

UC



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

Desktop



Web



Device



Access / Identity



Services

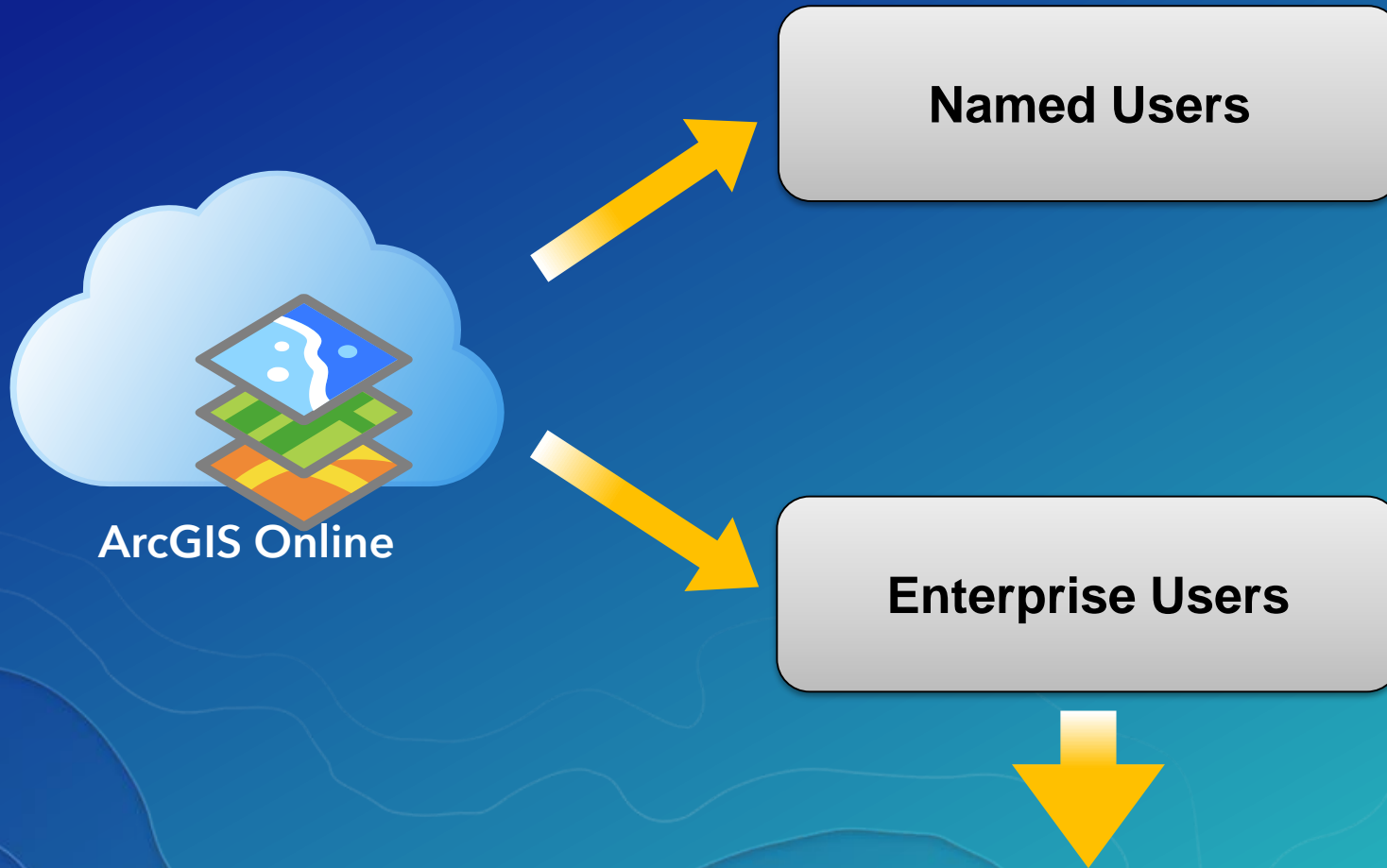


Server



Online Content and
Services

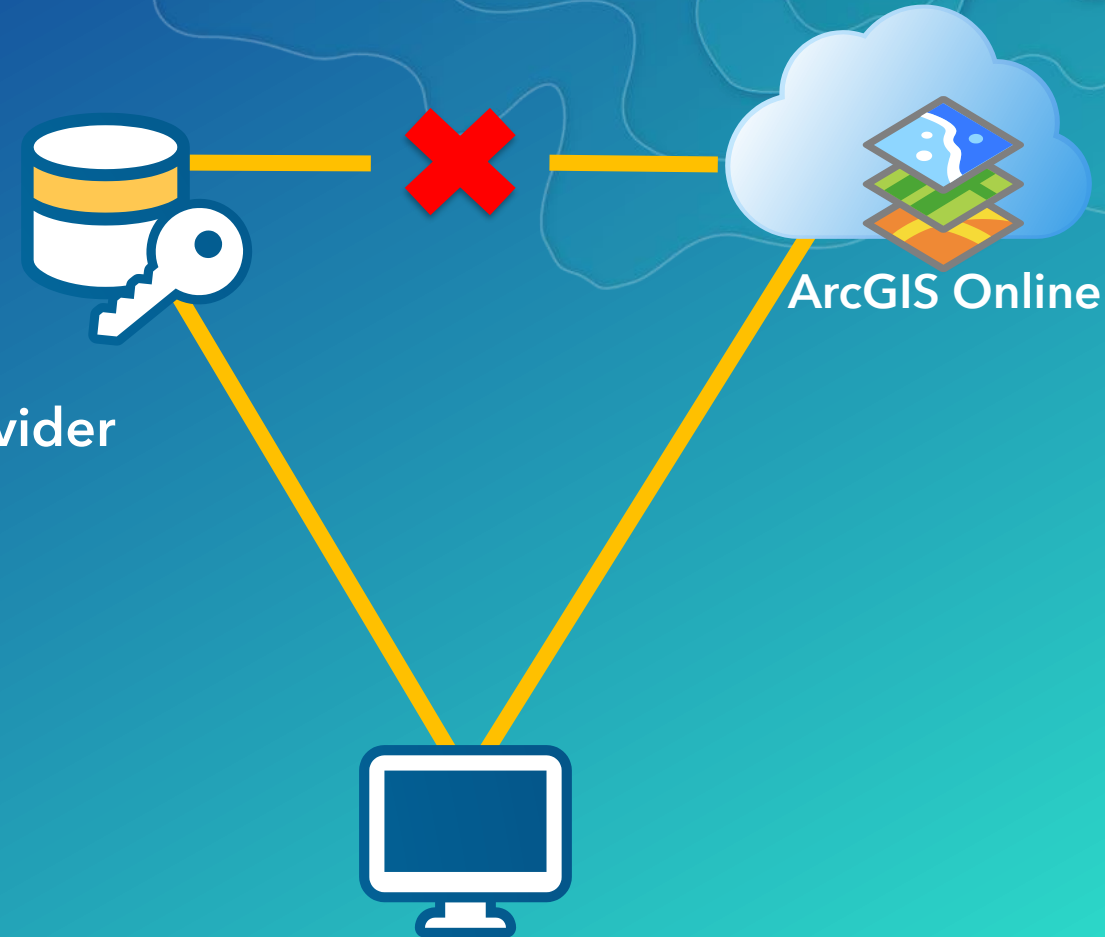
How to authenticate?



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



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



External Domain(s)



Firewall



DMZ



Firewall



Internal Domain

Meet the Players: Client

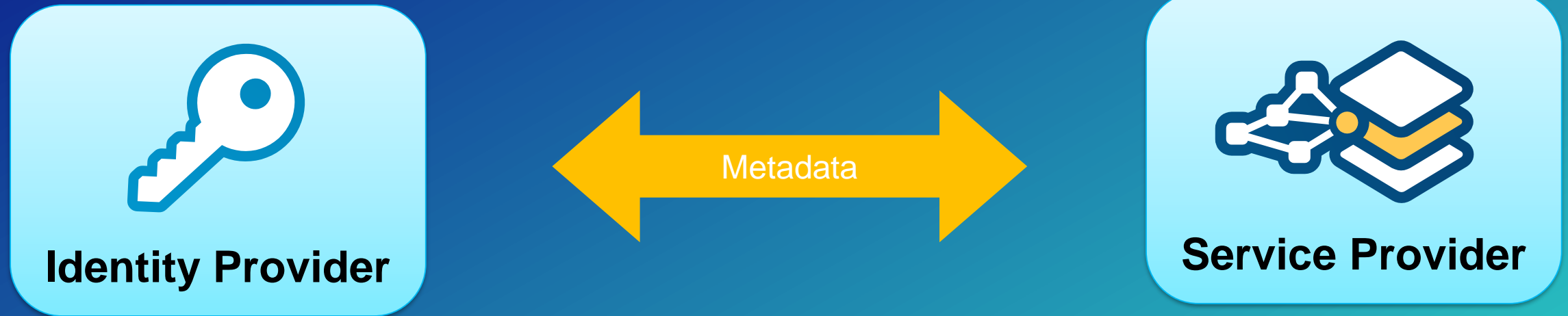
- Web browser
- ArcGIS for Desktop
- ArcGIS Pro
- Collector for ArcGIS



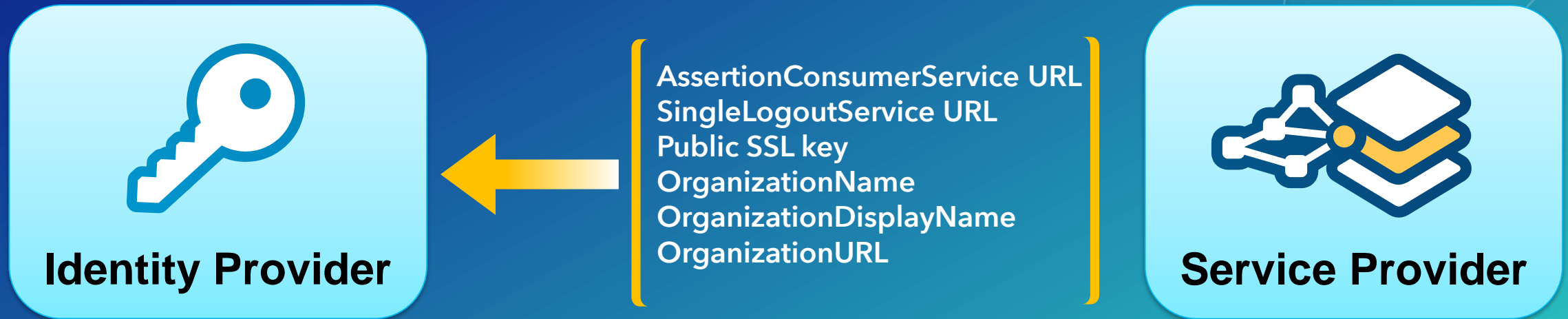
Relationships Are All About
Trust



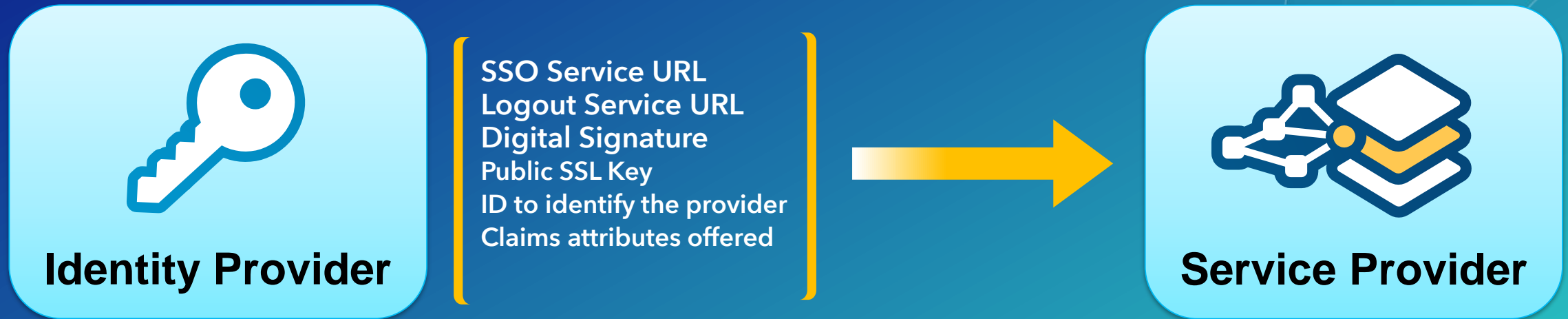
Relationships are all about Trust!



Relationships are all about Trust!



Relationships are all about Trust!



What Happens During SAML authentication



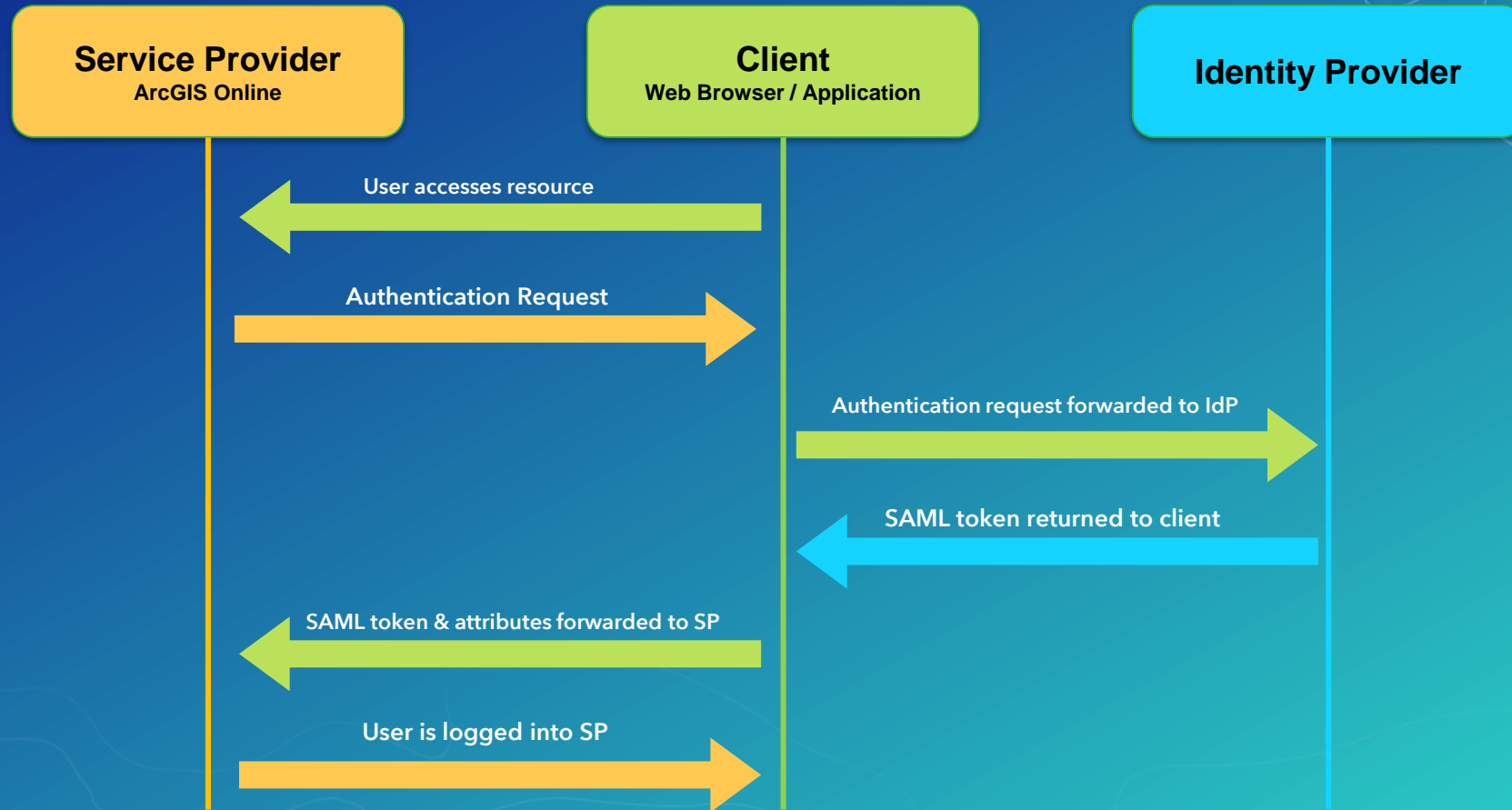
What happens during SAML authentication?

- 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



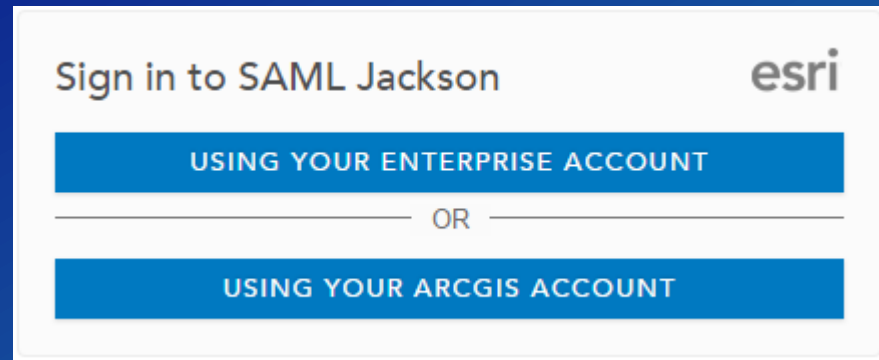
What happens during SAML authentication?

Service Provider Initiated Log In



What happens during SAML authentication?

Authentication Request

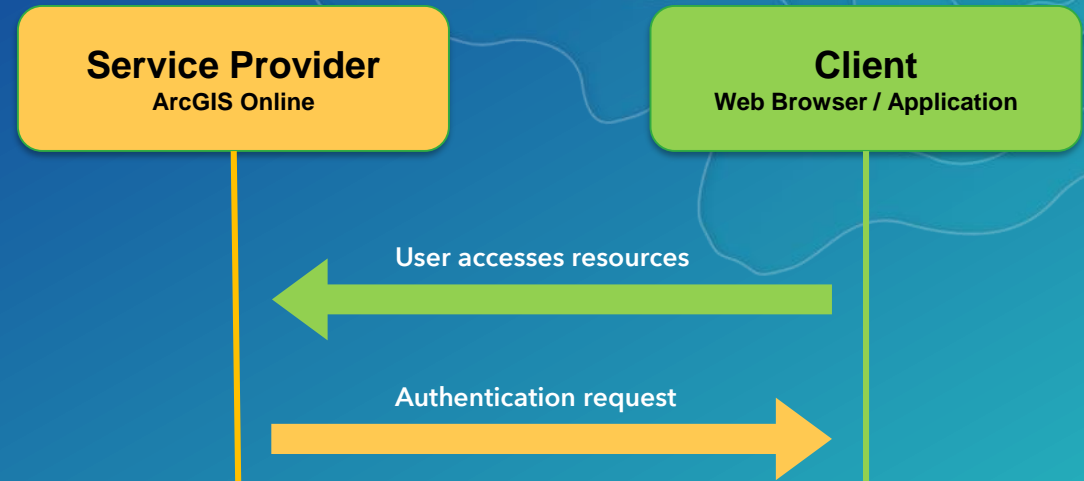


Sign in to SAML Jackson **esri**

USING YOUR ENTERPRISE ACCOUNT

OR

USING YOUR ARCGIS ACCOUNT

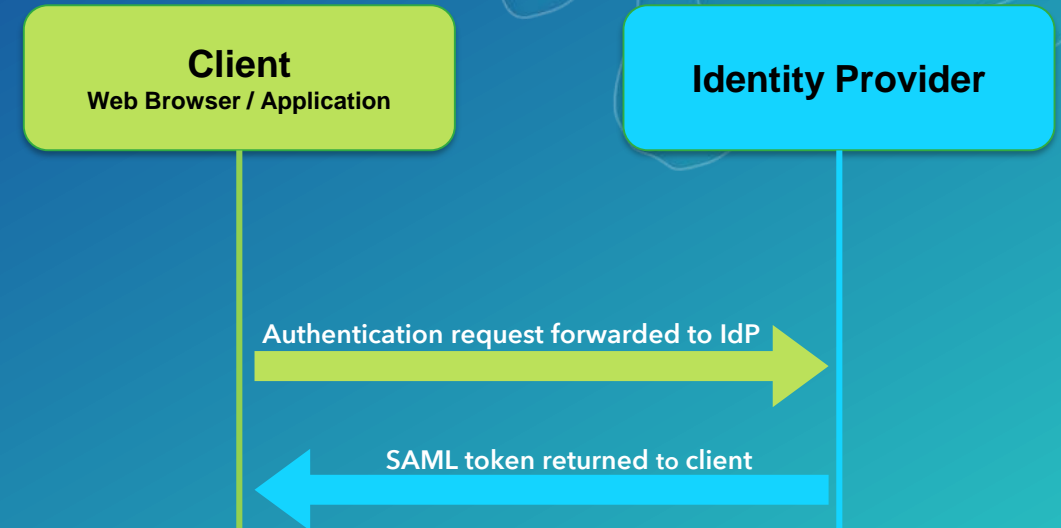


```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_MXHGFlwzfYcalbAY"
  Version="2.0"
  IssueInstant="2016-06-10T21:51:00Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  AssertionConsumerServiceURL="https://samljackson.maps.arcgis.com/sharing/rest/oauth2/saml/signin"
>
  <saml:Issuer>samljackson.maps.arcgis.com</saml:Issuer>
  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
    AllowCreate="true"
  />
</samlp:AuthnRequest>
```

What happens during SAML authentication?

Authentication Request

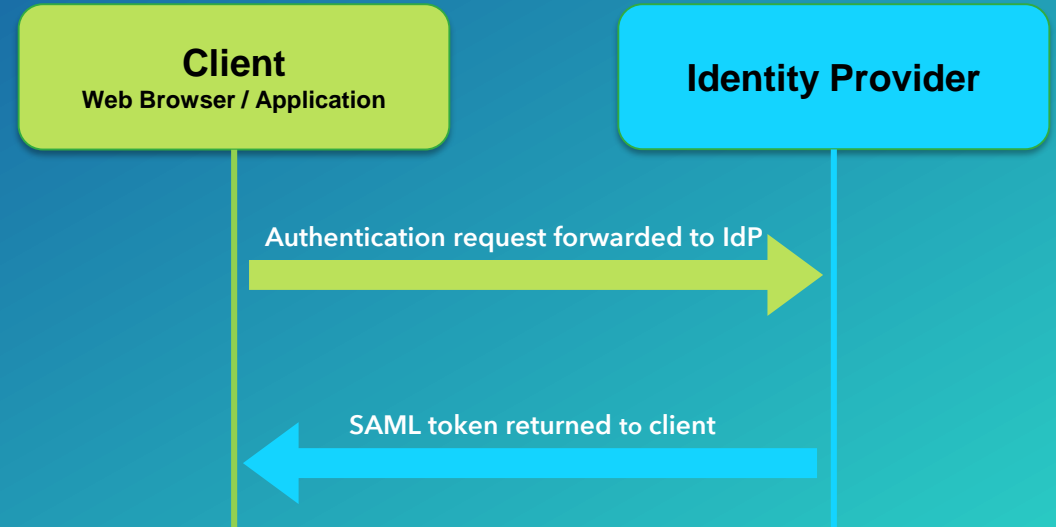
1. IdP checks if user is currently authenticated
2. If user is not currently authenticated, user is challenged for credentials
3. IdP attempts to authenticate user
4. A SAML assertion is generated and sent to the AssertionConsumerService URL



What happens during SAML authentication?

Authentication Response

```
<SAMLp:RESPONSE ID="_E5287FEE-C873-4381-B4E6-C1CF76ED06A8"
  VERSION="2.0"
  ISSUEINSTANT="2017-06-26T20:49:38.112Z"
  DESTINATION="HTTPS://SAMLJACKSON.MAPS.ARCGIS.COM/SHARING/REST/OAUTH2/SAML/SIGNIN"
  CONSENT="URN:OASIS:NAMES:TC:SAML:2.0:CONSENT:UNSPECIFIED"
  INRESPONSETO="_SDYAQJEKBJPQPRI"
  XMLNS:SAMLp="URN:OASIS:NAMES:TC:SAML:2.0:PROTOCOL"
>
<ISSUER XMLNS="URN:OASIS:NAMES:TC:SAML:2.0:ASSERTION">HTTP://RED-INF-ADFS-D3.ESRI.COM/ADFS/SERVICES/TRUST</ISSUER>
<SAMLp:STATUS>
  <SAMLp:STATUSCODE VALUE="URN:OASIS:NAMES:TC:SAML:2.0:STATUS:SUCCESS" />
</SAMLp:STATUS>
...
<SUBJECT>
  <NAMEID>CAME7624</NAMEID>
  <SUBJECTCONFIRMATION METHOD="URN:OASIS:NAMES:TC:SAML:2.0:CM:BEARER">
    <SUBJECTCONFIRMATIONDATA INRESPONSETO="_SDYAQJEKBJPQPRI"
      NOTONORAFTER="2017-06-26T20:54:38.112Z"
      RECIPIENT="HTTPS://SAMLJACKSON.MAPS.ARCGIS.COM/SHARING/REST/OAUTH2/SAML/SIGNIN"
    />
  </SUBJECTCONFIRMATION>
</SUBJECT>
<CONDITIONS NOTBEFORE="2017-06-26T20:49:38.097Z"
  NOTONORAFTER="2017-06-26T21:49:38.097Z"
>
  <AUDIENCERESTRICTION>
    <AUDIENCE>SAMLJACKSON.MAPS.ARCGIS.COM</AUDIENCE>
  </AUDIENCERESTRICTION>
</CONDITIONS>
<ATTRIBUTESTATEMENT>
  <ATTRIBUTE NAME="HTTP://SCHEMAS.XMLSOAP.ORG/WS/2005/05/IDENTITY/CLAIMS/GIVENNAME">
    <ATTRIBUTEVALUE>CAMERON KROEKER</ATTRIBUTEVALUE>
  </ATTRIBUTE>
  <ATTRIBUTE NAME="HTTP://SCHEMAS.XMLSOAP.ORG/WS/2005/05/IDENTITY/CLAIMS/EMAILADDRESS">
    <ATTRIBUTEVALUE>CKROEKER@ESRI.COM</ATTRIBUTEVALUE>
  </ATTRIBUTE>
</ATTRIBUTESTATEMENT>
<AUTHNSTATEMENT AUTHNINSTANT="2017-06-26T19:58:25.754Z"
  SESSIONINDEX="_5648C9BE-37E9-4C88-89CD-7F8001D8F081"
>
  <AUTHNCONTEXT>
    <AUTHNCONTEXTCLASSREF>URN:FEDERATION:AUTHENTICATION:WINDOWS</AUTHNCONTEXTCLASSREF>
  </AUTHNCONTEXT>
</AUTHNSTATEMENT>
</ASSERTION>
</SAMLp:RESPONSE>
```




What happens during SAML authentication?

Service Provider accepts SAML assertion

[EDIT MY PROFILE](#)

Cameron's Profile



First Name
Cameron

Last Name
Kroeker

Email
CKroeker@esri.com

Username
came7624_samljackson

Bio
Write something about yourself. You might include things like:

- Your organization
- Contact information
- Areas of expertise
- Interests
- Any other information you'd like others to know

Link Your ArcGIS Accounts
[Manage Linked Accounts](#)

Who can see your profile?
Organization

Language
English-English

Region
United States

Units
US Standard

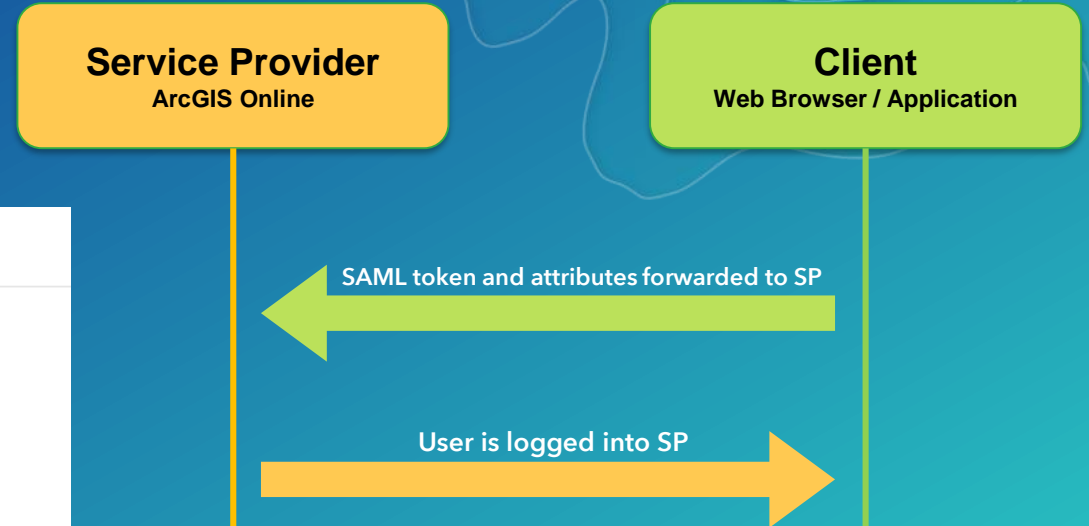
Level
2

Role
Administrator

Organization
SAML Jackson

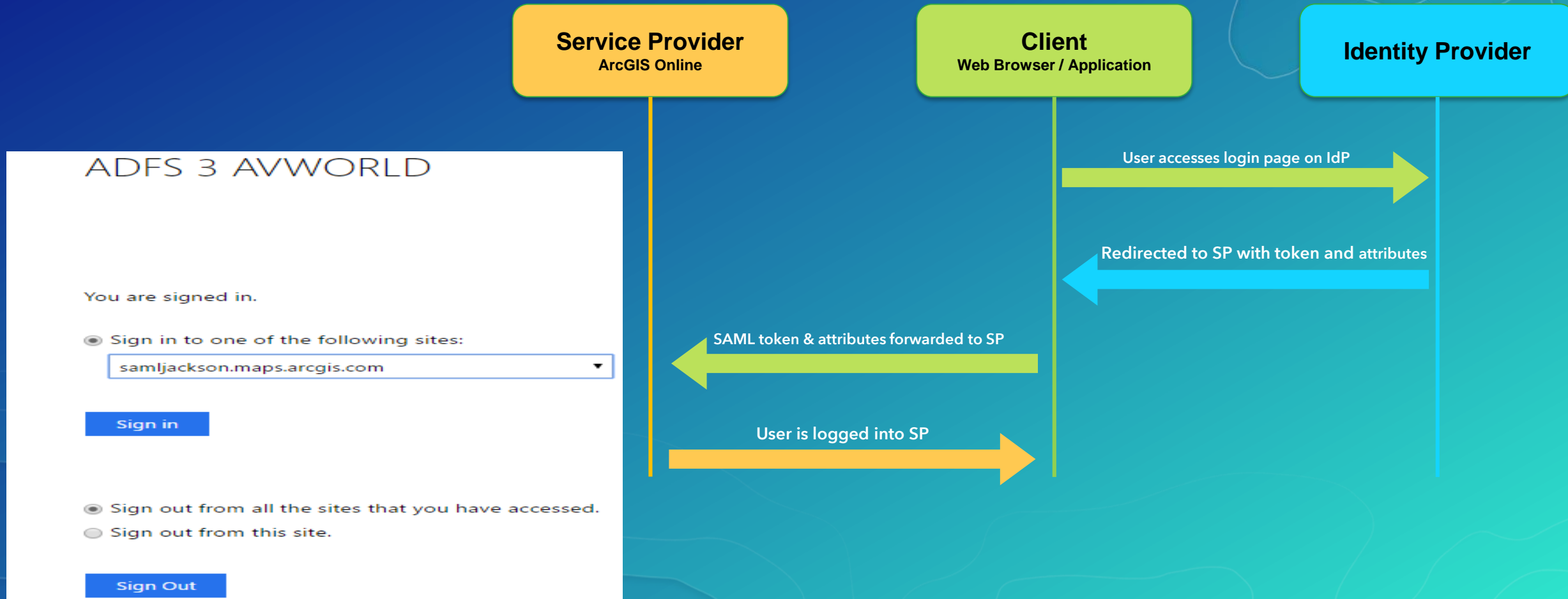
Organization URL
<https://samljackson.maps.arcgis.com>

Licensed Products
ArcGIS Pro



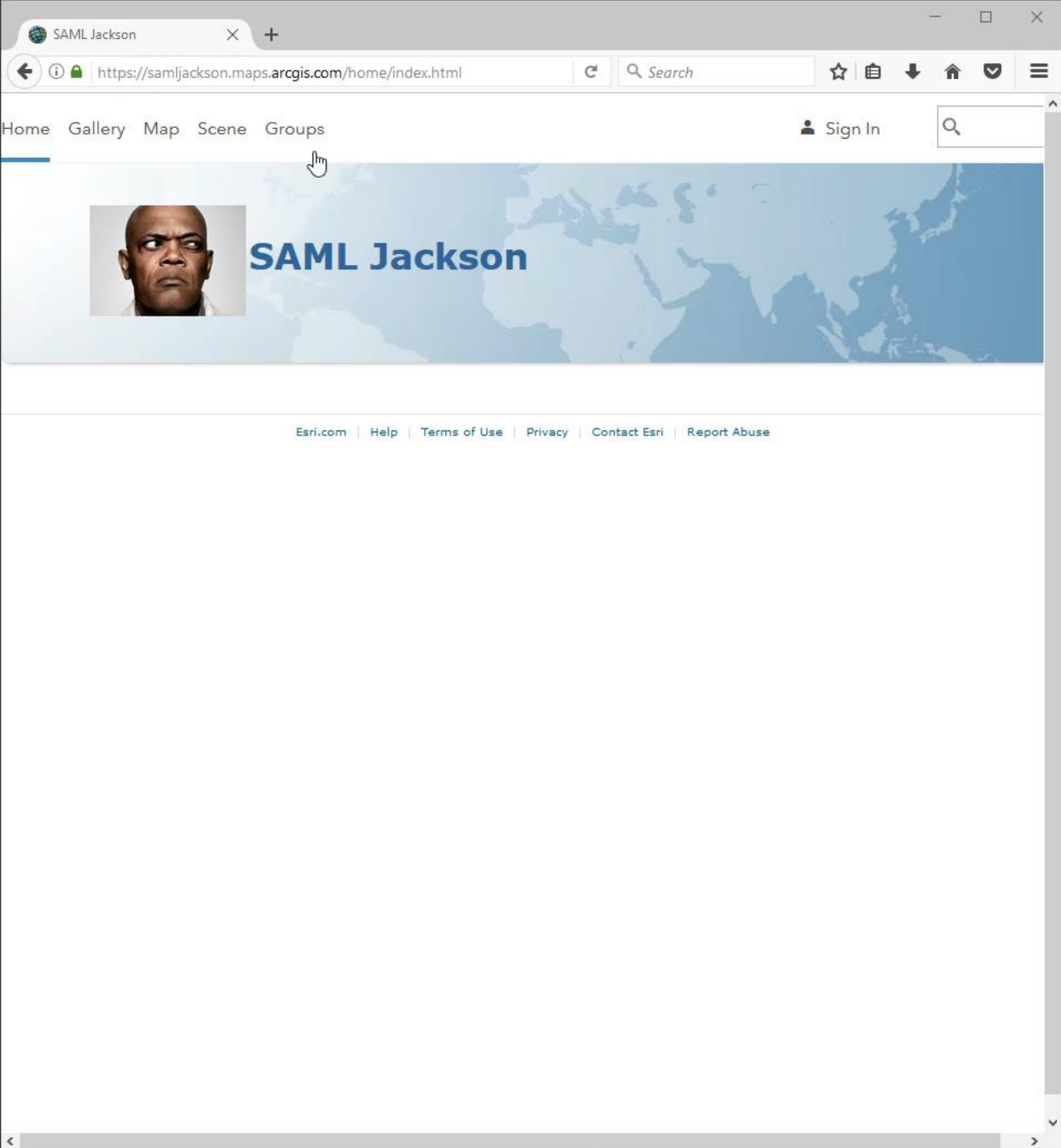
What happens during SAML authentication?

Identity Provider Initiated Log In



The background features a vibrant, abstract design. The upper portion is a textured wash of warm colors, ranging from deep red to bright orange. Below this, there are several layers of wavy, organic shapes in shades of orange, red, and pink, creating a sense of depth and movement. At the bottom of the image, a dark blue area contains a stylized, light blue map of a city grid, possibly representing a coastal urban area. The word "Demo" is centered in the middle of the image, overlaid on the orange and red background.

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/>
- **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

The background is a solid blue color with white, wavy, organic lines that resemble topographical map contours or liquid ripples. These lines are more prominent in the upper right and lower left corners, creating a sense of depth and movement.

Questions?



esri

THE
SCIENCE
OF
WHERE