate if the assertion needs to be encrypted. At this time, SP-supplied metadata files cannot be imported into Okta.
- IdP supplied metadata will provide the Single Sign On URL, the Entity ID and the x.509 certificate file required by the SP to decrypt the assertion.

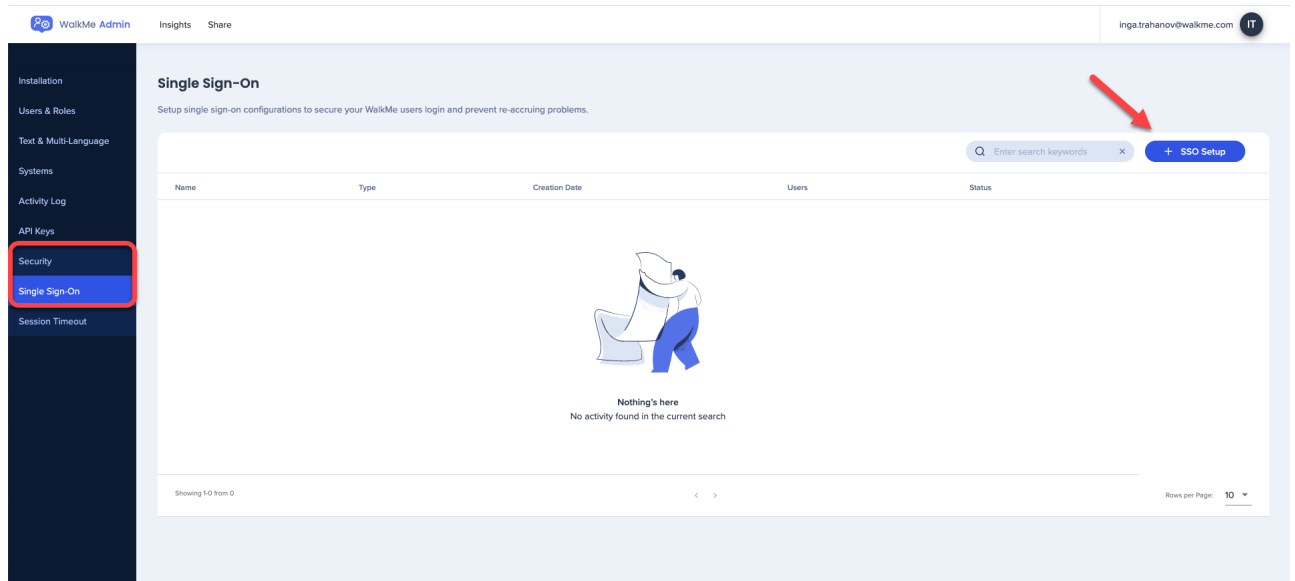
NameID: An attribute within the assertion that is used to specify the username

Service Provider (SP): The hosted resource or service that the user intends to access, such as Box, Workday®, Salesforce, a custom application, etc.

Single Sign On URL: The endpoint that is dedicated to handling SAML transactions. In the Okta SAML template setup screen, the SSO URL refers to the service provider's **ACS**.

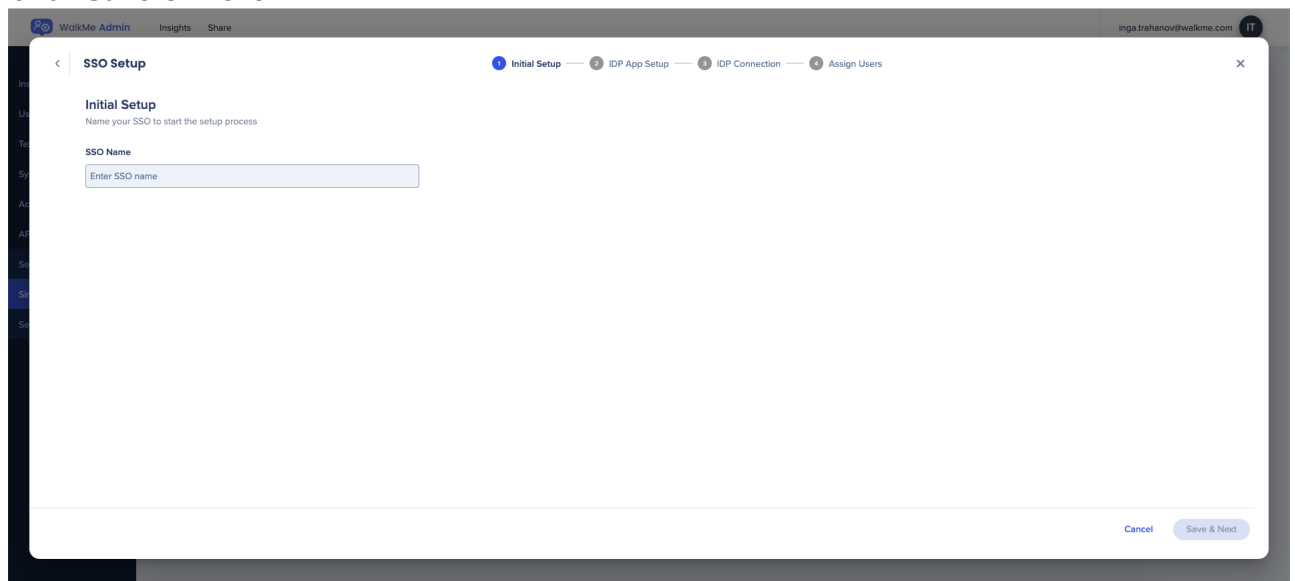
How It Works

1. Open the [Admin Center](#) at [admin.walkme.com](#)
 1. For EU users, go to [eu-admin.walkme.com](#)
2. Go to the **Security** page and then **Single Sign-On**
3. Click the **+ SSO Setup** button



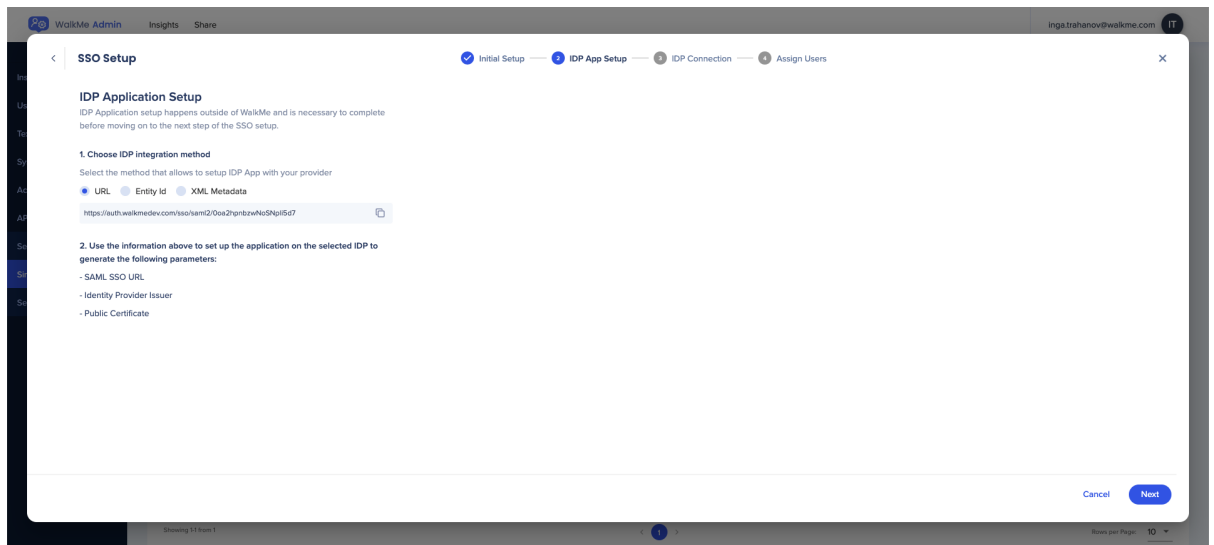
4. Enter the name of SSO

5. Click **Save & Next**



6. Choose the IDP Integration method:

- **URL**
- **Entity ID**
- **XML Metadata** – When choosing this method you can download the xml as a file

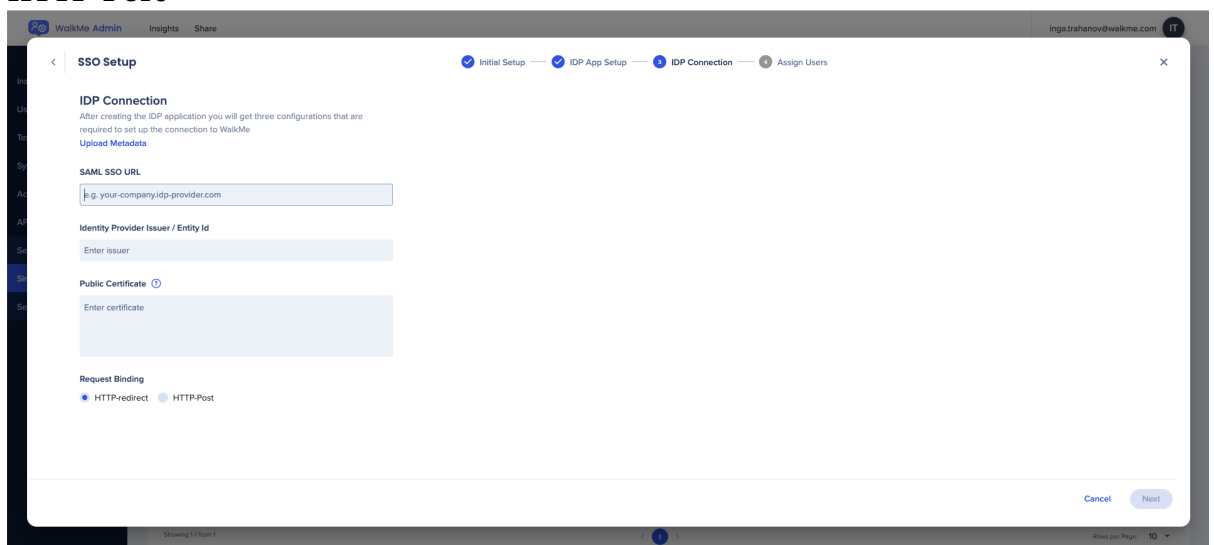



7. Enter the required details to complete SSO setup:

- **SAML SSO URL**
- **Identity Provider Issuer / Entity ID**
- **Public Certificate**

8. Choose the relevant request binding

- **HTTP-redirect**
- **HTTP-Port**

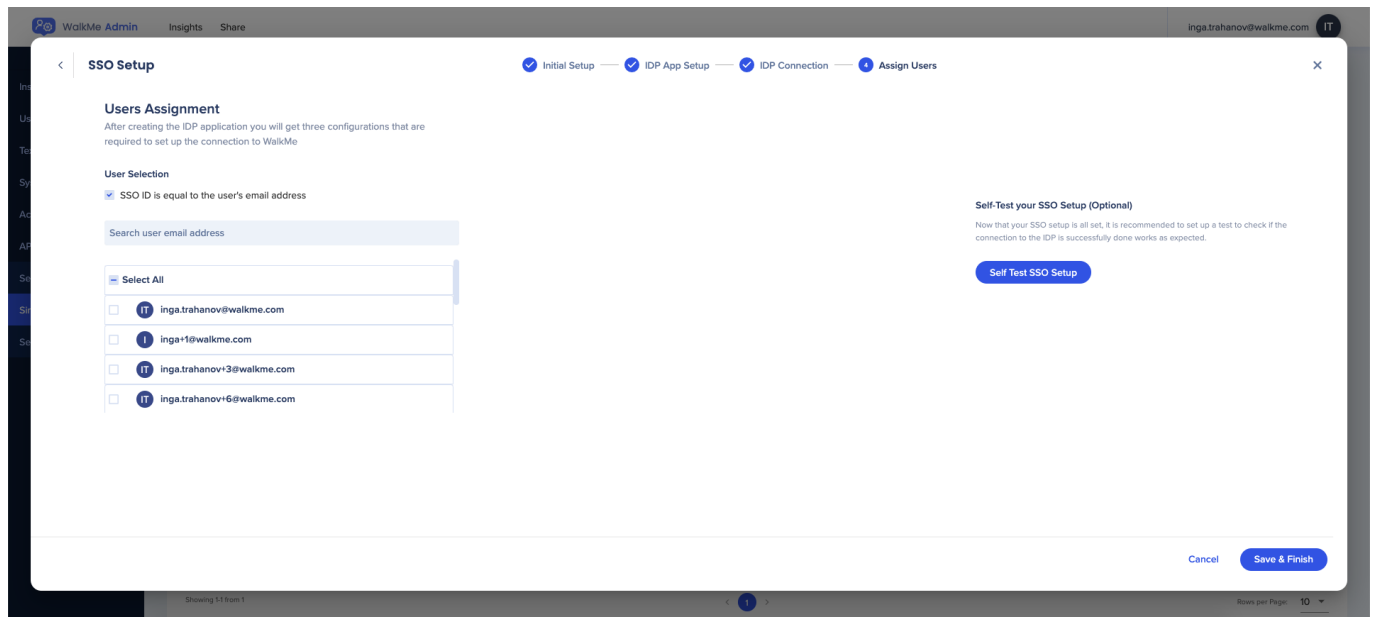


-  **Tip:** Click **Upload Metadata** to automatically fill all relevant fields

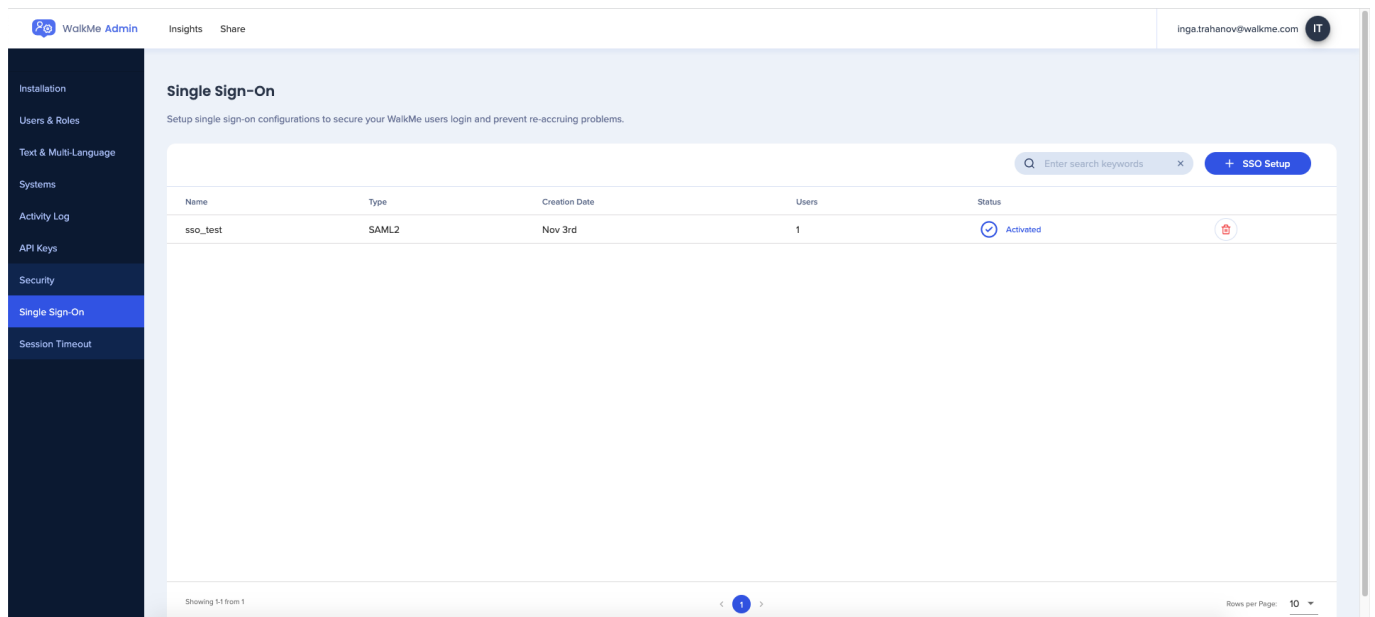
9. Select users to assign to the SSO

- You can search for and assign specific users or **Select All**
- The default SSO ID is email, but this can be modified if desired
- Use the **Test SSO Setup** button to check the SSO setup

10. Click **Save & Finish**



Once the SSO connection was added successfully you will be able to see it on the Single Sign-On page in the Admin Center.



For more information on configuring SSO for Azure AD, please refer to the following article:
[Microsoft Tutorial](#)

SSO Certificate

Note:

- WalkMe is moving to a new SSO solution provided by the leader in identity management, Okta, that offers higher availability, performance, and better monitoring and logging capabilities.
 - If your account is currently registered with WalkMe's legacy SSO, please contact whoever is managing your Single Sign-On internally, usually the Identity and Access Management or IT team, and have them follow the process below.
 - They will know the information that needs to be filled out to configure SSO.
1. Create a new SSO connection following [the steps above](#)
 2. In the 3rd step, you will be required to upload the new certificate and then finish the setup
 3. After the creation of the new SSO connection, all relevant links that are using the old SSO should be changed to the new one created in the setup

SSO Troubleshooting

What Causes SAML Errors?

SAML errors usually occur when there's missing or incorrect information entered during your SAML setup. You can resolve most of these issues from your IDP settings, but for some, you'll need to update your SSO settings in WalkMe as well.

SAML Error Messages

Error message	How to fix it
The SAML Response does not contain the correct Identity Provider Issuer. Please check that the Issuer URL in your [IDP] settings matches the Identity Provider Issuer below.	Check your IDP settings to ensure you have the right value copied over to your SSO configuration in Admin Center . The Issuer value in an IDP is typically referred to as an Issuer URL or Entity URL/ID .
The SAML Response is not signed. Please check your [IDP] settings.	Enable signing responses in your IDP settings. If you don't see these options, contact your IDP.

The SAML Response does not contain the correct Audience. Please check that the Service Provider URL in your [IDP] settings matches the Service Provider Issuer in Advanced Options below.	Make sure the Service Provider Issuer matches the Audience in your IDP settings. The Audience might also be called the SP Entity ID or Relying Party Identifier .
The Assertion of the SAML Response is not signed. Please check your [IDP] settings.	Enable signing assertions of responses in your IDP settings. If you don't see these options, contact your IDP.
The SAML Response does not contain the correct Destination, which should look something like https://auth.walkme.com/sso/saml2 . Please check your [IDP] settings.	Update the destination in your IDP. The value's name may vary, but it will typically be one of the following: Reply URL, ACS URL, Assertion Consumer Service URL, Trusted URL, or Endpoint URL.
The SAML Response is missing the ID attribute. Please check your [IDP] settings.	Make sure you're including the NameID as a claim sent in your IDP in the correct (Persistent) format.
Neither the SAML Response nor Assertion of the SAML Response are signed. Please check your [IDP] settings.	From your IDP settings, enable signing the response , the assertion of the response or both. If you don't see these options, contact your IDP.
The SAML Response is not signed (though there is a signed and encrypted Assertion with an EncryptedId). Apologies, but WalkMe doesn't support this format. Please check your [IDP] settings.	We don't support this format. Enable signing the response and make sure you're following the guidelines to set up your SSO properly.
The SAML Response is not version 2.0. Please check your [IDP] settings.	Make sure you're using SAML 2.0 in your IDP.
Hmm, it looks like the signature validation failed. Please check the signing certs in your [IDP] settings.	Update the certificate in your SSO configuration in Admin Center to match the certificate sent from your IDP.