Midaxo

Enterprise Identity Provider Connections

Single Sign-On on Midaxo+

October 2022

Single Sign-On

Midaxo is committed to maintaining a high level of information security, and Enterprise Identity Provider connections is one of the security features we provide as part of the product. This paper gives an overview of Single Sign-On (SSO) connections with external identity providers on Midaxo 2.0 Platform. Midaxo+ is the second-generation software architecture that Midaxo's products released after January 2021 are based on. This includes Pipeline+ and Deal+ products.

Implementation

Midaxo+ utilizes Auth0 for authentication and authorization, and for SSO.

SSO can be currently used for authenticating users that have been added to Midaxo platform. User permissions are managed in Midaxo platform and users email address is used to map the permissions for users authenticated with SSO. When SSO is enabled, default option is to force SSO for all users in the tenant. SSO connections are tenant specific and apply on all workspaces & processes that the tenant has.

Supported protocols for SSO are SAML 2.0 and OpenID Connect (OIDC).

Note: It is currently not possible to manage permissions through SAML / OIDC groups.

SAML 2.0

When integrating with Enterprise Identity Provider using SAML 2.0 connection, you should contact your Midaxo customer success manager and provide following information of your IdP:

- Sign In URL
- X509 Signing Certificate

Note: You may also provide this information as SAML metadata.

Your Midaxo customer success manager will set up the connection and provide you:

- Post-back URL / Assertion Consumer Service URL
- Entity ID
- Log-in link to access the application
- Encryption Certificate
    - EU: https://auth.app-eu.midaxo.com/pem?cert=connection
    - US: https://auth.app-us.midaxo.com/pem?cert=connection

When configuring the connection, please note following:

- You should use email address as a name identifier (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier)
- Signing algorithm is SHA256

Note: IdP initiated SSO is discouraged, and thus users should always use Midaxo's log in link to access the application.

Technical details: https://auth0.com/docs/connections/enterprise/saml

OpenID Connect (OIDC)

When integrating with Enterprise Identity Provider using OIDC connection, you should contact your Midaxo customer success manager and provide following information:

- Issuer URL
- Client ID

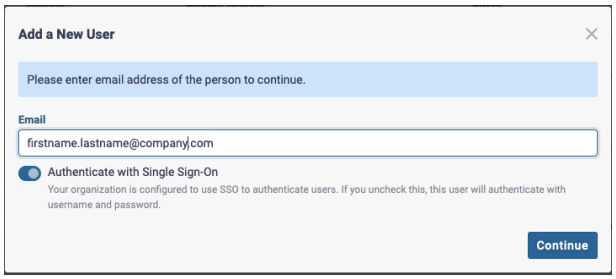
Your Midaxo customer success manager will set up the connection and provide you:

- Callback URL
    - EU: https://auth.app-eu.midaxo.com/login/callback
    - US: https://auth.app-us.midaxo.com/login/callback
- Log-in link to access the application

Technical details: https://auth0.com/docs/connections/enterprise/oidc

User management

Users and their permissions are managed in Midaxo+. To grant access through SSO, you first need to create the user with proper permissions in Midaxo+ user management. When SSO is enabled in your account, you can choose whether new user should be authenticated with SSO or with username/password:



When user is created, you need to define:

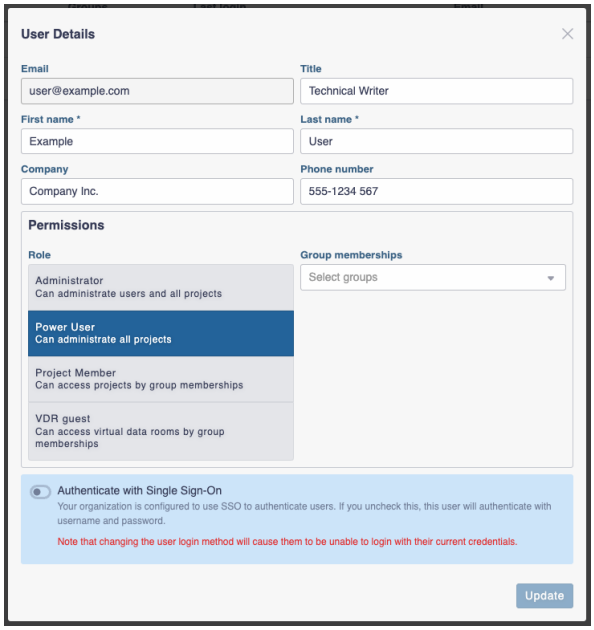
- Email address to identify SSO user
- First name and last name to identify user in user interface.
- Role to define which level of access the user should have to features.
- Groups (optional) to define the resources the user can access.

When user is first time logged in via tenant specific SSO, it is mapped to Midaxo user with same email address.

Note: Midaxo+ does not currently support auto provisioning of SSO users.

Updating existing users to login with Single Sign-On

If you have existing users in your Midaxo+ user management, you can change their login to Single Sign-On. Open the user's information dialog and toggle the setting "Authenticate with Single Sign-On" and click "Update". After this the user can login via Single Sign-On and their password-based login has been removed.



Log-in flow

SSO log-in is initiated from tenant specific log-in URL that will be provided for you (e.g., https://tenant.app-us.midaxo.com).

In this page there will be a button that redirects user to your organizations SSO Log-In page.

After successful log-in, user will land to Midaxo. If there is no corresponding user in Midaxo, an error will be displayed with a note to contact to your company's Midaxo administrator.