Organization-Specific Logins FAQ

FORMERLY REFERRED TO AS "ENTERPRISE LOGINS"

Date: Nov. 2021
Version: 1.92

Prepared by:
Esri Software Security & Privacy Team
SoftwareSecurity@esri.com

This FAQ (Frequently Asked Questions) provides answers to common security questions related to ArcGIS Organization-specific Logins, including Best Practice recommendations for SAML, OAuth & Open ID Connect. The intended audience includes ArcGIS Admins, Security Admins, and anyone implementing or managing the security settings of ArcGIS Online and ArcGIS Enterprise.

FAQ Contents

What are the best practices for ArcGIS with SAML Organization-specific Logins?

1. **Encrypt SAML Assertions**
   SAML implementations should always utilize Encrypted Assertions to mitigate the very real risk of account compromise associated with unencrypted SAML assertions. See: "Encrypt Assertions," within this document (Page 7).

2. **Encrypt Assertions using Strong Ciphers** (use GCM ciphers instead of CBC ciphers).
   CBC ciphers should not be used when encrypting SAML assertions, instead stronger GCM ciphers should be used. CBC ciphers have known vulnerabilities that may allow an attacker to decrypt assertions using brute-force methods. This is a setting that is configured within your Identity Provider.
   See: "Should I Encrypt Assertions with using Strong Ciphers?" within this document (Page 11).

3. **Enable Signed Requests & Sign using SHA256** hashing algorithms within:
   (ArcGIS Online/Enterprise > Organization > Settings > Security > SAML Login > Configure Login > Advanced > toggle "Require Signed Requests" and "Sign using SHA256")
   See: https://doc.arcgis.com/en/arcgis-online/administer/saml-logins.htm#ESRI_SECTION1_E8C7F86C02A04A778878B1327C633B36.

4. **Enforce HTTP Strict Transport Security (HSTS)**
   See: Enforce strict HTTPS communication, within this document (Page 6).

5. **Rotate Identity Provider Signing Certificates every 1-2 years**
   This is specific to your Identity Provider, for example, ADFS rotates certificates automatically by default (https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-emergency-ad-fs-certificate-rotation#determine-whether-ad-fs-renews-the-certificates-automatically).

What are the best practices for ArcGIS with Open ID Organization-specific Logins?

1. **Limit the scope of accounts that are authorized to sign in**
   Within the OpenID Connect Authorization Service, limit the scope of accounts that are authorized to sign in for the registered client (ArcGIS Online/Enterprise). This is particularly important when working with Google Open ID and other worldwide Authorization Servers, otherwise anyone with a Google Account will be able to login to your Organization.

2. **"Let new members join" "Upon invitation from an Admin**
   Alternatively, within ArcGIS Online/Enterprise, within *Organization > Security > Open ID Connect Login configuration*, ensure "**Let new members join" "Upon invitation from an Admin"** is selected. This puts the ArcGIS Administrator in full control of who can login to the Organization.

How can I login to ArcGIS with Organization-specific Logins?

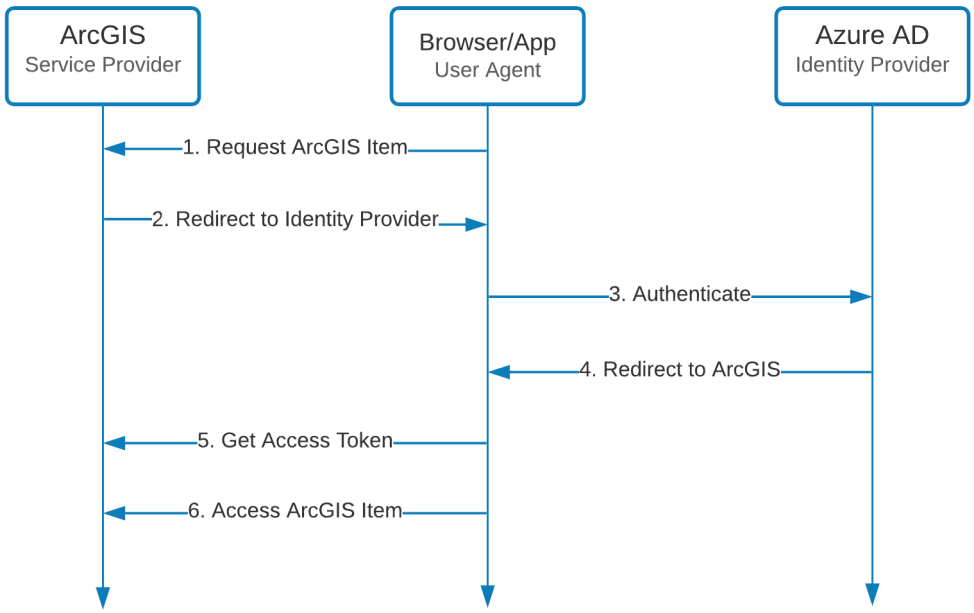
ArcGIS supports federated identity via SAML and OAuth/Open ID Connect authentication which enables your users to login with their organization accounts. With Organization-specific Logins, organizations can leverage existing security investments such multi-factor authentication, certificate authentication, and biometrics without additional administrative burden. See below for step-by-step guidance on configuring common identity providers with ArcGIS:

- Active Directory Federation Services, Azure Active Directory, Okta

How does SAML work with ArcGIS?

SAML utilizes certificate-based trust between ArcGIS (Service Provider) and your organization's Identity Provider (eg. Azure AD) to delegate the responsibility of authenticating users to your organization's Identity Provider (eg. Azure AD) instead of ArcGIS. The figure below generally describes this authentication flow:

1. User requests access to secure content hosted in ArcGIS.
2. ArcGIS redirects the user to the configured SAML Identity Provider (eg. Azure AD).
3. User authenticates (username/password, multi-factor, PKI, etc.) against the Identity Provider.
4. Identity Provider redirects user to ArcGIS, providing an Assertion of the user's identity.
5. ArcGIS validates the Assertion and provides an Access Token.
6. User requests secure content granted by the Access Token.



For more details see: Configure SAML Logins.

What is a SAML Assertion?

A SAML Assertion is XML identity passed from Identity Provider (eg. Azure AD, ADFS) to a Service Provider (eg. ArcGIS Online) by the User Agent (eg. your browser) following authentication. See the example below:

```
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">[redacted]</NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData InResponseTo="_tKlvMBYhZxCgCgPy"
      NotOnOrAfter="2021-01-08T23:58:37.588Z" Recipient="https://[redacted].maps.arcgis.com/sharing/rest/oauth2/saml/signin"/>
  </SubjectConfirmation>
</Subject>
```

In most cases the above Assertion is passed as a front-channel workflow and as such, is vulnerable to snooping and tampering. To address these risks, ensure the following are configured:

1. Enforce strict HTTPS communication
2. Enable Signed Requests & Assertions
3. Encrypt Assertions

Enforce strict HTTPS communication

Both Identity Provider and Service Provider systems involved in SAML Auth flows should require HTTPS and enable HSTS. As of December 8th, 2020, ArcGIS Online requires HTTPS via HSTS. If you are working with ArcGIS Enterprise, see: Enforce strict HTTPS communication for details on how to enable HSTS as well as HTTPS. Finally, refer to Identity Provider's documentation for to configure HTTPS and HSTS support.

Enable Signed Requests & Assertions

By enabling Signed Requests, the Service Provider (eg. ArcGIS Online) will sign authentication messages passed to the Identity Provider (eg. Azure AD) to verify the source (ArcGIS) is trusted. This setting is enabled within your ArcGIS Online / Enterprise Organization > Settings > Security > Logins > SAML login settings > Advanced Settings:

To ensure Assertions are signed, refer to your Identity Provider's documentation. Also see:

- Change certificate signing options and signing algorithm (Azure AD)
- Setup SAML Logins (ArcGIS Online)
- Best Practices for SAML security (ArcGIS Online)

Encrypt Assertions

Encrypting the SAML Assertion provided by the identity provider effectively converts the XML data structure into an encrypted block that prevents attackers from tampering with and replaying Assertions:

```
<Modulus>uAfz9e+CGUiSGP3LH9Hq4OaD468ZCaJp35doNWsHsO1NaNzb6lF1uv7r97L+2nHt9P0JF6A8SZVd&#xd;
nVMCQu4fgaKyH9lG7d/UHCXXKDK8PbZRhb1hEu1KGfBNkR0kO8QQhKKwSbkFLZ8Ln+Kes5RfX27l&#xd;
tMMM7fh1lfQSB82JJtMclyBA9MjoruWCHHP3kfJXdp77qpaDcvD+vKuieLuJcfkrwsb25VyA0c/T&#xd;
liUYo6ea5PVj936v4CzDyDuFaLo/ablnFf8ZOb5pIlUl3wAMYK+fcwe/P9RdX0uzjq9Ndn8+5oxO&#xd;
8fcsa7LT1G+pyJTsGRx9Lpp2Yk56kBs4tJ8wHQ==</Modulus>
```

To configure Encrypted Assertions, consider the following:

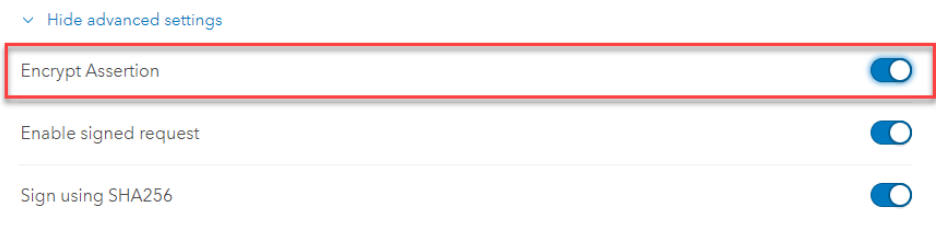
1. The Assertion must be encrypted by the Identity Provider (eg. Azure AD), using the public key supplied by the Service Provider (eg. ArcGIS Online). To do this, extract the certificate value:

   <ds:X509Certificate>PhDf……..9P5u==</ds:X509Certificate>

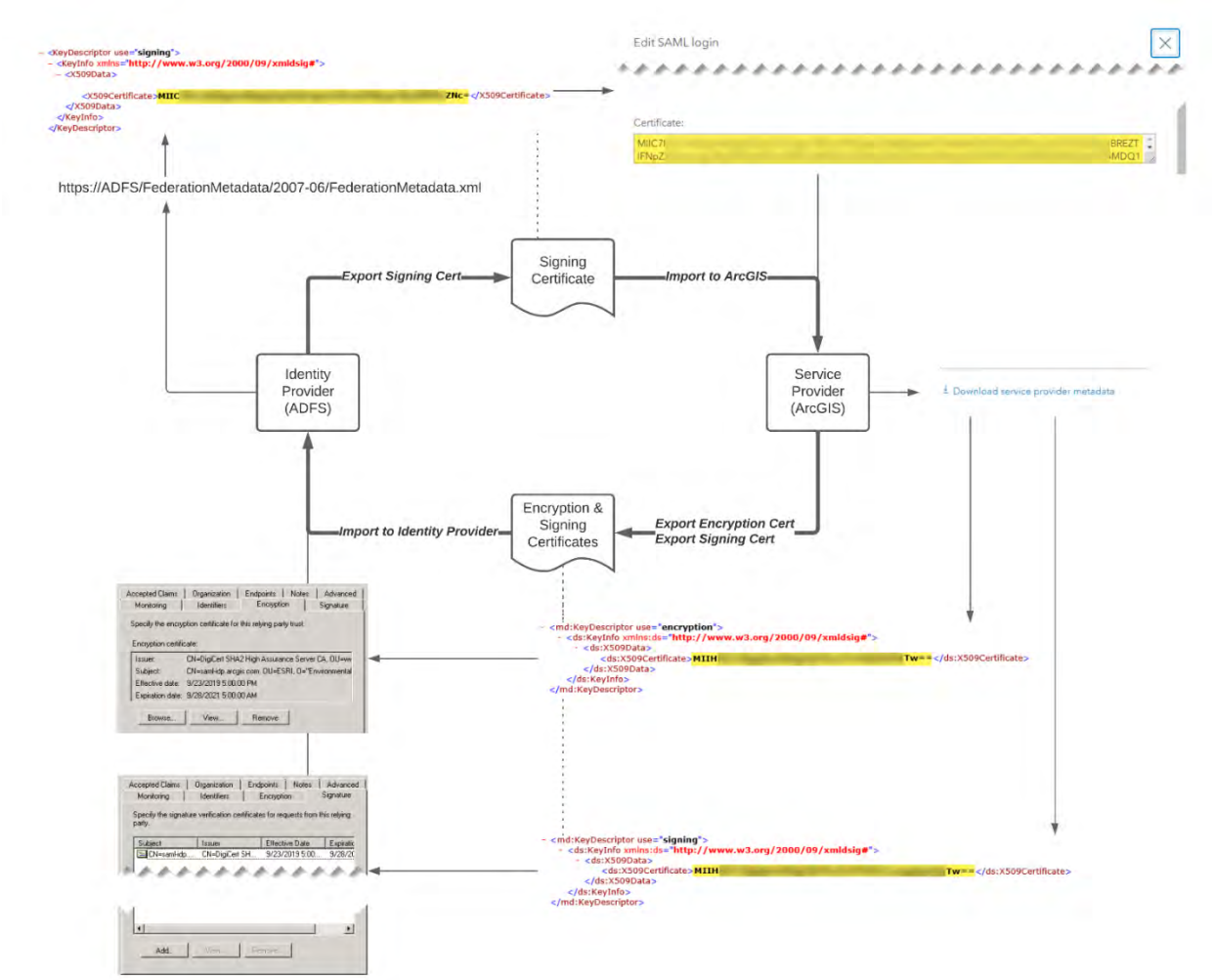
   from the ArcGIS Online Service Provider Metadata (ArcGIS Online Organization > Settings > Security > SAML login > Download Service Provider Metadata) and import this to your Identity Provider. (The above string can be saved to a text file (eg. samlsp.cer) and imported as a file if needed.)

   For information on where to import the Service Provider certificate see your Identity Provider's documentation: [How to: Configure Azure AD SAML token encryption]

2. ArcGIS Online must be configured to treat the inbound assertion as encrypted by toggling "Encrypt Assertion" within ArcGIS Online Organization > Settings > Security > SAML login > Advanced Settings > Encrypt Assertion.



How do I manage Certificates for SAML Encryption & Signing?



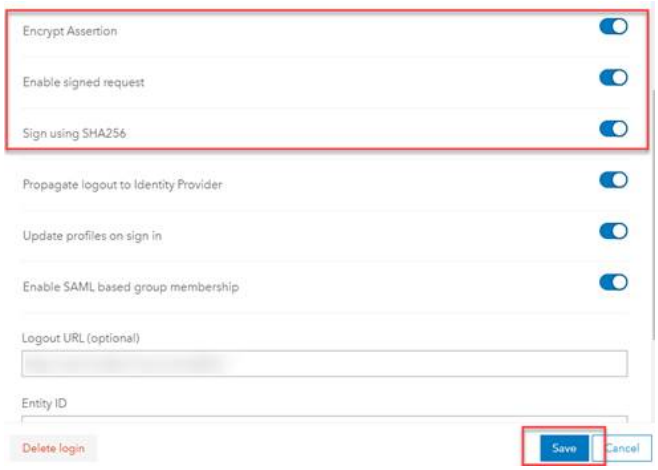
1. Ensure “Encrypt Assertion” and “Enabled signed request” are enabled within the ArcGIS Online Organization’s SAML login configuration.
   (Org > Settings > Security > Logins > SAML Login > Configure login)
2. Obtain the ArcGIS encryption & signing certificates from the ArcGIS Organization’s service provider metadata.
   (Org > Settings > Security > Logins > SAML Login > Configure login > service provider metadata)
3. Import the encryption & signing certificates into the identity provider (IDP).
4. Obtain the identity provider’s signing certificate from its federation metadata.
5. Import the certificate associated with the identity provider (IDP) into ArcGIS.
   (Org > Settings > Security > Logins > SAML Login > Configure login > Certificate)

For more details on Best practices for SAML Security see: https://doc.arcgis.com/en/arcgis-online/administer/saml-logins.htm#ESRI_SECTION1_E8C7F86C02A04A778878B1327C633B36

Where can I find Signing & Encryption Certificates?

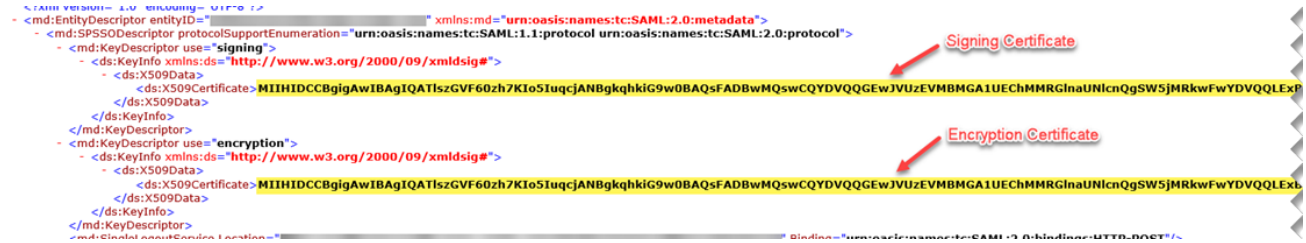
Signing & encryption certificates for ArcGIS Online SAML configuration are embedded in the service provider metadata XML file (`ORGNAME_sp_metadata.xml`) which can be downloaded from *ArcGIS Online (Org) > Settings > Security > Logins > SAML Login > Configure login > Download service provider metadata*. Here is the step by step process:

1. Ensure "***Encrypt Assertion***" and "***Enabled signed request***" (and ***Sign using SHA265*** as a best practice) are enabled within the ArcGIS Online Organization's SAML login configuration. (*Org > Settings > Security > Logins > SAML Login > Configure login > Encrypt Assertion | Enable signed request | Sign using SHA256 >* ***Save***).



2. Download the *service provider metadata* XML file (`ORGNAME_sp_metadata.xml`) from *Org > Settings > Security > Logins > SAML Login > Configure login >* ***Download service provider metadata*****.**

3. This will yield the following file the *service provider metadata* XML file (`ORGNAME_sp_metadata.xml`). If we open this file, we will see the *Signing Certificate* & *Encryption Certificate* contained within:



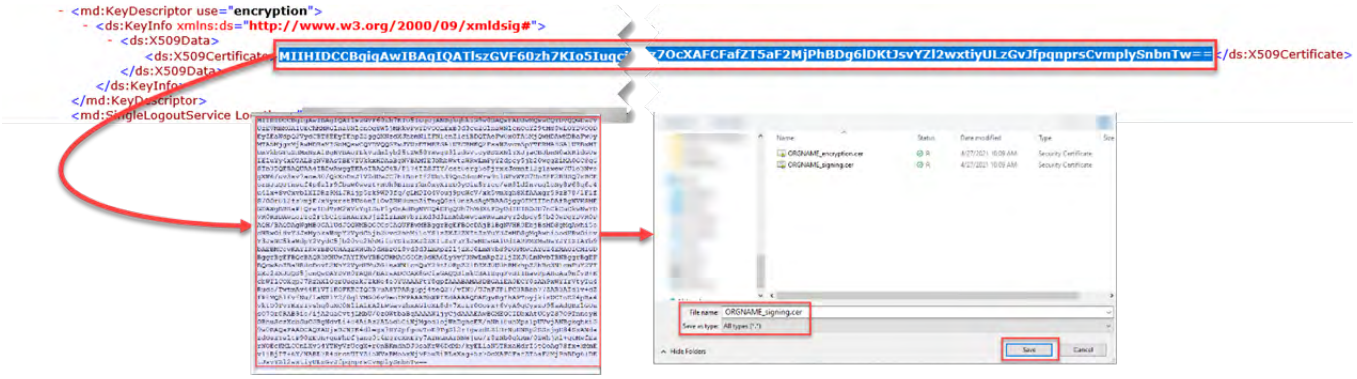
4. The service provider metadata XML file (`ORGNAME_sp_metadata.xml`) can typically be ingested and automatically configured by the Identity Provider (IDP), but if necessary these can be manually extracted into a text file such as `ORGNAME_encryption.cer` and `ORGNAME_signing.cer` files if required. Let's assume we need to do that, here is the process:

a. To save the **signing certificate**, open the downloaded `ORGNAME_sp_metadata.xml`:

i. *Copy* the *long string* of random-looking characters that fall between the `<ds:X509Certificate>` & `</ds:X509Certificate>` within the `<md:KeyDescriptor use="signing">` tag.

ii. **Paste** the long string into any text editor.

iii. Save the file as `ORGNAME_signing.cer` (ensure *Save as type:* is set to "*All types (*.*)*"):

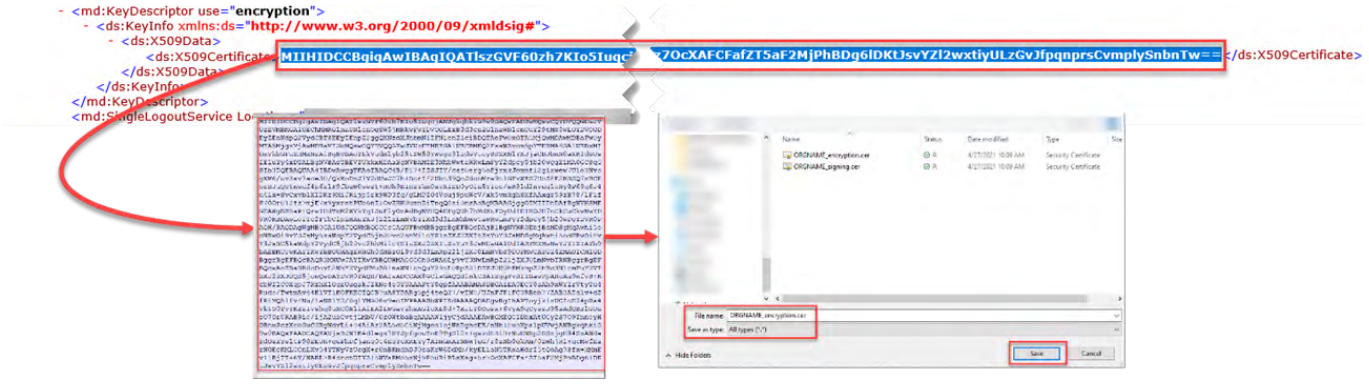


b. To save the **encryption certificate** open the downloaded `ORGNAME_sp_metadata.xml`:

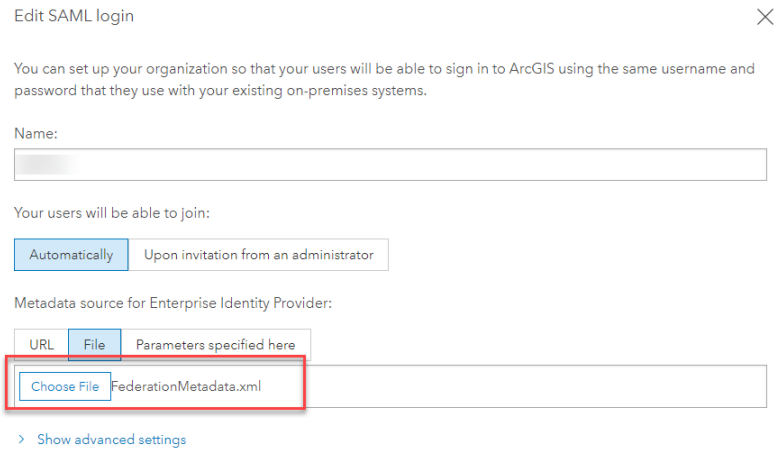
i. **Copy** the **long string** of random-looking characters that fall between **the** `<ds:X509Certificate>` & `</ds:X509Certificate>` within the `<md:KeyDescriptor use="encryption">` tag.

ii. **Paste** the **long string** into any text editor.

iii. Save the file as `ORGNAME_encryption.cer` (ensure *Save as type:* is set to "*All types (*.*)*"):



5. Once you have the **service provider metadata** XML file (`ORGNAME_sp_metadata.xml`), `ORGNAME_encryption.cer`, and `ORGNAME_signing.cer`, you have everything you need to configure any Identity Provider (IDP) to use ArcGIS Online as a SAML Service Provider (SP). See your Identity Provider's documentation on how to ingest these files as part of their SAML configuration.
6. To complete the configuration (to configure ArcGIS Online to use your Identity Provider (IDP)):
   a. **Export** the `FederationMetadata.xml` from your Identity Provider.
   (See step 6 of: https://doc.arcgis.com/en/arcgis-online/administer/configure-adfs.htm#GUID-6E16C8E9-9FFD-4D89-8FBB-E08828B5369F for guidance on how to obtain the FederationMetadata.xml from ADFS.)



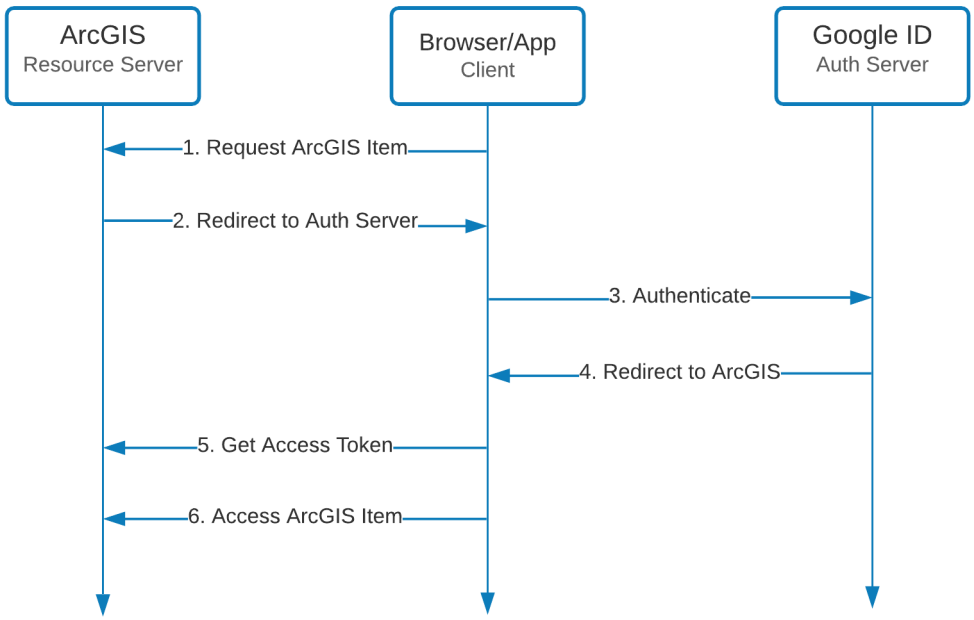
Should I Encrypt Assertions with using Strong Ciphers?

Yes. All ciphers are not equal, and not all SAML Identity Providers use strong ciphers by default. For example, ADFS 2.0 by default utilizes CBC based ciphers which have known weaknesses as described here: https://docs.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode. **Instead, SAML Identity Providers should be configured to use stronger, GCM-based ciphers**. In the case of ADFS 2.0, use the following guidance to exclude the weaker CBC-based ciphers in lieu of stronger GCM-based ciphers: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/manage-ssl-protocols-in-ad-fs#enabling-or-disabling-additional-cipher-suites.

How does OAuth / Open ID work with ArcGIS?

OAuth and its extension Open ID utilize an arrangement of App IDs and approved Redirect URL allowlists to delegate the responsibility of authenticating users to an OAuth/Open ID Auth Server (eg. Google ID). Because the OAuth standard doesn't provide a way to identify users, Open ID extends OAuth to require a JWT (Java Web Token) which contains user identity information. The figure below describes this authentication flow:

1. User requests access to secure content hosted in ArcGIS.
2. ArcGIS redirects the user to the configured Auth Server (eg. Google ID).
3. User authenticates (username/password, multi-factor, PKI, etc.) against the Auth Server.
4. Auth Server redirects user to ArcGIS, providing an JWT that includes the user's identity.
5. ArcGIS validates the JWT, then provides an Access Token.
6. User requests secure content granted by the Access Token.



For guidance on setting up OpenID Connect logins see: Set up OpenID Connect logins with ArcGIS.

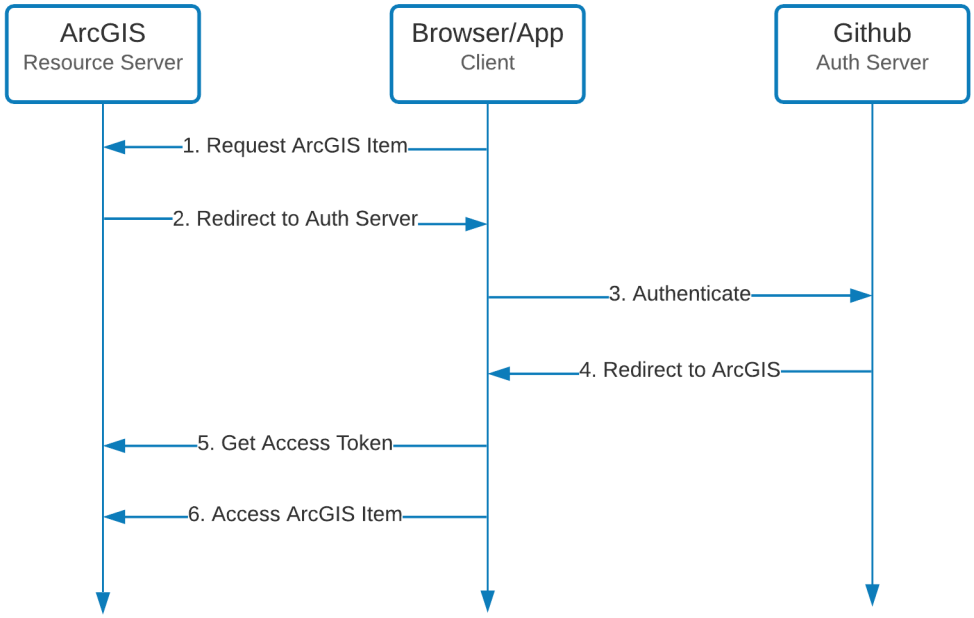
Can I also login with my Social Logins?

Yes. ArcGIS includes native support for several social network logins including Facebook, Google, Apple, and Github via OAuth. For information on globally or individually enabling/disabling social login support see: Configure security settings—Social logins

How do Social Logins work with ArcGIS?

Social Logins allow ArcGIS to delegate authentication to social networks' (eg. Facebook, Github, Google, Apple) OAuth Servers. Since these are OAuth flows, they follow a similar pattern to OAuth/Open ID:

1. User requests access to secure content hosted in ArcGIS.
2. ArcGIS redirects the user to the Social Login's Auth Server (eg. Github).
3. User authenticates (username/password, multi-factor, PKI, etc.) against Auth Server.
4. Auth Server redirects user to ArcGIS.
5. ArcGIS validates the OAuth state, then provides an Access Token.
6. User requests secure content granted by the Access Token.



For guidance on setting up Social Logins with ArcGIS see: Configure Social Logins with ArcGIS.

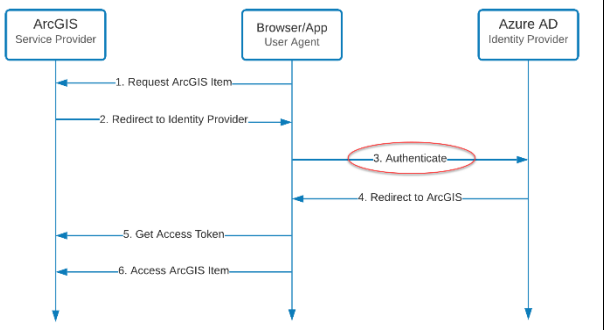
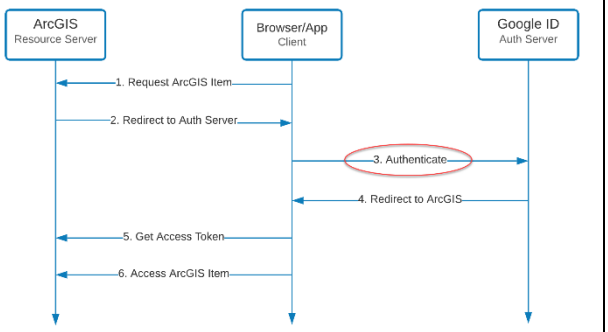
Can I login from multiple sources?

Yes, for example, ArcGIS can be configured to use Azure AD as a SAML 2.0 provider, Google Identity as an Open ID Connect provider, Github as a Social Login, and ArcGIS built-in accounts at the same time. Organizations may also support multiple concurrent SAML providers by configuring a Federation of Identity Providers.

Does ArcGIS Online store my Organization-specific Login password?

No. The diagrams below show the generic auth flows for SAML, OAuth/OpenID Connect when using Organization-specific Logins. As step 3 shows, the identity provider/auth server handles

and stores authentication credentials such as passwords, not ArcGIS. Once authenticated, users are redirected to ArcGIS for access.

SAML Auth Flow	OAuth / Open ID Connect / Social Auth Flow
	

Multi-factor Authentication (MFA)

Multi-factor Authentication requires users supply at least two distinct authentication methods such as a username/password + authenticator app making it highly effective at thwarting common attack vectors including Phishing and Spoofing. For details on enabling MFA for built-in accounts in ArcGIS Online see: Multifactor Authentication. For Organization-specific Logins, multi-factor authentication is configured within the Identity Provider. Refer to your Identity Provider's documentation to enable and configure this capability:

- How it works: Azure AD Multi-Factor Authentication (Azure AD)
- Microsoft Authenticator (Microsoft)

If Organization-specific Logins are enabled for ArcGIS, will users be automatically added?

When Organization-specific Logins are enabled, the administrator decides if they want to provide users with the ability to automatically join the organization or if the user must be invited. Administrators may also pre-import a list of users in bulk. For details on configuring this feature see: Configure SAML logins.

Is setting the "join automatically" or "by invitation" a one-time decision?

No, this configuration choice can be changed at any time.

What are the risks associated with allowing Organization-specific logins to "automatically join" and how can I mitigate them?

Depending on identity provider configuration, allowing Organization-specific logins to automatically join ArcGIS opens your ArcGIS organization to any users that can successfully authenticate against configured identity providers. To mitigate this risk, configure your identity provider/auth server to permit or deny sign in to ArcGIS based on a common criteria such as group membership. Refer to your identity provider's documentation to configure this feature:

- Create a Rule to Permit or Deny Users Based on an Incoming Claim (ADFS)
- Manage user assignment for an app in Azure Active Directory (Azure AD)

Does the ArcGIS Platform support both SP-Initiated logins and IDP-Initiated logins?

Yes. Both SP-Initiated logins and IDP-Initiated logins are supported. For details on SP-initiated logins vs IDP-initiated logins with ArcGIS see: SAML sign in experience.

Are there any reasons that ArcGIS Logins might be needed if using Organization-specific Logins?

ArcGIS Online Logins are useful for customers who want to provide access to collaborators external to their organization (e.g., contractors), for temporary access/testing, or service accounts. For example, an ArcGIS Online Login may be required to troubleshoot issues related to IDP failures or misconfigurations that result in users being unable to access ArcGIS Online Content.

What SAML providers does ArcGIS support?

Esri has documented the configuration of several SAML identity providers in the help documentation. More extensive implementation guidance is available for some IDPs at Trust.ArcGIS.com and include FAQ's such as this document. Theoretically, any SAML 2.0 or OAuth 2.0 compliant provider is configurable with ArcGIS. Below is a non-exhaustive list of IDPs that customers have successfully implemented with ArcGIS Online:

- Azure Active Directory
- Active Directory Federation Services (AD FS) 2.0 and later
- NetIQ Access Manager 3.2 and later
- OpenAM 10.1.0 and later
- Shibboleth 2.3.8 and later
- SimpleSAMLphp 1.10 and later
- CA SiteMinder 12.52 and later

- Okta SSO

Contact technical support if you are working with an IDP Esri has not documented.

If a user already has an existing ArcGIS Online Login does the Enterprise Login replace it?

No. A new account is created. Content may need to be migrated to the new account.

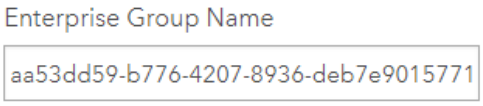
Can user roles be assigned in the identity provider?

No. Roles for ArcGIS users regardless of where they signed in from are managed within your ArcGIS > Organization > Members by users granted the "Administrator" role.

Can groups from a SAML based IDP be linked to ArcGIS Groups?

Yes. Enterprise groups from a SAML based IDP may be linked to ArcGIS Enterprise Groups, enabling item access management to flow from group assignments within your organization's security store.

1. Enable SAML based group membership within ArcGIS Organization security settings for your identity provider.



Enable SAML-based Group Membership

When is the best time to enable Organization-specific Logins?

It is best to enable Organization-specific Logins early in the deployment, prior to provisioning users if possible. The Organization-specific Logins establishes a new account, so if users join using an ArcGIS Online login (and add content), their content will need to be migrated to their Organization-specific Logins account. All users consume a named user license, meaning that when both Organization-specific Logins and Built-in logins exist for a single individual, two licenses are consumed until one of the logins is removed.

Does ArcGIS Enterprise support Organization-specific Logins?

Yes, beginning with ArcGIS 10.3 Esri added SAML compliant logins to ArcGIS Enterprise. In addition to SAML based enterprise logins, Active Directory, LDAP and other authentication methods are supported.

Does ArcGIS Maps for Office support Organization-specific Logins?

Yes, but Esri Maps for Office must be configured to log in to the Organization-specific URL. Go to File->Esri Maps and change the ArcGIS Connection URL. This option can also be configured during install.

Can organizations use the same identity provider (IDP) account to provide access to multiple ArcGIS Online organizations?

Yes, the same IDP can be federated to multiple ArcGIS Online or ArcGIS Enterprise Organizations. The ArcGIS Platform treats each organization as a separate tenant, requiring logins for each organization.

Can an ArcGIS Online organization support multiple Identity Providers?

As of the June 2018 release ArcGIS Online now supports identity federation. SAML IDP solutions themselves can use multiple user stores such as one from Microsoft Active Directory and one from LDAP to support these types of diverse needs.

What options are available for supporting internal users and public field workers with ADFS (Active Directory Federation Services)?

Organizations that need to provide Enterprise Login support to external clients (such as field workers) must allow inbound HTTPS connections to their Identity Provider (e.g. ADFS) from the public internet.

What is a common reason for ArcGIS Online being unable to validate a SAML Response from an identity provider (IDP)?

This is most often caused by expiration of the signing certificate supplied by the Identity Provider to ArcGIS Online / Enterprise. To resolve this, re-import the Federation Metadata provided from

the Identity Provider into ArcGIS Online / Enterprise under Organization > Settings > Security > SAML Login > Metadata source for Enterprise Identity Provider.