Using Your Own Authentication System with ArcGIS Online

Daniel Urbach and Cameron Kroeker
Agenda

- The ArcGIS Platform
- What is SAML?
- Meet the Players
- Relationships Are All About Trust
- What Happens During SAML Authentication
- Demo
- Groups and Federation
- Questions?
The ArcGIS Platform
The ArcGIS Platform

Clients

Desktop

Web

Device

Access / Identity

Services

Server

Online Content and Services
How to authenticate?

ArcGIS Online

Named Users

Enterprise Users

SAML Authentication
What is SAML?
What is SAML?

- Security Assertion Markup Language
- Based on XML and open source standard
- Web browser single sign-on
- Separating the Identity Store from the Service Provider
SAML Request

- Identity of issuer making the request
- Format of username to return

```xml
<SAML:ASSERTION xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="NDBIFENMKWNZUJMN"
    VERSION="2.0"
    ISSUER="2018-07-03T21:12:04Z"
    PROTOCOLBINDING="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    ASSERTIONCONSUMERSERVICEURL="https://samljackson.maps.arcgis.com/sharing/rest/oauth2/saml/SIGNIN"
ALLOWCREATE="true"
/></SAML:ASSERTION>
```
SAML Response

- Verification of authentication
- User attributes:
  - NameID
  - GivenName
  - Email Address
  - Groups
Meet the Players
Service Provider, Identity Provider and Client
Meet the Players: Service Provider

- Provides web-based consumables to the end-user
- Requires authentication
- ArcGIS Online
Meet the Players: Identity Provider (IdP)

- Provides cross-domain authentication
- Uses HTTP/HTTPS
- Active Directory Federated Services, OpenAM, etc
- Can authenticate via existing user stores (AD, LDAP, etc)
Meet the Players: Identity Provider (IdP)

Typical SAML Provider Architecture

- **ArcGIS Online**
- **External Domain(s)**
- **Client**
- **Firewall**
- **DMZ**
- **IdP: ADFS**
- **Firewall**
- **Active Directory**
- **Internal Domain**
Meet the Players: Client

- Web browser
- ArcGIS for Desktop
- ArcGIS Pro
- Collector for ArcGIS
Relationships Are All About Trust
Relationships are all about Trust!

Identity Provider

Metadata

Service Provider
Relationships are all about Trust!

Identity Provider

AssertionConsumerService URL
SingleLogoutService URL
Public SSL key
OrganizationName
OrganizationDisplayName
OrganizationURL

Service Provider
Relationships are all about Trust!

Identity Provider

- SSO Service URL
- Logout Service URL
- Digital Signature
- Public SSL Key
- ID to identify the provider
- Claims attributes offered

Service Provider
What Happens During SAML authentication
The SAML Login Experience

Service Provider Initiated Log On

Identity Provider Initiated Log On
What happens during SAML authentication?
What happens during SAML authentication?

Authentication Request

Service Provider
ArcGIS Online

Client
Web Browser / Application

User accesses resources

Authentication request

Start Here
What happens during SAML authentication?

Authentication Request

Client
Web Browser / Application

Identity Provider

Authentication request forwarded to IdP

SAML token returned to client
What happens during SAML authentication?

Service Provider accepts SAML assertion
What happens during SAML authentication?

Service Provider Initiated Log In

**Ticket Booth (IdP)**
- **SP-Initiated**
- **Start Here**
- **Swing by Here**
- **Finish**

**Service Provider**
- ArcGIS Online

**Client**
- Web Browser / Application

**Identity Provider**

- User accesses resource
- Authentication Request
- Authentication request forwarded to IdP
- SAML token returned to client
- SAML token & attributes forwarded to SP
- User is logged into SP
Demo
What happens during SAML authentication?

Identity Provider Initiated Log In
Groups and Federation
New Feature: Enterprise Group Membership

• Allows enterprise groups to be linked to ArcGIS Online groups
• No need to invite users to a group!
New Feature: SAML Federation

- Allows for flexibility in which IdP to use
- inCommon, Switchoai
Please Take Our Survey on the App

Download the Esri Events app and find your event

Select the session you attended

Scroll down to find the feedback section

Complete answers and select “Submit”