MORNINGSTAR Wealth

Morningstar ByAllAccounts SAML Connectivity Guide

AccountView Version:	2.44
Document Version:	2
Document Issue Date:	September 28, 2023

Technical Support:	(866) 856-4951
Telephone:	(781) 376-0801
Fax:	(781) 376-8040
Web:	byallaccounts.morningstar.com

About this document 2
Related Documents 2
ByAllAccounts SAML Support 2
Configuring ByAllAccounts SAML Support 3
Identity Provider (IDP) Information 4
Partner Contact for SAML Information 4
Partner IDP Information 4

About this document

This document is used during the ByAllAccounts implementation process to collect information required to establish SAML trust between the ByAllAccounts Partner (IdP) and the ByAllAccounts Service Provider (SP).

Related Documents

- For information about single sign-on (SSO), refer to: *AccountView Single Sign-On (SSO) Guide* http://www.byallaccounts.net/Manuals/Accountview/AccountView_SingleSignOn.pdf
- For information on creating users via DataConnect, refer to: *DataConnect V4 Ultra User Guide* http://www.byallaccounts.net/Manuals/DataConnect/DataConnect_V4_Ultra_User_Guide.PDF

ByAllAccounts SAML Support

ByAllAccounts supports SAML2 for IdP-initiated Single Sign-on via HTTP POST. ByAllAccounts will configure one or more SAML realms for each ByAllAccounts partner depending on the partner's implementation model for their customers.

ByAllAccounts creates a firm for the Partner's customer. That firm is configured to require SAML authentication for SSO users. The partner can create individual ByAllAccounts users (Advisors and/or Investors), designate them as SSO, and then retain the unique ByAllAccounts Person ID (BAAPersonId). Later, when the partner wants to launch AccountView via SAML for that user, the partner provides the BAAPersonId to identify the target user.

BAAPersonId:

- uniquely identifies that person within the entire ByAllAccounts system.
- is the only piece of information needed to identify the user.
- is the case-sensitive name of the SAML Attribute that you must pass when making the SAML exchange.

The following OWASP diagram shows the sequence of actions in an IdP-initiated single sign-on:

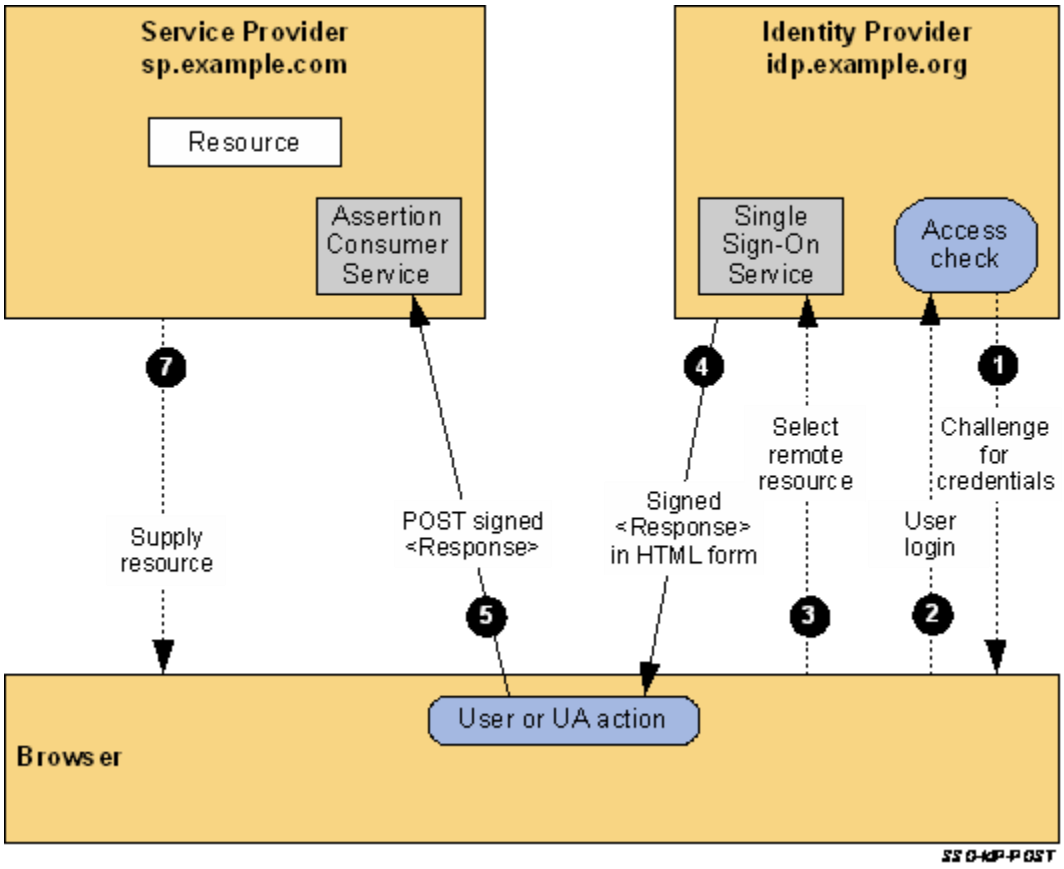

Diagram source: OWASP

Additional notes about ByAllAccounts SAML support:

- All the communication between the SP and the IDP is over HTTPS.
- SAML requests and responses will be signed and encrypted.

Configuring ByAllAccounts SAML Support

The configuration process is as follows:

1. The partner provides contact information for SAML configuration to Morningstar.
2. The partner provides SAML metadata and certificates for applicable environments to Morningstar. Typically this information differs between pre-production and production.
3. Morningstar ByAllAccounts uses the partner-provided information to configure the partner in a SAML circle of trust.
4. Morningstar ByAllAccounts sends the Service Provider (SP) metadata to the partner to complete the SAML configuration on the IdP side.
5. A live test of the configuration is performed by launching the partner application in a browser, logging in to that application, selecting the ByAllAccounts link from within the application, and confirming that AccountView is successfully launched for the target user.

IDENTITY PROVIDER (IDP) INFORMATION

Please provide the details in the following tables.

Partner Contact for SAML Information

Company Name:	
Contact Name:	
Contact Number:	
Email:	

Partner IDP Information

If the following information will vary for different customers of partner, then please describe the variation.

1. Issuer Name:	
2. SAML Metadata – name of the attribute that partner will use to provide the target BAA Person Id.	
a. Pre-Production:	
b. Production:	
3. Single Sign-on URL:	
a. Pre-Production:	
b. Production:	

Appendix A: Terminology

- **SSO**: Single Sign On
- **SAML**: Security Assertion Markup Language
- **SAML Assertion**: contains the packet of security or decision information.
- **Binding Profile**: For Web applications, two common bindings are HTTP Redirect Binding and HTTP Post Binding.
- **IDP (Identity Provider)**: A system that trusts the user by authenticating the user. Also known as Session Authority.
- **SP (Service Provider)**: A system that trusts the IDP and therefore trusts the user. Also known as session participant.
- **Assertion Consumer App**: Part of the SP that validates the SAML Assertion sent from IDP and redirects to the relay state URL.
- **Issuer**: Name of the IDP. This will be part of the SAML Assertion.
- **IDP certificate**: x509 certificate generated by IDP and provided to SP. The IDP certificate will be part of the SAML Assertion.
- **Entity ID**: Name of the SP. This will be part of the SAML Assertion.
- **Assertion Consumer Service URL**: A URL where IDP submits the SAML Assertion. Also known as Login URL. The Assertion Consumer Service URL will be part of the SAML Assertion.
- **Relay State URL**: A URL of the actual service that the user wants to consume. Also known as Target URL.