A Practical Guide to ArcGIS Online Security

Andrea Rosso

Jeff Smith
ArcGIS Online – A Multi-Tenant System
Topics

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

Groups

Portal

Items

Users

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/jIgL9msH9O1208GGb

{  
    "access": "public",  
    "allSSL": true,  
    "commentsEnabled": true,  
    "culture": "en",  
    "thumbnail": "thumbnail.jpg",  
    "units": "english",  
    "urlKey": "yoururl",  
    ...
}

JS API:

portal = new Portal()
Items

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

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

```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

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

JS API:

```javascript
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

```json
{
  "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

- Editor Tracking Options
  - Editors can only see their own features
  - Editors can only edit their own features
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
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
Integrating Apps with ArcGIS Online using OAuth

1. Register Application
2. Sign In
3. Redirect_uri
4. client_id
5. Portal

client_id
Demo
Registered Web Application
Organizational Controls

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

- Trusted Servers
- Allow Portal Access
Trusted Servers

- A list of servers to where credentials will be passed when making a CORS request to access secured resources.
Demo

Trusted Servers
SAML Access from an ArcGIS Enterprise Web Application

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

Allow Portal Access
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 Polices

• 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
Privacy & Compliance

Privacy

- TRUSTe
- Privacy Shield Framework

Compliance

- FISMA Authorization & Accreditation
- FedRAMP

Answers

- trust.arcgis.com
- CSA Cloud Security Alliance®
Please Take Our Survey! – No more memorizing Session ID numbers!! 😊

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”