Digioh SSO

Last Modified on 06/10/2026 11:02 pm EDT

Digioh SSO is an Enterprise-Level Feature. Please check with your Digioh CSM or Support Team to confirm you have it so we can enable it for you.

Digioh supports Single Sign-On (SSO) using the **OpenID Connect (OIDC)** protocol. OIDC is a modern, secure authentication standard supported by major identity providers, including **Okta, Auth0, Microsoft Entra ID (Azure Active Directory), and Google.**

SSO allows your team to sign in to Digioh using your organization's existing identity provider, reducing password management and improving security.

How Digioh SSO Works (Overview)

Digioh uses the **OAuth 2.0 Authorization Code flow** with OpenID Connect.

At a high level:

1. A user selects **Sign in with SSO** on the Digioh login page
2. The user is redirected to your identity provider
3. The user authenticates successfully
4. Your identity provider redirects the user back to Digioh
5. Digioh validates the authentication response and signs the user in

No passwords are stored or managed by Digioh.

Required Redirect URI (Important)

When configuring SSO with **any identity provider**, you must configure the following redirect URI **exactly as shown**:

https://account.digioh.com/Login/LoginOIDCToken

Requirements:

- Case-sensitive
- No trailing slash
- No query parameters
- Must be configured as a **Web / Callback / Sign-in Redirect URI**

This is the **only redirect URI required** for Digioh SSO.

What You'll Need to Provide to Digioh

To enable SSO, please email the following information from your identity provider to **support@digioh.com**.

You may need to create an "app" or "application integration" in your identity provider first.

Required Information

1. **OpenID Configuration URL** This URL exposes your identity provider's OpenID Connect configuration.

Examples:

- Okta: https://your-domain.okta.com/.well-known/openid-configuration
- Auth0: https://your-tenant.auth0.com/.well-known/openid-configuration
- Microsoft Entra ID: https://login.microsoftonline.com/{tenant-id}/v2.0/.well-known/openid-configuration

If you're unsure of the exact URL, you can provide the domain you authenticate with (for example, acme.okta.com), and Digioh Support can help confirm it.

2. **Client ID** This value is generated by your identity provider when you create the Digioh SSO application.

3. **Client Secret** This is also generated by your identity provider and is used by Digioh to securely complete the authentication process. Treat this value like a password. If it expires or is rotated, Digioh will need the updated value.

Note for Microsoft Entra ID:

For Microsoft Entra ID, we recommend using Digioh Shared Azure AD App

Information Required by Digioh

Item	Required
Tenant ID	Yes
Admin Consent	Yes

Setup Steps

1. Obtain your **Tenant ID**
    - Azure Portal → Azure Active Directory → Overview

2. Grant admin consent using the URL provided by Digioh
    - Must be completed by a Global Administrator

3. Email support@digioh.com with the required infomations.

If your organization requires full control over the app registration, we also offer Private App Registration. To enable this, please reach out to support@digioh.com .

Supported Identity Providers

Digioh supports **any standards-compliant OpenID Connect provider**, including but not limited to:

- Okta
- Auth0
- Microsoft Entra ID (Azure Active Directory)
- Google Workspace

Testing Your SSO Setup

Once Digioh has completed the configuration, please take the following steps:

1. Go to the Digioh login page (https://account.digioh.com/Login/External)
2. Select **Sign in with SSO**
3. Authenticate with your identity provider
4. Confirm you are redirected back to Digioh and logged in successfully

If you encounter an error, please capture the **exact error message and timestamp** and include it when contacting support. This information will be necessary to troubleshoot why the configuration isn't working as expected.

Common Troubleshooting Tips and Tricks

- **Redirect URI errors** Ensure the redirect URI matches exactly: https://account.digioh.com/Login/LoginOIDCToken
- **Invalid client credentials** Verify the Client ID and Client Secret are correct and not expired.
- **Missing email address** Your identity provider must include a user email in the ID token (commonly email or preferred_username).

Need Help?

If you have questions or need assistance setting up SSO, contact **support@digioh.com** with:

- Your identity provider name
- The requested configuration values
- Any error messages you encounter

Our support team will be happy to help you get up and running.