



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.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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

Legal Notice	2
Contents	4
Chapter 1: SaaS Partner Introduction	6
Overview	6
Partnership Process	6
Prerequisites	6
Target ArcGIS Online Services	7
Chapter 2: Configuring CA SiteMinder (12.52) as Identity Provider	8
Configure Identity Provider and Service Provider Entities	8
Configure Federation Partnership between CA – SiteMinder (IDP) & ArcGIS Online (SP)	11
Configure Partnership	12
Federation Users	12
Assertion Configuration	12
SSO and SLO	13
Configure Signature and Encryption	14
Partnership Activation	15
Chapter 3: Configuring Service Provider	16
Configure SAML 2.0 SSO in ArcGIS Online	16
Chapter 4: Federation Testing & Target Services	18
Federation Testing	18
Accessing various ArcGIS Online services	20
ArcGIS Online Organization Content Management	20
ArcGIS Online Organization Web Application Authoring	21
ArcGIS Online Organization Routing Service	22
ArcGIS Online Organization Geocoding Service	23
ArcGIS Online Organization Mobile Service	24
ArcGIS Online Organization Service Publishing	25
Chapter 5: Exception Handling	26
Exception Cases	27
When the SiteMinder Partnership is Inactive	27
User who is not in the ArcGIS Online Organization trying to login through SiteMinder	27
Expired certificate on SiteMinder Side	27

When Service Provider Assertion Consumer URL was Misconfigured on the SiteMinder Side 29

When Identity Provider Entity ID was Misconfigured on the Target Application Side 29

When Identity Provider SSO URL was Misconfigured on the Target Application Side .. 29

When Identity Provider Certificate was Misconfigured on the Target Application Side . 29

Chapter 6: Summary..... 30

Chapter 1: SaaS Partner Introduction

This section contains the following topics:

[Overview](#)

[Partnership Process](#)

[Prerequisites](#)

[Target ArcGIS Online URLs](#)

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 the Identity Provider and Service Provider Entities](#)

[Configure Federation Partnership between CA-Siteminder \(IDP\) & ArcGIS Online \(SP\)](#)

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”

Entity Type
Entity Location: Local
Entity Type: SAML2 IDP

Entity Details
Entity ID: smidp
Entity Name: smidp
Description:
Base URL: https://cloudfed3.cloudminderdemo.com
Default SLO Confirm URL: https://cloudfed3.cloudminderdemo.com
SOAP Artifact Resolution URL: https://cloudfed3.cloudminderdemo.com/affwebservice/public/saml2ars
SSO Service URL: https://cloudfed3.cloudminderdemo.com/affwebservice/public/saml2sso
SLO Service URL: https://cloudfed3.cloudminderdemo.com/affwebservice/public/saml2slo
SLO SOAP Service URL: https://cloudfed3.cloudminderdemo.com/affwebservice/public/saml2slosoap
User Consent Service URL: https://cloudfed3.cloudminderdemo.com/affwebservice/public/saml2userconsent
Attribute Service URL: https://cloudfed3.cloudminderdemo.com/affwebservice/public/saml2attrsvc
SOAP Manage NameID Service URL: https://cloudfed3.cloudminderdemo.com/affwebservice/public/saml2nidsoap

Default Signature and Encryption Options
Signing Private Key Alias: signingcert
Signed Authentication Requests Required: No

Supported Name ID Formats and Attributes

Supported Name ID Formats	Supported Assertion Attributes	
Selected Formats	Assertion Attribute	Supported 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.

1 Select File 2 Choose Entity 3 Import Certificates 4 Confirm

• =Required

• Metadata file: C:\fakepath\metadata(3)

Import As: Remote Entity Partnership (and Local Entity)

Operation: Create New Update Existing

1 Select File 2 Choose Entity 3 Import Certificates 4 Confirm

• =Required

Select Entity Defined in Metadata File

Select	Entity ID	Entity Name	Entity Type	SAML Token Type	Entity Location
<input checked="" type="radio"/>	smtest.maps.arcgis.com	AGOLSP	SAML 1.1 Consumer		Remote

1-1 of 1

- 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: smttest.maps.arcgis.com Entity Name: AGOLSP Description: AGOLSP Imported via metadata			
Remote Assertion Consumer Service URLs			
Index	Binding	URL	Default
1	HTTP-POST	https://smttest.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

The screenshot shows the 'Configure Partnership' step of a 6-step wizard. The steps are: 1. Configure Partnership (active), 2. Federation Users, 3. Assertion Configuration, 4. SSO and SLO, 5. Signature and Encryption, and 6. Confirm.

Required Fields:

- Partnership Name: AGOLSP
- Description: SiteMinder IdP <-> AGOL SP
- Local IDP ID: smidp
- Remote SP ID: smtest.maps.arcgis.com
- Base URL: https://cloudfed3.cloudminderdemo.com
- Skew Time (Seconds): 30

There are 'Get Updates' buttons next to the Local IDP ID and Remote SP ID fields.

User Directories and Search order:

- Available Directories:** FederationWSCustomUserStore, SAML2FederationCustomUserStore
- Selected Directories:** neteauto

Below the directories are sections for 'Time Restrictions' and 'IP Restrictions'.

Federation Users

- Configure Federation Users – Accept default values

The screenshot shows the 'Federation Users' step of the configuration wizard. The steps are: 1. Configure Partnership, 2. Federation Users (active), 3. Assertion Configuration, 4. SSO and SLO, 5. Signature and Encryption, and 6. Confirm.

Federated Users Table:

Directory	User Class	User Name / Filter By	Exclude	Delete
neteauto	All Users in Directory		<input type="checkbox"/>	

An 'Add Row' button is located in the top right corner of the table.

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.

Assertion Configuration Attributes

Assertion Attribute	Retrieval Method	Format	Type	Value	DN Spec	Encrypt	Delete
email	SSO	Unspecified	User Attribute	mail		<input type="checkbox"/>	
givenname	SSO	Unspecified	User Attribute	givenName		<input type="checkbox"/>	

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://smttest.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://smttest.maps.arcgis.com/sharing/rest/oauth2/saml/signin>)*

Authentication

Authentication Mode: Local Delegated Credential Selector

Authentication URL: <https://cloudfed3.cloudminderdemo.com/affwebservices/redirectsp/>

Configure AuthContext: Use Predefined Authentication Class Automatically Detect Authentication Class

Authentication Class: urn:oasis:names:tc:SAML:2.0:ac:classes:Password

Ignore RequestedAuthContext

Update session for ForceAuth

Idle Timeout: 1 : 0 (Hours:Minutes)

Maximum Timeout: 2 : 0 (Hours:Minutes)

SSO

- Authentication Request Binding: HTTP-Redirect HTTP-POST
- SSO Binding: HTTP-Artifact HTTP-POST Enable Enhanced Client or Proxy Profile
- Audience:
 - Accept ACS URL in the Authrequest
- Transactions Allowed:
- SSO Validity Duration (Seconds):
- Recommended SP Session Duration: Use Assertion Validity Customize
 - Enable Negative Authentication Response
 - Enable User Consent
- User Consent Service URL:
- User Consent Post Form:
- Minimum Authentication Level:
- Custom Post Form:
- Set 'OneTimeUse' Condition

Remote Assertion Consumer Service URLs

Index	Binding	URL	Default	Delete
1	HTTP-POST	https://smtest.maps.arcgis.com/sharing/rest/oauth2/saml/signin	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Manage Name ID

Attribute Service

- Enable
- Required Signed Attribute Query
- Enable Proxied Query
- Validity Duration Seconds:
- Signing Options:

Back Channel

The Back Channel Authentication Method configuration is shared for all services using the configured channel (Incoming/Outgoing). Please note that if you selected Client Cert as your Back Channel Authentication Method, you must use SSL for all your endpoint URLs, including SSO, Assertion Consumer, SLO, Artifact Resolution, etc.

Incoming Configuration

Authentication Method:

Outgoing Configuration

Authentication Method:

IDP Discovery

- Enable IDP Discovery
 - Service URL:
 - Common Domain:
 - Enable Persistent Cookie

Status Redirect URL

Please enter redirect URLs and modes for the statuses listed below.

- Enable Server Error Redirect
 - Server Error Redirect URL:
 - 302 No Data
- Enable Invalid Request Redirect
 - Invalid Request Redirect URL:
 - 302 No Data
- Enable Unauthorized Access Redirect
 - Unauthorized Access Redirect URL:
 - 302 No Data

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

[1 Configure Partnership](#)
[2 Federation Users](#)
[3 Assertion Configuration](#)
[4 SSO and SLO](#)
[5 Signature and Encryption](#)
[6 Confirm](#)

Signature

Disable Signature Processing

Signing Private Key Alias: signingcert
 Signing Algorithm: RSAwithSHA1
 Verification Certificate Alias: signingcert
 Artifact Signature Options: Sign Neither
 Post Signature Options: Sign Assertion
 Require Signed Authentication Requests
 Require Signed ArtifactResolve
 Sign ArtifactResponse

Encryption

Encryption Options: Encrypt Name ID Encrypt Assertion
 Encryption Certificate Alias: Select one...
 Block Algorithm: 3DES
 Key Algorithm: RSA-V15
 Decryption Private Key Alias: Select one...

- Confirm the values and finish Partnership.

Partnership Activation

- Activate the created Partnership.

Actions	Name	Local Type	Local Entity ID
Action	AGOLSP	SAML2 IDP	smidp
Action	View	SAML2 IDP	smidp
Action	Modify	SAML2 IDP	smidp
Action	Export Metadata	SAML2 IDP	smidp
Action	Duplicate	SAML2 IDP	smidp
Action	Activate		
Action	Delete	Activate federation partnership AGOLSP	

Chapter 3: Configuring Service Provider

This section contains the following topics:

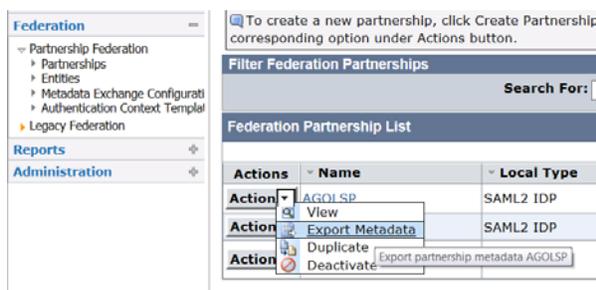
[Configure SAML 2.0 SSO in ArcGIS Online](#)

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/.](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.



Set Identity Provider

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

Name:

Your users will be able to join:
 Automatically Upon invitation from an administrator

Metadata for the Enterprise Identity Provider will be supplied using:
 A URL A File Parameters specified here

File:
 smidpMetadata.xml

[Show advanced settings](#)

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

Security

Configure the security settings for your organization.

Policies

 Allow access to the organization through SSL only.

- Save your ArcGIS Online Security Settings.

- General
- Home Page
- Gallery
- Map
- Item Details
- Groups
- Utility Services
- Roles
- Security
- Open Data

Security

Configure the security settings for your organization.

Policies

Allow access to the organization through SSL only.
 Allow anonymous access to your organization.
 Allow only standard SQL queries.

Sharing and Searching

Members can share content outside the organization.
 Members can search for content outside the organization.

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.

Chapter 4: Federation Testing & Target Services

This section contains the following topics:

[Federation Testing](#)

[Accessing Various ArcGIS Online Services](#)

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.



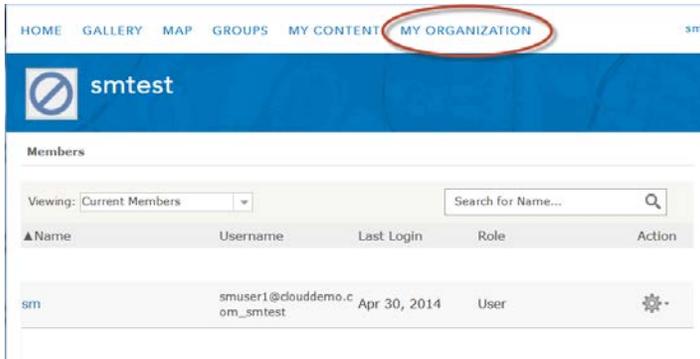
- This will automatically direct the user to the login page of Identity Provider (SiteMinder).
- Enter the credentials and click login:



- 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

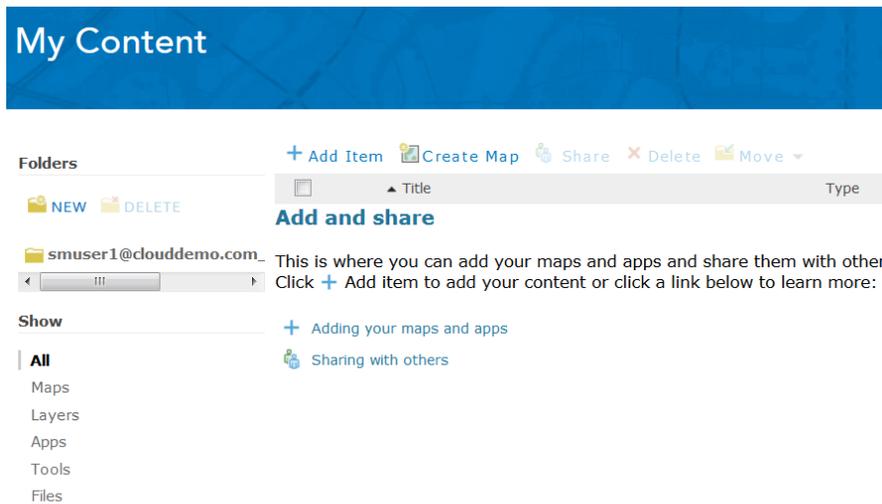
After federation login to ArcGIS Online, the following services can be accessed by the user:

- 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:

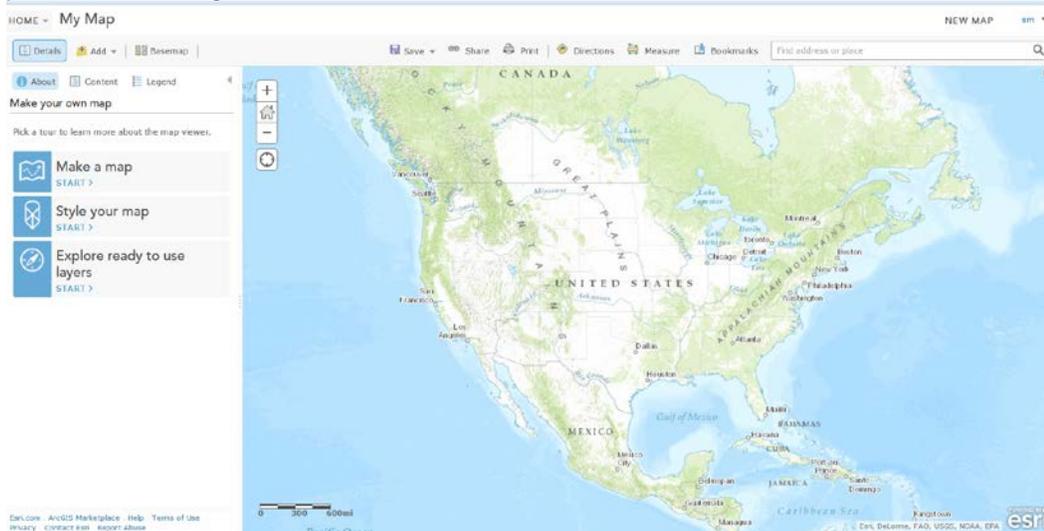
- URL - <https://<org>.maps.arcgis.com/home/content.html>
- Type in the login credentials at the Identity Provider site and get to ArcGIS Online My Content



ArcGIS Online Organization Web Application Authoring

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

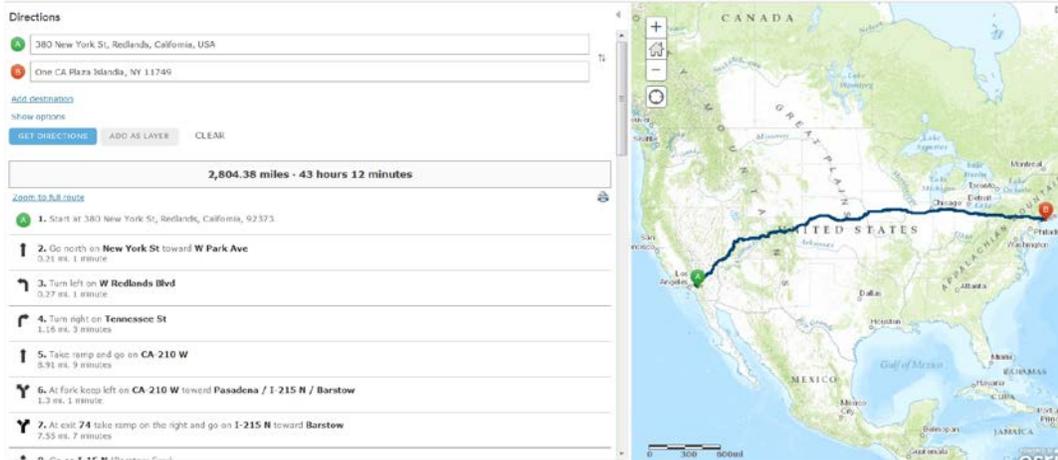
- URL - <https://<org>.maps.arcgis.com/home/webmap/viewer.html?useExisting=1>
- Type in the login credentials at the Identity Provider site and get to ArcGIS Online Web Application Authoring service.



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”



Directions

380 New York St, Redlands, California, USA

One CA Plaza Barstow, WY 11749

[Add destinations](#)

Show options

GET DIRECTIONS **ADD AS LAYER** **CLEAR**

2,804.38 miles · 43 hours 12 minutes

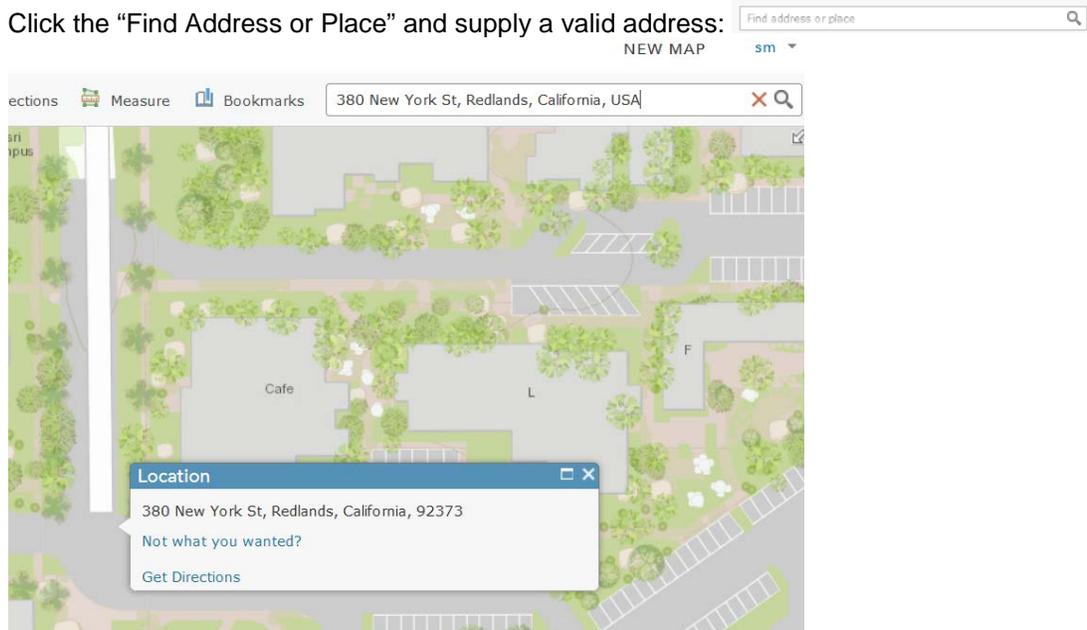
[Zoom to full route](#)

1. Start at 380 New York St, Redlands, California, 92373.
2. Go north on **New York St** toward **W Park Ave**
0.31 mi. 1 minute
3. Turn left on **W Redlands Blvd**
0.27 mi. 1 minute
4. Turn right on **Tennessee St**
1.16 mi. 3 minutes
5. Take ramp and go on **CA 210 W**
5.91 mi. 9 minutes
6. At fork keep left on **CA 210 W** toward **Pasadena / I-215 N / Barstow**
1.3 mi. 1 minute
7. At exit **24** take ramp on the right and go on **I-215 N** toward **Barstow**
7.53 mi. 7 minutes

ArcGIS Online Organization Geocoding Service

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

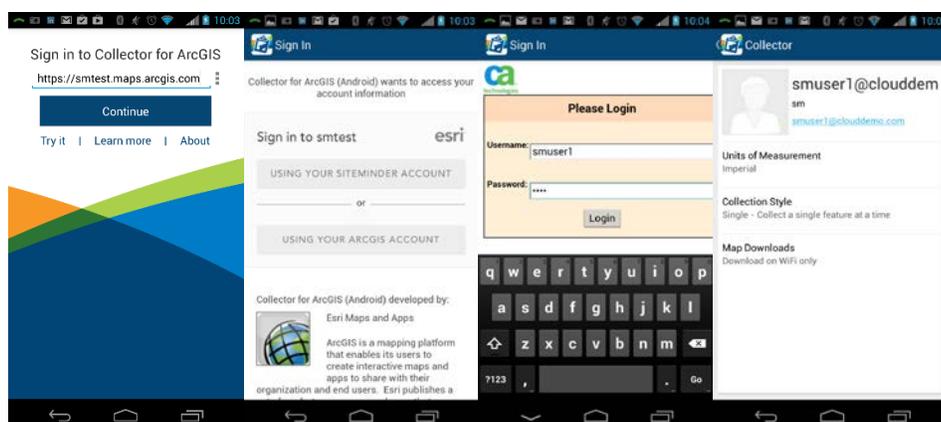
- URL - <https://<org>.maps.arcgis.com/home/webmap/viewer.html?useExisting=1>
- Type in the login credentials at the Identity Provider site and get to ArcGIS Online Geocoding Service.
- Click the “Find Address or Place” and supply a valid address:



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.*)



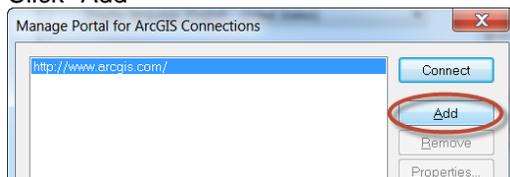
- Click “Advanced...”



- Click “Manage Portal Connections...”



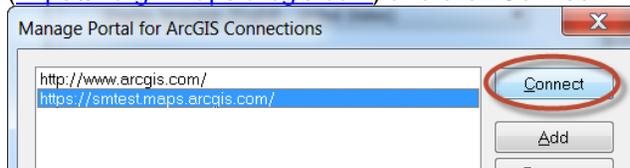
- Click “Add”



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

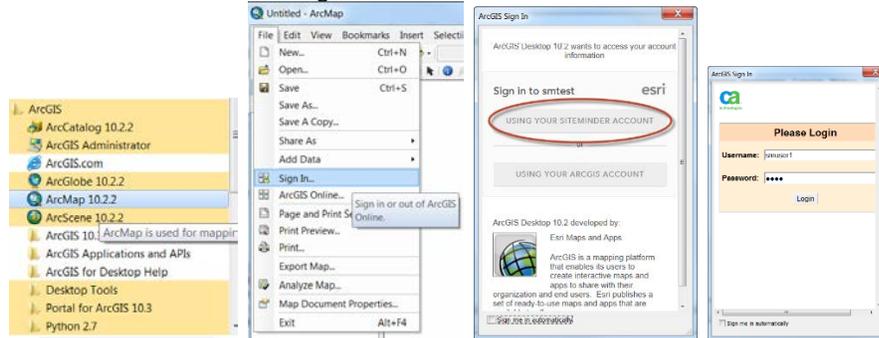


- Select the newly created connection to the ArcGIS Online Organization (<https://<org>.maps.arcgis.com>) and click Connect.



- 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:

[When the SiteMinder Partnership is Inactive](#)

[User who is not in the ArcGIS Online Organization trying to login through SiteMinder](#)

[Expired certificate on SiteMinder side](#)

[When Service Provider Assertion Consumer URL was Misconfigured on the SiteMinder Side](#)

[When Identity Provider Entity ID was Misconfigured on the Target Application Side](#)

[When Identity Provider SSO URL was Misconfigured on the Target Application Side](#)

[When Identity Provider Certificate was Misconfigured on the Target Application Side](#)

Exception Cases

When the SiteMinder Partnership is Inactive

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

The following error occurred: 403 - Request Forbidden. Transaction ID: d5ddb24a-950bf795-1a3cf7c7-0bcb12dc-82689d7c-bc failed.

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.

This account is setup with sign in by invitation only, you need to receive an invitation from the account administrator



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-
piblpghaigikhdieoilebpfaoibohmamp1" IssueInstant="2012-12-27T13:29:00Z" Ver-
sion="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>

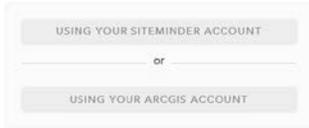
Message that appears on browser

The following error occurred: 500 - Internal Error occurred while trying to process the request. Transaction ID: 276f8b31-154b7a4b-383eba10-7ee1a10f-e2c34b

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.