CLOUDFLARE
AREA 1 SECURITY

Portal Single Sign-on (SSO)

Deployment and Configuration Guide

SSO Overview

For added security and convenience, Cloudflare Area 1 offers support for SAML-based single sign-on (SSO) logins to our portal. Organizations will be able to choose between having users access the Area 1 security data with a username and password + two-factor authentication (2FA) code, or having them use an SSO provider, such as OneLogin or Okta, to access the portal.

SAML Configuration Options:

1. *Identity Provider Initiated (IDP) SAML*

   Identity Provider (IDP) (e.g. OneLogin) Initiated configurations require that the IDP be accessible to the Area 1 infrastructure in order to successfully authenticate users. At the most basic level the user selects an application from their IDP and the IDP communicates with the OneLogin portal using a SAML assertion to provide identity information for the user requesting to login to the Area 1 Security portal.

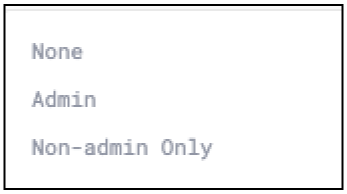
2. *SP-Initiated SAML*

   SP-Initiated configurations are the most common SAML authentication mechanisms. The main difference compared to IDP is that the Service Provider (SP) (e.g. Area 1) does not require any direct connection to the IDP in order to authenticate a user. The user's browser provides the ability for the SAML exchange to occur but the SP and the IDP do not directly communicate with each other.

Version: 1.3

All Area 1 SAML Setup:

1. The first step, if you don't have one already, is to select and set up an SSO provider (such as Onelogin or Okta) which will manage the user interface and settings for your organization.
2. You can turn on the feature in the Area 1 portal from the SSO settings page: https://horizon.area1security.com/settings/single-sign-on
3. SSO enforcement

   None

   Admin

   Non-admin Only

   a. **None** - Each user can choose between SSO or Username, Password + 2FA (recommended setting while testing SSO).
   b. **Admin** - This setting will force only Admin to use SSO only. The exception is that the user who enables this setting will still be able to login using Username, Password + 2FA. This is a backup so that your organization does not get locked out of the portal in emergencies.
   c. **Non-Admin Only** - this option will require that all "Read only" and "Read & Write" users use SSO to access the portal. Admins will still have the option to use either SSO or Username, Password + 2FA.

4. **SAML SSO Domain** - This is the domain that points to the SSO provider.

5. **METADATA XML** - You will need to copy and paste the SAML XML Metadata settings from your provider into Area 1. These settings (and even their exact text descriptions) are in different locations depending on your SSO provider.
   Please contact your SSO provider or Area 1 support for assistance with this step if you run into any issues.

Identity Provider SAML Setup:

The values to be configured in the IdP setup are as follows:

SAML Consumer URL: https://horizon.area1security.com/api/users/saml

A customer parameter must also be added to the SAML assertion.

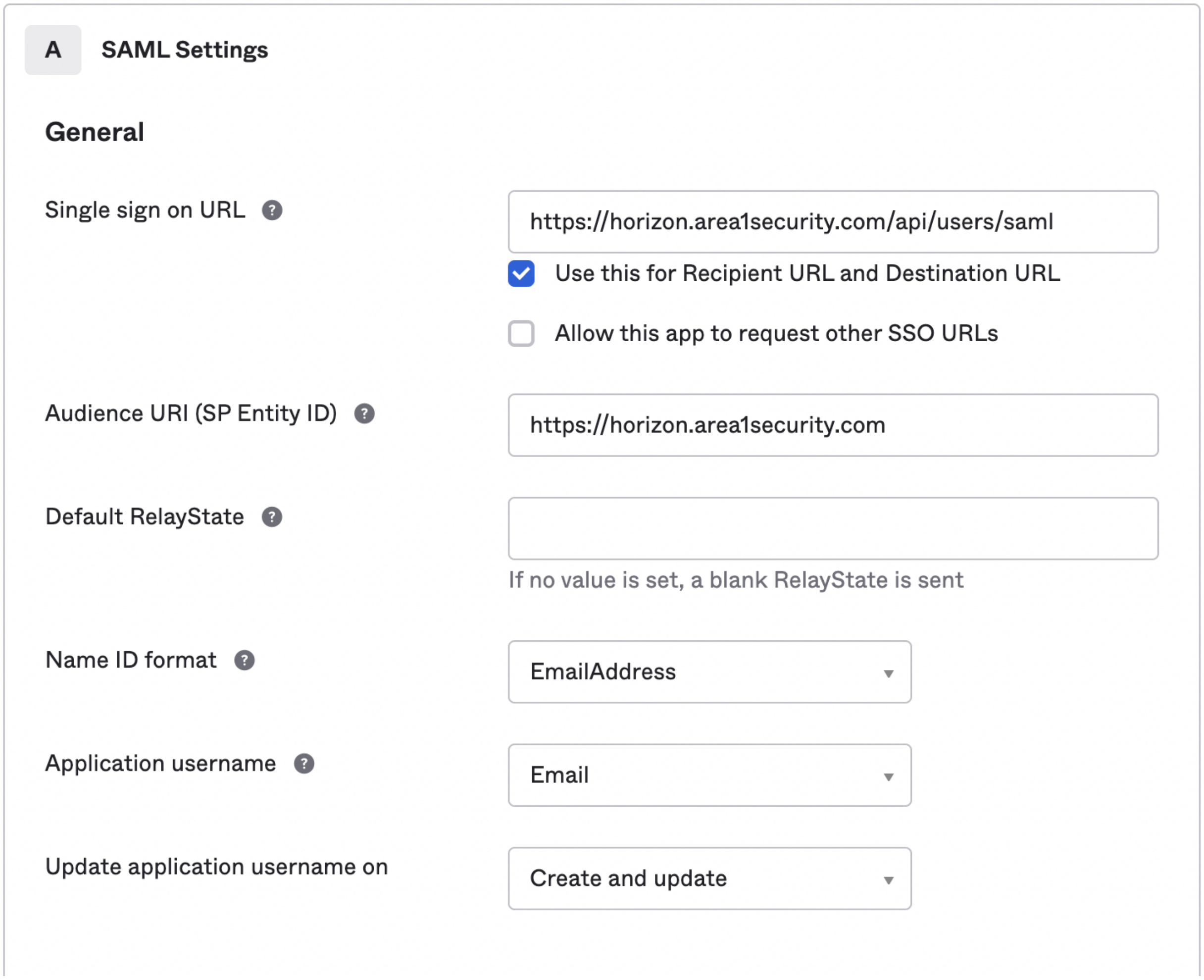
NameID field must use Email Address

Parameter: email

Value = Email of user. Should match the email the user has already had created in the Area 1 portal

Entity ID: https://horizon.area1security.com

Screenshot below for reference:



A SAML Settings

General

Single sign on URL: https://horizon.area1security.com/api/users/saml

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://horizon.area1security.com

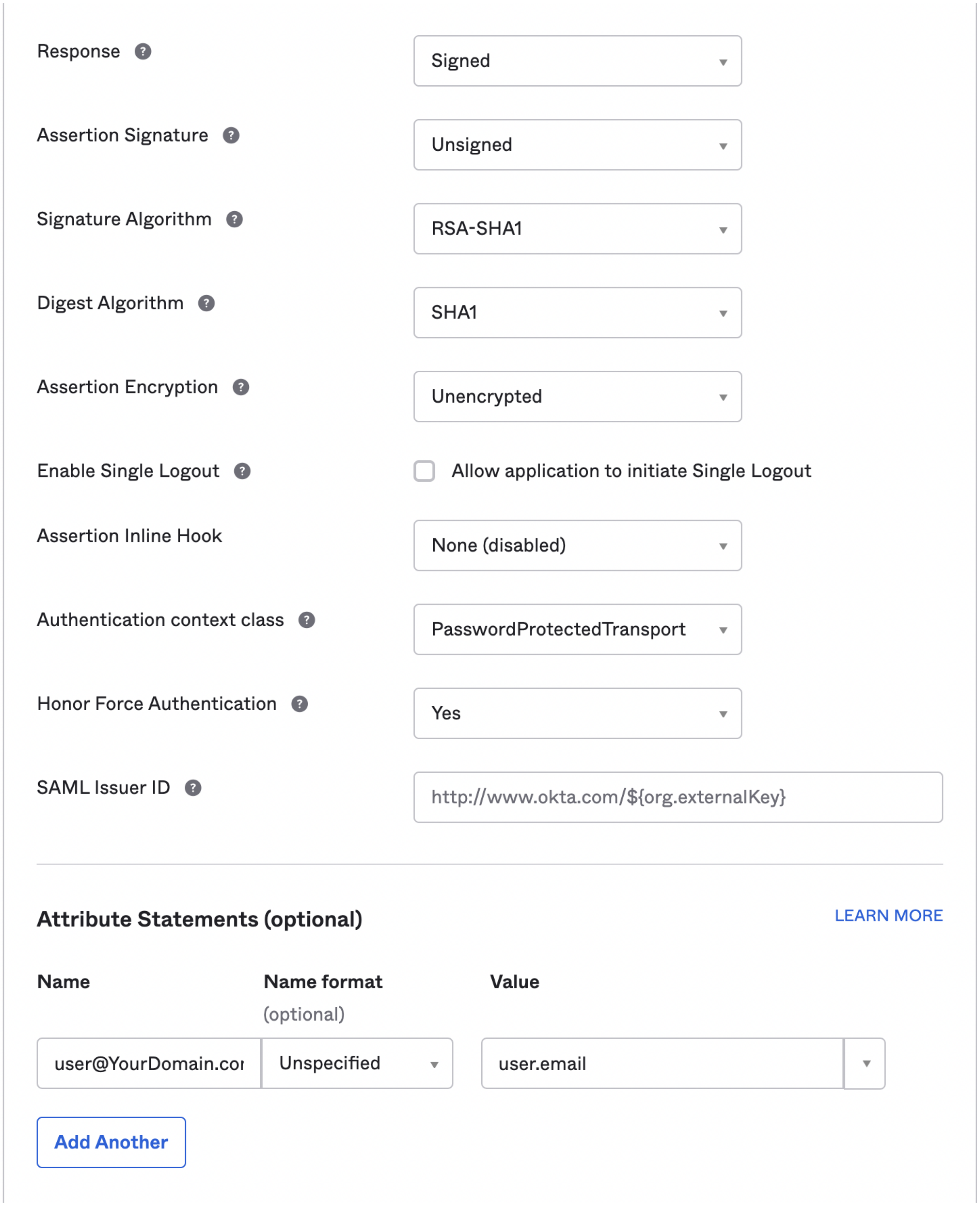
Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: EmailAddress

Application username: Email

Update application username on: Create and update



Response ?	Signed ▾
Assertion Signature ?	Unsigned ▾
Signature Algorithm ?	RSA-SHA1 ▾
Digest Algorithm ?	SHA1 ▾
Assertion Encryption ?	Unencrypted ▾
Enable Single Logout ?	□ Allow application to initiate Single Logout
Assertion Inline Hook	None (disabled) ▾
Authentication context class ?	PasswordProtectedTransport ▾
Honor Force Authentication ?	Yes ▾
SAML Issuer ID ?	http://www.okta.com/${org.externalKey}

Attribute Statements (optional)

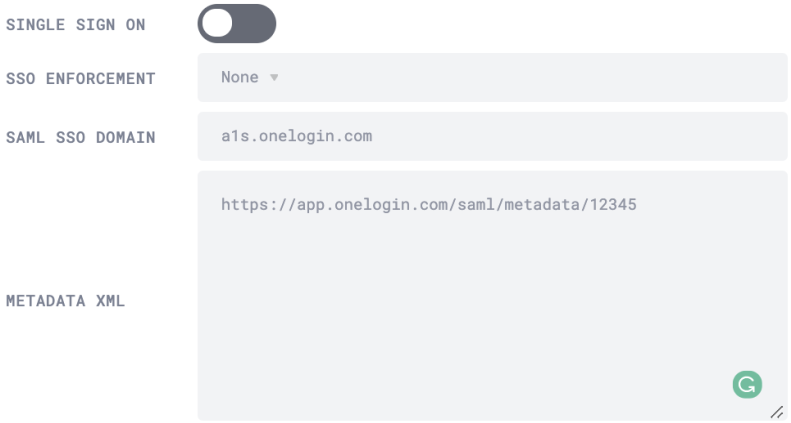
Name	Name format (optional)	Value
user@YourDomain.coı	Unspecified ▾	user.email ▾

Once you have the above configured and the SAML icon created download the metafile.

Copy and paste it into the box “METADATA XML”

To test - On the landing page of your SAML solution. Locate the ICON you have created
for SSO login with Area 1 Security.

*the user must already have an account with Area 1's portal.



SINGLE SIGN ON

SSO ENFORCEMENT: None

SAML SSO DOMAIN: a1s.onelogin.com

METADATA XML: https://app.onelogin.com/saml/metadata/12345

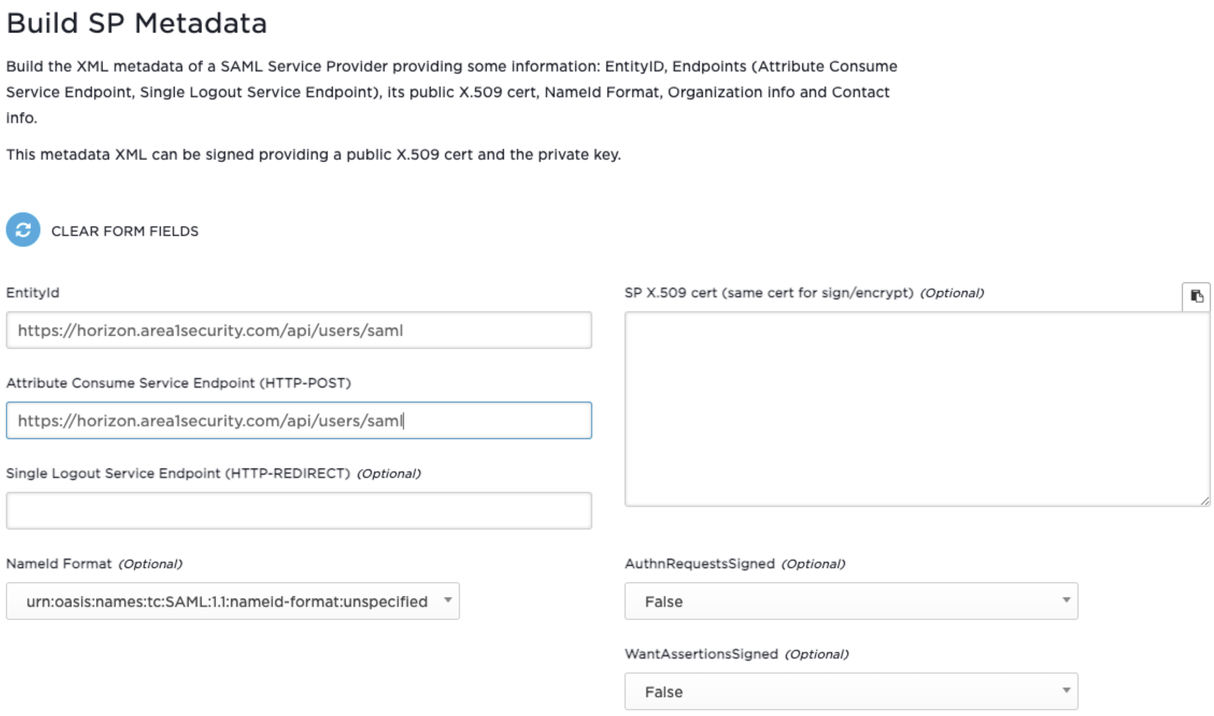
The above configuration is sufficient if you are configuring IDP-initiated SAML setup but if you are configuring SP-initiated please continue with the below setup.

Troubleshooting:

1) Check to see if the user exists in Area 1 portal
2) Check to see if you are using email address as an attribute
3) Check to see if you are using SHA 1
4) Check to see if encryption is set to 2048
5) For other custom SAML setup where “Service Provider” (like Area1) XML metadata is essential, you can use third party tools to generate the XML Metadata.

   For example:

   Using OneLogin’s SAML tool to build SP Metadata:
   https://www.samltool.com/idp_metadata.php



Build SP Metadata

Build the XML metadata of a SAML Service Provider providing some information: EntityID, Endpoints (Attribute Consume Service Endpoint, Single Logout Service Endpoint), its public X.509 cert, NameId Format, Organization info and Contact info.

This metadata XML can be signed providing a public X.509 cert and the private key.

EntityId
https://horizon.area1security.com/api/users/saml

Attribute Consume Service Endpoint (HTTP-POST)
https://horizon.area1security.com/api/users/saml

Single Logout Service Endpoint (HTTP-REDIRECT) *(Optional)*

NameId Format *(Optional)*
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

SP X.509 cert (same cert for sign/encrypt) *(Optional)*

AuthnRequestsSigned *(Optional)*
False

WantAssertionsSigned *(Optional)*
False

**Use https://horizon.area1security.com/api/users/saml for the EntityId and Attribute Consume Service Endpoint (HTTP-POST) fields. The rest of the fields are optional and can be left blank.

If you require assistance, please reach out to support@area1security.com.