ArcGIS Platform FAQ
Enterprise Logins via SAML 2.0

Date: September 10, 2018
Version: 1.6

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

What are Enterprise Logins? ......................................................................................................... 1
Can an organization use both Enterprise Logins and ArcGIS Logins? ........................... 1
If an organization configures Enterprise Logins will the user still have to enter a user name and password? .............................................................................................................. 1
If Enterprise Logins are enabled for an ArcGIS Online Organization, will users be automatically added? ........................................................................................................................ 1
Is setting the “auto-join” or “by invitation” a one-time decision? .............................. 1
Does the ArcGIS Platform support both SP-Initiated logins and IDP-Initiated logins? ..................................................................................................................................................... 1
Are there any reasons that ArcGIS Logins might be needed if using Enterprise Logins? .......................................................................................................................................................................................... 1
What Enterprise Identity Providers (IDPs) does ArcGIS support? .............................. 2
Do Enterprise Logins require that everyone in the identity provider (IDP) store be provided a login to the ArcGIS Online Organization? .............................................................................. 2
If a user already has an existing ArcGIS Online Login does the Enterprise Login replace it? .............................................................................................................................................. 3
How do customers migrate content in the same organization from one account to another? .............................................................................................................................................. 3
Can user roles be assigned in the identity provider? ........................................................... 3
Can enterprise groups from a SAML based IDP be linked to ArcGIS Enterprise Groups? .................................................................................................................................................. 3
When is the optimal time to enable Enterprise Logins? ..................................................... 3
Do Enterprise Logins apply the same to ArcGIS Enterprise? ............................................ 3
Should an ArcGIS Online or ArcGIS Enterprise Login from the default user store be deleted if a user is provided an Enterprise Login? .............................................................................. 3
Does Esri Maps for Office support Enterprise Logins? ........................................................ 3
Can organizations use the same identity provider (IDP) account to provide access to multiple ArcGIS Online organizations? .......................................................................................................................... 4
Does an organization need to deploy the identity provider (IDP) to a public network to support Enterprise Logins? .......................................................................................................................... 4
Can an ArcGIS Online organization support multiple Identity Providers? ............................ 4
What options are available for securely supporting internal users with ADFS (Active Directory Federation Services)? .......................................................................................................................... 4
How does an organization configure ArcGIS Online to work with an identity provider (IDP) deployed to a private network? .......................................................................................................................... 5
What are the benefits to exposing the identity provider (IDP) to a public network?
................................................................................................................................................................... 5

What options are available for supporting internal users and public field workers with ADFS (Active Directory Federation Services)?............................................................. 5

What are the risks to exposing the identity provider (IDP) to a public network? ...6

What is a common reason for ArcGIS Online being unable to validate a SAML Response from an identity provider (IDP)?.................................................................6

Are Enterprise Logins integrated with Esri applications beyond ArcGIS Online and ArcGIS Enterprise?.................................................................................................6
What are Enterprise Logins?
Enterprise logins allow an organization’s members to log into ArcGIS Online and ArcGIS Enterprise using the same logins that they use to access their other enterprise systems such as Microsoft Active Directory or LDAP via the security standard SAML 2.0. Over 300 ArcGIS Online organizations have implemented Enterprise Logins.

Can an organization use both Enterprise Logins and ArcGIS Logins?
Yes, in fact when the user goes to the Organization’s ArcGIS Online or ArcGIS Enterprise URL, they will be presented with both options by default. When working with ArcGIS Online, the option to use an Enterprise Login will only be available from the Organization’s URL, a user will not see this option from the main ArcGIS.com login page. Organizations may disable the ability to log in with ArcGIS Online or Portal for ArcGIS built-in identity stores, allowing only Enterprise logins.

If an organization configures Enterprise Logins will the user still have to enter a user name and password?
Perhaps. This feature depends on Identity Provider (IDP) support for Single Signon and the browser (Internet Explorer passes credentials automatically in a Windows infrastructure). There may be situations where the user is required to enter their enterprise user name and password.

If Enterprise Logins are enabled for an ArcGIS Online Organization, will users be automatically added?
No, when Enterprise Logins are enabled, the administrator has the option to determine if they want to provide the users with the ability to automatically join the organization or if the user must be invited. ArcGIS Enterprise administrators may import a list of enterprise users in bulk using the supplied command line tools.

Is setting the “auto-join” or “by invitation” a one-time decision?
No, this configuration option can be changed at any time.

Does the ArcGIS Platform support both SP-Initiated logins and IDP-Initiated logins?
Yes, Both SP-Initiated logins and IDP-Initiated logins are supported. The option to sign in using an ArcGIS account directly from the enterprise’s login manager is not available with IDP logins. To sign in to the organization using ArcGIS accounts, members need to access their organization website directly.

Are there any reasons that ArcGIS Logins might be needed if using Enterprise Logins?
ArcGIS Online Logins are useful for customers who want to provide access to collaborators external to their organization (e.g., contractors). Esri applications supporting Enterprise Logins include:
Native apps built on ArcGIS Runtime currently only support Portals that are configured with SP initiated logins. Any app that opens in a web browser, or can display a web view within the app, is capable of using IdP initiated logins.

**What Enterprise Identity Providers (IDPs) does ArcGIS support?**
Esri has documented the configuration of several IDPs in the help documentation. More extensive implementation guidance is available for some IDPs. These are published to the [Trust.ArcGIS.com](https://www.Trust.ArcGIS.com) best practices site, and include FAQ’s such as this document.

Theoretically, any SAML 2.0 compliant provider is configurable with ArcGIS Online or ArcGIS Enterprise. Below is a non-exhaustive list of IDPs that customers have successfully implemented with ArcGIS Online:

- 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.

**Do Enterprise Logins require that everyone in the identity provider (IDP) store be provided a login to the ArcGIS Online Organization?**
No, but this is dependent on the IDP capabilities. For example, groups can be configured in Active Directory that are then used to federate with ArcGIS Online.
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.

How do customers migrate content in the same organization from one account to another?
Techniques for moving content between users vary, depending on the quantity of content that the user owns. If the user owns little content, this can be done manually using the existing ArcGIS Online tools. If the user owns considerable content, [python scripts](#) are available to support automating the process of migrating items and group memberships in bulk.

Can user roles be assigned in the identity provider?
No, the identity provider only provides the authentication, the authorization is still provided by ArcGIS Online or ArcGIS Enterprise. Administrators may define a default role for Portals configured to allow users to automatically join. If users join by invitation, the role can be established prior to them joining.

Can enterprise groups from a SAML based IDP be linked to ArcGIS Enterprise Groups?
Yes. At ArcGIS 10.6, [enterprise groups from a SAML based IDP may be linked to ArcGIS Enterprise Groups](#).

When is the optimal time to enable Enterprise Logins?
It is best to enable Enterprise groups early in the deployment, prior to provisioning users if possible. The Enterprise Login 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 Enterprise Login account. All users consume a named user license, meaning that when both Enterprise IDP based and built-in logins exist for a single individual, two licenses are consumed until one of the logins is removed.

Do Enterprise Logins apply the same to ArcGIS Enterprise?
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.

Should an ArcGIS Online or ArcGIS Enterprise Login from the default user store be deleted if a user is provided an Enterprise Login?
Yes, if the user doesn’t have a need for it, and the content has been migrated, the account can be deleted or disabled.

Does Esri Maps for Office support Enterprise Logins?
Yes, but Esri Maps for Office has to 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.

Does an organization need to deploy the identity provider (IDP) to a public network to support Enterprise Logins?
No, Enterprise Logins will function normally with an IDP deployed to a private network. The only requirement is that the client (web browser, mobile device, ArcGIS Desktop) can connect to the IDP on the private network.

Can an ArcGIS Online organization support multiple Identity Providers?
As of the June 2018 release ArcGIS Online now supports identity federation. Many SAML IDP solutions themselves can utilize 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 securely supporting internal users with ADFS (Active Directory Federation Services)?
Figure 1 below illustrates a typical “Internal Network” which provides proof of concept and security through isolation. In this model, clients will (1) establish an outbound HTTP/HTTPS connection to ArcGIS Online, and then (2) be referred to the ADFS server for authentication. This pattern is recommended for organizations with all internal users and/or VPN support for external users.

Figure 1 - ArcGIS Online SAML 2.0 Federation (Internal Users)
How does an organization configure ArcGIS Online to work with an identity provider (IDP) deployed to a private network?
Instead of providing an URL to ArcGIS Online, upload the IDP metadata file as described in “Step 3,” of the, “Set up your organization with an enterprise identity provider”.

What are the benefits to exposing the identity provider (IDP) to a public network?
A publicly deployed IDP enables field workers, data collectors, or other users without access to the private network to use their organization credentials with ArcGIS Online.

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 provide a means for clients to establish outbound HTTP/HTTPS connections to their Identity Provider (ADFS.) From an ArcGIS Online perspective, organization can meet this need by allowing public networks inbound access to their ADFS deployment. Organizations may further enhance the security of this pattern by deploying an “ADFS Proxy” in their DMZ, as shown in Figure 2 below. For information on how to deploy the ADFS Proxy role in you environment, refer to Microsoft’s guidance.

Figure 2 - ArcGIS Online SAML 2.0 Federation (Internal & External Users)
What are the risks to exposing the identity provider (IDP) to a public network? Providing public network access to resources does impart risk, particularly when that system is responsible for processing authentication. Esri's Security Standards & Architecture team is also available to provide ArcGIS security consulting services to help ensure the security and productivity of your GIS.

What is a common reason for ArcGIS Online being unable to validate a SAML Response from an identity provider (IDP)? This failure could be caused when ArcGIS Online is trying to validate an incoming encrypted assertion. In order for ArcGIS Online to process an assertion provided by an IDP, ensure the assertions being sent to ArcGIS Online are not encrypted and do not require signing, as those capabilities are currently not supported by ArcGIS Online.

Are Enterprise Logins integrated with Esri applications beyond ArcGIS Online and ArcGIS Enterprise? No. Many organizations do not want to automatically integrate their Enterprise Logins with applications beyond ArcGIS Online or ArcGIS Enterprise to ensure a strong, segmented security posture that support a FISMA security accreditation. For Enterprise logins, Esri maintains very little information on the user as all information about the user is handled by the customer's own enterprise systems. To use Esri.com apps, an Enterprise Login user would need to create a separate account at http://accounts.esri.com which will be separate from their Enterprise Login organization account.