SAML Single Sign-On

Sales Staff Documentation

Guide for Magento administrators, technical project owners, and implementation teams.

LAST UPDATED
2026-10-13

SOURCE
Open this article online

EXTENSION
Magento 2 Extension Sales Staff

SAML Single Sign-On

The SAML add-on lets Staff users sign in through a SAML 2.0 identity provider. It supports service-provider initiated login, automatic creation of a Staff record on first successful login, claim mapping and single logout.

Staff SAML and Staff TFA are alternative login packages. They cannot be installed together because `mageb2b/staff-tfa` declares a Composer conflict with `mageb2b/staff-saml`. Use SAML when an identity provider controls Staff sign-in. Use Staff TFA when representatives keep their Staff password and add an authenticator code.

Terms used in this article

- **SAML** — a standard that lets one central system (the identity provider) confirm a user's identity to another system (here: the shop).
- **IdP (identity provider)** — the external system that authenticates the user, for example Microsoft Entra ID or Okta.
- **SP (service provider)** — the shop side that trusts the IdP's answer; in this setup, Magento.
- **ACS URL (assertion consumer service)** — the shop URL the IdP sends the signed login answer to.
- **Claim** — a named attribute in the IdP's answer, such as the user's email or group.
- **X.509 certificate** — the public key the shop uses to verify that an answer really comes from your IdP.
- **NameID** — the persistent identifier the IdP assigns to a user, stored on the Staff record.
- **SP-initiated login** — the user starts at the shop's login page and is redirected to the IdP (the alternative, IdP-initiated, starts inside the provider's portal).

Install

```
composer require mageb2b/staff-saml:*
php bin/magento module:enable MageB2B_StaffSaml
php bin/magento setup:upgrade
php bin/magento setup:di:compile
php bin/magento cache:flush
```

Configure it under **Stores > Configuration > MageB2B > Staff > SAML settings**. Keep password login available until the full SAML flow has been tested with an ordinary representative and an emergency recovery account.

Exchange these values with the identity provider

The default endpoints are:

- Assertion Consumer Service: `https://<store-domain>/staff_saml/index/callback`
- SAML login start: `https://<store-domain>/staff_saml/index/login`
- Single logout endpoint: `https://<store-domain>/staff_saml/index/logout`

Magento needs the IdP entity identifier, SSO URL, logout URL and public X.509 certificate. The IdP needs the Staff service-provider identifier and ACS URL. The module uses HTTP POST for the assertion callback and HTTP Redirect for IdP sign-in and logout.

If the **SP Identifier** field is empty, the module uses the store base URL. Set an explicit identifier when the IdP requires a stable entity ID that differs from the current base URL.

Map identity claims

Map the claim paths for:

- email, which identifies the Staff account
- first name and last name
- group value
- Magento website code

The shipped Microsoft-style defaults cover email, given name and surname. Group and website mappings are empty until you configure them.

On first successful login, the module creates an active Staff account with the asserted email, name, website and persistent SAML NameID. On later logins it loads the Staff record by email and website. A disabled Staff account remains blocked even when the IdP authentication succeeds.

Group-to-attribute mapping

The **Group to attributes mapping** field accepts JSON. Its keys are asserted group values; each value contains Staff fields to apply. For example:

```
{
  "field-sales": {
    "group_id": 3,
    "access_all_customers": 0,
    "can_create_customer": 1,
    "can_edit_item_price": 0
  }
}
```

Use the exact group value sent by the IdP, not the human-readable display label unless they are identical. The default group value is used when no group claim is supplied. Keep the mapping limited to known Staff fields and review any permission-expanding change as an access-control change.

Safe rollout

1. Configure SAML at website scope if different websites use different identity providers or claims.
2. Test with password login still enabled.
3. Confirm first-login provisioning creates the expected website, group and permissions.
4. Disable the Staff account in Magento and confirm the IdP can no longer sign it in.
5. Test logout and a new login in a clean browser session.
6. Only then enable **Disable login with username/password**.

The default for password login is disabled when SAML is active, so treat the first production configuration carefully. An incorrect certificate, claim name, website code or IdP URL can lock all representatives out.

Behavior on the storefront

While SAML is enabled, the **Account settings** link (`staff/index/account`) is removed from the Staff navigation. In addition, a SAML-managed staff account — one with a stored SAML NameID — is redirected to the Staff dashboard when it opens the account page directly. The local profile fields such as the password no longer apply to those accounts, which is why the page is locked. Staff accounts that are not linked to the IdP keep their account page.

Custom code can deep-link into the Staff area after SSO by storing a target path in the Staff session under `staff_saml_redirect_url_after_login` before starting `staff_saml/index/login`. The login request passes that value to the IdP as RelayState, and the callback redirects to it only when it validates as an internal path — the store base URL or a root-relative path.

Troubleshooting

- **Invalid response or signature:** paste the current IdP signing certificate without changing its contents and check the IdP entity ID.
- **Staff email is empty:** the configured email claim path does not match the assertion.
- **Wrong website:** verify the asserted website code exists; otherwise the current website is used.
- **Wrong permissions:** compare the asserted group value with the JSON keys and validate the referenced Staff group ID.
- **Redirect loop:** confirm the store uses its public HTTPS base URL and that the ACS URL matches the IdP registration exactly.
- **Disabled user still reaches the IdP:** that is expected; Magento rejects the Staff session after the assertion is processed.

Configuration reference

Group	Fields
General	Enable SAML, disable password login, group-to-attribute JSON, default group value, login button text
Identity provider	SP identifier, IdP identifier, IdP login/logout URLs, IdP public certificate
Main attribute mapping	Email, first name, last name, group and website claim paths

Related: Staff Groups and Common Issues.