SAML Configuration for Advarra SSO

November 25, 2024

Table of Contents

Introduction

Advarra Single Sign-On (SSO) is an authentication method that provides a more streamlined experience, allowing users to use one set of credentials to log in to multiple Advarra applications, when those application environments are on Advarra Cloud and configured to use Advarra SSO. Users logged in with SSO are directed to the Advarra One homepage, which allows them to navigate to any SSO-enabled applications to which they have access. This contrasts with previous functionality where users needed separate credentials for each application they accessed. For organizations using SAML, Advarra SSO reduces the number of SAML connections to maintain to one instead of one for each application instance, as was previously required.

Advarra SSO supports SAML 2.0 authentication via a customer's own identity provider (IdP). This document walks you through the process needed to configure this form of authentication. Your technical team works alongside Advarra to complete the necessary setup.

Setup Steps

To complete this setup, please follow these steps:

1. Contact your Advarra Project or Support representative to initiate the SAML configuration process, providing the following information:
    a. A list of IdPs that will authenticate Advarra SSO users from your organization.
    b. For each of the identified IdPs:
        i. Name and email of a technical contact who can configure the IdP. Advarra will work with this contact.
        ii. Name and email of a user who will test and verify the configuration by logging in to Advarra SSO. This can be the same technical contact from item i, or another business user.
        iii. A copy of IdP metadata, if the IdP metadata is common between all service providers (SP). This is typically true for Shibboleth IdPs but not for Okta or Microsoft Azure AD.
        iv. List of all email domains and subdomains that can be present in the email claim in SAML responses from this IdP.
2. Advarra completes some initial configuration and provides your technical team with the necessary service provider SAML metadata and certificates.
3. After you receive this information from Advarra, complete the IdP side of the SAML configuration, using the detailed SAML specification below as a guide.
4. After the IdP configuration is complete, provide your SAML metadata and certificate to your Advarra contact.
5. Advarra completes the SAML configuration on the service provider side and confirms that a login test can be carried out.
6. You confirm that a login is successful via SAML SSO.

For help troubleshooting your SAML 2.0 configuration, please reach out to your Advarra Project or Support representative. If necessary, a call can be arranged to complete and troubleshoot SAML configuration. Please make sure you have a SAML/SSO administrator available to attend the configuration meeting.

SAML 2.0 Detailed Specification

IdP Settings

Entity ID

Enter the SAML Entity ID for your identity provider. The value must match the Entity ID used by your IdP and have a maximum length of 1024 characters. This value is found in the IdP metadata as the “entityID” attribute of the “EntityDescriptor” element.

Single Sign On URL

Enter an IdP endpoint to which single sign-on requests will be directed. This value is a URL with a maximum length of 256 characters, and it must start with *https*. This is the single sign-on service binding using the “HTTP-Redirect” method:

```
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
```

x.509 Signing Certificate

Enter the IdP's public key certificate that is used to sign authentication requests. This value must be a valid Base64-encoded certificate with a maximum length of 5000 characters.

Require Signature on Message

The type of authentication signature that should be used when configuring a SAML realm. We require signature on Message (without signature on Assertion) to ensure the integrity of the entire SAML message. This is to prevent malicious tampering of the entire XML payload that could lead to XXE or other XML-based attacks.

Encryption Not Supported

We do not support encrypted messages or assertions at this time.

NameId Type

The NameId must be of type “persistent." The value should be a non-changing opaque identifier (for example, UUID, or another generated identifier).

```
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
```

Email Claim

We require an email claim to be sent as an additional assertion along with the NameId claim. This allows us to properly verify and match the user account within the SP to the one identified by the IdP.

for example, `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`

> Note: In accordance with industry standards and security best practices, Advarra SSO does not currently support email aliases.

Signature Algorithm

Select the signature algorithm to use when verifying SAML 2.0 authentication requests. This is set to SHA256withRSA by default. Other options are SHA1withRSA, SHA384withRSA, and SHA512withRSA.

User Access at the IdP Level

We recommend that you do not restrict user access at the IdP level, as managing access at that level across applications can be difficult. User access is controlled at both the Advarra One and application levels. If you do need to use access groups to control access at the IdP level, be sure to design a clear workflow for managing all users.

Updating SAML Certificates

We recommend that you take note of the expiration date of your IdP certificate and reach out to your Advarra Project or Support representative a few months prior to that date.

Update process:

- Contact your Advarra Project or Support representative to get support updating your certificate. Be prepared to generate and provide the new IdP x509 certificate (in text format) that you received from your IdP administrators.
- Advarra updates the certificate stored on our end with your newly provided one.
- Test authentication with someone on your team to verify the change.

Linking to Advarra One

To add a link to Advarra One to your organization's existing SSO homepage, you can add a tile with a link or web shortcut to https://one.advarracloud.com. Advarra doesn't support IdP-initiated login, so you must also hide the application tile with the SAML configuration.