Using Your Own Authentication System with ArcGIS Online

Cameron Kroeker and Gary Lee
Agenda

• ArcGIS Platform Structure
• What is SAML?
• Meet the Players
• Relationships Are All About Trust
• What Happens During SAML Authentication
• Demo
• FAQs
• Questions?
ArcGIS Platform Structure

Clients

Access / Identity

Services

Desktop

Web

Device

Server

Online Content and Services
How to authenticate?

ArcGIS Online

- Named Users
- Enterprise Users

SAML Authentication
What is SAML?

• Security Assertion Markup Language
• Based on XML
• Web browser single sign-on
• Separating the Identity Store from the Service Provider
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

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

- Web browser
- ArcGIS for Desktop
- ArcGIS Pro
- Collector for ArcGIS

ArcGIS Online
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
What happens during SAML authentication?

- Requests sent via HTTP/HTTPS in XML format
- Client acts as the middleman between the SP and IdP
- Service Provider Initiated Log on
- Identity Provider Initiated Log on
What happens during SAML authentication?

Service Provider Initiated Log In

**Service Provider**
ArcGIS Online

- User accesses resource
- Authentication Request
- SAML token & attributes forwarded to SP
- User is logged into SP

**Client**
Web Browser / Application

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

Authentication Request

Service Provider
ArcGIS Online

Client
Web Browser / Application

User accesses resources

Authentication request

<authn:AuthnRequest xmlns:authn="urn:oasis:names:tc:SAML:2.0:assertion"
                   xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
                   ID="_MXHGFlwzfYcalbAY"
                   Version="2.0"
                   IssueInstant="2016-06-10T21:51:00Z"
                   ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                   AssertionConsumerServiceURL="https://samlJackson.maps.arcgis.com/sharing/rest/oauth2/saml/signin"
                   >

  <saml:Issuer>samlJackson.maps.arcgis.com</saml:Issuer>

  <saml:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
                     AllowCreate="true"/>

<br />
</authn:AuthnRequest>
What happens during SAML authentication?

Authentication Request

1. IdP checks if user is currently authenticated
2. If user is not currently authenticated, user is challenged for credentials
3. IdP attempts to authenticate user
4. A SAML assertion is generated and sent to the AssertionConsumerService URL
What happens during SAML authentication?

**Authentication Response**

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

- **Service Provider**: ArcGIS Online
- **Client**: Web Browser / Application

1. **User is logged into SP**
2. SAML token and attributes forwarded to SP
What happens during SAML authentication?

Identity Provider Initiated Log In

Service Provider
ArcGIS Online

Client
Web Browser / Application

Identity Provider

User accesses login page on IdP
Redirected to SP with token and attributes
SAML token & attributes forwarded to SP
User is logged into SP

ADFS 3 AVWORLD

You are signed in.

- Sign in to one of the following sites:
  samljackson.maps.arcgis.com

- Sign in

- Sign out from all the sites that you have accessed.
  Sign out from this site.

- Sign Out
Demo
FAQs

- **After enabling SAML accounts, can built-in accounts be removed?**
  - Yes, but it is recommended to keep at least one built-in account as an administrator.

- **I would like to replace my built-in account with a SAML account, what happens to the content?**
  - Once the SAML account has been created, and signed in successfully the content can be transferred using the ArcGIS Online Assistant: [https://ago-assistant.esri.com/](https://ago-assistant.esri.com/)

- **Which attributes does ArcGIS Online support?**
  - NameID (Mandatory), GivenName (Optional), Email or Mail (Optional)

- **What are some common SAML 2.0 Identity Providers?**
  - Active Directory Federation Services, Okta, OpenAM, Shibboleth