

Last Modified: June, 29, 2016

ArcGIS Online is a complete, Cloud-Based Mapping Platform. ArcGIS Online comes with a suite of basemaps, high-resolution imagery, and the highest rated demographic data. Using it user can create 2D and 3D maps with the built-in map viewer and scene viewer.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and ArcGIS.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

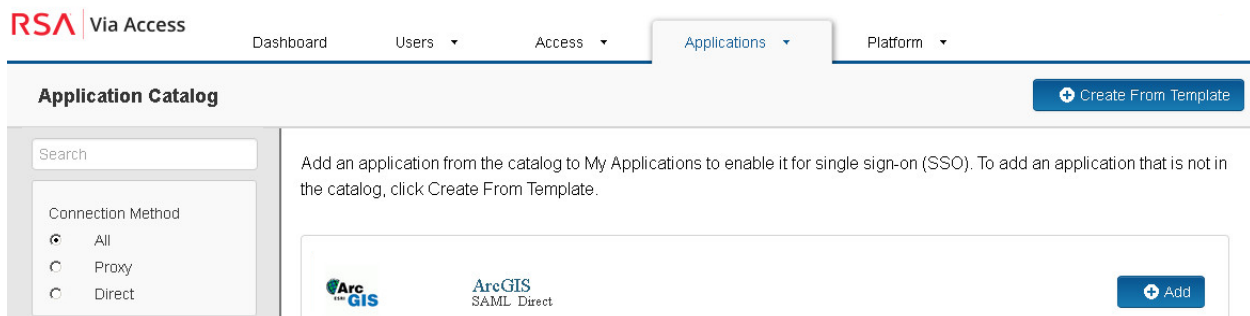
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure ArcGIS to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure


1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for ArcGIS.



3. On the Basic Information page, specify the application name and click **Next Step**.

 **Note:** The following SP-initiated configuration works for both IDP-initiated and SP-initiated connections.

4. On the Connection Profile page, choose **SP –initiated** and modify the Connection URL by replacing **<DOMAIN>** with your account domain name.
5. Select binding method **POST**.


Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded


6. Scroll down to **SAML Identity Provider (Issuer)** section.

Identity Provider URL 

Issuer Entity ID 

Default (idp_id): arcgistest

Override

SAML Response Signature 

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

 Private Key Loaded



 Certificate Loaded

CN=gs.local, Valid Until:
12/10/2019

Include Certificate in Outgoing Assertion

- a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure ArcGIS.
- b. Select **Choose File** and upload the private key.
- c. Select **Choose File** and upload the public certificate.
- d. Select the checkbox **Include Certificate in Outgoing Assertion**.

7. Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.maps.arcgis.com/sharing/rest/oauth2/saml/signin

Audience (Service Provider Entity ID) ?

<DOMAIN>.maps.arcgis.com

- a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your account domain name.
 - b. In the **Audience (Service Provider Entity ID)** field, replace <DOMAIN> with your account domain name.
8. Scroll down to the User Identity section. Select **Email Address** for Identifier Type and Property **mail**.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

9. Click **Show Advanced Configuration**.

10. Scroll down to **Uncommon Formatting SAML Response Options**, select **Assertion within response**.

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

Entire SAML response Assertion within response

Signature Algorithm rsa-sha1 ▼

Digest Algorithm sha1 ▼

Encrypt Assertion

 No certificate loaded

Choose File

Encryption Algorithm Triple DES ▼

Encryption Key Transport RSA15 ▼

Relay State URL Encoding

Receive Relay State URL - encoded by SP (in incoming request)

Send Relay State URL - encoded by IDP

Include Issuer NameID Format

NameID Format Unspecified ▼

11. Click **Next Step**.

12. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed ▼

Cancel

Next Step →

13. Click **Next Step**.

14. On the **Portal Display** page, select **Display in Portal**.
15. Click **Save and Finish**.
16. Click **Publish Changes**. Your application is now enabled for SSO.



17. Navigate to **Applications > My Applications**.
18. Locate ArcGIS in the list and from the **Edit** pulldown select **Export Metadata**.



Next Steps

[Configure ArcGIS to Use RSA SecurID Access as an Identity Provider](#)

Configure ArcGIS to Use RSA SecurID Access as an Identity Provider

1. Login into your ArcGIS account with username and password.
2. Go to **My Organization > Edit Settings > Security > Enterprise Logins**
3. Select **SET IDENTITY PROVIDER**.

Enterprise Logins



You can set up your organization so that your users will be able to sign in to ArcGIS using the same username and password that they use with your existing on-premises systems.

The key to this is through a technology known as identity federation that this section will help you set up through two actions.

SET IDENTITY PROVIDER

GET SERVICE PROVIDER

4. Specify Name of Identity Provider for e.g. **RSASecurIDAccess**.
5. For option **Your users will be able to join**, select **Automatically**.
6. Choose **Role they will be assigned** as **User / Publisher**.
7. Choose Metadata option as a **File** or **Parameters specified here**.
8. In case of select option **Parameters specified here**, put **Identity Provider URL** from page 2 step 6 in the Login URL (Redirect) and Login URL (POST) fields.
9. Copy X509Certificate from RSA cert.pem file and paste in section **Certificate** as shown below.

Edit Identity Provider



Specify the properties to establish your organization's Enterprise Identity Provider.

Name:

RSA Via Access

Your users will be able to join:

Automatically Upon invitation from an administrator

Role they will be assigned: User

Metadata for the Enterprise Identity Provider will be supplied using:

A URL A File Parameters specified here

Login URL (Redirect):

https://portal.sso2.pe-lab.co

Login URL (POST):

https://portal.sso2.pe-lab.co

Certificate:

```
MIICsjCCAZqgAwIBAgIGAVWScvfNMA0GCSqGSIb3DQEBCwUAMBoxGDAWBgNVBA
MT
D3NzbzUucGUTbGFilMnVbTAeFw0xNjA2MjcxNTIwNTZaFw0yMDA2MjcxNTIwNTZa
MBoxGDAWBgNVBAMTD3NzbzUucGUTbGFilMnVbTCCAS1wDQYJKoZIhvcNAQEBBQ
```

Show advanced settings

UPDATE IDENTITY PROVIDER

CANCEL

10. Click on **Update Identity Provider**.
11. Click on **Save**.