Sisukord

SAML SSO Configuration Guide 3
Prerequisites 3
Step 1: Open the SAML SSO Configuration 3
Step 2: Create a New Configuration 3
Step 3: Fill in the Button Title 3
Step 4: Configure the IdP Settings 3
Login URL (required) 3
Logout URL (optional) 4
Metadata URL (required) 4
Step 5: Configure Name ID Mapping 4
Step 6: Save the Configuration 5
Step 7: Manage Certificates 5
Importing Certificates 5
Certificate Rollover 5
Certificate Table 5
Step 8: Test the Configuration 6
Editing an Existing Configuration 6
Deleting a Configuration 6
Troubleshooting 6

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: 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.

Step 2: Create a New Configuration

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

add_new_button_img_here

Step 3: 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“).

button_title_field_img_here

Step 4: 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.

login_url_field_img_here

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

idp_login_url_img_here

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.

logout_url_field_img_here

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.

idp_logout_url_img_here

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.

metadata_url_field_img_here

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)

idp_federation_metadata_url_img_here

Step 5: 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.

name_id_mapping_field_img_here

Step 6: Save the Configuration

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

save_button_img_here

Step 7: Manage Certificates

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

certificates_section_img_here

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**.

import_certificates_button_img_here

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 8: 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.

login_page_sso_button_img_here

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.

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.