CONVERGENT

Sanctum Hub

Single Sign-On Setup Guide

For IT Administrators

June 2026 | Version 1.0

Overview

Sanctum supports Single Sign-On (SSO) for vendor and client organizations. Once configured, your users can authenticate to Sanctum using your existing identity provider — no separate Sanctum password required.

SSO in Sanctum supports:

- New user provisioning — Sanctum can automatically create accounts for SSO users on first login (if enabled)
- Role assignment — Users can be assigned roles automatically based on their email address patterns
- Force SSO — Prevent users from logging in with a password, requiring SSO exclusively
- Multiple configurations — Configure more than one SSO provider for your organization

Supported Protocols

Protocol	Best For
SAML 2.0	Enterprise identity providers (Okta, Ping, ADFS, OneLogin, Entra ID via SAML)
Microsoft / Azure AD	Microsoft 365 / Entra ID environments using OAuth2
Google Workspace	Google-managed organizations
OpenID Connect (OIDC)	Modern identity providers with OIDC support (Okta, Auth0, Ping, Keycloak)
Generic OAuth 2.0	Custom or internal OAuth2-capable identity providers
GitHub	Development-focused organizations using GitHub for identity

Prerequisites

Before beginning, ensure you have:

- Admin access to your identity provider (Okta, Azure, Google Workspace, etc.)
- Admin access to your Sanctum organization (Owner or Admin role)
- A list of your users' email addresses that will use SSO
- Agreement from Convergent to enable SSO for your account (required before configuration is visible)
- HTTPS available at your identity provider's endpoints (required in production)

Protocol Setup Instructions

SAML 2.0

SAML 2.0 is the recommended protocol for most enterprise environments (Okta, ADFS, OneLogin, Ping, and Entra ID via SAML).

What You Provide to Convergent

Item	Description
IdP Entity ID	The unique identifier for your identity provider
IdP SSO URL	The URL Sanctum will redirect users to for authentication
IdP SLO URL	(Optional) The URL for single logout
IdP X.509 Certificate	The public certificate your IdP uses to sign SAML assertions
NameID Format	Usually urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

What Convergent Provides to You

Item	Value
SP Entity ID	https://[your-subdomain].sanctumhub.io/saml/[idp-name]/metadata
ACS URL	https://[your-subdomain].sanctumhub.io/saml/[idp-name]/acs
SLO URL	https://[your-subdomain].sanctumhub.io/saml/[idp-name]/sls
Metadata XML URL	https://[your-subdomain].sanctumhub.io/saml/[idp-name]/metadata

Setup Steps

In your Identity Provider:

1. Create a new SAML application in your IdP
2. Set the ACS URL (also called 'Reply URL', 'Assertion Consumer Service', or 'Single Sign-On URL') to the value provided by Convergent
3. Set the Entity ID (also called 'Audience', 'SP Entity ID', or 'Identifier') to the SP Entity ID provided by Convergent
4. Set the NameID format to emailAddress
5. Configure the IdP to send the user's email address as the NameID
6. (Optional) Configure attribute statements to send first_name, last_name, or displayName
7. Download your IdP's metadata XML or copy the certificate, SSO URL, and Entity ID

In Sanctum:

1. Navigate to your Organization → Settings → SSO
2. Click Add SSO Configuration
3. Select SAML 2.0 as the protocol
4. Enter a display name (e.g. 'Okta SAML')
5. Paste the values from your IdP: IdP Entity ID, IdP SSO URL, IdP X.509 Certificate
6. (Optional) Paste the IdP SLO URL
7. Click Save

Okta: Create a SAML 2.0 app (not OIDC). The 'Single Sign-On URL' field is your ACS URL. The 'Audience URI' is your SP Entity ID. Download the certificate from View SAML setup instructions → Identity Provider Certificate.

Microsoft ADFS: Create a Relying Party Trust using the SP metadata URL. ADFS will auto-populate most settings from the metadata document.

Microsoft / Azure AD (OAuth2)

Use this if your organization uses Microsoft 365 or Entra ID and prefers the OAuth2 flow over SAML.

What You Provide to Convergent

Item	Description
Tenant ID	Your Azure AD tenant ID (found in Azure Portal → Entra ID → Overview)
Client ID	The Application (client) ID of the app you register
Client Secret	A secret you generate in the app registration

What Convergent Provides to You

Item	Value
Redirect URI	https://[your-subdomain].sanctumhub.io/auth/azure/callback

Setup Steps

In Azure Portal:

1. Go to Entra ID → App registrations → New registration
2. Name the application (e.g. 'Sanctum')
3. Set Supported account types to 'Accounts in this organizational directory only'
4. Set the Redirect URI to the value provided by Convergent (type: Web)
5. Click Register. Copy the Application (client) ID and Directory (tenant) ID
6. Go to Certificates & secrets → New client secret. Set an expiry and click Add. Copy the secret value immediately
7. Go to API permissions → Add permission → Microsoft Graph → Delegated permissions
8. Add: openid, profile, email, User.Read
9. Click Grant admin consent

In Sanctum:

1. Navigate to Organization → Settings → SSO → Add SSO Configuration
2. Select Microsoft Azure
3. Enter your Client ID, Client Secret, and Tenant ID
4. Click Save

Google Workspace (OAuth2)

What You Provide to Convergent

Item	Description
Client ID	OAuth2 client ID from Google Cloud Console
Client Secret	OAuth2 client secret
Allowed domains	(Optional) Restrict to your Google Workspace domain

What Convergent Provides to You

Item	Value
Authorized Redirect URI	https://[your-subdomain].sanctumhub.io/auth/google/callback

Setup Steps

1. Go to Google Cloud Console → APIs & Services → Credentials → Create Credentials → OAuth 2.0 Client ID
2. Select Web application
3. Add the redirect URI provided by Convergent under Authorized redirect URIs
4. Click Create. Copy the Client ID and Client Secret
5. Ensure the Google People API is enabled (APIs & Services → Library)
6. In Sanctum, add an SSO configuration, select Google, and enter both values

OpenID Connect (OIDC)

Use OIDC for modern identity providers such as Okta, Auth0, Ping Identity, or Keycloak.

What You Provide to Convergent

Item	Description
Issuer URL	The base URL of your OIDC provider (e.g. https://your-org.okta.com/oauth2/default)
Client ID	The client/application ID
Client Secret	The client secret
Scopes	(Optional, defaults to openid profile email)

What Convergent Provides to You

Item	Value
Redirect URI	https://[your-subdomain].sanctumhub.io/auth/oidc/callback

Sanctum fetches your provider's OIDC discovery document automatically from {issuer_url}/.well-known/openid-configuration. Your issuer URL must be publicly accessible over HTTPS.

Setup Steps — Okta

1. Create a new OIDC Web Application in Okta
2. Add the redirect URI to the Sign-in redirect URIs
3. Enable Authorization Code grant type
4. Copy the Client ID and Client Secret
5. Note your Okta domain — issuer URL is typically https://your-org.okta.com/oauth2/default
6. In Sanctum, add an SSO configuration, select OpenID Connect, and enter all values

Auth0: The issuer URL is your Auth0 domain: https://your-tenant.auth0.com/. Add the callback URL to Allowed Callback URLs in your Auth0 application settings.

Keycloak: The issuer URL follows the pattern: https://your-keycloak-host/realms/your-realm. Enable Standard flow in the client settings.

Generic OAuth 2.0

For internal or custom identity providers that support the OAuth 2.0 Authorization Code flow.

What You Provide to Convergent

Item	Description
Client ID	Your OAuth2 client/application ID
Client Secret	Your OAuth2 client secret
Authorization URL	The endpoint users are redirected to for login
Token URL	The endpoint Sanctum calls to exchange the code for a token
User Info URL	The endpoint Sanctum calls to fetch user profile data
Scopes	Space-separated list of scopes (e.g. openid profile email)

What Convergent Provides to You

Item	Value
Redirect URI	https://[your-subdomain].sanctumhub.io/auth/oauth2/callback

GitHub (OAuth2)

What You Provide	Description
Client ID	GitHub OAuth App client ID
Client Secret	GitHub OAuth App client secret

What Convergent Provides	Value
Callback URL	https://[your-subdomain].sanctumhub.io/auth/github/callback

1. Go to GitHub → Settings → Developer settings → OAuth Apps → New OAuth App
2. Set the Authorization callback URL to the value provided by Convergent
3. Click Register application and generate a client secret
4. In Sanctum, add an SSO configuration, select GitHub, and enter both values

Attribute Mapping

Sanctum maps your identity provider's user attributes to Sanctum user fields. Default mappings:

Sanctum Field	SAML Default	OAuth / OIDC Default
Email	NameID or email attribute	email claim
First Name	first_name or givenName	given_name or first_name
Last Name	last_name or sn	family_name or last_name
Display Name	displayName or cn	name
Unique ID	NameID	sub

If your provider uses different attribute names, Convergent can configure a custom attribute mapping. Provide the exact attribute names your IdP sends.

Assessor Role Assignment

Users whose email matches any of these patterns can automatically receive the Assessor role:

- Exact match: admin@yourcompany.com
- Wildcard: *@yourcompany.com (all users from your domain)
- Partial wildcard: assessor.*@yourcompany.com

Testing Your Configuration

1. Navigate to Organization → Settings → SSO
2. Find your SSO configuration and click Test
3. You will be redirected through the full SSO flow
4. On completion, Sanctum displays a test result page showing: whether authentication succeeded, user attributes received, any warnings, and mapped Sanctum user fields

The test flow does not log you in or create a user account. It is a read-only diagnostic.

Common test warnings:

• Auto-create users is disabled — Users who don't already have a Sanctum account will not be able to log in via SSO until this is enabled or accounts are pre-created

• Force SSO is not enabled — Users can still log in with a password. Enable Force SSO once you've confirmed SSO works for all users

Enabling Force SSO

Force SSO prevents users from authenticating with a password. Enable this only after:

1. All users in your organization have tested SSO successfully
2. You have confirmed the SSO configuration works end-to-end
3. You have a break-glass admin procedure with Convergent in case the IdP is unavailable

To enable: Organization → Settings → SSO → Edit configuration → toggle Force SSO → Save

Troubleshooting

"Invalid SSO configuration for this organization"

The SSO configuration saved in Sanctum is incomplete or missing required fields. Re-check the configuration in Organization → Settings → SSO and ensure all required fields are filled in.

"Authentication failed" / "Could not retrieve user information"

- OAuth/OIDC: Verify the client ID and client secret are correct. Check that the redirect URI registered in your IdP exactly matches what Sanctum is using (including trailing slashes)
- SAML: Verify the IdP certificate is the currently active signing certificate. Expired certificates are a common cause of this error
- OIDC: Confirm the issuer URL is accessible from Sanctum's servers (not behind a firewall or on an internal network)

"Redirect loop detected"

Sanctum detected more than 3 consecutive SSO redirects without a successful login. Causes:

- The redirect URI in your IdP does not match Sanctum's callback URL
- The authorization URL or token URL is incorrect
- Your IdP is redirecting back to Sanctum's login page instead of completing authentication

Clear your browser cookies and try again. If it persists, check the redirect URI configuration in your IdP.

"User not found and auto-create is disabled"

The authenticated user does not have a pre-existing Sanctum account and automatic user provisioning is disabled. Either pre-create the user's account in Sanctum (Organization → Members → Invite) or enable Auto-create users in the SSO configuration.

"SAML assertion signature validation failed"

The IdP certificate stored in Sanctum does not match the certificate used by your IdP to sign the SAML assertion. Update the certificate in Sanctum's SSO configuration. If your IdP has rolled certificates, update immediately.

"OIDC discovery document could not be fetched"

The issuer URL is unreachable from Sanctum's servers. Verify:

- The URL uses HTTPS
- The URL is publicly accessible
- {issuer_url}/.well-known/openid-configuration returns valid JSON when accessed from outside your network

"Private network address detected"

Sanctum's production environment will not connect to internal/private IP addresses. Your IdP endpoints must be publicly reachable.

Users logged in but missing their name or have an empty profile

The attribute mapping is not returning user profile data. Check that your IdP is configured to send given_name, family_name, and email (or equivalent attributes). Contact Convergent to configure a custom attribute mapping.

Configuration Reference

Field	Type	Description
provider	enum	saml2, google, azure, github, oidc, oauth2
name	string	Display name shown on the login button
enabled	boolean	Whether this SSO config is active
force_sso	boolean	Prevents password login for org members
auto_create_users	boolean	Creates Sanctum accounts on first SSO login
client_id	string	OAuth2/OIDC client ID
client_secret	encrypted	OAuth2/OIDC client secret
issuer_url	string	OIDC issuer (discovery base URL)
authorization_url	string	OAuth2 authorization endpoint
token_url	string	OAuth2 token endpoint
user_info_url	string	OAuth2 userinfo endpoint
entity_id	string	SAML IdP Entity ID
sso_url	string	SAML IdP SSO URL
slo_url	string	SAML IdP Single Logout URL
x509_cert	text	SAML IdP signing certificate
attribute_mapping	JSON	Custom field mappings from IdP attributes
assessor_emails	JSON array	Email patterns that trigger Assessor role
provider_name	string	Internal name for SAML IdP (used in URLs)

For setup assistance, contact Convergent at support@convergentds.com