CA SiteMinder Federation Runbook for ArcGIS Online

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com or SoftwareSecurity@esri.com.

Contents

Chapter 1: SaaS Partner Introduction

This section contains the following topics:

Overview

The scope of the document is to provide the necessary steps to configure the federation partnership to achieve SSO (Single-Sign-On) between CA SiteMinder 12.52, acting as the Identity Provider (IDP), and ArcGIS Online acting as the Service Provider (SP).

Partnership Process

The partnership creation for each partner involves the following steps:

1. Installing and configuring the prerequisites
2. Configuring SiteMinder as an Identity Provider
3. Configuring the Service Provider
4. Testing the Federated SSO

Prerequisites

- Installation of CA SiteMinder 12.52 Suite
- Configuration and testing of User store and Session store
- Creation of Signed Certificate by a well-known CA such as VeriSign, Entrust, Thawte or Go Daddy for Identity Provider Digital Signature.
- **Important!** - Protect Identity Provider Authentication URL with a policy using CA SiteMinder 12.52

Identity Provider Authentication URL is protected by creating following objects:

- Authentication Scheme
- Domain
- Realm
- Rule & Policy

Notes: Protecting the Authentication URL ensures that a user requesting a protected federated resource is presented with an authentication challenge if they do not have a SiteMinder session at the Identity Provider.

- Tenant environment at ArcGIS Online Login URL - https://<org>.maps.arcgis.com/home/signin.html

Target ArcGIS Online Services

The following services of ArcGIS Online have been tested for federation using CA SiteMinder 12.52 as Identity Provider.

ArcGIS Online Organizations -> https://<org>.maps.arcgis.com/home/signin.html

Chapter 2: Configuring CA SiteMinder (12.52) as Identity Provider

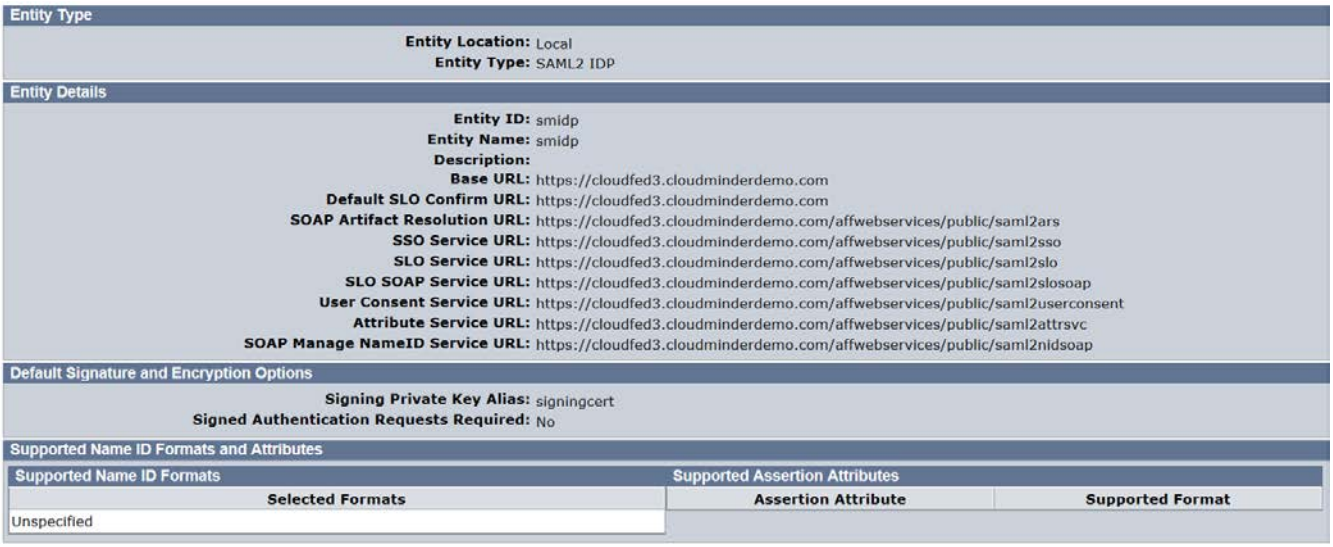
This section contains the following topics:

Configure Identity Provider and Service Provider Entities

To create Entities, Login to CA SiteMinder and get to Federation -> Partnership Federation -> Entity -> Create Entity

Local Entity Creation

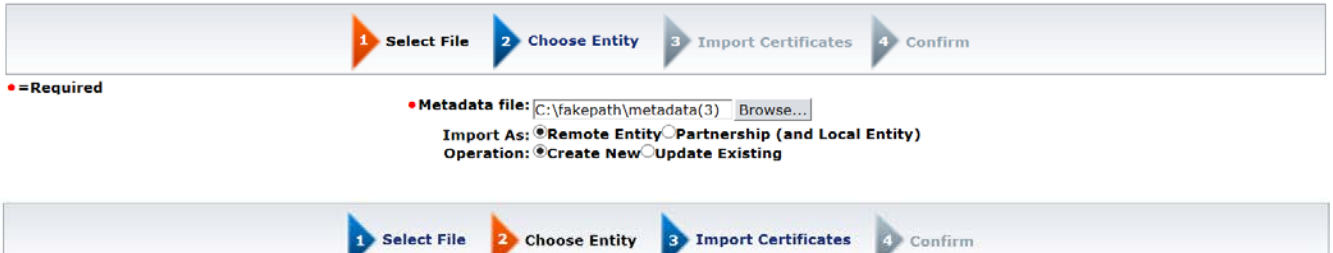
- Configure Local Identity Provider Entity with following details:
    - Entity Location – Local
    - Entity Type – SAML2 IDP
    - Entity ID – Any *(Relevant ID)*
    - Entity Name – Any *(Relevant name)*
    - Description – Any *(Relevant description)*
    - Base URL – https://<FWS_FQDN> where FWS_FQDN is the fully-qualified domain name for the host serving SiteMinder Federation Web Services. This is pre-populated by SiteMinder.
    - Signing Private Key Alias – Select the correct private key alias or import one if not done already
    - Signed Authentication Requests Required – No
    - Supported NameID format – “Unspecified”

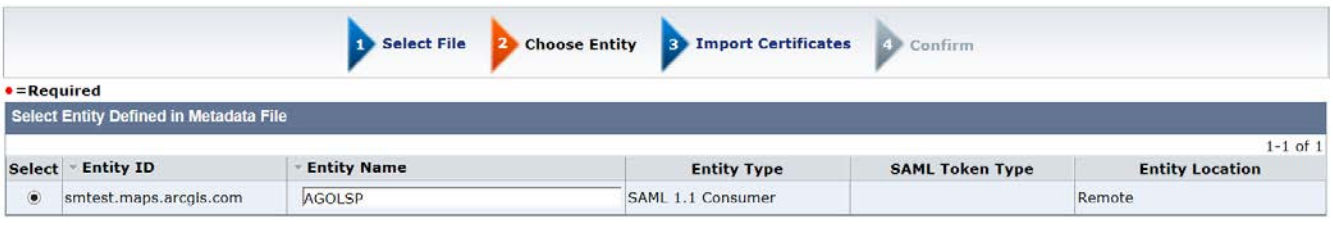


Remote Entity Creation

Remote Entity can be created either through metadata import (recommended) or manually.

- To configure Remote SP Entity by importing Metadata, select Import Metadata
  - Create ArcGIS Online Remote Entity with following details
    - Metadata File: Supply metadata.xml file obtained from the ArcGIS Online Organization > MY ORGANIZATION > EDIT SETTINGS > SECURITY > GET SERVICE PROVIDER.
    - Import As – Remote Entity
    - Operation – Create New
    - Accept remaining values and click Finish.





- Accept remaining values and click Finish.
- Modify the Entity that was just created above as follows:

- Assertion Consumer Service URL - *https://<org>.maps.arcgis.com/sharing/rest/oauth2/saml/signin*
- Verification Certificate Alias – This can be left blank. Otherwise, select the correct certificate or import one if not done already. This is used to verify the signature in incoming requests. If a certificate alias was specified, also check "Sign Authentication Requests."
- Supported NameID Format – "Unspecified"

Entity Type

Entity Location: Remote
Entity Type: SAML2 SP

Entity Details

Entity ID: smtest.maps.arcgis.com
Entity Name: AGOLSP
Description: AGOLSP Imported via metadata

Remote Assertion Consumer Service URLs

Index	Binding	URL	Default
1	HTTP-POST	https://smtest.maps.arcgis.com/sharing/rest/oauth2/saml/signin	Yes

Remote SLO Service URLs

Binding	Location URL	Response Location URL

Manage Name ID Service URLs

Binding	Location URL	Response Location URL

Signature and Encryption Options

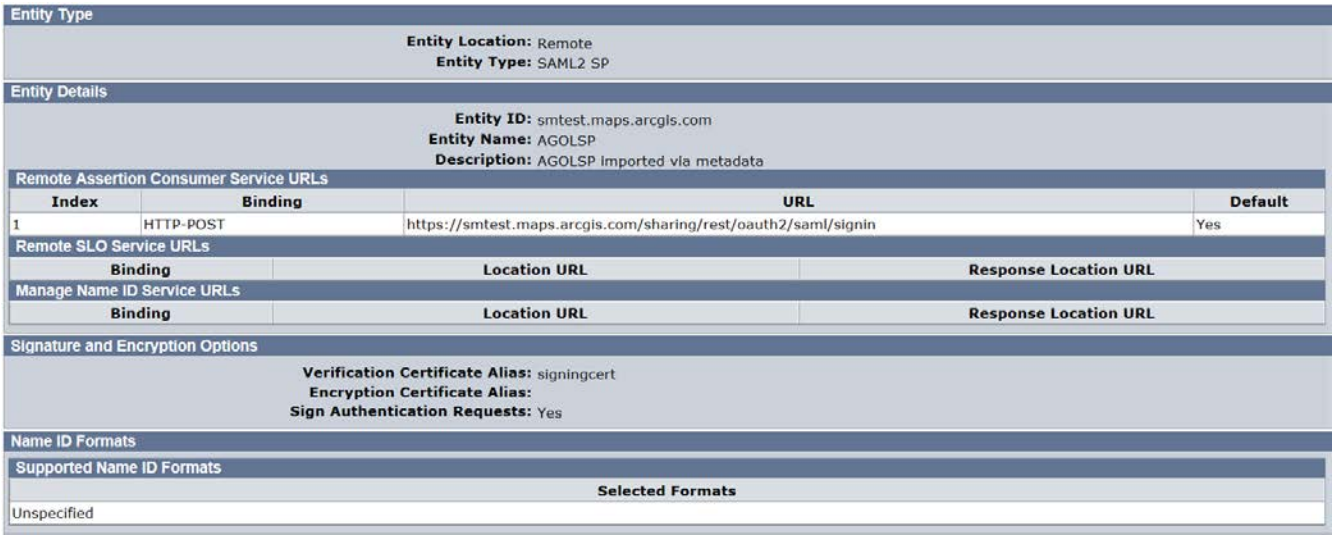
Verification Certificate Alias: signingcert
Encryption Certificate Alias:
Sign Authentication Requests: Yes

Name ID Formats

Supported Name ID Formats

Selected Formats
Unspecified

- To configure Remote SP Entity manually, select Create Entity
    - Create ArcGIS Online Remote Entity with following details
        - Entity Location – Remote
        - New Entity Type – SAML2 SP
        - Entity ID – <org>.maps.arcgis.com
        - Entity Name – Any *(Relevant name)*
        - Description – Any *(Relevant description)*
        - Assertion Consumer Service URL - *https://<org>.maps.arcgis.com/sharing/rest/oauth2/saml/signin*
        - Verification Certificate Alias – This can be left blank. Otherwise, select the correct certificate or import one if not done already. This is used to verify the signature in incoming requests. If a certificate alias was specified, also check "Sign Authentication Requests."
        - Supported NameID Format – "Unspecified"



Entity Type

Entity Location: Remote
Entity Type: SAML2 SP

Entity Details

Entity ID: smtest.maps.arcgis.com
Entity Name: AGOLSP
Description: AGOLSP Imported via metadata

Remote Assertion Consumer Service URLs

Index	Binding	URL	Default
1	HTTP-POST	https://smtest.maps.arcgis.com/sharing/rest/oauth2/saml/signin	Yes

Remote SLO Service URLs

Binding	Location URL	Response Location URL

Manage Name ID Service URLs

Binding	Location URL	Response Location URL

Signature and Encryption Options

Verification Certificate Alias: signingcert
Encryption Certificate Alias:
Sign Authentication Requests: Yes

Name ID Formats

Supported Name ID Formats

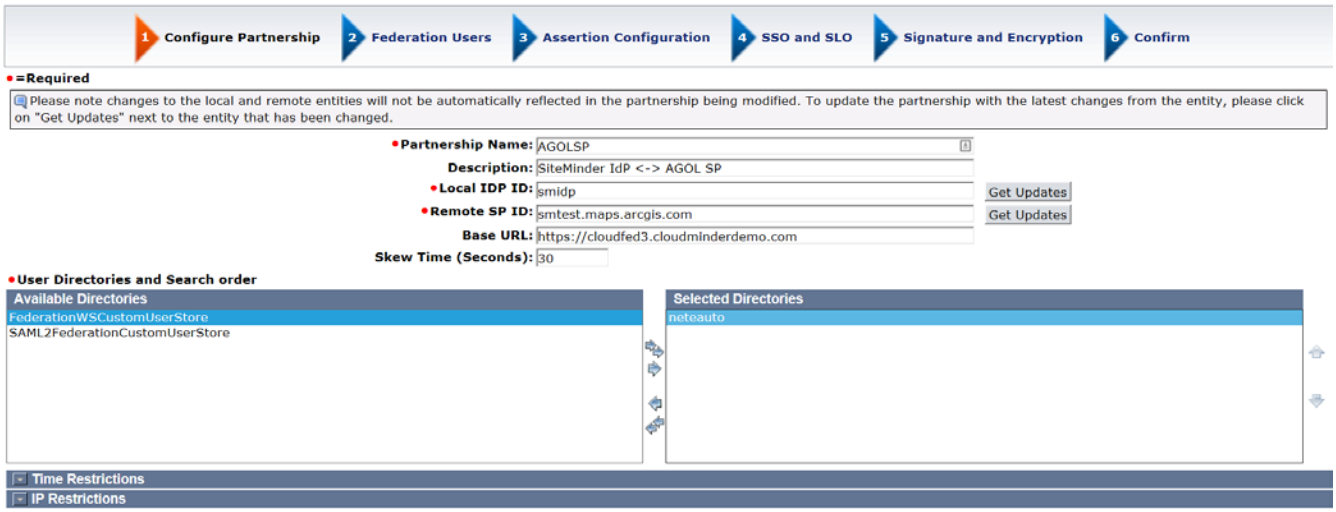
Selected Formats
Unspecified

Configure Federation Partnership between CA – SiteMinder (IDP) & ArcGIS Online (SP)

Login to CA SiteMinder and navigate to Federation -> Partnership Federation -> Create Partnership (SAML 2 IDP -> SP)

Configure Partnership

- Add Partnership Name – Any *(Relevant Name)*
- Description – Any *(Relevant description)*
- Local IDP ID – Select Local IDP ID
- Remote SP ID – Select Remote SP ID
- Base URL – Will be pre-populated
- Skew Time – Any
- User Directories and Search Order – Select required Directories in required search order. Proceed to Next Page



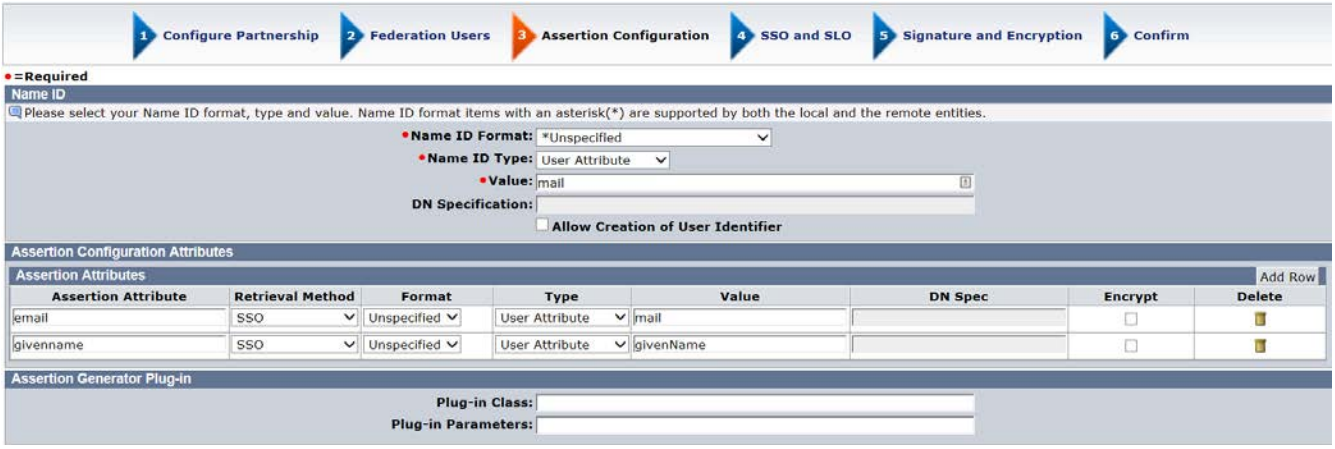
Federation Users

- Configure Federation Users – Accept default values

Assertion Configuration

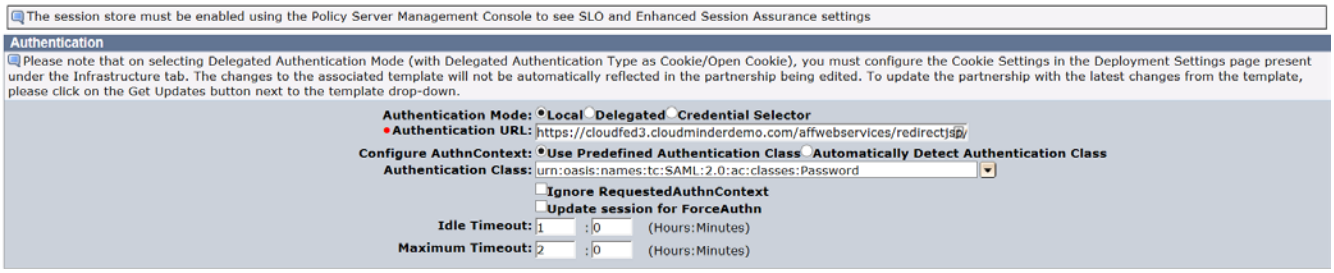
- Name ID Format – "Unspecified"
- Name ID Type – User Attribute

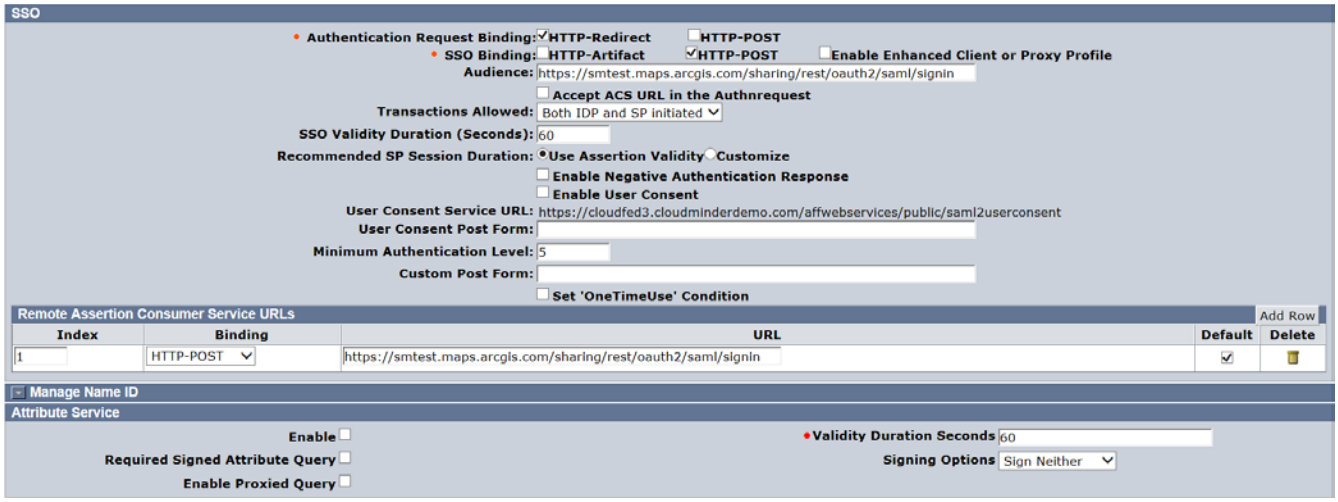
- Value – Should be the name of the user attribute containing the email address or user identifier. *In this example, the name is 'mail'.*
- Assertion Attributes – Optionally, ArcGIS Online can read two additional attributes associated with the `Name ID` value to populate email address and full name supplied by the `email` and `givenname` attributes respectively as shown in the screenshot below.

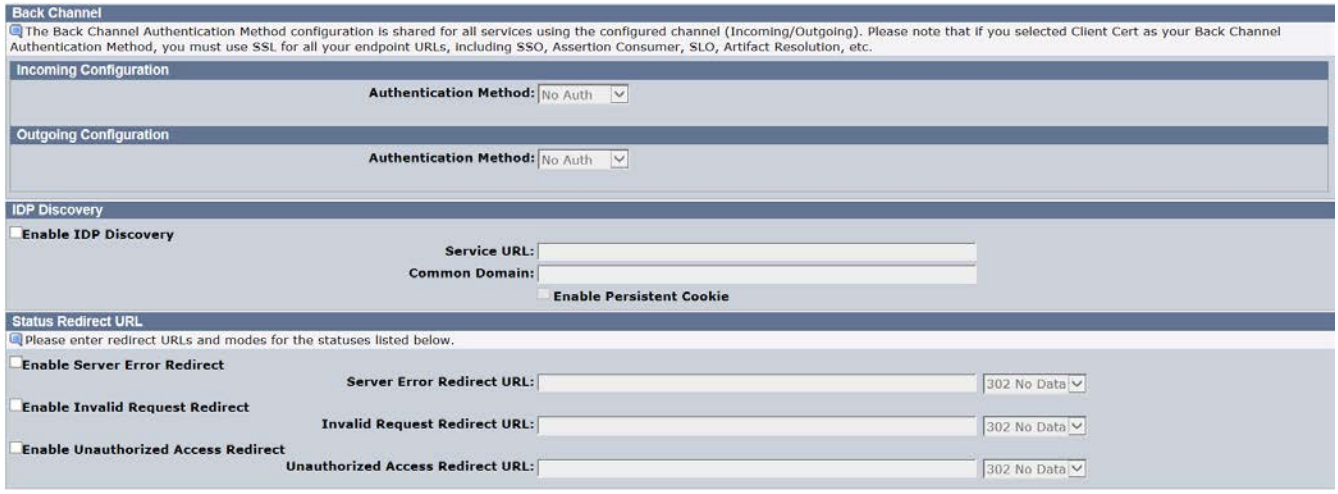


SSO and SLO

- Add Authentication URL. This should be an URL that is protected by SiteMinder
- SSO Binding – HTTP-Post
- Audience - https://<org>.maps.arcgis.com/sharing/rest/oauth2/saml/signin where <org> is the name of your ArcGIS Online organization. *(The example shown here is https://smtest.maps.arcgis.com/sharing/rest/oauth2/saml/signin)*
- Transaction Allowed – Both IDP and SP initiated
- Assertion Consumer Service URL – Index = 1, Binding = HTTP-POST, URL = https://<org>.maps.arcgis.com/sharing/rest/oauth2/saml/signin where <org> is the name of your ArcGIS Online organization. *(The example shown here is https://smtest.maps.arcgis.com/sharing/rest/oauth2/saml/signin)*

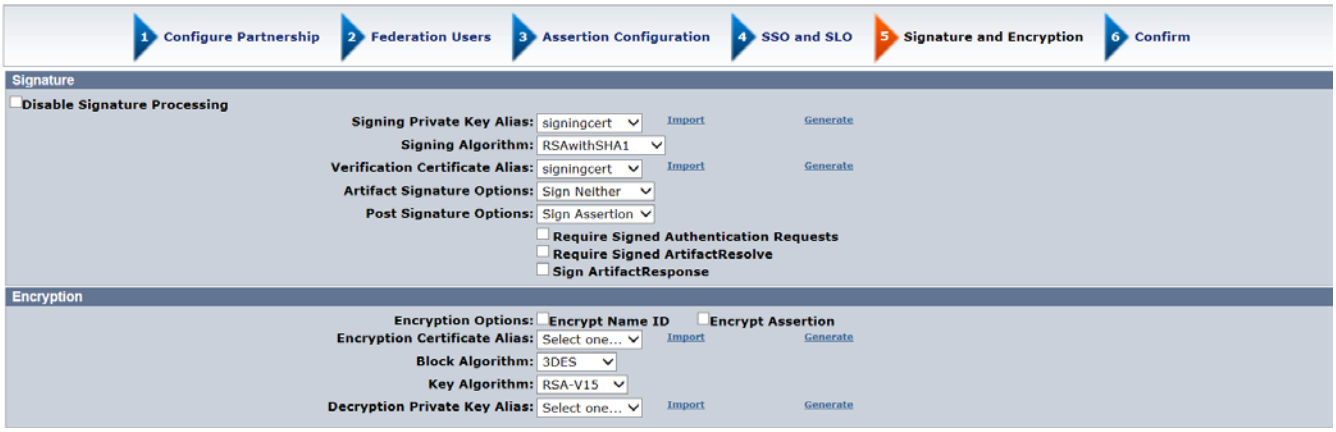






Configure Signature and Encryption

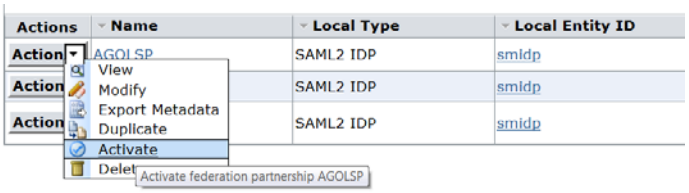
- Signing Private Key Alias – Check if correct Private Key Alias is selected
- Verification Certificate Alias – Check if correct Verification Certificate Alias is selected



- Confirm the values and finish Partnership.

Partnership Activation

- Activate the created Partnership.



Chapter 3: Configuring Service Provider

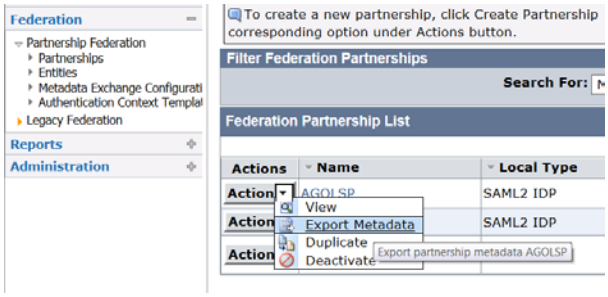
This section contains the following topics:

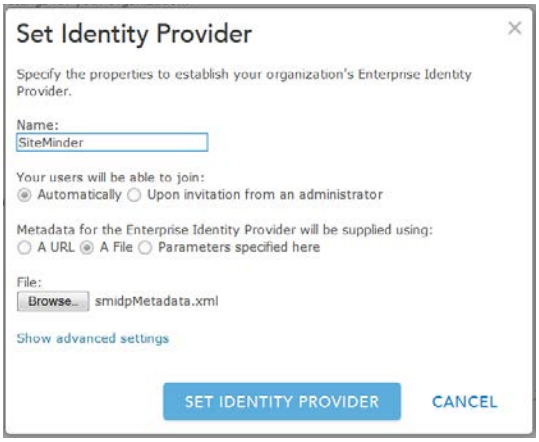
Configure SAML 2.0 SSO in ArcGIS Online

✓ Before configuring SAML 2.0 SSO in ArcGIS Online you must Create a free-trial (http://www.arcgis.com/features/free-trial.html) or purchase a full ArcGIS Online "Organization" account (http://www.esri.com/apps/Products/AGOL/subscription/.)

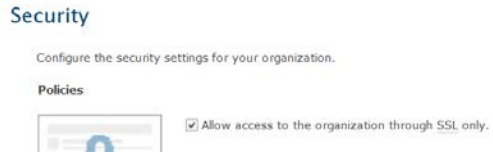
Follow the steps given below to configure the SAML SSO in ArcGIS Online

1. Within your ArcGIS Online Organization, click "My Organization" > "Edit Settings" > "Security" > "SET IDENTITY PROVIDER" setting the configuration as described:
   a. Name – *Your Organization's Name*
   b. Your users will be able to join: – Automatically
   c. Metadata for the Enterprise Identity Provider will be supplied using: - A File *Upload the Site Minder Partnership Identity Provider Metadata file.*

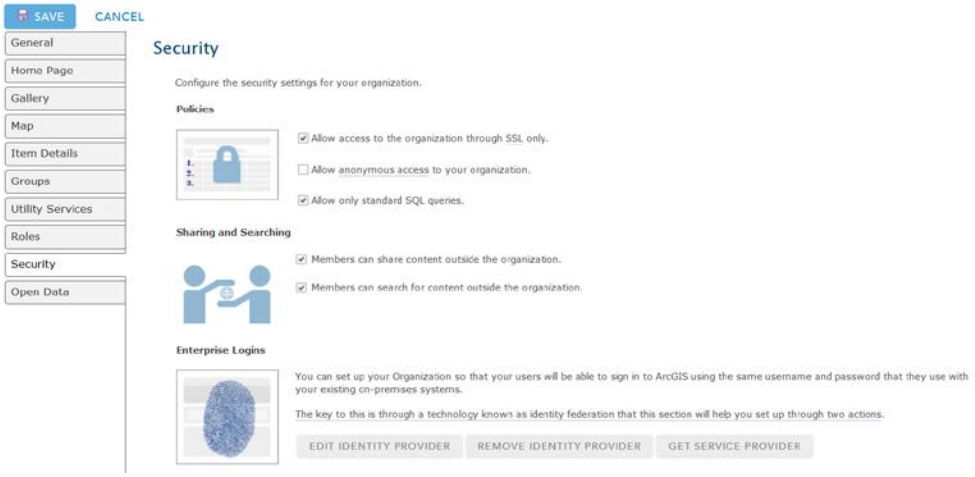




2. Optional: Within your ArcGIS Online Organization, click “My Organization” > “Edit Settings” > “Security” > Check “Allow access to the organization through SSL only”



3. Save your ArcGIS Online Security Settings.



Chapter 4: Federation Testing & Target Services

This section contains the following topics:

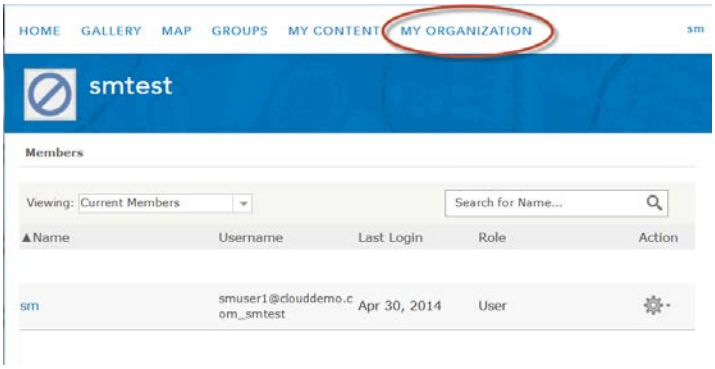
Federation Testing

- Access the Service Provider (ArcGIS Online) initiated login URL https://<org>.maps.arcgis.com/home/signin.html and click “USING YOUR <ORG> ACCOUNT” as shown below.

- This will automatically direct the user to the login page of Identity Provider (SiteMinder).
- Enter the credentials and click login:

- Upon a successful login, the user is automatically directed back to the Service Provider (ArcGIS Online). The account will be automatically created if needed, and the user name or the `givenname` value (if available) will be displayed in the upper right corner.

- Finally, click "My Organization" to verify the OAuth token was created successfully for the user, and that the Service Provider (ArcGIS Online) recognizes the user.



Accessing various ArcGIS Online services

After federation login to ArcGIS Online, the following services can be accessed by the user:

ArcGIS Online Organization Content Management

ArcGIS Online Organization Web Application Authoring

ArcGIS Online Organization Routing

ArcGIS Online Organization Geocoding

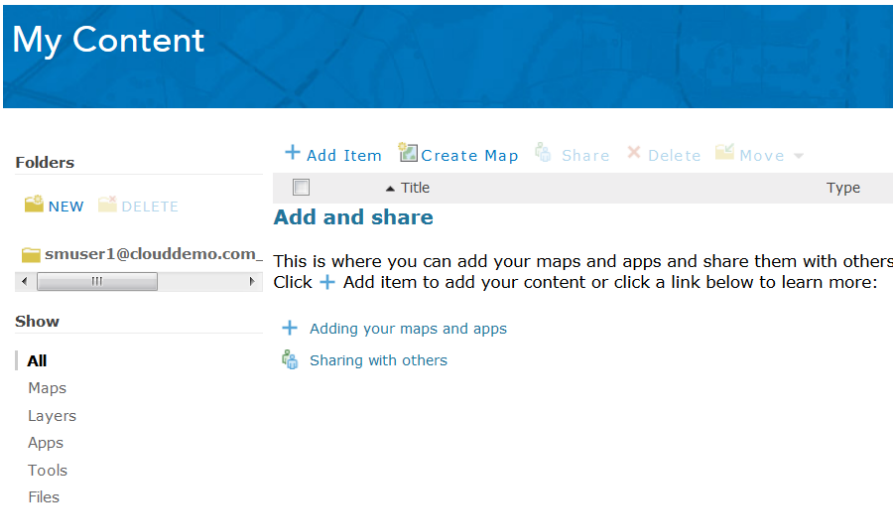
ArcGIS Online Organization Mobile Services

ArcGIS Online Organization Service Publishing

ArcGIS Online Organization Content Management

To get to ArcGIS Online Organization Content Management directly via federated login use the following steps:

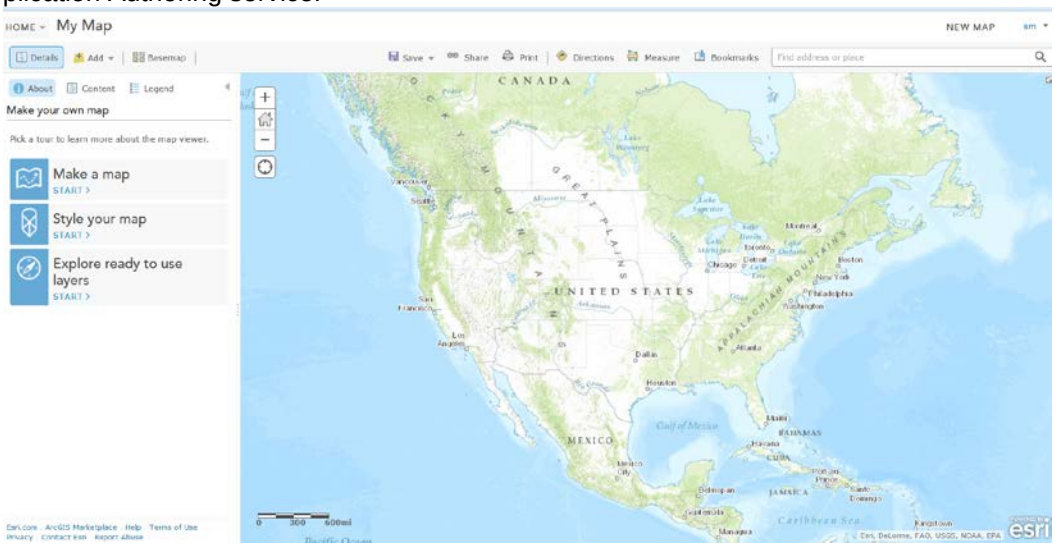
- URL - https://<org>.maps.arcgis.com/home/content.html
- Type in the login credentials at the Identity Provider site and get to ArcGIS Online My Content



ArcGIS Online Organization Web Application Authoring

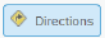
To get to ArcGIS Online Organization Web Application Authoring directly via federated login use the following steps:

- URL - https://<org>.maps.arcgis.com/home/webmap/viewer.html?useExisting=1
- Type in the login credentials at the Identity Provider site and get to ArcGIS Online Web Application Authoring service.

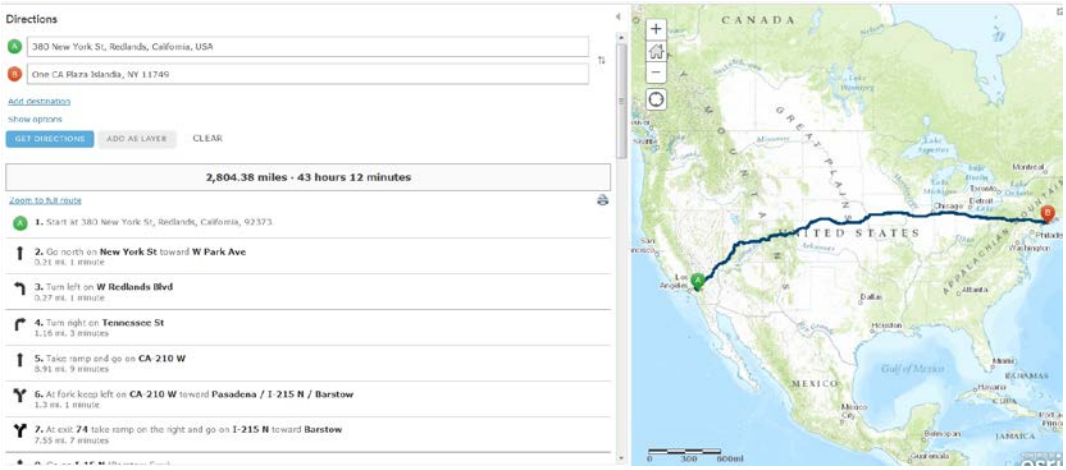


ArcGIS Online Organization Routing Service

To get to ArcGIS Online Organization Geocoding/Routing Service directly via federated login use the following steps:

- URL - https://<org>.maps.arcgis.com/home/webmap/viewer.html?useExisting=1
- Type in the login credentials at the Identity Provider site and get to ArcGIS Online Routing Service.
- Click the “Directions” link: 

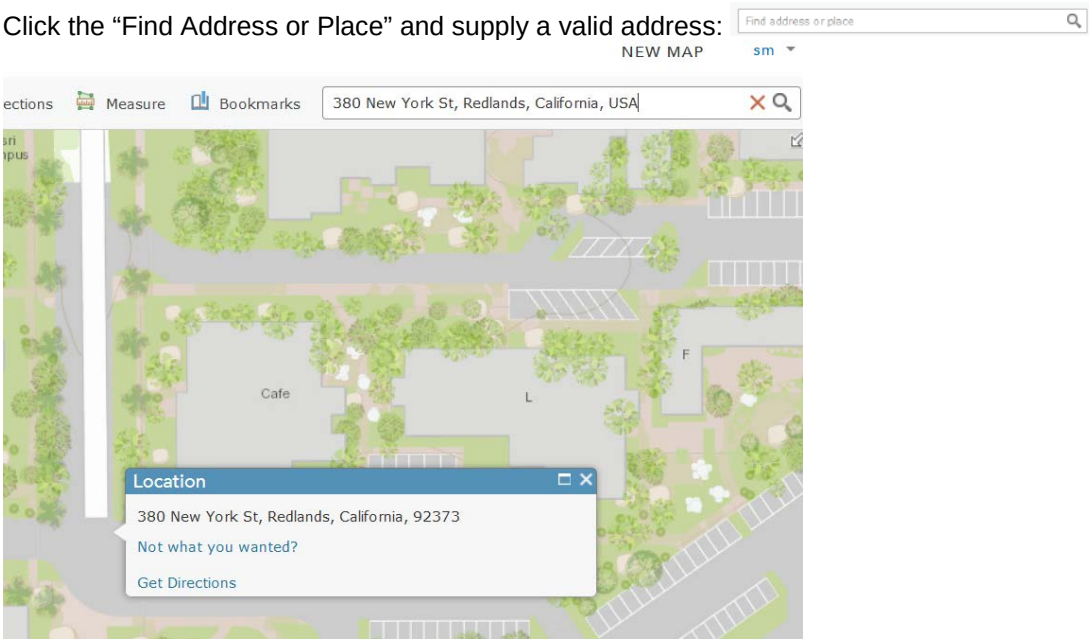
and supply a source and destination, then click “Get Directions”



ArcGIS Online Organization Geocoding Service

To get to ArcGIS Online Organization Geocoding Service directly via federated login use the following steps:

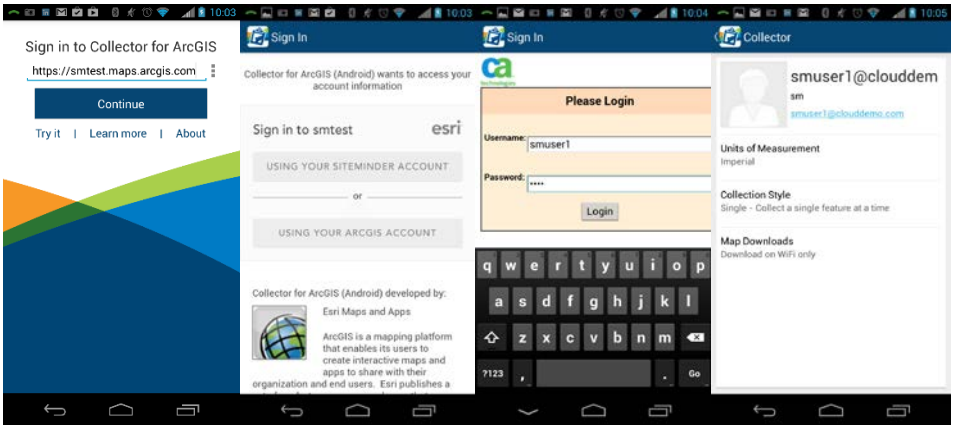
- URL - https://<org>.maps.arcgis.com/home/webmap/viewer.html?useExisting=1
- Type in the login credentials at the Identity Provider site and get to ArcGIS Online Geocoding Service.
- Click the “Find Address or Place” and supply a valid address:



ArcGIS Online Organization Mobile Service

To get to ArcGIS Online Organization Mobile Service directly via federated login use the following steps:

- Download the “ArcGIS Collector App” from the App Store for your Mobile Device.
- Launch the ArcGIS Collector App from your mobile device.
- At the “Sign in to Collector for ArcGIS” screen, supply the URL of your ArcGIS Online Organization (https://<org>.maps.arcgis.com/) and click “Continue”
- At the Sign In to <ORG> screen, tap “USING YOUR <ORG> ACCOUNT”
- The app will redirect the user to the SiteMinder Identity Provider login screen. Supply valid credentials then tap “Login”
- The app will return to the Collector screen. To verify sign-in, tap the Settings Icon > Settings where the user login will display.



**This workflow is currently unavailable for the “Collector for iOS” app.*

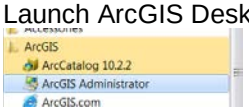
ArcGIS Online Organization Service Publishing

Note: This workflow requires the following:

- ✓ An installed & licensed copy of ArcGIS for Desktop 10.2 or Later
- ✓ An ArcGIS Online Organization with sufficient credits to support service publishing. See http://www.arcgis.com/features/plans/pricing.html for details.
- ✓ The account used to sign-in to the ArcGIS Online Organization must be granted, at minimum, the "Publisher" role. See http://doc.arcgis.com/en/arcgis-online/administer/change-roles.htm for details on how to administer user roles within ArcGIS Online Organizations.

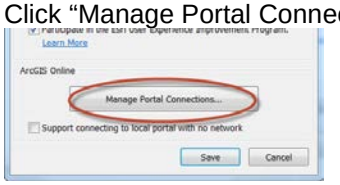
Follow these steps to proceed with ArcGIS Online Organization Service Publishing:

- Launch ArcGIS Desktop Administrator 10.2 or Later *(10.2.2 pictured here.)*

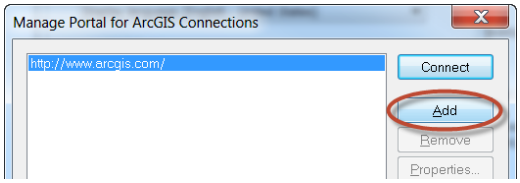


- Click "Advanced…"

- Click "Manage Portal Connections…"

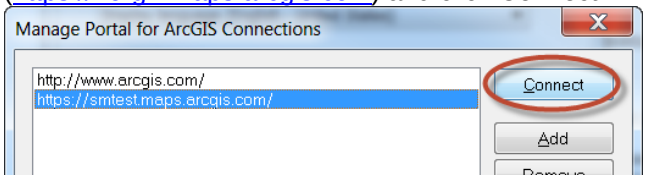


- Click "Add"



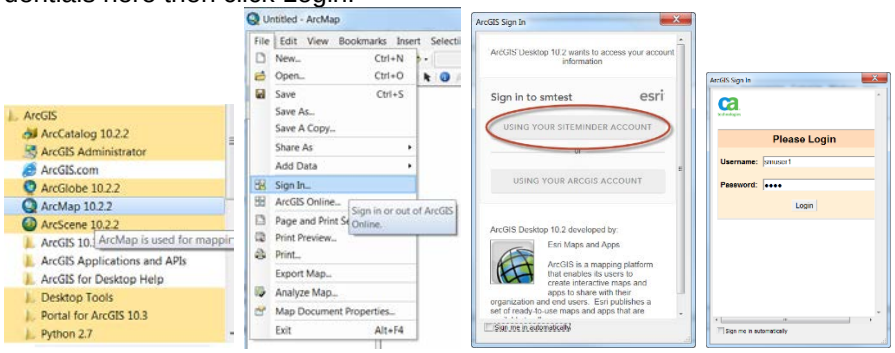
- Supply the URL of the ArcGIS Online Organization configured to use the Site Minder federated login (https://<org>.maps.arcgis.com) then click OK.

- Select the newly created connection to the ArcGIS Online Organization (https://<org>.maps.arcgis.com) and click Connect.



- Click OK at each opened screen to completely exit the ArcGIS Desktop Administrator application.

- Launch ArcMap version 10.2 or later *(10.2.2 pictured here.)*
- Within ArcMap click File > Sign In…
- Click Sign in to <org> USING YOUR <ORG> ACCOUNT.
- Optionally, check “Sign me in automatically” to automate this process the next time ArcGIS Desktop is loaded.
- The dialog will redirect to the Site Minder Identity Provider login screen. Enter valid credentials here then click Login.



- Once signed in, Feature and Tiled services can be published from ArcMap to the ArcGIS Online Organization. For details on this workflow, see the “Publish an ArcMap Document” section of the ArcGIS Online web help here.

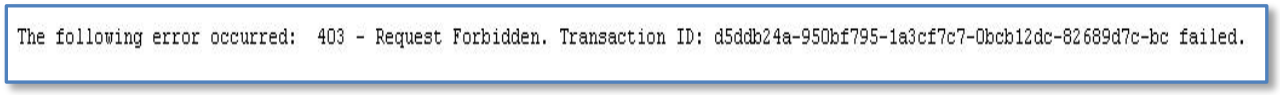
Chapter 5: Exception Handling

This section contains the following exceptions:

Exception Cases

When the SiteMinder Partnership is Inactive

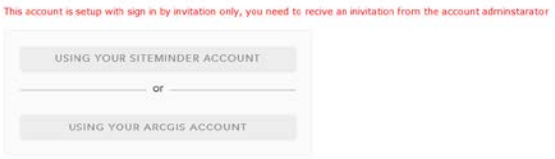
When SiteMinder Partnership is Inactive or not Defined, following error appears on browser



User who is not in the ArcGIS Online Organization trying to login through SiteMinder

UserID used → smuser1

Result → Authentication at the ArcGIS Online Organization fails and displays the error given below.



Logs -> No specific logs recorded within ArcGIS Online Organization.

Expired certificate on SiteMinder Side

Condition – When SiteMinder signing certificate is expired.

Log File Information appears to be like this

<Response ID="_5e705c022c4ce8c6c8a5c39a057e3eb211d0" InResponseTo="fjedijk-piblphaigikhdieoilebpfaoibohmampl" IssueInstant="2012-12-27T13:29:00Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:protocol">

<ns1:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity" xmlns:ns1="urn:oasis:names:tc:SAML:2.0:assertion"></ns1:Issuer>

<Status>

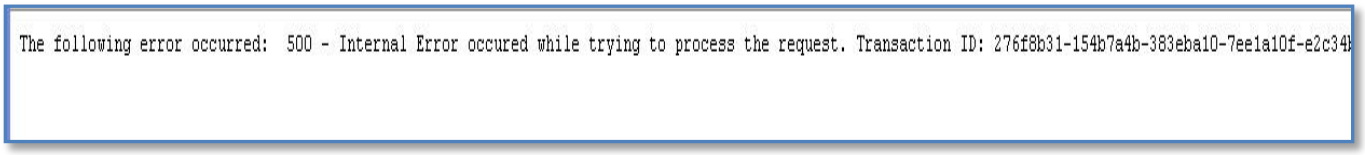
<StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder"/>

<StatusMessage>Error Signing Assertion.</StatusMessage>

</Status>

</Response>

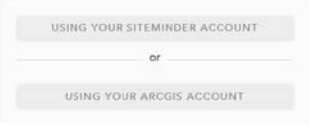
Message that appears on browser □



When Service Provider Assertion Consumer URL was Misconfigured on the SiteMinder Side

Condition – Service Provider (ArcGIS Online) Entity contains invalid Assertion URL

Result – Service Provider (ArcGIS Online) does not permit access. ArcGIS Online redirects to sign in page. *Or* browser appears to "hang" displaying a blank screen.



When Identity Provider Entity ID was Misconfigured on the Target Application Side

Condition – Identity Provider Entity ID is Misconfigured within ArcGIS Online.

Result – There is no noticeable impact of this other than cosmetic changes to the login button on the ArcGIS Online side:

When Identity Provider SSO URL was Misconfigured on the Target Application Side

Condition – Identity Provider SSO URL was Misconfigured within ArcGIS Online

Result – When a user is prompted to sign in "USING YOUR <ORG> ACCOUNT", they will land at a page that looks like this:

When Identity Provider Certificate was Misconfigured on the Target Application Side

Condition – Identity Provider Certificate was Misconfigured within ArcGIS Online

Result – When a user is prompted to sign in "USING YOUR <ORG> ACCOUNT", they will land at a page that looks like this:

Unable to login using Idp Error validating SAML response Could not parse certificate: java.io.IOException: Incomplete BER/DER data

Chapter 6: Summary

- ✓ Each Organization within ArcGIS Online supports federation to a single Identity Provider Only.
- ✓ ArcGIS Online Organization administrators may grant non-federated “ArcGIS Online” accounts access to the Organization as well.
- ✓ It is possible to federate multiple ArcGIS Online Organizations to a Site Minder Identity Provider following the steps below:

    1. Acquire via purchase/trial multiple ArcGIS Online Organizations, one for each organizational unit.
    2. Within SiteMinder, create a single “Local Entity” following the workflow here.
    3. For each ArcGIS Online Organization, create a “Remote Entity” within SiteMinder following the workflow here.
    4. For each ArcGIS Online Organization, follow the “Configure Federation Partnership between CA – SiteMinder (IDP) & ArcGIS Online (SP)” workflow here.
    5. For each ArcGIS Online Organization, follow the “Configure SAML 2.0 SSO in ArcGIS Online” workflow here.

    This allows a large organization to empower smaller organizational units (departments, sub-corporations, groups, etc) to administer their own ArcGIS Online Organization yet support SSO to the entire organization.