SHOWMGR
PRODUCTION SIMPLIFIED

Connect your organization's single sign-on (SSO) to ShowMgr

Summary

This guide is for client IT administrators connecting an existing identity provider to ShowMgr using **SAML 2.0** or **OpenID Connect (OIDC)**.

Agree on one protocol with ShowMgr and obtain the approved connection values for your environment. Complete **section 2A for SAML** or **section 2B for OIDC**, then follow the pilot-testing steps.

1. Confirm the scope and request your connection values

Send your ShowMgr project contact:

- Your company name, identity provider, tenant or organization ID, and IT contact.
- The requested environment and preferred sign-in button label.
- Pilot-user email addresses, identifying existing ShowMgr accounts and guest users.

Before configuration, agree on the environment and protocol, and obtain the exact ShowMgr sign-in / start URL and connection values for that protocol.

Do not enter placeholders or vendor sample values into your identity provider. Use the approved values from ShowMgr with the provider-specific steps later in this article.

2A. SAML: metadata-based setup

Complete this section only when SAML is the agreed protocol.

Configure your SAML application

Setting	Configure as
Identifier / Entity ID / Audience	The exact SAML Entity ID provided by ShowMgr.
Reply / ACS URL	The exact SAML ACS / Reply URL provided by ShowMgr. Use HTTP POST.
NameID	The stable identifier agreed with ShowMgr, including its format and case. Do not change existing user identifiers.
Email claim	The proposed claim name is **email**, with no namespace and a value for every user. Confirm the exact mapping with ShowMgr.
Display-name claim	The **name** claim is optional.

Signing: confirm the profile with ShowMgr. The proposed profile is to sign both the response and assertion using SHA-256. Agree on encryption and signed-request requirements before setup.

Send to ShowMgr

- The application's metadata URL or XML file. Include the issuer and SSO URL if they are not in the metadata.
- The public signing certificate, its expiry date, and the renewal contact.
- The exact NameID and claim definitions.

2B. OIDC: web-application setup

Complete this section only when OIDC is the agreed protocol.

Configure your OIDC application

Setting	Configure as
Application type	Confidential web application (server-side), not a single-page app (SPA).
Sign-in flow	Authorization Code, not implicit flow.
Web / sign-in redirect URI	The exact OIDC redirect URI provided by ShowMgr.
Scopes	**openid profile email**
Required claims	A stable **sub** identifier and a populated **email** claim.
Token-endpoint authentication	**client_secret_post**. The application credentials are sent in the token request body.

Send to ShowMgr

- The issuer URL and discovery URL.
- The client ID.
- The client secret **value**, not the secret ID, together with its expiry date and renewal contact.

Share the client secret only through the agreed secure channel. If your policy prohibits sharing client secrets, agree on a SAML connection with ShowMgr instead.

3. Assign pilot users, test, and approve

1. Assign only the approved pilot users or groups and keep multifactor authentication (MFA) policies in place.
2. Send the requested configuration details to your ShowMgr project contact and wait for readiness confirmation. Keep existing login methods in place.
3. After ShowMgr confirms readiness, start at the approved ShowMgr sign-in URL. Verify the user's account permissions, rejection of unapproved users, and logout behavior.
4. Obtain approval from both teams before rollout.

If sign-in leads to registration or pending approval, contact ShowMgr to review account linking. **Do not create a duplicate account.**

> **Access and security**
>
> **SSO sign-in alone does not grant ShowMgr access or permissions.**
>
> Never send passwords, private keys, or sign-in tokens. Notify ShowMgr before changing user identifiers, certificates, or secrets.

Identity-provider quick steps

Use the steps for your provider and agreed protocol with the connection values supplied by ShowMgr. Vendor sample values must not replace your approved values.

Microsoft Entra ID | SAML or OIDC

SAML

1. Go to **Enterprise applications > New application > Create your own application** and select the non-gallery option.
2. Open **Single sign-on > SAML**. Enter the Entity ID and ACS / Reply URL from section 2A.
3. Confirm the proposed new claim mappings below with ShowMgr before applying them.

- **NameID:** user.objectid, using the Persistent format.
- **Email:** map user.mail to the claim named email, with no namespace. The source field must be populated.
- **Optional display name:** map user.displayname to the claim named name.

OIDC

1. Go to **App registrations > New registration**. Choose **single tenant** and the **Web** platform.
2. Enter the redirect URI from section 2B. Configure the **openid**, **profile**, and **email** permissions, then create an approved client secret.
3. Send ShowMgr the tenant-specific issuer and discovery URLs and the remaining details listed in section 2B. Share the secret only through the agreed secure channel.

Check email values: an email scope or optional claim does not guarantee a value. Verify that email is populated for each pilot user.

For either protocol

On the enterprise application, set **Assignment required?** to **Yes** and assign approved pilot users or groups. For OIDC, obtain administrator consent where required.

Microsoft Entra SAML setup

Microsoft Entra OIDC setup

Okta | SAML or OIDC

Go to **Applications > Create App Integration** and select the agreed protocol.

SAML

1. Choose **SAML 2.0**.
2. Set **Single sign-on URL** to the ACS URL from section 2A and **Audience URI** to the Entity ID from section 2A.
3. Configure NameID and Attribute Statements. Send ShowMgr the metadata from the **Sign On** section.

OIDC

1. Choose **OIDC - Web Application** and use **Authorization Code** flow.
2. Enter the redirect URI from section 2B. Use **client_secret_post** for token-endpoint authentication, not Basic.
3. Send ShowMgr the intended authorization-server issuer and the remaining details listed in section 2B.

For either protocol: assign only approved users or groups.

Okta SAML setup

Okta OIDC setup

Google Workspace | SAML

1. Go to **Admin console > Apps > Web and mobile apps > Add app > Add custom SAML app**.
2. Enter the ACS URL and Entity ID from section 2A. Select **Signed response** for the proposed signing profile, subject to confirmation with ShowMgr.
3. Map **Primary email** to the app attribute named **email**.
4. Use the agreed stable NameID rather than accepting the primary-email default without review. Add a custom directory attribute if needed.
5. Limit **User access** to pilot groups or organizational units. Send ShowMgr the downloaded IdP metadata.

Start URL and RelayState: leave optional Start URL or default RelayState settings blank unless supplied by ShowMgr. Preserve RelayState received in sign-in requests.

Start the pilot at the approved ShowMgr sign-in URL, not the Google test button.

This is managed Google Workspace SAML, not personal Google social login.

Google Workspace SAML setup

Other providers: confirm SAML/OIDC compatibility with ShowMgr before configuration.