A Practical Guide to ArcGIS Online Security

Andrea Rosso
Jeff Smith

2018 Esri DEVSummit Conference | Palm Springs, CA
ArcGIS Online – A Multi-Tenant System
Topics

- Portal Information Model
- Feature Layer Security
- Authentication and SAML integration
- Integrating your apps with OAuth 2.0
- Portal Security Settings
Portal Information Model

REST API ➔ https://www.arcgis.com/sharing/rest

Web and Runtime SDKs
- Javascript
- Android
- iOS
- Java
- macOS
- .NET
- Qt
- Python
Portal

- Your Organization
- Custom Url (yoururl.maps.arcgis.com)
- Public or Private

https://www.arcgis.com/sharing/rest/portals/jIL9msH90I208GGb

```javascript
portal = new Portal()
```
Items

- Typed
  - Web Map
  - Services
  - Data
  - ...

- Private by default
- Can Share to
  - Groups
  - Organization
  - Everyone/Public

JS API:
```javascript
var item = new PortalItem({
    id: "1ae674dcf9c2440197b36bff57718e0c",
    "owner": "sampleuser",
    "title": "Restaurant Finder",
    "type": "Web Mapping Application",
    "snippet": "Palm Springs Restaurant Finder",
    "thumbnail": "thumbnail/RF_Thumbnail.jpg",
    "url": "https://hostname/index.html",
    "access": "public",
});
item.load();
```
Users

- Users own items and groups
- Discoverable
  - No one
  - Organization
  - Everyone

- Users have a profile
- Users have a Role

https://www.arcgis.com/sharing/rest/community/users/sampleuser

```js
{  
  "username": "SampleUser",  
  "fullName": "Sample User",  
  "culture": "en",  
  "region": "WO",  
  "units": "metric",  
  "thumbnail": "thumbnail.jpg",  
...
}
```

JS API:

```js
portal.user.fetchItems().then(
    function(fetchItemResult){
      fetchItemResult.items.forEach(
        function(item){
          title = item.title;
        });
    });
```
User Roles

- **Built-in Roles**
  - Administrator
  - Publisher
  - User
  - Viewer

- **Custom Roles**
  - Templates
  - Fine Grained Privileges

https://www.arcgis.com/sharing/rest/community/users/sampleuser

```json
{
  "username": "SampleUser",
  "fullName": "Sample User",
  ...
  "role": "org_admin",
  "privileges": [
    "features:user:edit",
    "features:user:fullEdit",
    "marketplace:admin:manage",
    "marketplace:admin:purchase",
    "marketplace:admin:startTrial",
    "opendata:user:designateGroup",
    "opendata:user:openDataAdmin",
    "portal:admin:assignToGroups",
    "portal:admin:changeUserRoles",
    "portal:admin:deleteGroups",
    ...
  ]
}```
Groups

- Contain Items and Users
- Users have access to items in group
- Groups can be visible to:
  - No one (private)
  - Organization
  - Everyone
  - Items do not inherit visibility
- Group owners can share items to their own groups
- Use cases
  - Access
  - Collections

https://www.arcgis.com/sharing/rest/community/groups/47261cd6c04b426789babc3f101a4c03

{  
  "id": "47261cd6c04b426789babc3f101a4c03",  
  "title": "Living Atlas: People",  
  "isInvitationOnly": true,  
  "owner": "esri_atlas",  
  "sortField": "title",  
  "sortOrder": "asc",  
  "isViewOnly": false,  
  "thumbnail": "people.jpg",  
  "access": "public",  
  ...  
}
Groups with Update Capability

- **Specialized Groups**
  - All members can update included items

- **Restrictions**
  - Can only be created by Admins
  - Items and Users must be within Org
  - Capability cannot be toggled

- **Use Cases**
  - Shift Operators
  - Collaborative Editing
Feature Layer Security and Editing

- **Users who always can edit**
  - Owner
  - Admins
  - Members of Groups w/ Update

- **Enable Editing**
  - Anyone who can access the service
  - Options
    - Add, update and delete features
    - Only update feature attributes
    - Only add new features
  - Custom Roles can have Edit or Edit with full control privileges

- **Options**
  - Add, update and delete features
  - Only update feature attributes
  - Only add new features

Custom Roles can have Edit or Edit with full control privileges.
Hosted Feature Layer Views

- A Feature Layer based on another Feature Layer
- Can have different settings:
  - Sharing
  - Editing
  - Export
  - Filters
  - Metadata
  - Time settings
- Can only be created by owner of base layer
- “Allow only standard SQL queries” should be true
Authentication Options

ArcGIS Account

Social Account

Enterprise Account
Enterprise Identities

- Use your own identity provider
  - SAML 2.0
  - ADFS
  - NetIQ Access Manager
  - Shibboleth
  - ....
- Can add users:
  - Automatically upon login
  - With an Invitation
- Can use ArcGIS Online identities with Enterprise Identities
- Enterprise groups are now supported
Demo

Configure ArcGIS Online with enterprise identity provider
Integrating ArcGIS Online with Apps using OAuth 2.0

- OAuth 2.0 is a standard for handling authentication decisions among various web-enabled devices and servers.
Integrating Web Apps with ArcGIS Online using OAuth

1. Register Application

2. Sign In

3. Redirect_uri

4. Portal

(client_id)
Integrating Apps with ArcGIS Online using OAuth

1. Register Application
2. Sign In
3. Redirect_uri

client_id

Portal
Trust Boundaries

ArcGIS Online

Esri Apps
- Geonet
- Training
- My Esri
- ..... 

Trusted Apps:
- App Launcher Apps
- Marketplace Apps

Other Third Party Apps

Esri Access
Login
Demo

Registered Web Application
Organizational Controls

- Use only HTTPS
- Anonymous Access
- Standardized Queries
- Disable User Profile
- Sharing to Everyone
Organizational Controls

- Social Logins
- Allow Portal Access

Social Logins

You can set up your organization so that your members will be able to sign up and sign in to ArcGIS using the logins that they use with social networks like Facebook and Google.

Configure

Allow Portal Access

Do you need members of your organization to use enterprise logins to access secured content through web applications hosted on other portals? If so, add the portal instance (e.g., https://webadaptor.domain.com/arcgis) hosting those applications to the list below. The map viewer and the web applications hosted under the Apps folder of the specified portal will be able to access your organization. Portals your organization collaborates with automatically have access to your organization.

Add Portal

Portals:

https://devsummit1.webgisesting.net/portal
SAML Access from an ArcGIS Enterprise Web Application

Bring secure layers from ArcGIS Online into a central web mapping application
Demo

Allow Portal Access
Organizational Controls

- Allow Origins
- Trusted Servers

**Allow Origins**

ArcGIS Online allows an organization to limit the web application domains that can connect via Cross-Origin Resource Sharing (CORS) to the ArcGIS REST API. By default, the ArcGIS REST API is open to CORS requests from an application on any domain. Administrators can limit CORS access to specific domains by specifying the domains in the list below. For example, if you have a web application hosted on acme.com and you want to limit CORS access to only acme.com, you will need to enter acme.com in the list below. Note that applications running on arcgis.com are always allowed REST API access to ArcGIS Online.

![Add Domain Button]

Domains

https://toddor4.arcgis.com

**Trusted Servers**

Configure the list of trusted servers you wish your organization to send credentials to when working with services secured with web-tier authentication. Changes made to this list are only applied when Save is clicked.

![Add Server Button]

Servers

devsummit1.webgistesting.net
Restrict Cross-Domain (CORS) Requests

- For JavaScript applications, a common method used to make cross domain requests is called a CORS request (cross origin resource sharing).
- Primarily used when making cross domain POST requests.
Trusted Servers

- A list of servers to where web-tier credentials will be passed when an ArcGIS Online web map application makes a CORS request to a secured resource.
Demo

Trusted Servers
Administrator Controls on Users

- Admins can
  - Manage Items, Groups, Profile
  - Disable Users
  - Delete Users
  - Reset User’s Password
  - Change Role
  - Enable Esri Access
Multi-Factor Authentication

- Additional security with second factor at login
- Support for Google Authenticator or MS Authenticator
- Admin needs to enable for Organization
- Must have 2 admins
- Users setup their own Multi-factor
Password Policies

- Default Password Policy
  - 8 characters with at least 1 number
- Can Customize
  - Complexity
  - History
  - Expiration
Keeping Track of Usage

- Status Reports
  - Credits
  - Content
  - Members
  - Groups
Cloud Infrastructure Provider Compliance

- ArcGIS Online Utilizes World-Class Cloud Infrastructure Providers
  - Microsoft Azure
  - Amazon Web Services
Please Take Our Survey!

Download the Esri Events app and find your event

Select the session you attended

Scroll down to the “Feedback” section

Complete Answers, add a Comment, and Select “Submit”