Sisukord

SAML SSO Configuration Guide

This guide walks you through setting up a SAML Single Sign-On (SSO) identity provider (IdP) in Directo.

Prerequisites

- You have permissions to change Directo system settings
- Administrator access to your Identity Provider (e.g., Microsoft Entra ID, Okta, Google Workspace)
- Your IdP's SAML configuration details (Login URL, Metadata URL)

Step 1: Configure Your Identity Provider

Before configuring Directo, you need to register Directo as a Service Provider (SP) in your Identity Provider. Use the following values:

Parameter	Value
Reply URL / ACS (Assertion Consumer Service)	`https://login.directo.ee/api/saml/callback`
Entity ID / Identifier	The default value is https://login.directo.ee/api/saml/callback. The SAML SSO Entity ID (or Identifier) is a unique identifier for the Identity Provider (IdP) or Service Provider (SP). If the system-provided default value is not suitable, industry best practice is to use a unique URL in URI format or a designated URN. **It must be strictly unique within the system (Identity Provider)!**
Name ID format	`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` (if using Email mapping) or `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` (if using Username mapping)

Where to configure:

- **Microsoft Entra ID**: Azure Portal → Enterprise Applications → New Application → Create your own application → Integrate any other application (Non-gallery) → Single sign-on → SAML → Basic SAML Configuration → Edit
- **Okta**: Applications → Create App Integration → SAML 2.0 → Configure SAML → General settings
- **Google Workspace**: Admin Console → Apps → Web and mobile apps → Add app → Add custom SAML app → Service provider details

Important: The Reply URL / ACS and Entity ID values must match exactly, including the protocol (https) and path. Mismatched values will cause authentication failures.

Step 2: Open the SAML SSO Configuration

Navigate to the SAML SSO configuration page in Directo. You will see a list of existing IdP configurations, or an empty list if none have been configured yet.

From the main menu: Settings → Common Settings → SSO Saml Login settings. Or use the search feature.

Step 3: Create a New Configuration

1. Click the **Add new** button.
2. You will be taken to the IdP configuration form.

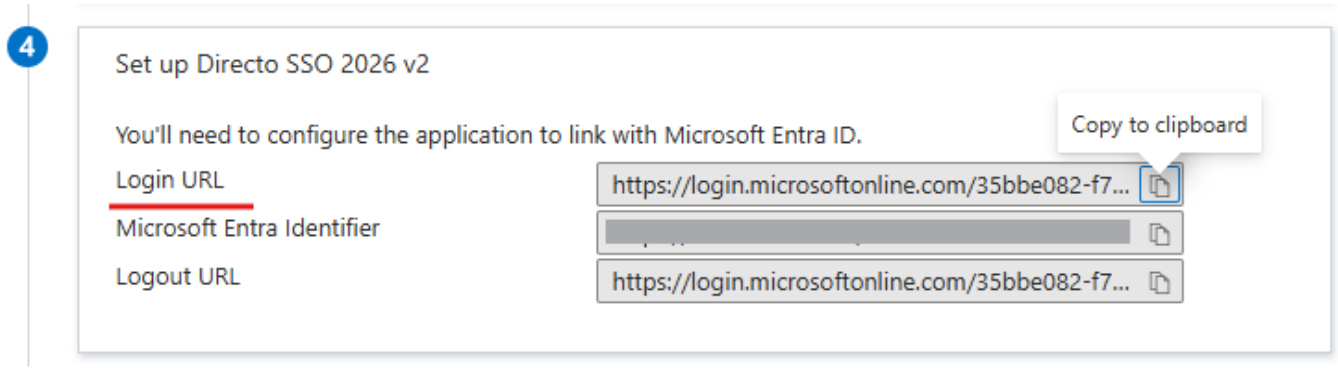
Step 4: Fill in the Button Title

Enter a descriptive name in the **Button title** field. This is the label that will appear on the SSO login button on the Directo login page (e.g., „Login with Azure AD“ or „Company SSO“).

Step 5: Configure the IdP Settings

Login URL (required)

Enter the **Login URL** (also known as SSO URL or SAML Endpoint) from your Identity Provider. This is the endpoint where Directo sends SAML authentication requests.



Where to find it:

- **Microsoft Entra ID**: Azure Portal → Enterprise Applications → Your App → Single sign-on → Login URL
- **Okta**: Applications → Your App → Sign On tab → Identity Provider Single Sign-On URL
- **Google Workspace**: Admin Console → Apps → Web and mobile apps → Your App → SSO URL

Logout URL (optional)

Enter the **Logout URL** (also known as SLO URL or Single Logout Endpoint). This enables single logout — when a user logs out of Directo, they are also logged out of the IdP session.

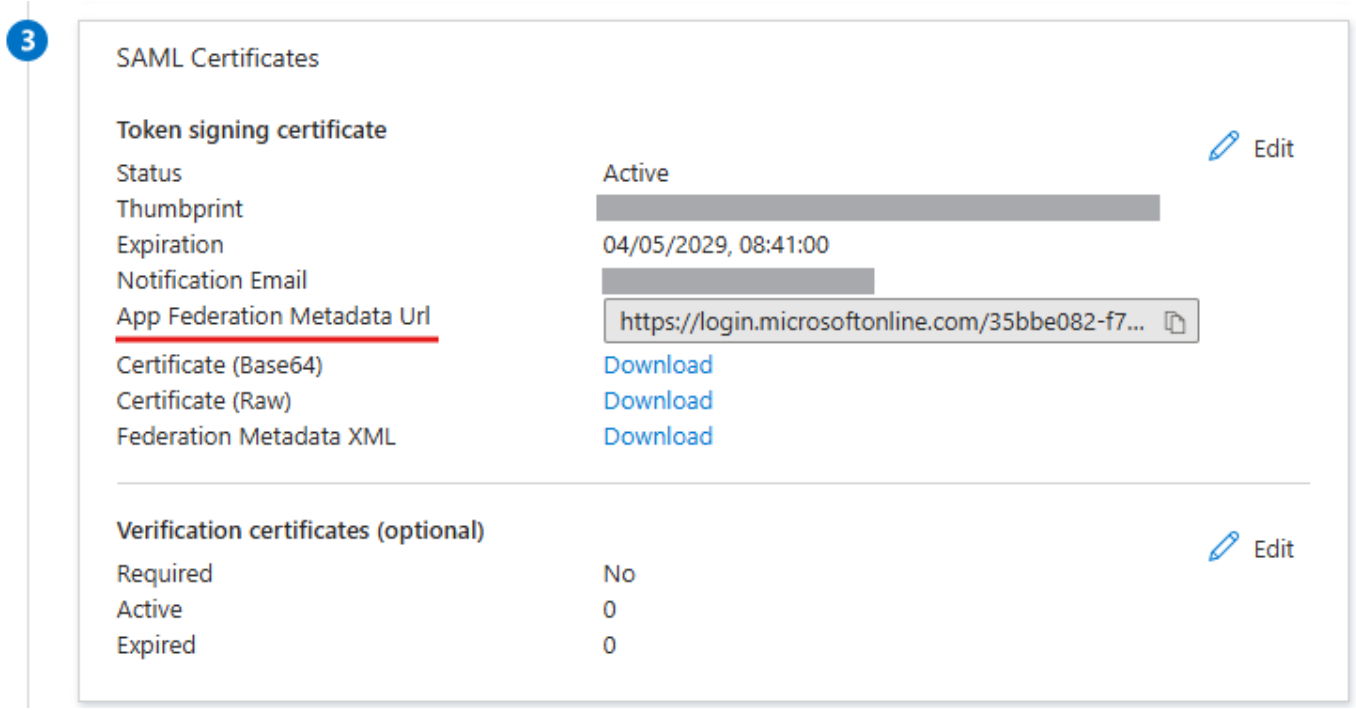
Where to find it: Look for „SLO URL“, „Logout URL“, or „Single Logout Endpoint“ in the same section as the Login URL in your IdP.

Metadata URL (required)

Enter the **Metadata URL** that points to your IdP's SAML metadata XML document. This URL contains the IdP's signing certificates, endpoints, and other configuration details.

Where to find it:

- **Microsoft Entra ID**: Azure Portal → Enterprise Applications → Your App → Single sign-on → App Federation Metadata Url
- **Okta**: Applications → Your App → Sign On tab → Metadata URL
- **Google Workspace**: Admin Console → Apps → Web and mobile apps → Your App → Download metadata (use the URL, not the file)



(Azure SSO pictured above)

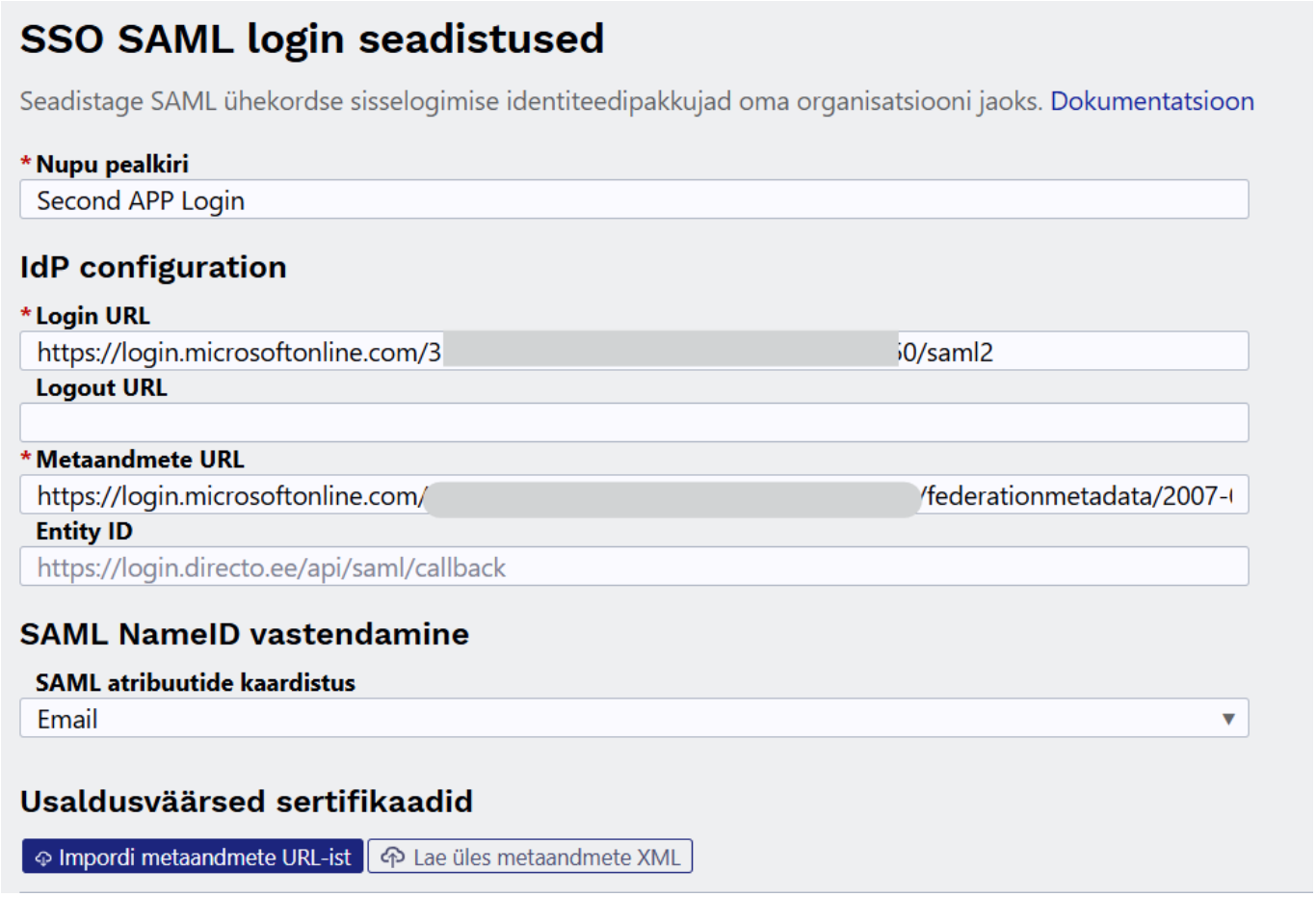
Step 6: Configure Name ID Mapping

Under **SAML Name ID Mapping**, select how the IdP identifies users:

- **Email** — The IdP sends the user's email address as the Name ID. Directo matches this to the user's email in the system.
- **Username** — The IdP sends the username as the Name ID. Directo matches this to the user's username in the system.

Choose the option that matches how your IdP is configured to send the Name ID claim.

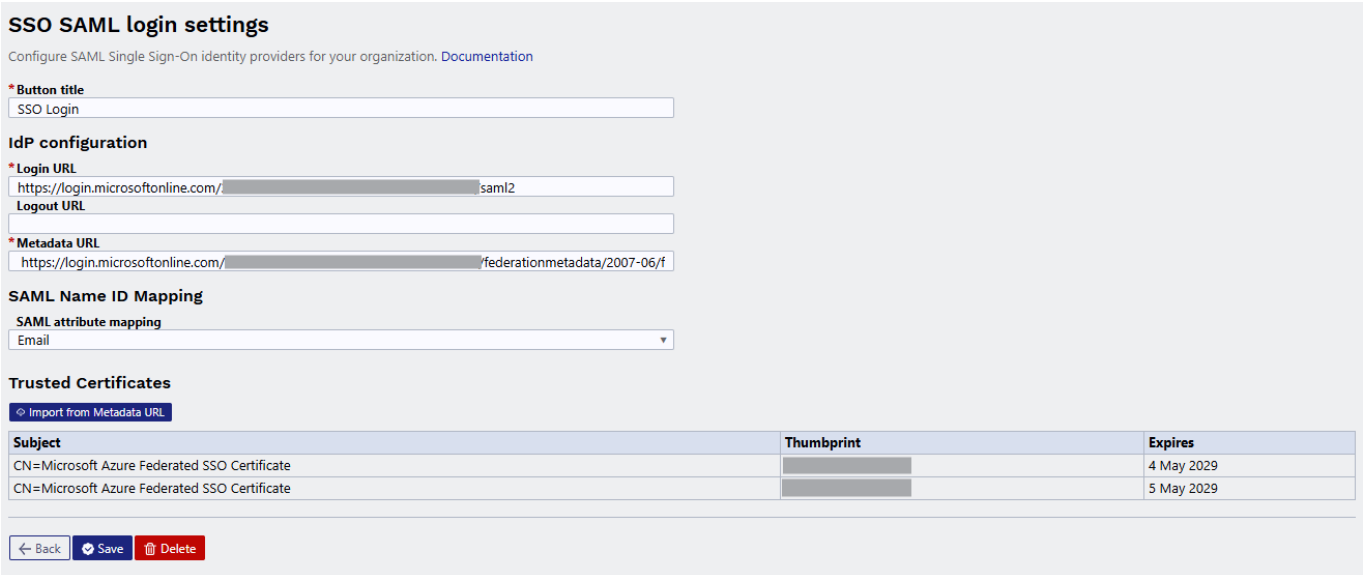
Step 7: Save the Configuration



Click **Save**. If you provided a Metadata URL, Directo will automatically import the IdP's signing certificates during the first save.

Step 8: Manage Certificates

After saving, the **Trusted Certificates** section appears below the form. This section shows the signing certificates imported from your IdP's metadata.



Importing Certificates

- Certificates are automatically imported from the Metadata URL on first save.
- To manually import or re-import certificates, click **Import from Metadata URL**.

Certificate Rollover

When your IdP rotates its signing certificate:

1. Add the new certificate in your IdP configuration.
2. Open the corresponding IdP configuration in Directo.
3. Click **Import from Metadata URL** to import the new certificate.
4. Both the old and new certificates will be trusted during the transition period.

Certificate Table

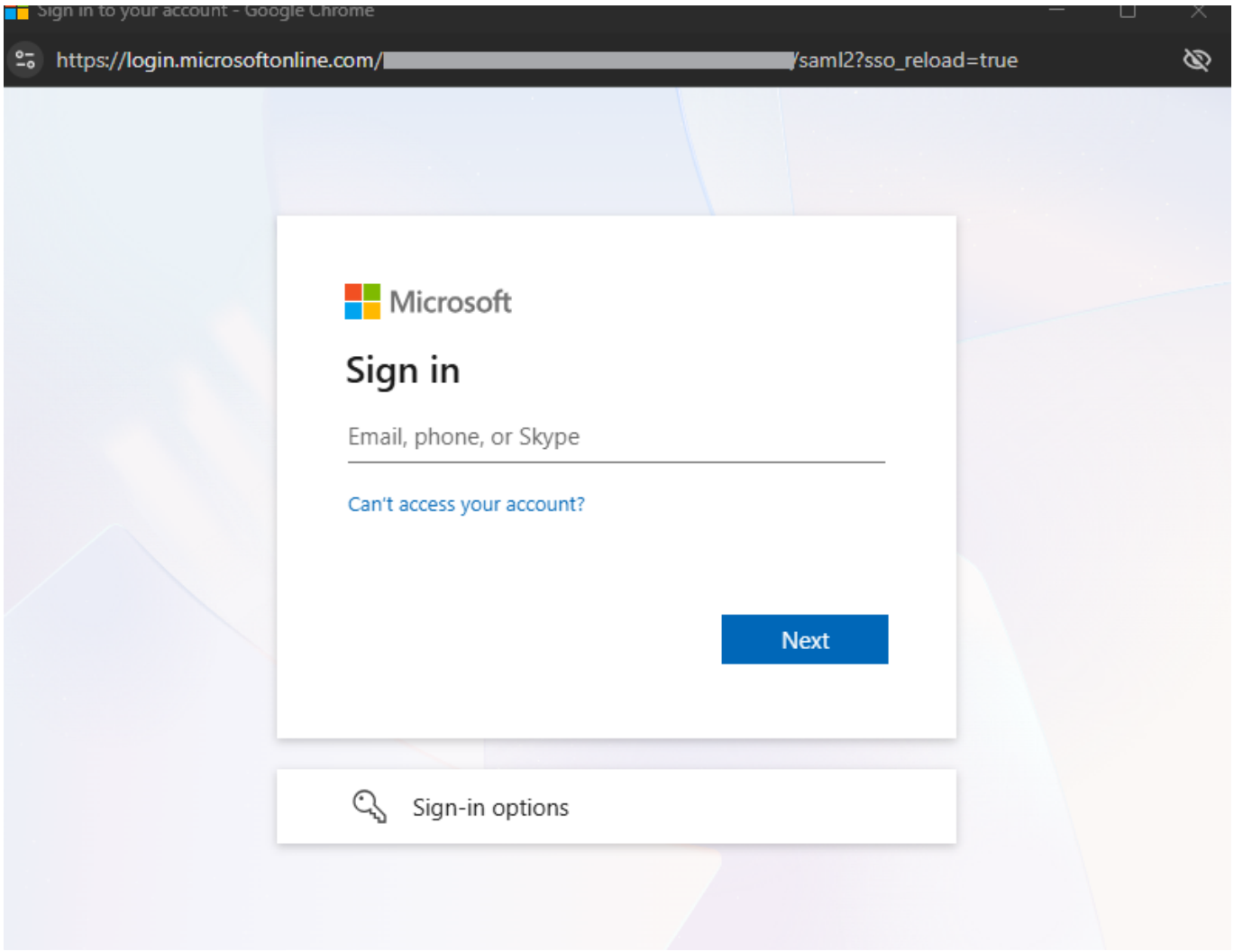
The certificate table shows:

Column	Description
Subject	The certificate's subject (typically the IdP's domain)
Thumbprint	A unique identifier for the certificate (truncated for readability)
Expires	The certificate's expiration date. A warning icon appears if the certificate has expired.

Step 9: Test the Configuration

1. Open the Directo login page in a new browser window or incognito/private window.
2. You should see a new SSO button with the title you configured.
3. Click the button and verify that you are redirected to your IdP's login page.


Directo
develop baas OÜ
Kasutaja
ID-kaart
Mobiil-ID
Smart-ID
Kasutaja
Parool
Sisene
SSO Login
Näita parooli
Unustasid parooli?
Wiki
65553334
info@directo.ee
Isikuandmete kaitse



1. After authenticating with the IdP, you should be redirected back to Directo and logged in.

Editing an Existing Configuration

1. Click on the configuration row in the list.
2. Update the fields as needed.
3. Click **Save**.

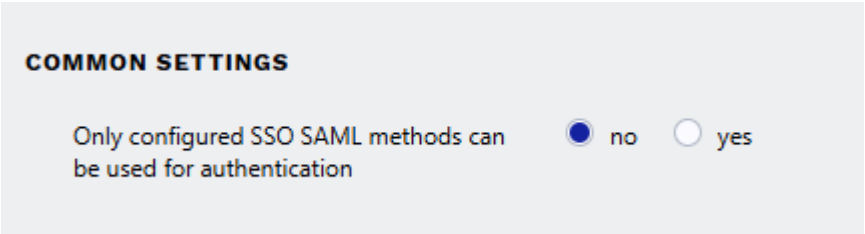
Deleting a Configuration

1. Click on the configuration row in the list.
2. Click the **Delete** button.
3. Confirm the deletion in the dialog.

Warning: Deleting an IdP configuration will immediately prevent users from logging in via that SSO method.

Warning: If you have enabled „Only configured SSO SAML methods can be used for

authentication“ and you delete all login methods you can lock yourself out of your application.



Troubleshooting

Problem	Solution
SSO button does not appear on login page	Verify the configuration is saved and the Button title is set.
„Invalid signature“ error after login	Re-import certificates from the Metadata URL. The IdP may have rotated its signing certificate.
User cannot be found after SSO login	Check the Name ID Mapping setting. Ensure the IdP sends the correct attribute (email or username) and that it matches the user's record in Directo.
Metadata URL returns an error	Verify the URL is correct and accessible. Some IdPs require the app to be activated before the metadata URL is available.