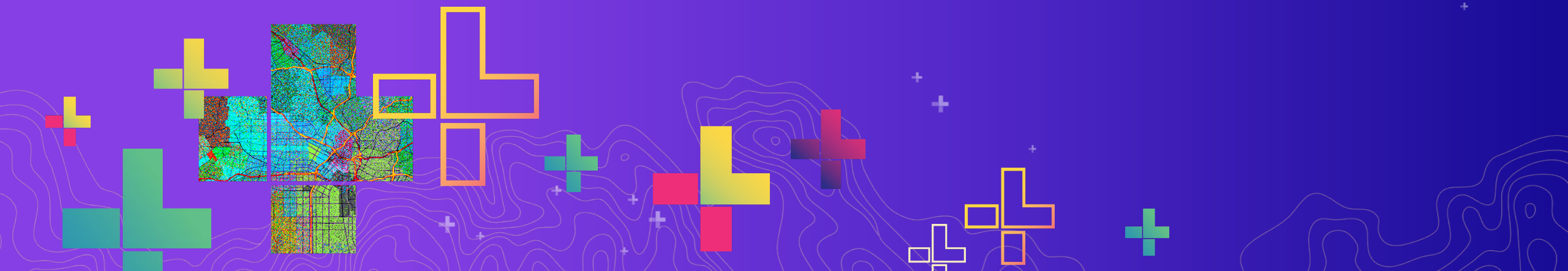
esri | THE SCIENCE OF WHERE

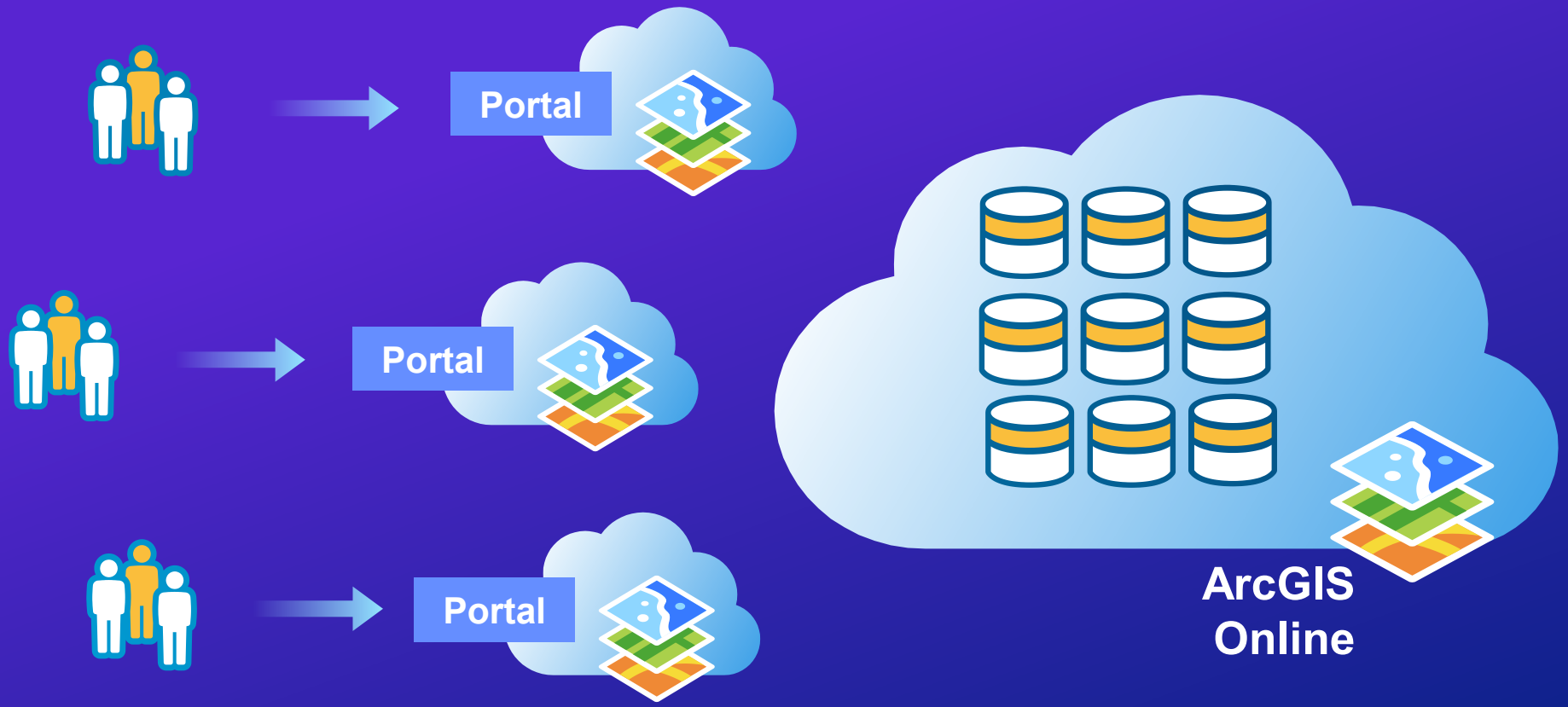
A Practical Guide to ArcGIS Online Security

Andrea Rosso, Jeff Smith

2020 ESRI DEVELOPER SUMMIT | Palm Springs, CA



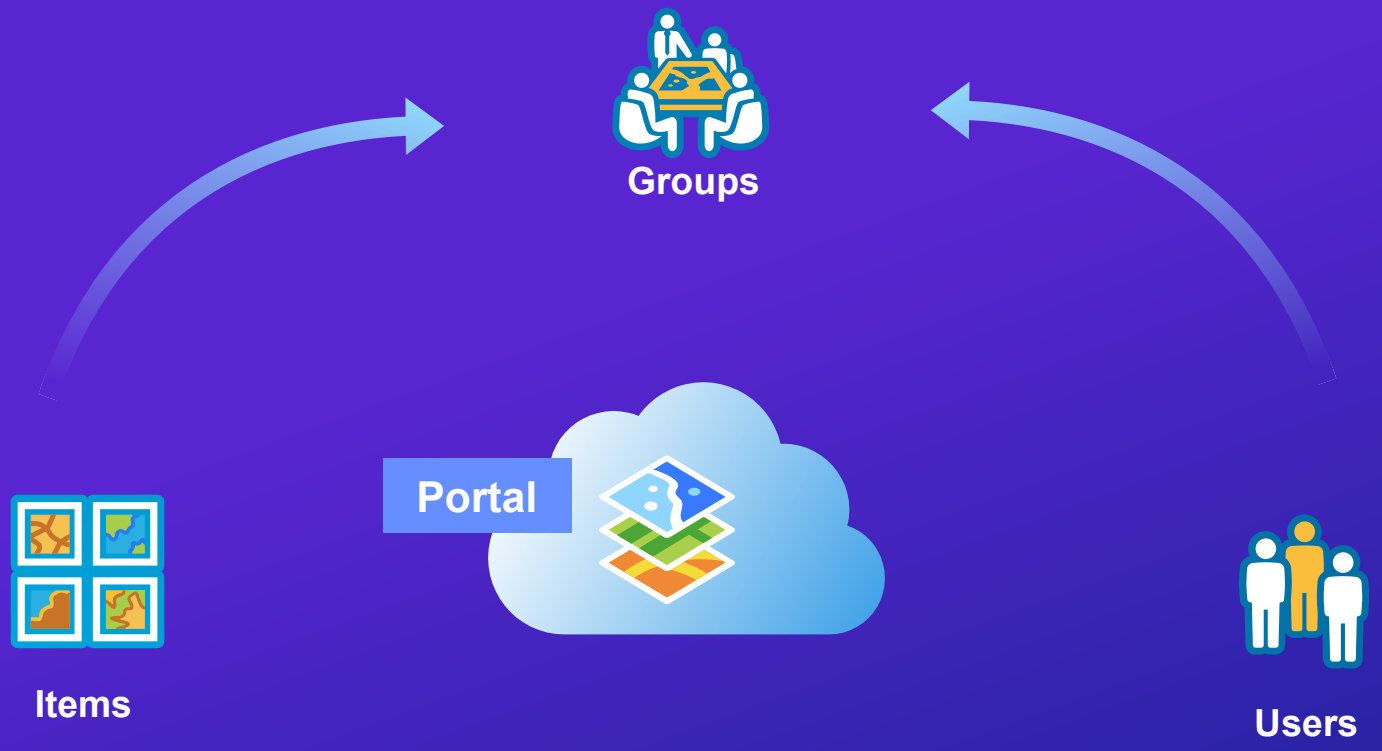
ArcGIS Online – A Multi-Tenant System



Topics

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

Portal Information Model

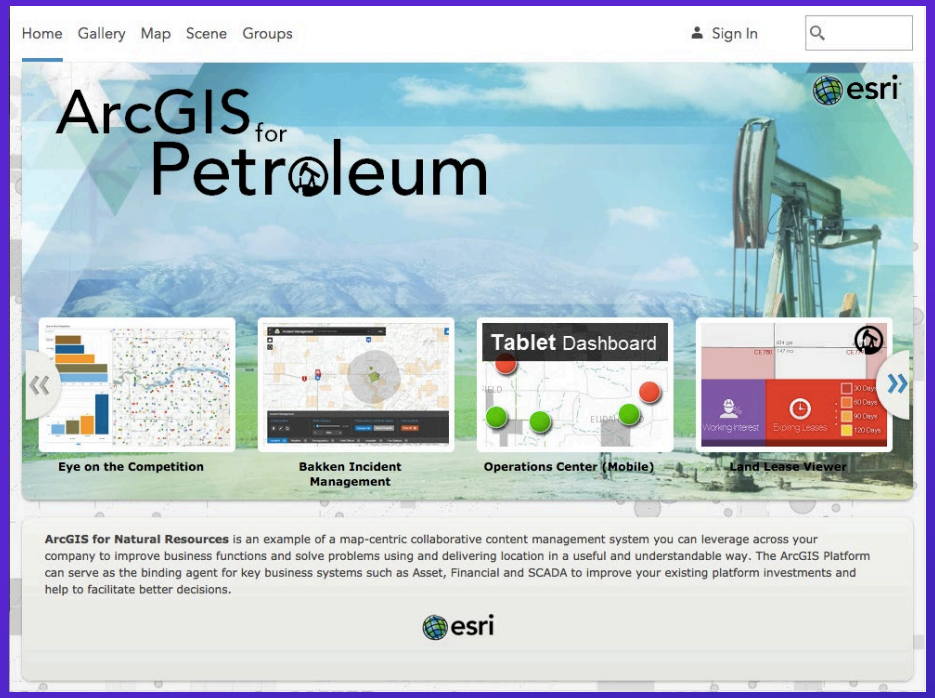


REST API → https://www.arcgis.com/sharing/rest

Web and Runtime SDKs

- Javascript
- Android
- iOS
- Java
- macOS
- .NET
- Qt
- Python

Portal



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

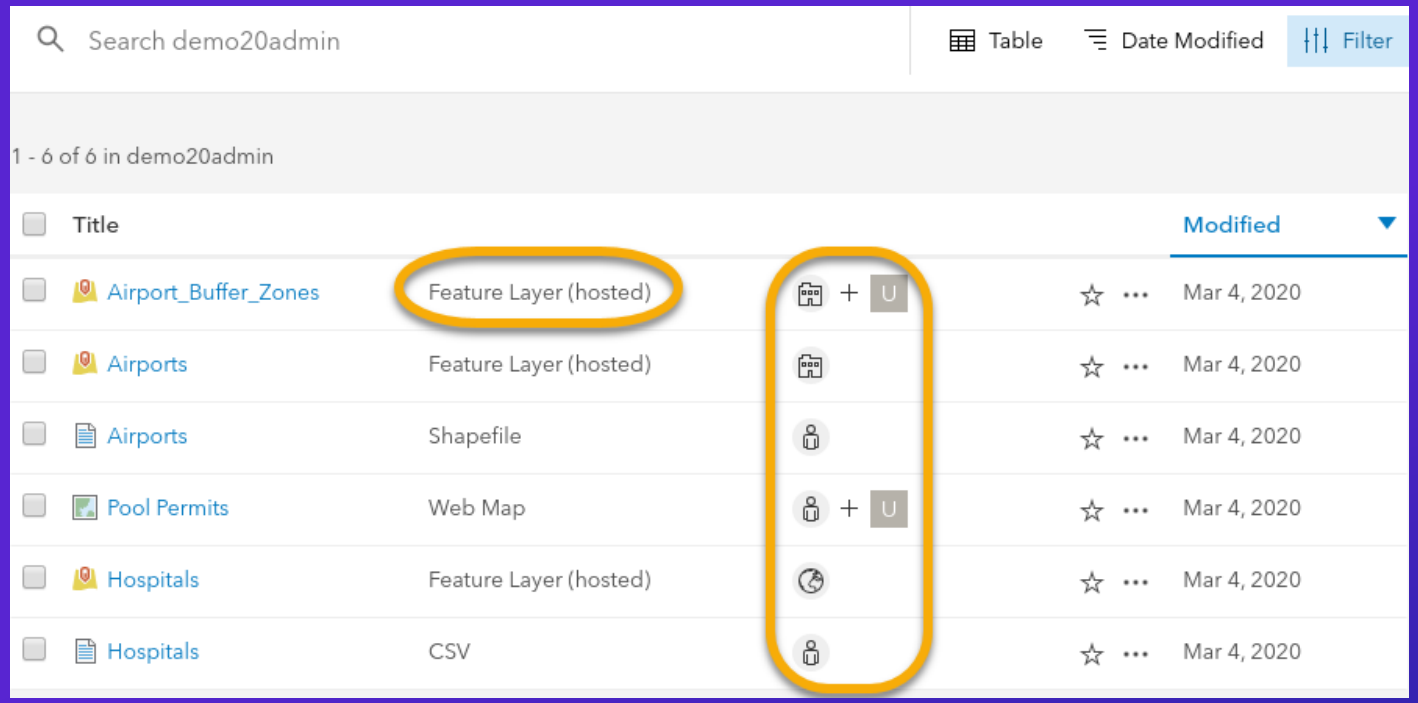
```
https://www.arcgis.com/sharing/rest/portals/jIL9msH9OI208GGb

{
  "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

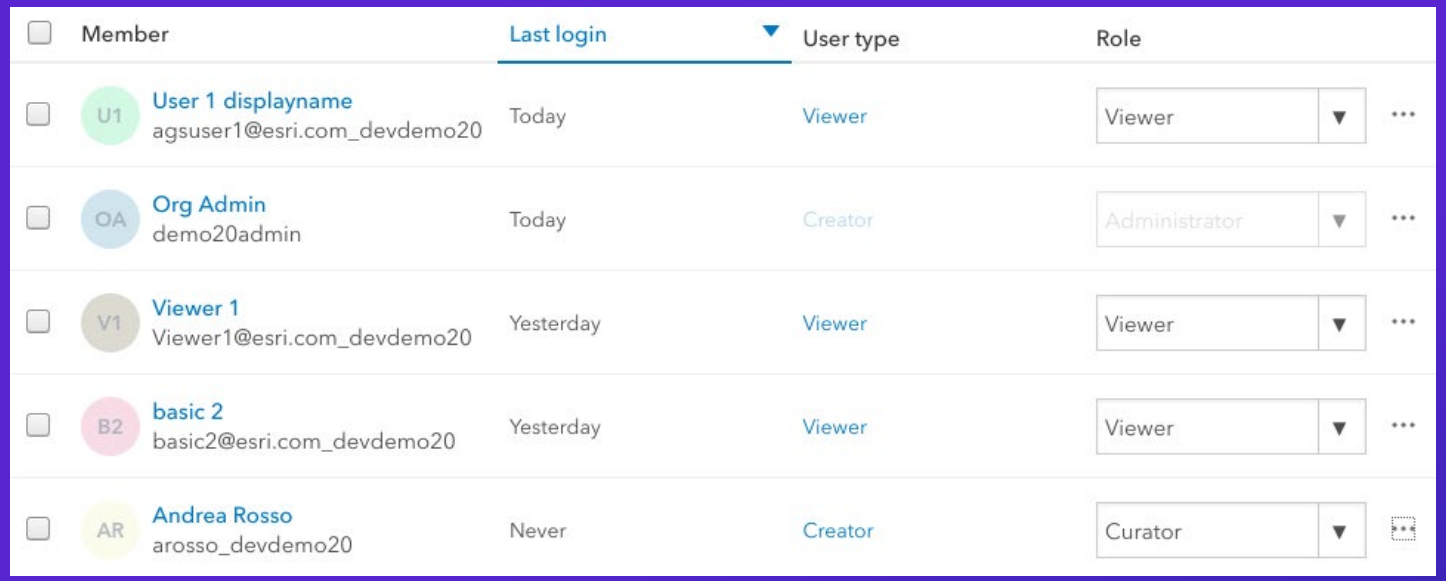
```
https://www.arcgis.com/sharing/rest/content/items/1ae674dcf9c2440197b36bff57718e0c

{
  "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:

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

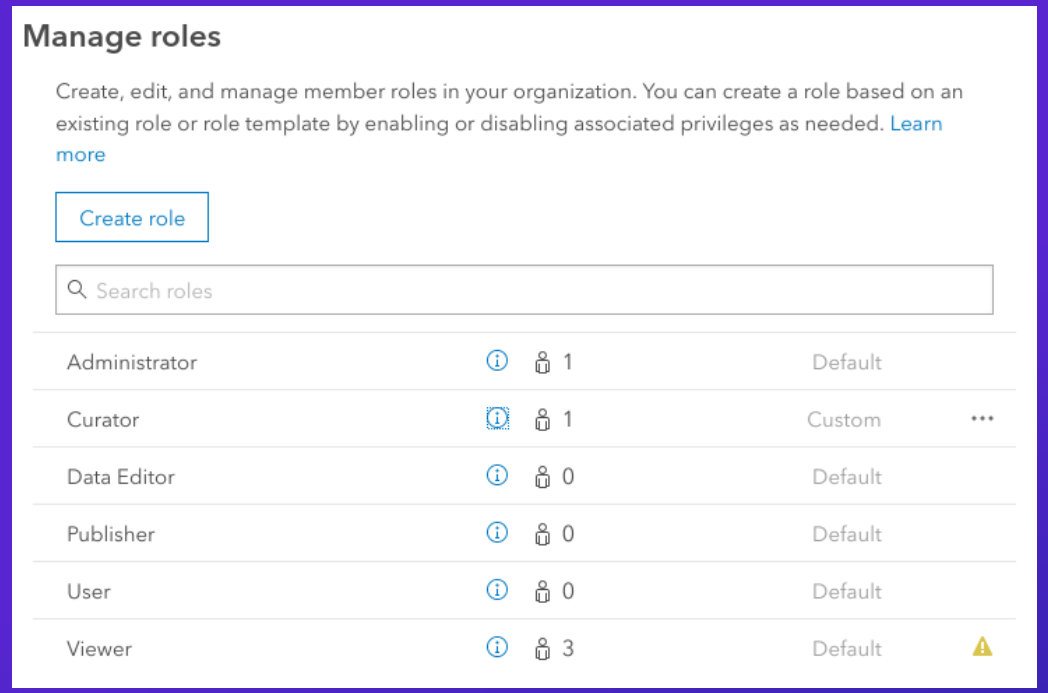
```
https://www.arcgis.com/sharing/rest/community/users/sampleuser

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

JS API:

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

User Roles

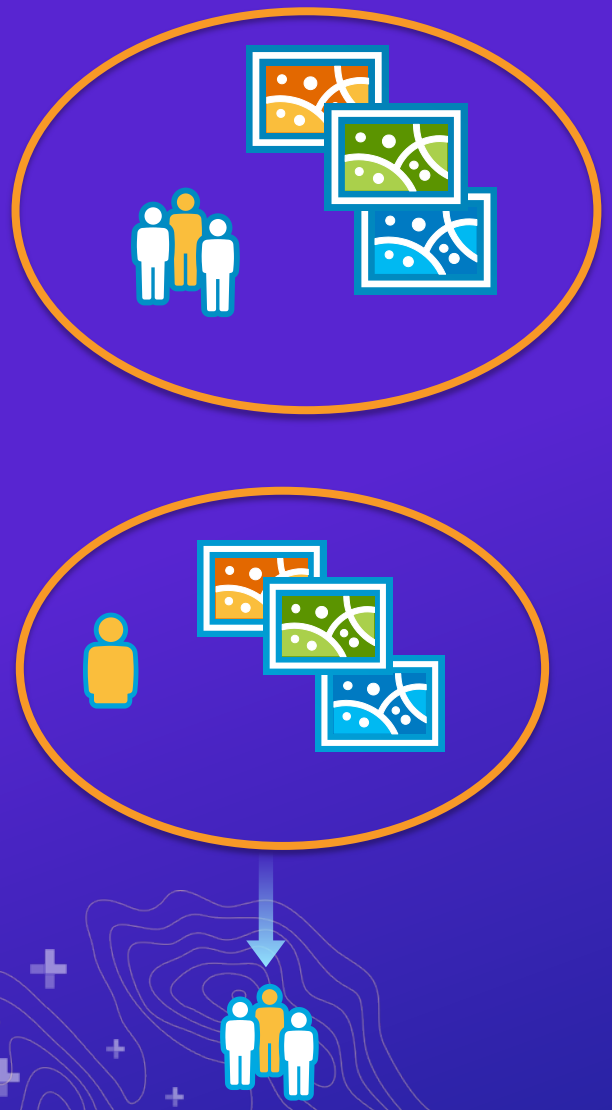


- **Built-in Roles**
  - Administrator
  - Data Editor
  - Publisher
  - User
  - Viewer
- **Custom Roles**
  - Templates
  - Fine Grained Privileges

```
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



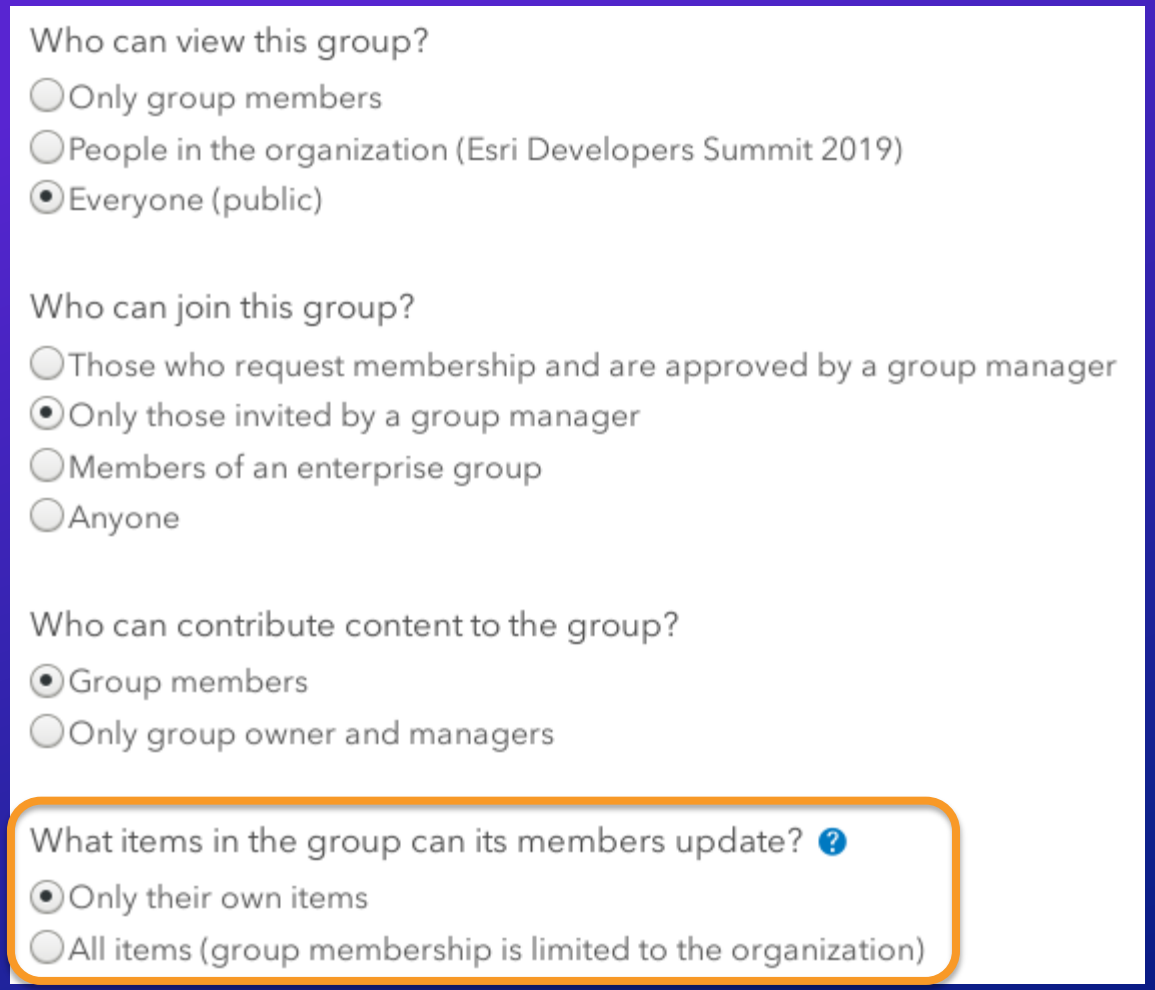
- Contain Items and Users
- Users have access to items in group
- Groups can be visible to:
  - No one (private)
  - Organization
  - Everyone
  - Items do not inherit visibility
- Group owners can share items to their own groups
- Use cases
  - Access
  - Collections

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

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

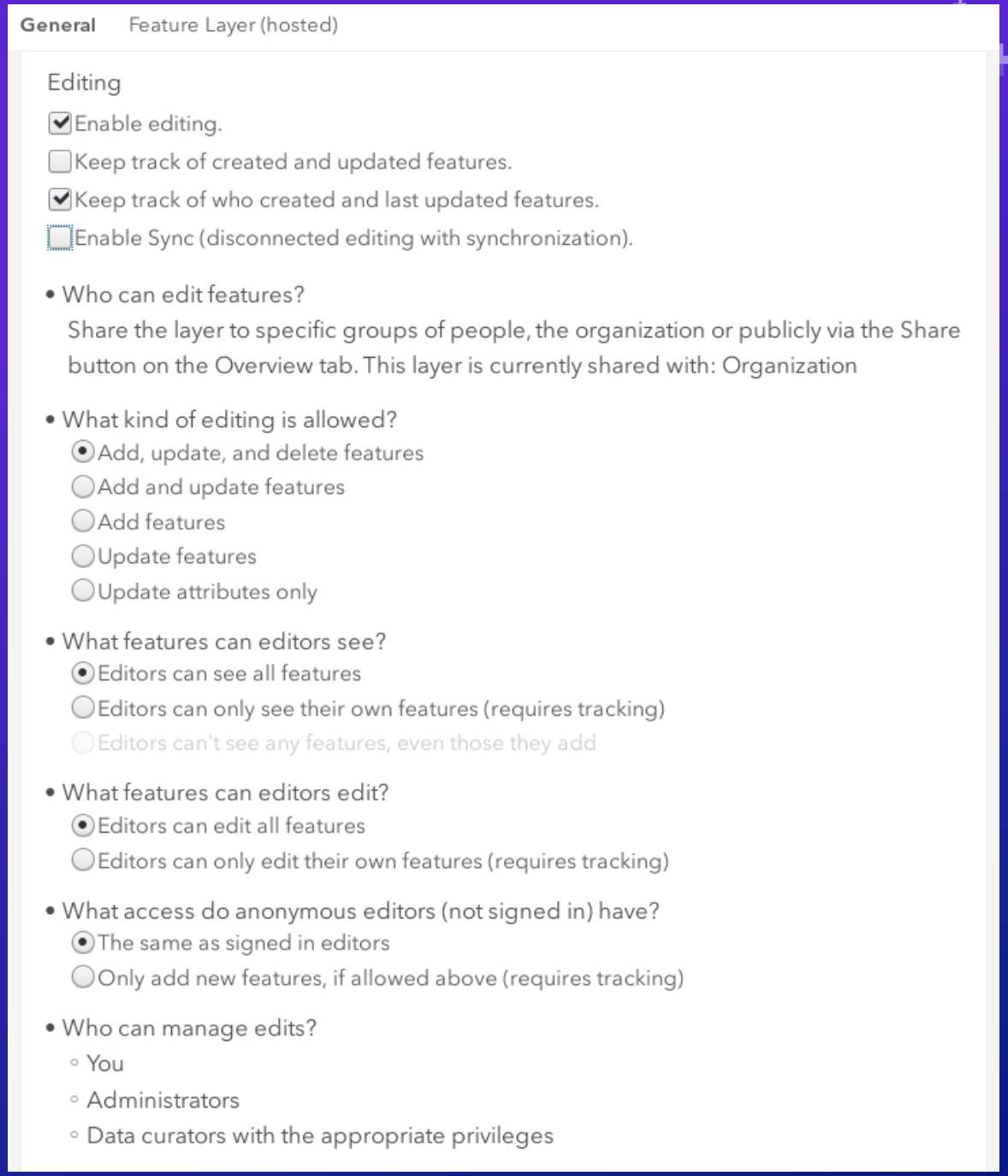
Groups with Update Capability

- 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



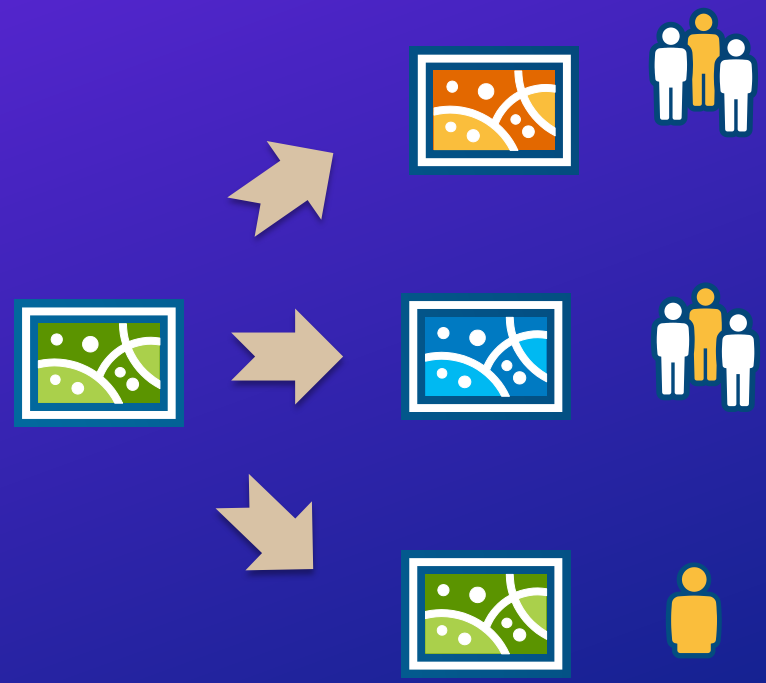
Feature Layer Security and Editing

- 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
    - …



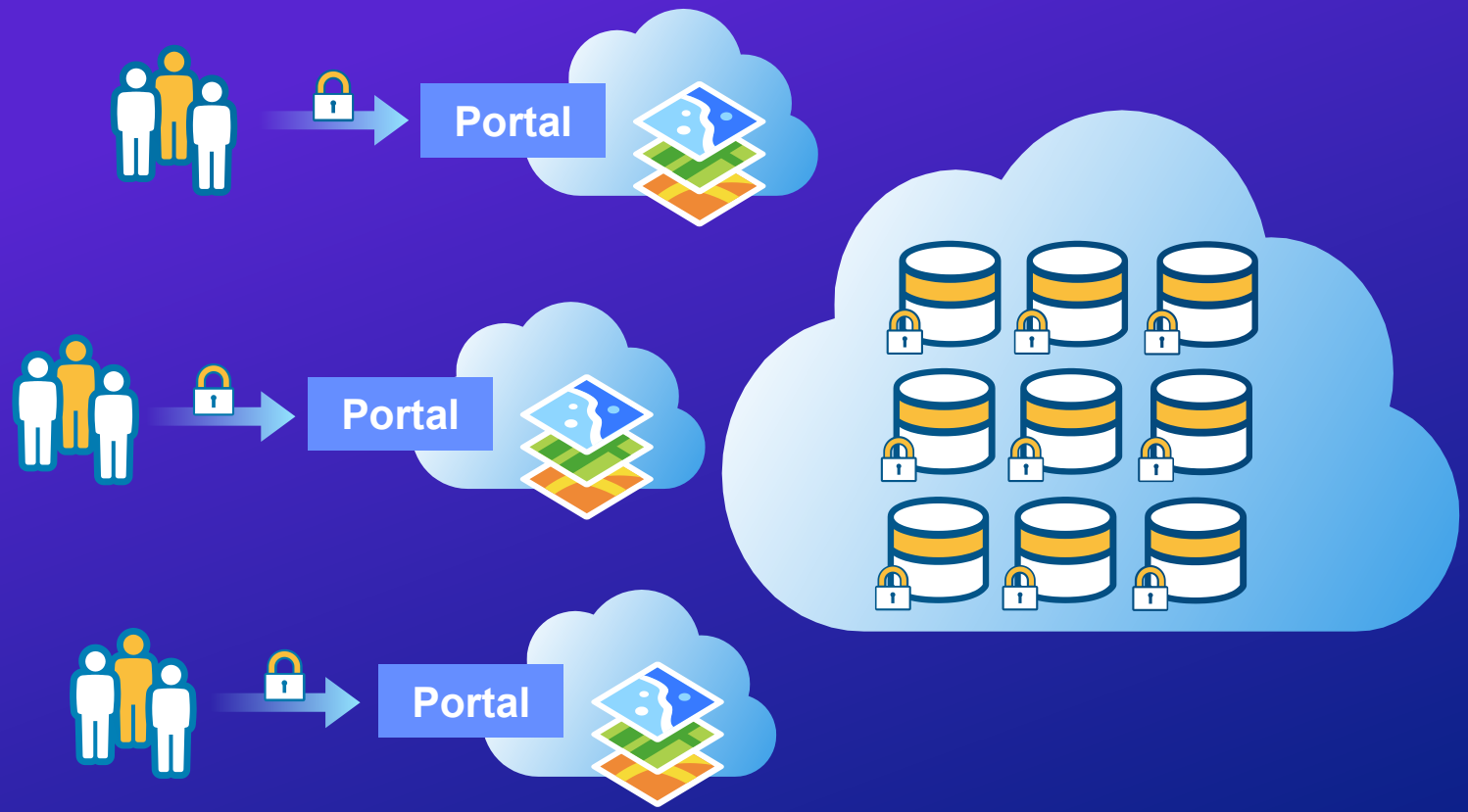
Hosted Feature Layer Views

- 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

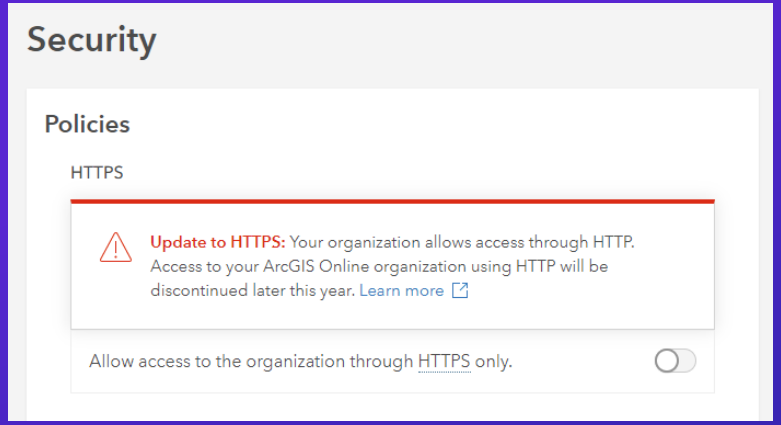


Encryption

- Encryption in Transit
  - HTTPS
  - HSTS
  - Older subscriptions might still allow http
- Encryption at Rest
  - All customer data is encrypted at rest



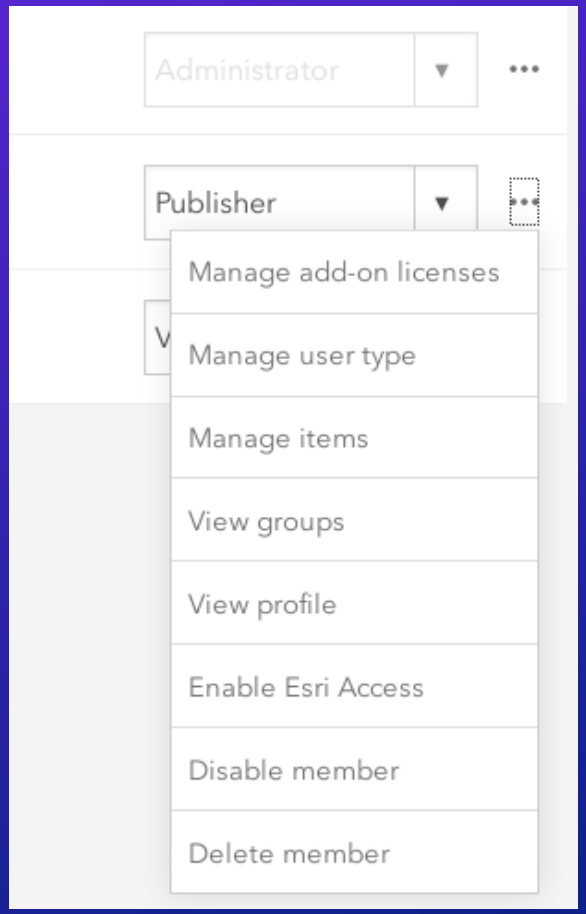
ArcGIS Security Update – HTTPS Only



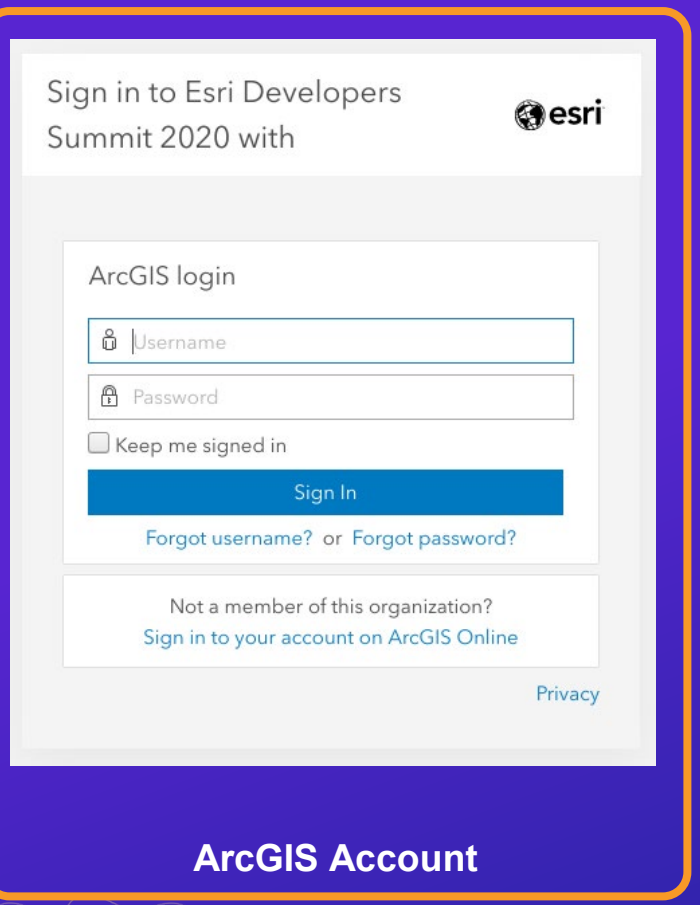
- **Esri is committed to ensuring your content is secure**
  - TLS 1.2 implemented in 2019
  - HTTPS Only / HSTS to be enforced *late September 2020*
- **What does this mean for you?**
  - Browser calls to HTTP endpoints will fail due to mix-content blocking
  - HTTP requests to ArcGIS Online will be redirected to HTTPS. Clients limited to HTTP only will fail.
- **What do you need to do?**
  - Validate your ArcGIS Online org utilizes HTTPS only immediately.
    - *If not, enforce HTTPS for your orgs ASAP and validate clients/scripts can use HTTPS*
    - Launch AGO Security Advisor tool to check your org settings @ Trust.ArcGIS.com
  - Keep an eye out for additional announcements and support guidance pages

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

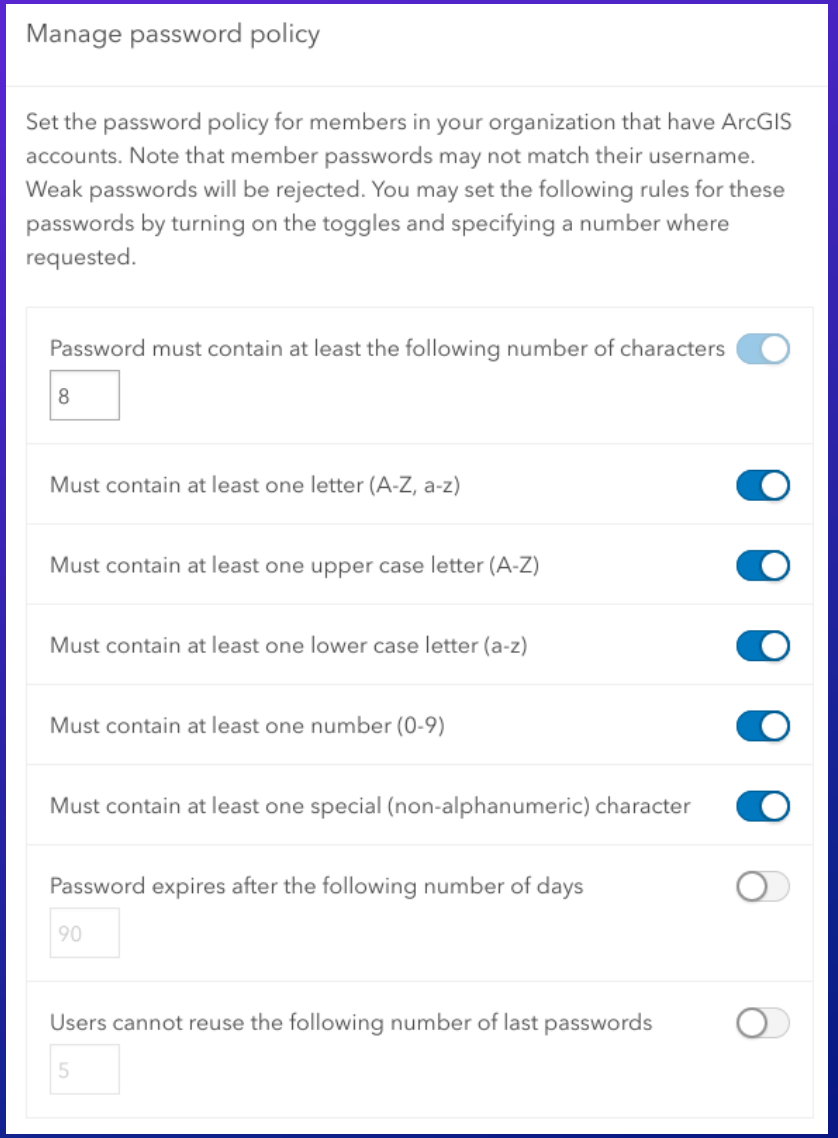


Authentication Options – ArcGIS Accounts

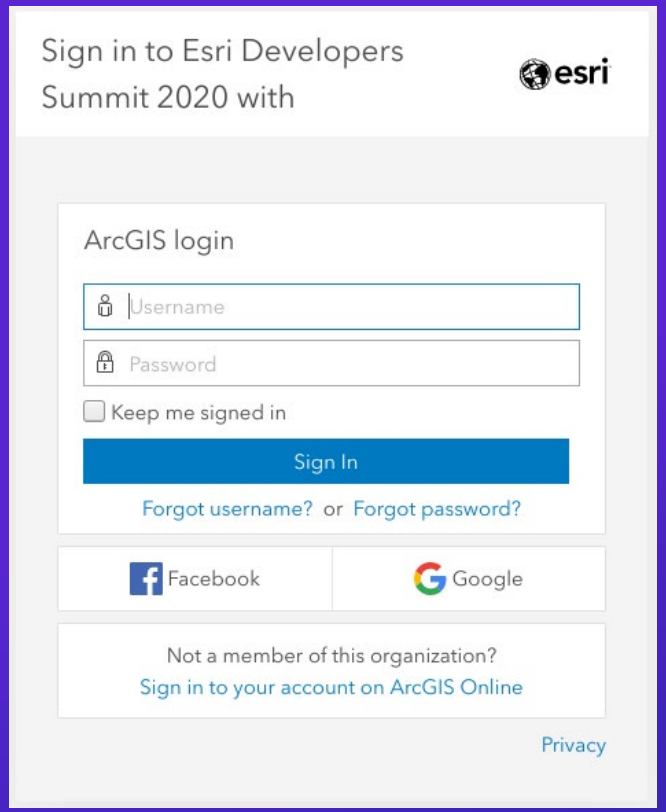


ArcGIS Account

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



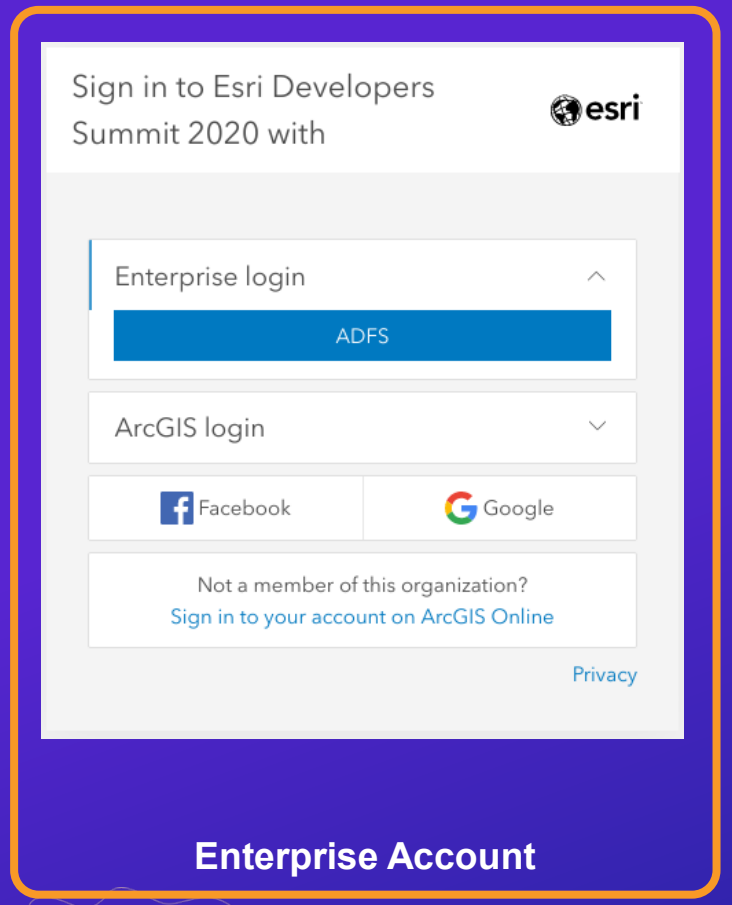
Authentication Options – Social Accounts



Social Account

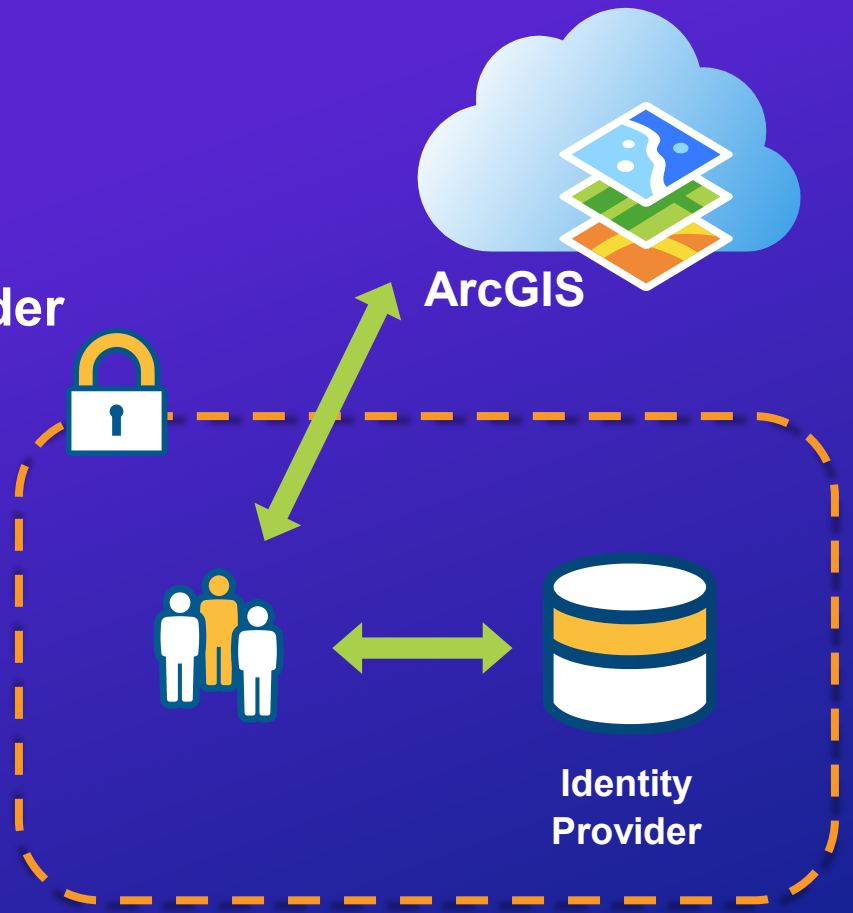
- Google or Facebook (or Github)
- Administrator can enable

Authentication Options – Enterprise IDP



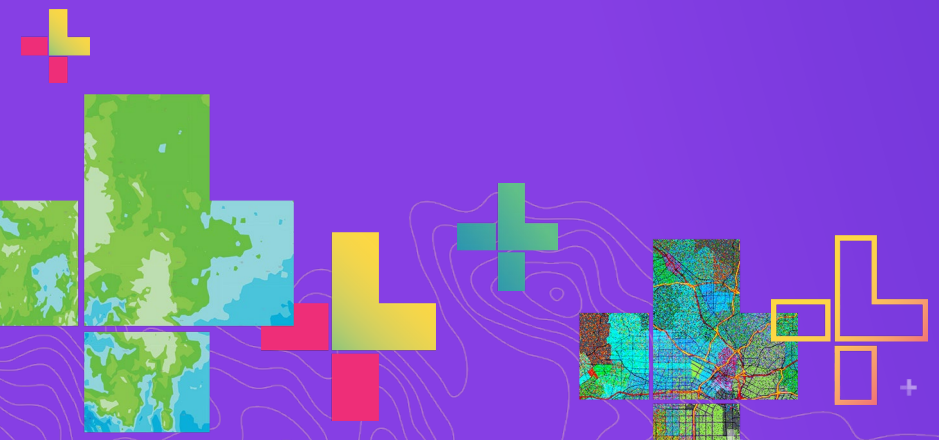
Enterprise Account

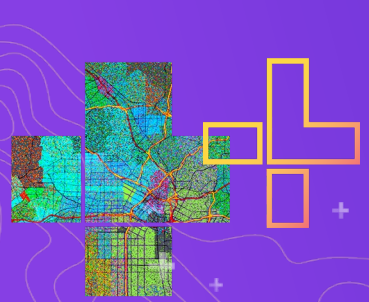
- Use your own identity provider
  - SAML 2.0
    - ADFS
    - NetIQ Access Manager
    - Shibboleth
    - ….
- Can add users:
  - Automatically upon login
  - With an Invitation
- Can use ArcGIS or Social with Enterprise Identities
- Enterprise groups are supported



Configure ArcGIS Online with enterprise identity provider

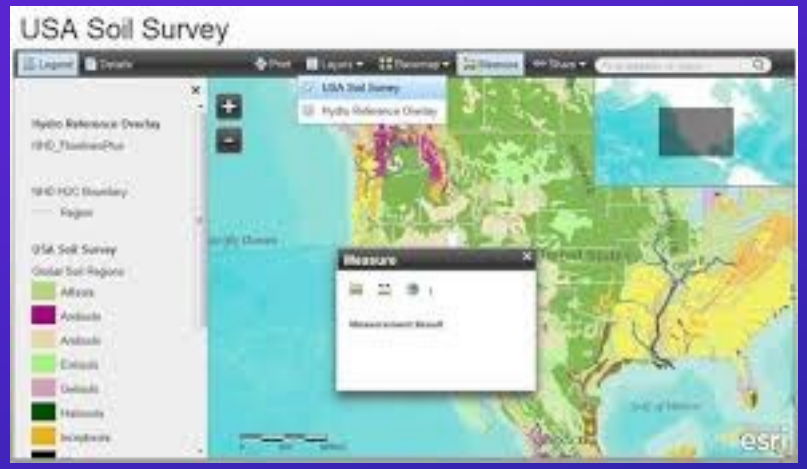
Demo

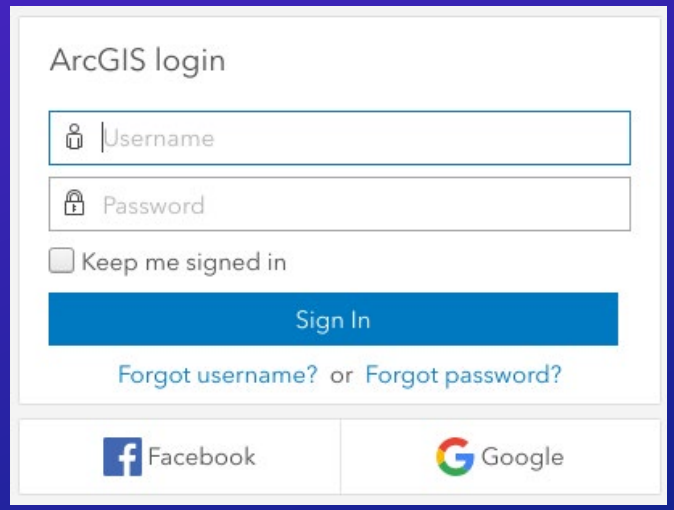




Integrating ArcGIS Online with Apps using OAuth 2.0

- OAuth 2.0 is a standard for handling authentication decisions among various web-enabled devices and servers.

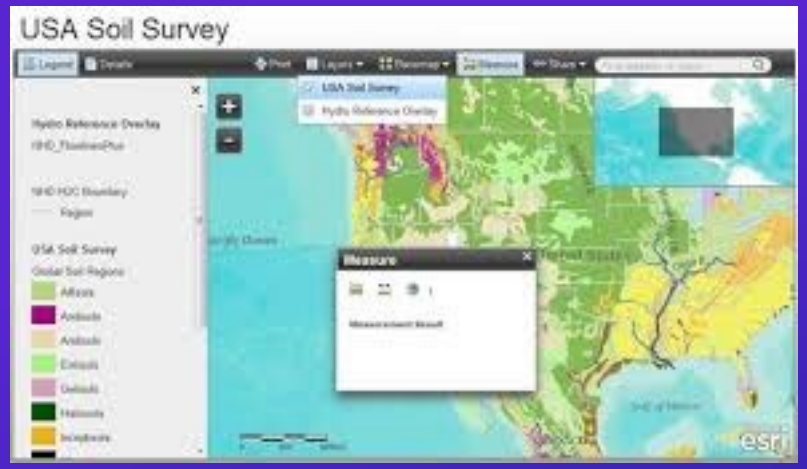




Integrating Web Apps with ArcGIS Online using OAuth

1 Register Application

client_id

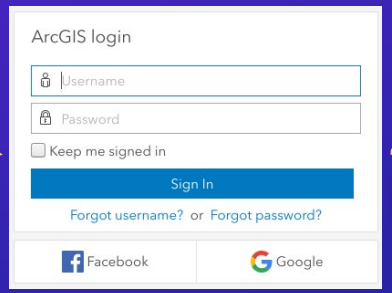


4

A

Portal

client_id



A

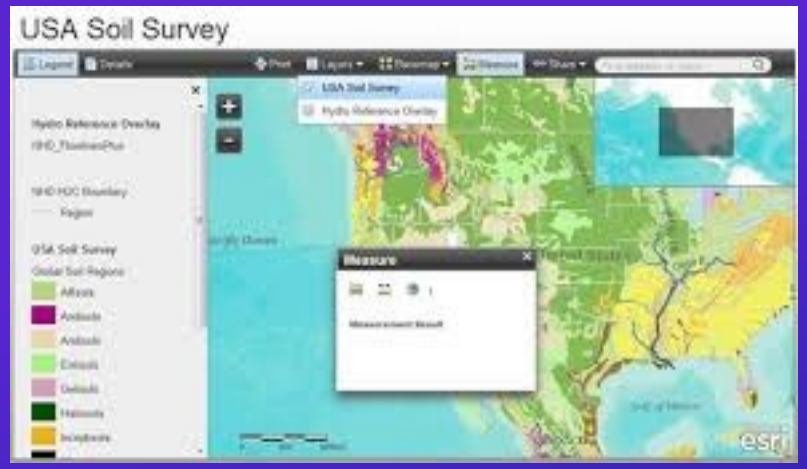
2 Sign In

3 Redirect_uri

Integrating Apps with ArcGIS Online using OAuth

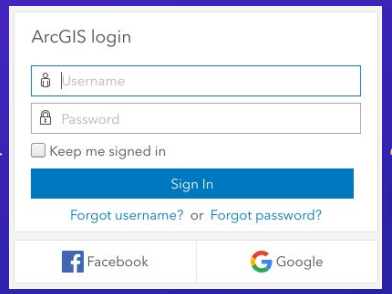
1 Register Application

client_id



client_id

2 Sign In



R

3 Redirect_uri

5

A

Portal

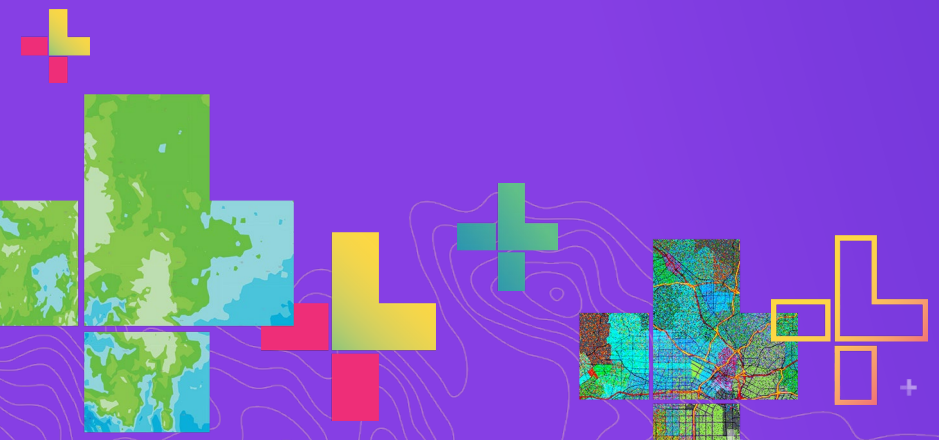
A

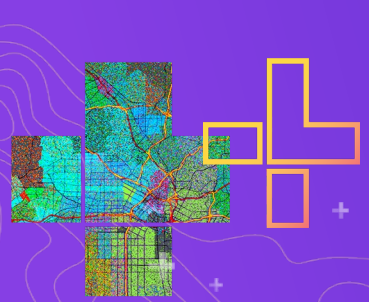
4

R

Registered Web Application

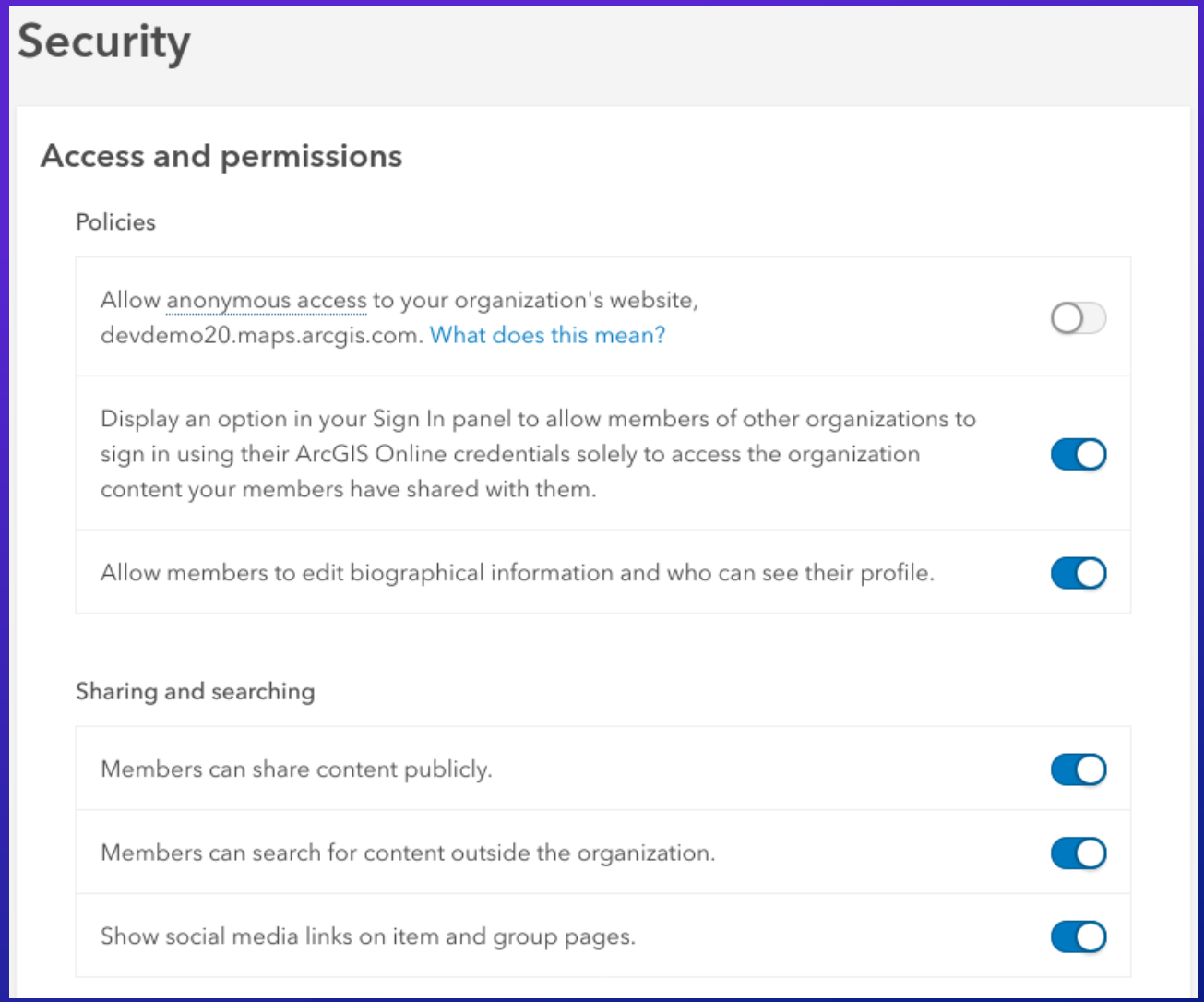
Demo





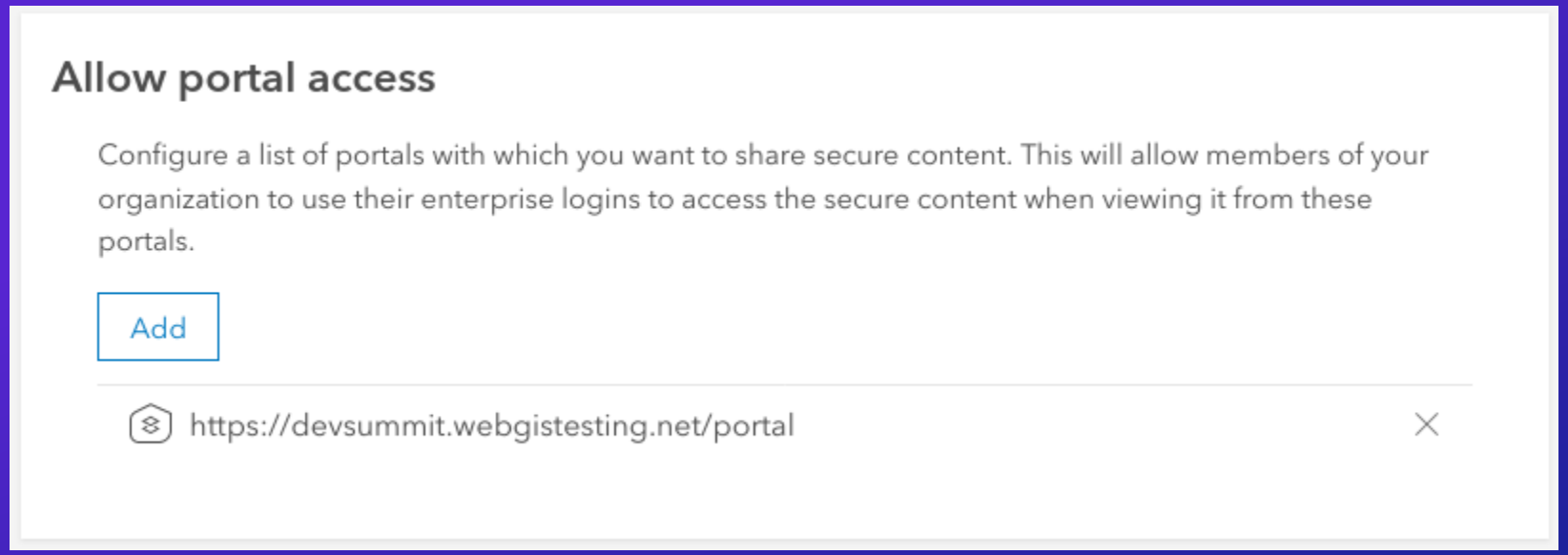
Organizational Controls

- Anonymous Access
- Profile Visibility
- Sharing to Everyone



Organizational Controls

- **Allow Portal Access**

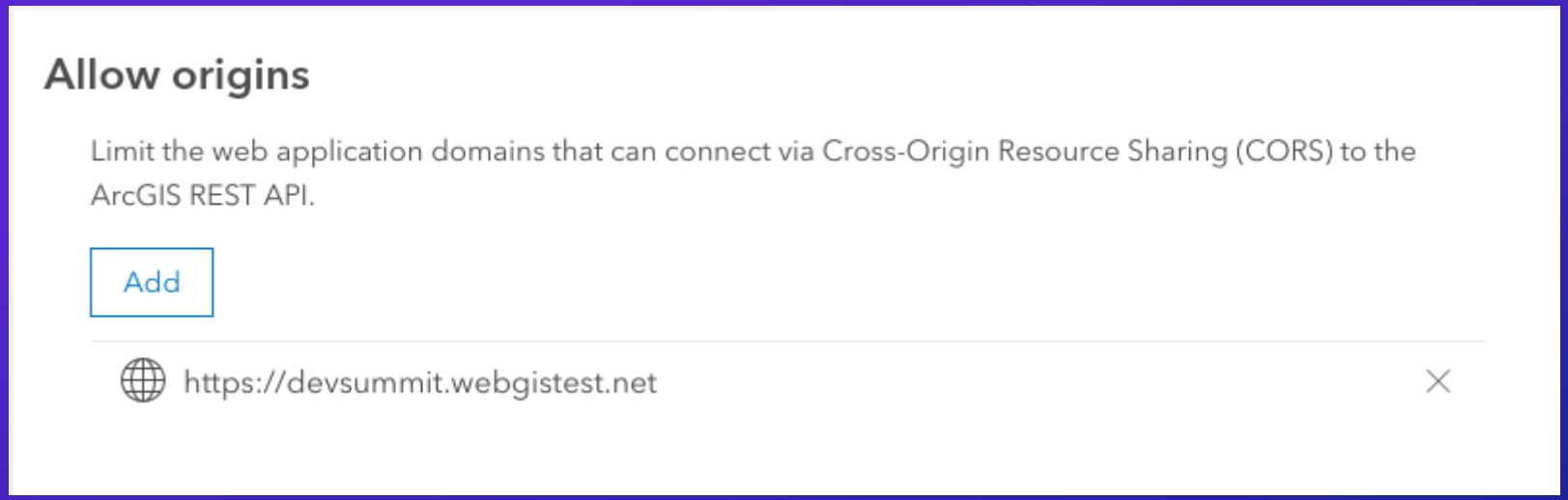


SAML Access from an ArcGIS Enterprise Web Application

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

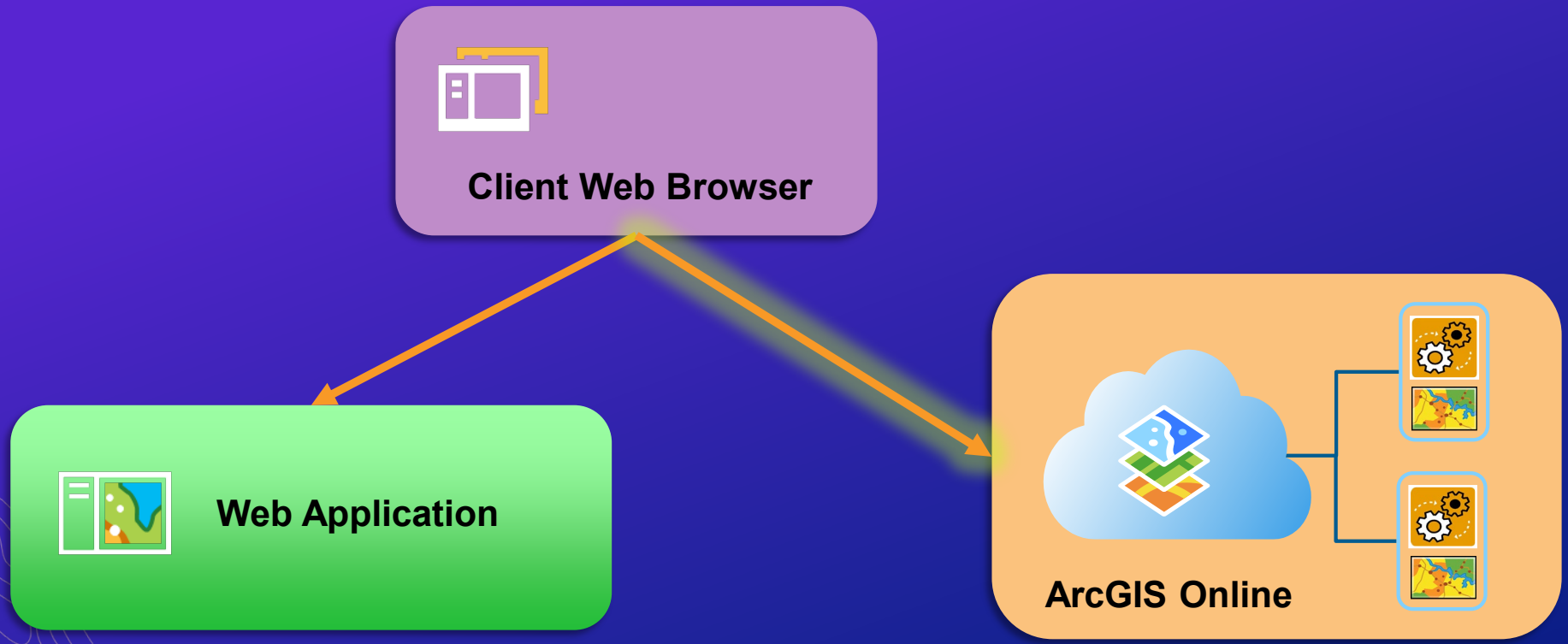
Organizational Controls

- **Allow Origins**



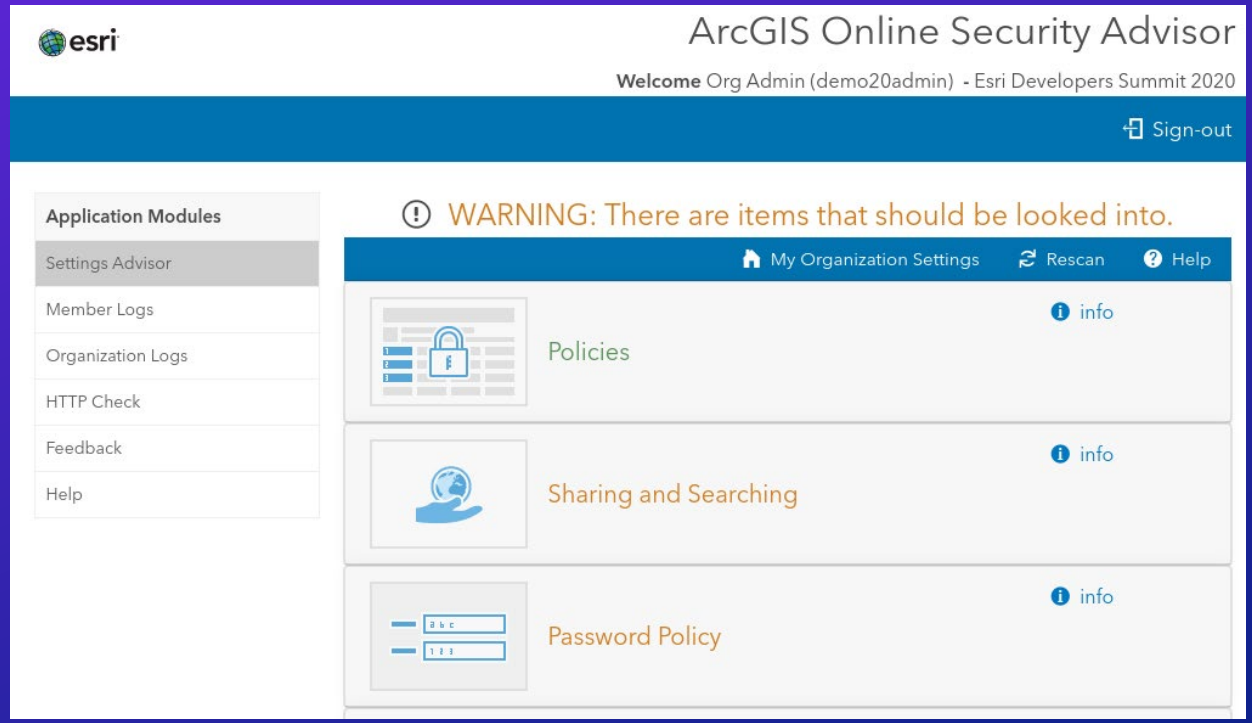
Restrict Cross-Domain (CORS) Requests

- 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



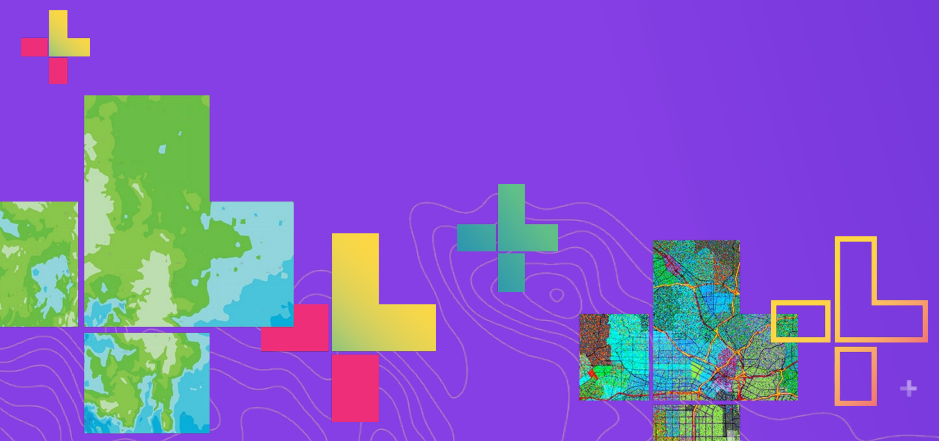
ArcGIS Online Security Advisor

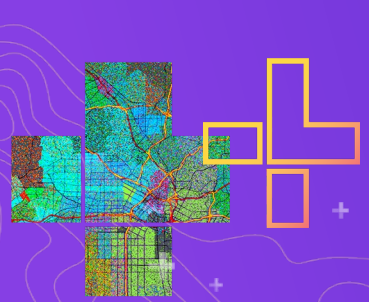
- A tool created by the Esri Software Security & Privacy Team to help advise on your ArcGIS Online security settings and review your logs
- Accessible from top menu bar on https://trust.arcgis.com
- Requires an ArcGIS Online administrator account



ArcGIS Online Security Advisor

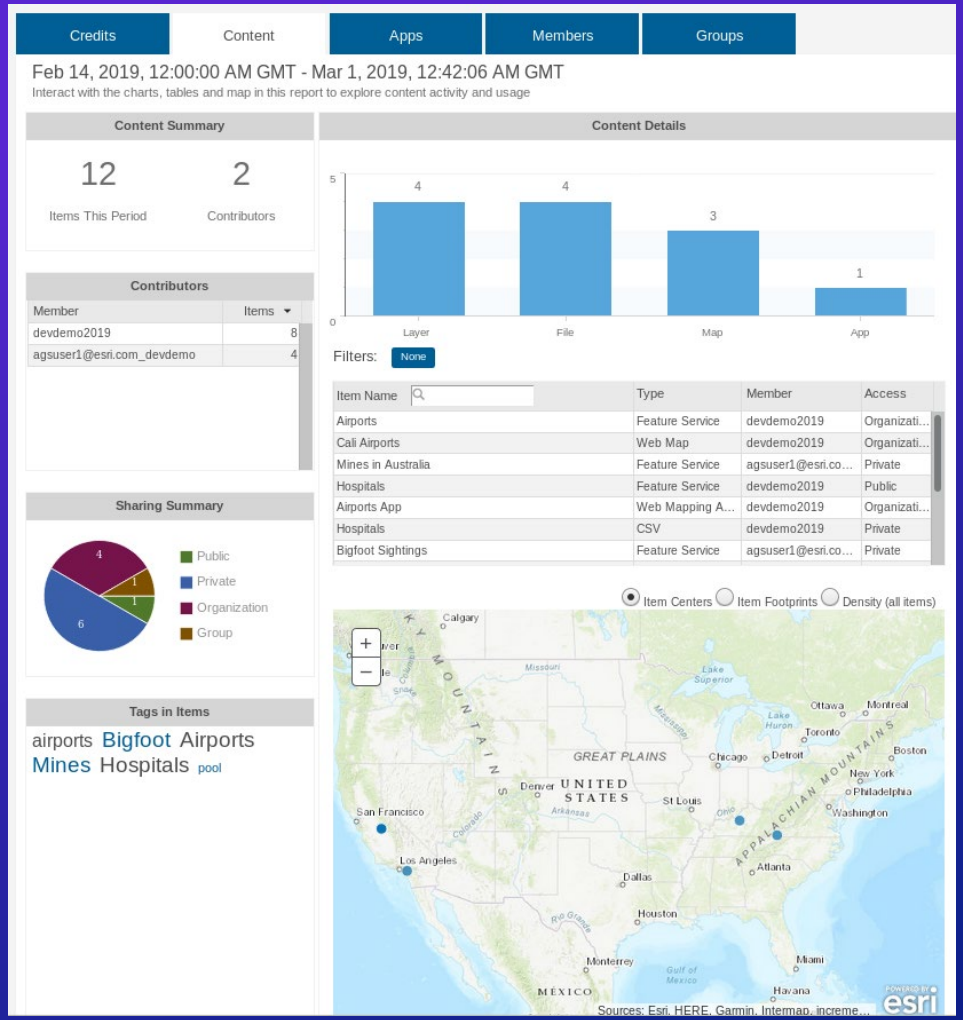
Demo





Keeping Track of Usage

- **Status Reports**
  - Credits
  - Content
  - Apps
  - Members
  - Groups
- **Activity Log**
  - Export as CSV
  - Audit log of changes to Organization



Cloud Infrastructure Provider Compliance

- **ArcGIS Online Utilizes World-Class Cloud Infrastructure Providers**
  - **Microsoft Azure**
  - **Amazon Web Services**

Privacy & Compliance