SHIELDSPHERE

Single Sign-On

your identity provider decides who gets in

How enterprise single sign-on works in ShieldSphere, what your IT team sets up in Microsoft Entra ID or Okta, what ShieldSphere needs from you, what a new user experiences on first sign-in, and what to check when something does not match. For IT and account administrators.

ADMIN GUIDE – FOR ADMINISTRATORS | VERSION 1.0 | SCREENS CAPTURED NOVEMBER 2026

WHAT'S IN THIS GUIDE

1 What SSO does and who sets it up

2 What you give ShieldSphere

3 Set up your identity provider

4 Roles and default access

5 Go live and the first sign-in

6 The SSO status page

7 Day-to-day administration

8 Troubleshooting

ShieldSphere single sign-on lets your team sign in through your own identity provider using SAML 2.0, with Microsoft Entra ID and Okta covered here. It is an Enterprise feature that ShieldSphere sets up with your IT team. Accounts are created automatically on first sign-in, with a role taken from the user's identity provider groups.

1 What SSO does and who sets it up

With SSO on, your people sign in with the credentials they already use at work, and your identity provider, not ShieldSphere, decides who gets in.

When a user from your email domain types their address on the ShieldSphere sign-in page, the password box is replaced by a **Continue with SSO** button. They authenticate at your identity provider and return to ShieldSphere signed in. Multi-factor authentication stays where you already enforce it, at the identity provider.

Your IT team

Creates the application in Entra ID or Okta, assigns users, and sends ShieldSphere the connection details.

ShieldSphere

Enters your configuration, connects the provider, tests it and switches it on during a managed setup. You do not configure anything inside ShieldSphere yourself.

Your account owner

Can see a read-only SSO status page in Settings, covered in section 6.

AVAILABILITY

SSO is an Enterprise feature. To get it, ask your ShieldSphere contact to switch it on for your organization before setup begins. Until then the Settings page tells you SSO is not available.

PASSWORD SIGN-IN STAYS AVAILABLE

ShieldSphere does not turn off password sign-in when SSO goes live. This is deliberate: your account owner keeps a password as the way back in if your identity provider is ever unreachable, and the owner role cannot be granted through SSO at all.

2 What you give ShieldSphere

Before the setup call, send ShieldSphere the following. You will make these decisions with your safety and IT leads together.

ITEM	DETAIL
Metadata URL	Your identity provider's federation metadata URL. If your provider cannot publish a URL, tell us and send the metadata XML instead.
Email domains	Each domain whose users should sign in with SSO, such as *yourcompany.com*, one per line.
Group-to-role map	Each identity provider group and the ShieldSphere role it should receive: admin, member or viewer (section 4).
Default role	The role for anyone who signs in but is in no mapped group. Member is the usual choice.
Default sites	Which site or sites a new user can see on arrival. Leave this blank and new users can sign in but see nothing until an administrator grants access.
Existing accounts	Tell us if anyone on those domains already has a ShieldSphere password account (section 8).

GROUP NAMES MUST MATCH EXACTLY

ShieldSphere matches group names character for character, including capitalization and any prefix, against what your provider sends. *Acme-Safety-Admins* and *acme safety admins* are different groups. If a user lands on the default role when you expected a higher one, this is the first thing to check.

3 Set up your identity provider

Your ShieldSphere contact sends you the exact values to paste into your provider. Use them as sent.

VALUE	WHAT TO ENTER
ACS URL (Reply URL, Recipient, Destination)	Sent by your ShieldSphere contact
SP Entity ID (Audience URI, Identifier)	Sent by your ShieldSphere contact
NameID format	EmailAddress
Where users start	https://shieldspheresafety.com/client-login

ShieldSphere expects three claims in the sign-in assertion: **email** (also the NameID), **name**, and **groups**. Name them exactly that and no extra mapping is needed. If your provider uses longer schema-style claim names, tell us during intake.

Microsoft Entra ID

1

Create the application

In Entra ID go to **Enterprise applications**, choose **New application**, then **Create your own application**. Name it ShieldSphere and pick the non-gallery option.

2 Configure SAML

Under **Single sign-on** choose **SAML**. In **Basic SAML Configuration** set the Identifier to the SP Entity ID and the Reply URL to the ACS URL above. Leave Sign on URL, Relay State and Logout URL blank.

3 Set the claims

In **Attributes & Claims**, set the Name ID to the user's email in email address format, confirm claims named *email* and *name* return the email and display name, and add a group claim named *groups* that emits readable group names.

4 Assign users and copy the metadata URL

Under **Users and groups**, assign the users or groups who should have access; only assigned users can sign in. Then copy the **App Federation Metadata Url** from the SAML Certificates section and send it to ShieldSphere.

Okta

1 Create a SAML 2.0 app integration

Under **Applications**, choose **Create App Integration**, select **SAML 2.0**, and name it ShieldSphere.

2 Enter the SAML settings

Set the single sign-on URL to the ACS URL and the Audience URI to the SP Entity ID. Set Name ID format to EmailAddress and Application username to Email.

3 Add the statements

Add attribute statements *email* (user.email) and *name* (user.displayName), and a group attribute statement named *groups* with a filter that returns the group names you mapped.

4 Assign users and copy the metadata URL

Assign the users or groups on the **Assignments** tab. On the **Sign On** tab copy the Identity Provider metadata URL and send it to ShieldSphere.

> **OTHER PROVIDERS**
>
> This guide documents Entra ID and Okta. If you use a different SAML 2.0 provider, tell your ShieldSphere contact before you start so setup can be confirmed for it.

4 Roles and default access

Access is decided at the user's first sign-in, from the groups your provider sends.

ROLE	WHAT IT CAN DO
Admin	Full access to the organization's safety data and settings, and can manage other users' site access.
Member	Day-to-day work at assigned sites and their safety records.
Viewer	Read-only access to assigned sites.

1. ShieldSphere reads the user's groups and matches them against your group-to-role map.
2. If the user is in several mapped groups, the highest role wins: admin over member over viewer.
3. If the user is in no mapped group, they get your default role.

The **owner** role is never granted through SSO. Each organization keeps one human owner, set up with ShieldSphere directly, so your identity provider cannot create one. If your plan's number of admin seats is already full when someone mapped to admin first signs in, that user is given the default role instead. Ask your ShieldSphere contact if you need more admin seats.

New users also receive the default sites you chose, and nothing else. They can be given more sites afterward from the Team page; see the Team guide.

CHANGES IN YOUR DIRECTORY DO NOT FOLLOW PEOPLE AUTOMATICALLY

Role and site access are set when a user first signs in. If you move someone to a different group later, their ShieldSphere role does not change on its own. Tell your ShieldSphere contact and the change is applied for you.

5 Go live and the first sign-in

Setup follows a fixed order so that nobody is locked out.

1. You return the details in section 2 and build the application in your provider, assigning one pilot user.
2. ShieldSphere enters your configuration, connects the provider and tests it. SSO is not switched on until the test passes.
3. If anyone on your domain already has a password account, that is dealt with first (section 8).
4. ShieldSphere switches SSO on and your pilot user signs in.
5. Once the pilot works, you assign everyone else in your provider.

What a new user sees

1 **Type the work email**

On the sign-in page, the user enters their email. The password box is replaced by a note, *Your organization uses single sign-on. Continue with your identity provider.*, and a **Continue with SSO** button.

2 **Authenticate at your provider**

They are redirected to your provider, sign in the way they normally do, and return to ShieldSphere.

3 Land on the dashboard

On the first visit their account is created with the role from their groups and the default sites. After that, signing in is the same button each time. The mobile app offers the same **Continue with single sign-on** route; see the Mobile App guide.

A user can also be authenticated by your provider without having a workspace, for example if setup is incomplete. They see *Your single sign-on worked, but your ShieldSphere workspace isn't set up yet* and are signed out. They should contact their administrator.

6 The SSO status page

Your organization's account owner can check on SSO at any time. The page is read-only.

```
Settings → Single Sign-On
```

SHOWN	MEANING
Connection status	**Active** means SSO is live. **Inactive** means it has been switched off. **In setup** and **In setup (testing)** mean setup is not finished.
Identity provider	**Connected** or **Not connected**.
Last successful login	When someone last signed in through SSO.
Last connection test	When the connection was last tested, with a tick or cross for the result.
Default role	The role given to users in no mapped group.
Configured domains	The email domains that route to SSO.
Role mapping	Each group and the role it grants.

The page does not let you edit anything. To change a setting, email ShieldSphere support. If SSO has not been switched on for your organization the tab does not appear, and if it is on but setup

has not started you see *SSO setup not started*.

7 Day-to-day administration

TASK	HOW
Add a user	Assign them to the ShieldSphere application in your provider. Their account is created when they first sign in.
Remove a user	Unassign them in your provider. ShieldSphere does not support automated user removal, so if access must end at once, also tell your ShieldSphere contact.
Change a role	Move them between groups in your provider, then ask your ShieldSphere contact to apply it (section 4).
Change groups, domains or roles mapped	Email ShieldSphere support. Configuration changes are made by ShieldSphere.
Turn SSO off	Ask ShieldSphere. It takes effect for everyone, including people who have signed in before, and your configuration is kept so it can be switched back on.
Sessions	SSO sessions follow ShieldSphere's normal session length. When one ends the user signs in again, usually a quick redirect. Signing out of ShieldSphere does not sign them out of your provider.

8 Troubleshooting

WHAT YOU SEE	LIKELY CAUSE AND FIX
No Continue with SSO button after typing the email	The domain is not configured, or SSO is not yet active. Check the status page, or ask ShieldSphere. The page answers the same for every address on a domain, so it cannot tell you whether one person exists.
Single sign-on is temporarily unavailable for your organization	SSO has been switched off, or its status is not Active. Contact ShieldSphere. Your account owner can still use a password.
User signed in but has the wrong role	Compare the group names your provider sends with the map. They must match exactly. A provider that does not send the groups claim places everyone on the default role.
User can sign in but sees no sites	No default sites were set. An administrator grants access from the Team page.
Your single sign-on worked, but your workspace isn't set up yet	The user was authenticated, but ShieldSphere could not place them in your organization. Confirm setup is complete and ask ShieldSphere to check.
User signed in as someone else	The provider asserts whoever is signed in at the provider, not necessarily the email typed. Have the user sign out of the identity provider and try again.
Sign-in fails for someone who used ShieldSphere before	A single email cannot be both a password account and an SSO account. ShieldSphere handles this as a separate

	managed migration before go-live, because it affects historical records such as policy acknowledgments. Do not delete or recreate accounts yourself.
The user is not allowed to use the application in the provider	They are not assigned to the ShieldSphere application. Assign them in your provider.