A Practical Guide to ArcGIS Online Security

Andrea Rosso
Jeff Smith
ArcGIS Online – A Multi-Tenant System
Topics

- Portal Information Model
- Feature Layer Security
- User Administration and Authentication
- Integrating your apps with OAuth 2.0
- Portal Security Settings
- Encryption and Compliance
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/ILLmsH90I208Ggb

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

JS API:

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

- Typed
  - Web Map
  - Services
  - Data
  - …

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

https://www.arcgis.com/sharing/rest/content/items/1ae674dcf9c2440197b36bff57718e0c

```json
{
  "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",
}
```

JS API:

```javascript
var item = new PortalItem(
  {
    id: "1ae674dcf9c2440197b36bff57718e0c"
  });
item.load();
```
Users

- Users own items and groups
- Discoverable
  - No one
  - Organization
  - Everyone
- Users have a profile
- Users have a Role

More information:

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

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

Sample JSON:

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

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

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

---

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

```
{
  "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

Who can view this group?
- Only group members
- People in the organization (Esri Developers Summit 2019)
- Everyone (public)

Who can join this group?
- Those who request membership and are approved by a group manager
- Only those invited by a group manager
- Members of an enterprise group
- Anyone

Who can contribute content to the group?
- Group members
- Only group owner and managers

What items in the group can its members update?
- Only their own items
- All items (group membership is limited to the organization)
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
    - ...

Options:
- Add, update and delete features
- Only update feature attributes
- Only add new 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
User Administration and Authentication

- **Add Users**
  - Pre-Create users with username/password
  - Send user an email invitation with username
  - Send user an email invitation for new user
  - Auto join (if using Enterprise logins)

- **Admins can**
  - Manage licenses and user types
  - Manage Items, Groups, Profile
  - Disable and Delete Users
  - Reset User’s Password
  - Change Role
Authentication Options – ArcGIS Accounts

- **Username and Password Accounts**
- **Multi-Factor Authentication**
  - Google or Microsoft Authenticator
  - Recommended for Administrators
  - Must have 2 Administrators
- **Password Policy**
  - Length
  - Complexity
  - Expiration
  - History

**Password Policy**
Set the password policy for members in your organization that have ArcGIS accounts. Note that member passwords may not match their username. Weak passwords may be rejected. You may set the following rules for these passwords by checking them on and specifying a number where requested.

Passwords must
- ✔ Contain at least the following number of characters: 12
- ✔ Contain at least one letter (A–Z, a–z)
- ✔ Contain at least one upper case letter (A–Z)
- ✔ Contain at least one lower case letter (a–z)
- ✔ Contain at least one number (0–9)
- ✔ Contain at least one special (non-alphanumeric) character
- ✔ Expire after the following number of days: 90
- ✔ Not reuse the following number of last passwords: 5
Authentication Options – Social Accounts

- Google or Facebook
- Administrator can enable
Authentication Options – Enterprise IDP

• 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 or Social with Enterprise Identities

• Enterprise groups are supported
Configure ArcGIS Online with enterprise identity provider

Demo
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
   - client_id

2. Sign In
   - client_id

3. Redirect_uri

4. Portal
Integrating Apps with ArcGIS Online using OAuth

1. Register Application
   - client_id

2. Sign In
   - client_id

3. Redirect_uri

4. A

5. A

Portal
Registered Web Application

Demo
Organizational Controls

- Anonymous Access
- Profile Visibility
- Sharing to Everyone

Security
Configure the security settings for your organization.

Policies

- Allow anonymous access to your organization's website, devdemo.maps.arcgis.com. What does this mean?
  - Allow members to edit biographical information and who can see their profile.

Sharing and Searching

- Members can share content publicly.
- Members can search for content outside the organization.
- Show social media links on item and group pages.
Organizational Controls

- 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 instances (e.g., https://webadaptor.domain.com/arcgis) hosting these 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. Portal's your organization collaborates with automatically have access to your organization.

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

Bring secure layers from ArcGIS Online into a central web mapping application
Allow Portal Access

Demo
Organizational Controls

- 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.

Domains

https://devsummit.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
Keeping Track of Usage

- **Status Reports**
  - Credits
  - Content
  - Apps
  - Members
  - Groups

- **Activity Log**
  - Export as CSV
  - Audit log of changes to Organization
Encryption

• Encryption in Transit
  - HTTPS
  - HSTS
  - Older subscriptions might still allow http

• Encryption at Rest
  - All customer data is encrypted at rest
ArcGIS Security Update – TLS 1.2

• Esri is committed to using the latest industry standards and best practices for security protocols

• On April 16, 2019, we are updating ArcGIS Online to enforce the use of TLS (Transport Layer Security) version 1.2

• What Does This Mean For You?
  - Users of most ArcGIS software or custom solutions using Esri technology may be affected by this planned update - If you have not updated and validated your system's support for TLS v1.2 only, you may lose your ability to connect to ArcGIS Online.

• What Do You Need to Do?
  - Go to the Esri TLS Support page for information, patches, and instructions for updating software:

  support.esri.com/en/tls
Cloud Infrastructure Provider Compliance

• ArcGIS Online Utilizes World-Class Cloud Infrastructure Providers
  - Microsoft Azure
  - Amazon Web Services
Privacy & Compliance

Privacy

- TRUSTe
- Privacy Shield Framework
- GDPR

Compliance

FedRAMP

Answers

trust.arcgis.com

CSA Cloud Security Alliance
Please Take Our Survey on the App

Download the Esri Events app and find your event

Select the session you attended

Scroll down to find the feedback section

Complete answers and select “Submit”
Presentation Title

Presenter Names
Click Here
For DEMO
Sample Name Here
Please Take Our Survey on the App

Download the Esri Events app and find your event

Select the session you attended

Scroll down to find the feedback section

Complete answers and select “Submit”