ArcGIS Online: An Introduction to Security, Privacy & Compliance

Michael Young – CISO Products, Esri Software Security & Privacy

Randall Williams – PSIRT, Esri Software Security & Privacy

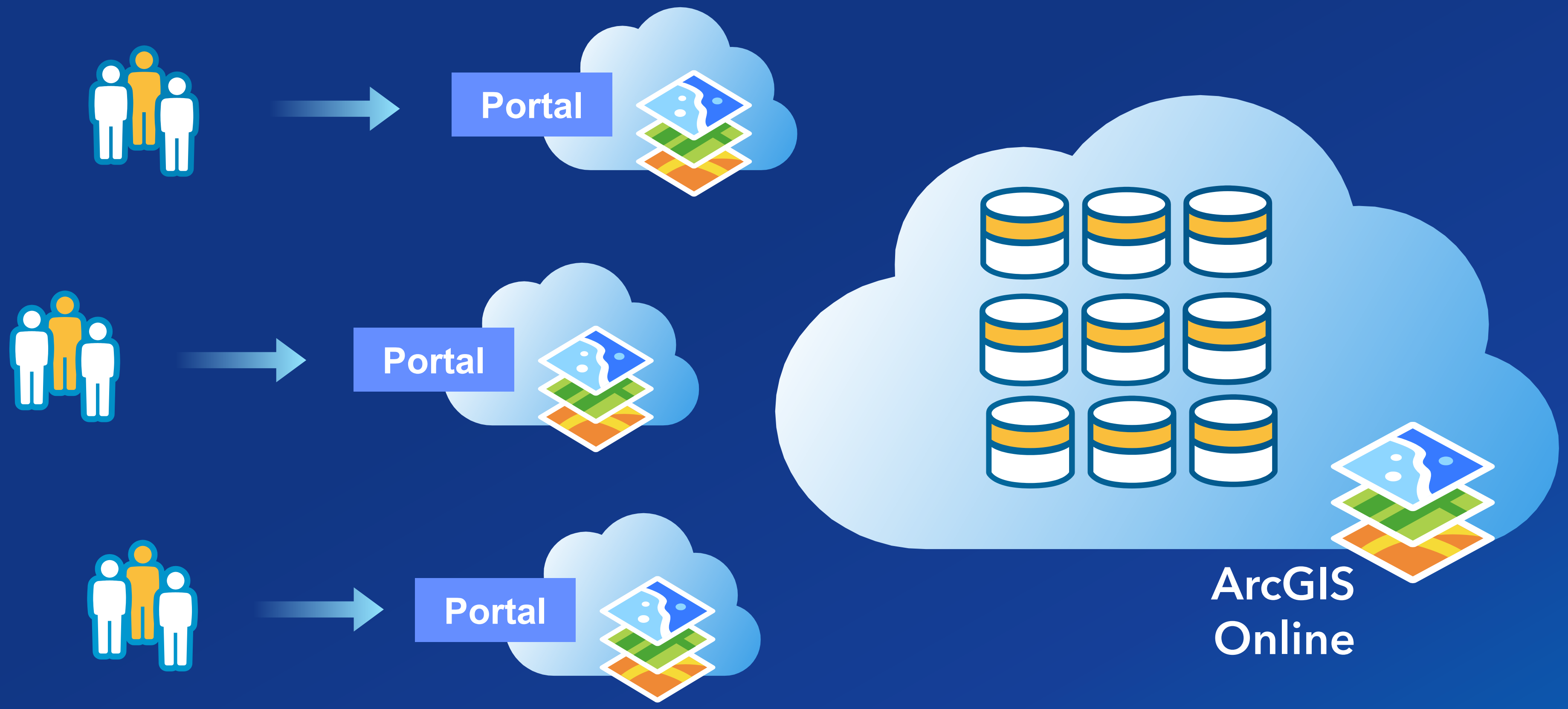
Agenda

- Platform Security
- Deployment Architecture
- Compliance (FedRAMP & more)
- Security Advisor Tool / HTTPS Only

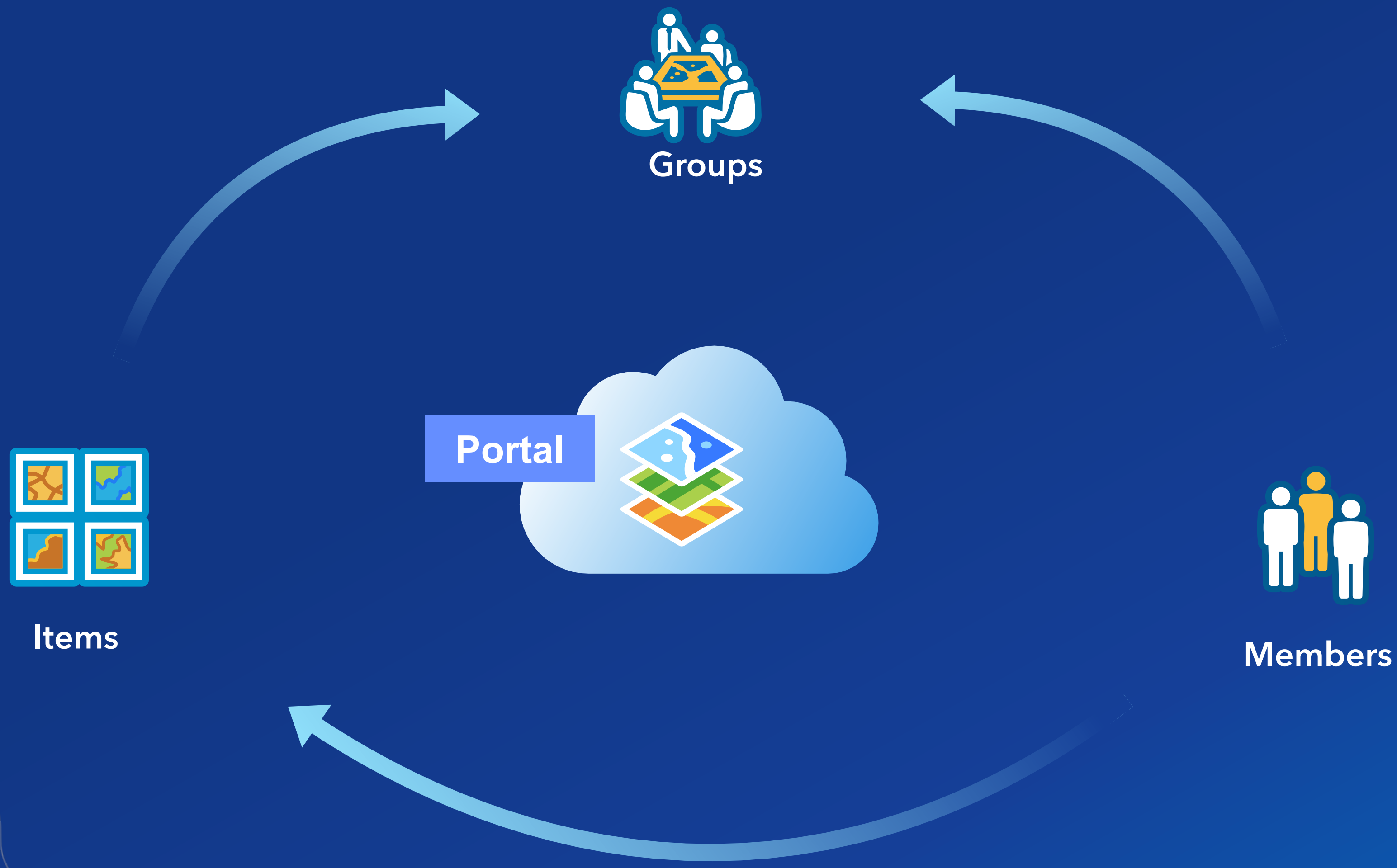
Platform Security

Randall Williams

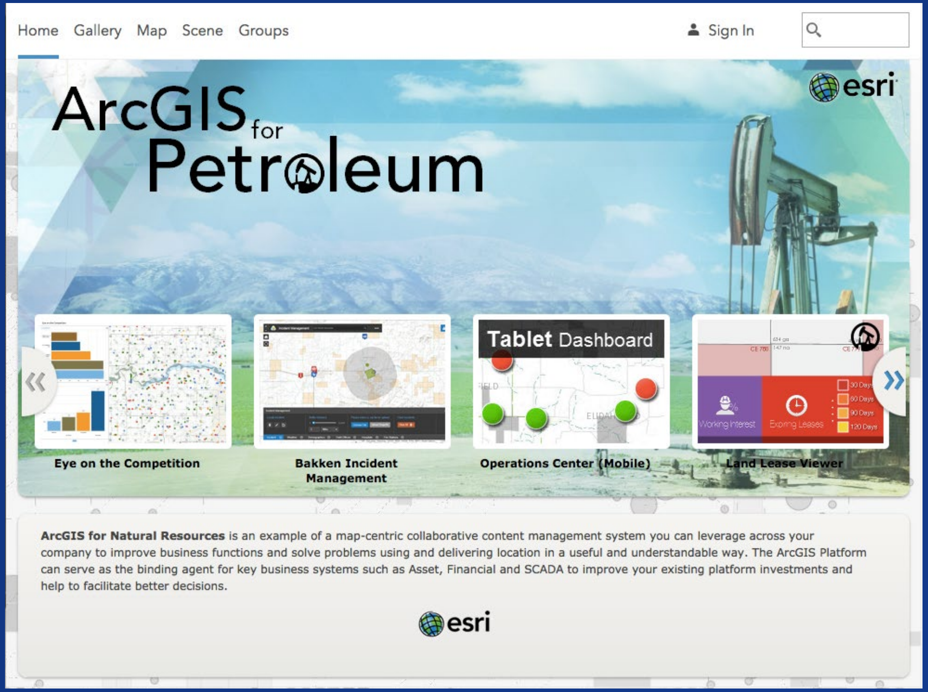
ArcGIS Online – A Multi-Tenant System



Portal Information Model



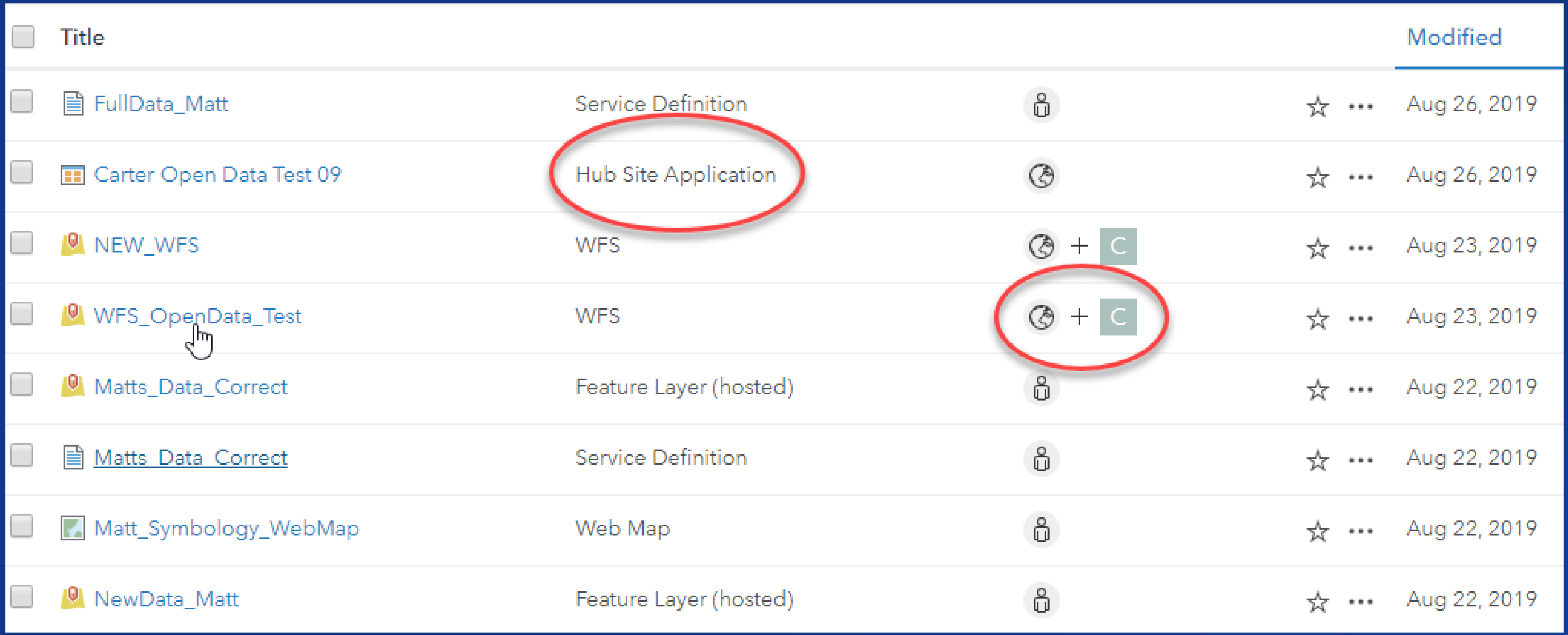
Portal



ArcGIS for Natural Resources is an example of a map-centric collaborative content management system you can leverage across your company to improve business functions and solve problems using and delivering location in a useful and understandable way. The ArcGIS Platform can serve as the binding agent for key business systems such as Asset, Financial and SCADA to improve your existing platform investments and help to facilitate better decisions.

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

Items



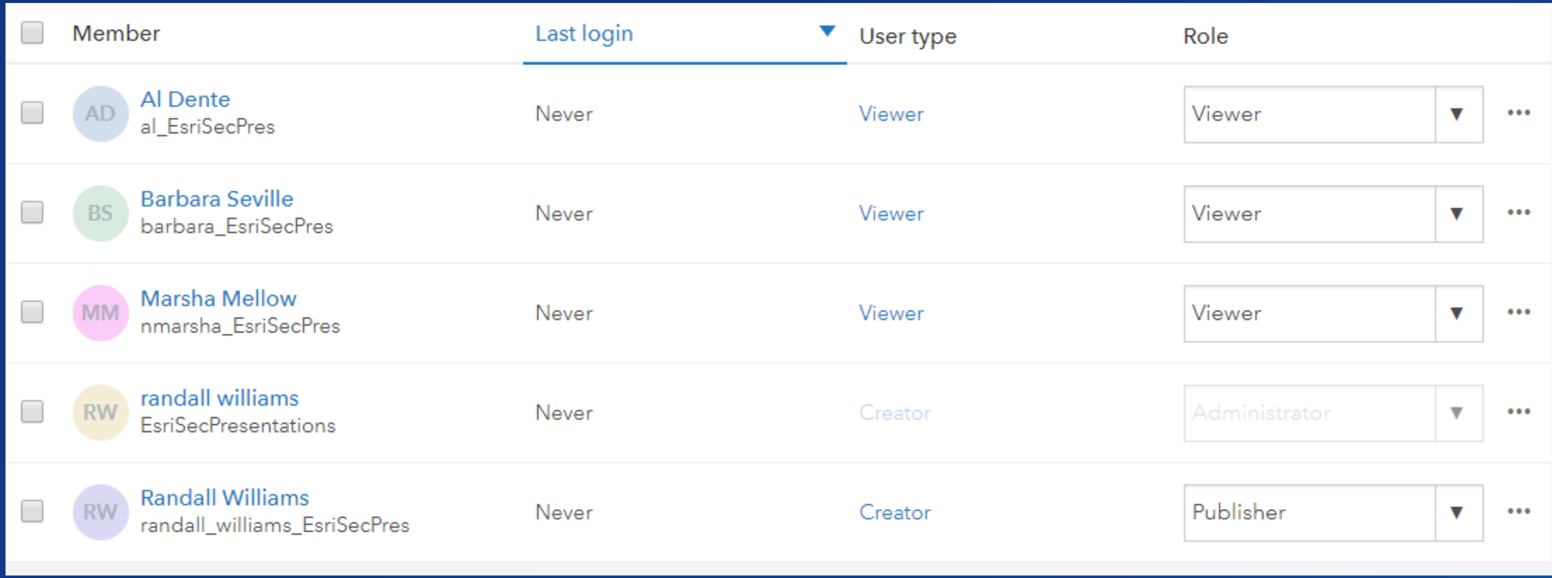
□ Title				Modified
□ FullData_Matt	Service Definition	🔒	☆ •••	Aug 26, 2019
□ Carter Open Data Test 09	Hub Site Application	🌐	☆ •••	Aug 26, 2019
□ NEW_WFS	WFS	🌐 + C	☆ •••	Aug 23, 2019
□ WFS_OpenData_Test	WFS	🌐 + C	☆ •••	Aug 23, 2019
□ Matts_Data_Correct	Feature Layer (hosted)	🔒	☆ •••	Aug 22, 2019
□ Matts_Data_Correct	Service Definition	🔒	☆ •••	Aug 22, 2019
□ Matt_Symbology_WebMap	Web Map	🔒	☆ •••	Aug 22, 2019
□ NewData_Matt	Feature Layer (hosted)	🔒	☆ •••	Aug 22, 2019

- Types
  - Web Map
  - Services
  - Data
  - …

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

Members (Users)

- Members own items and groups
- Members have a profile
- Configurable Discoverability
  - No one
  - Organization
  - Everyone
- Members have a Role
- Members have a User Type

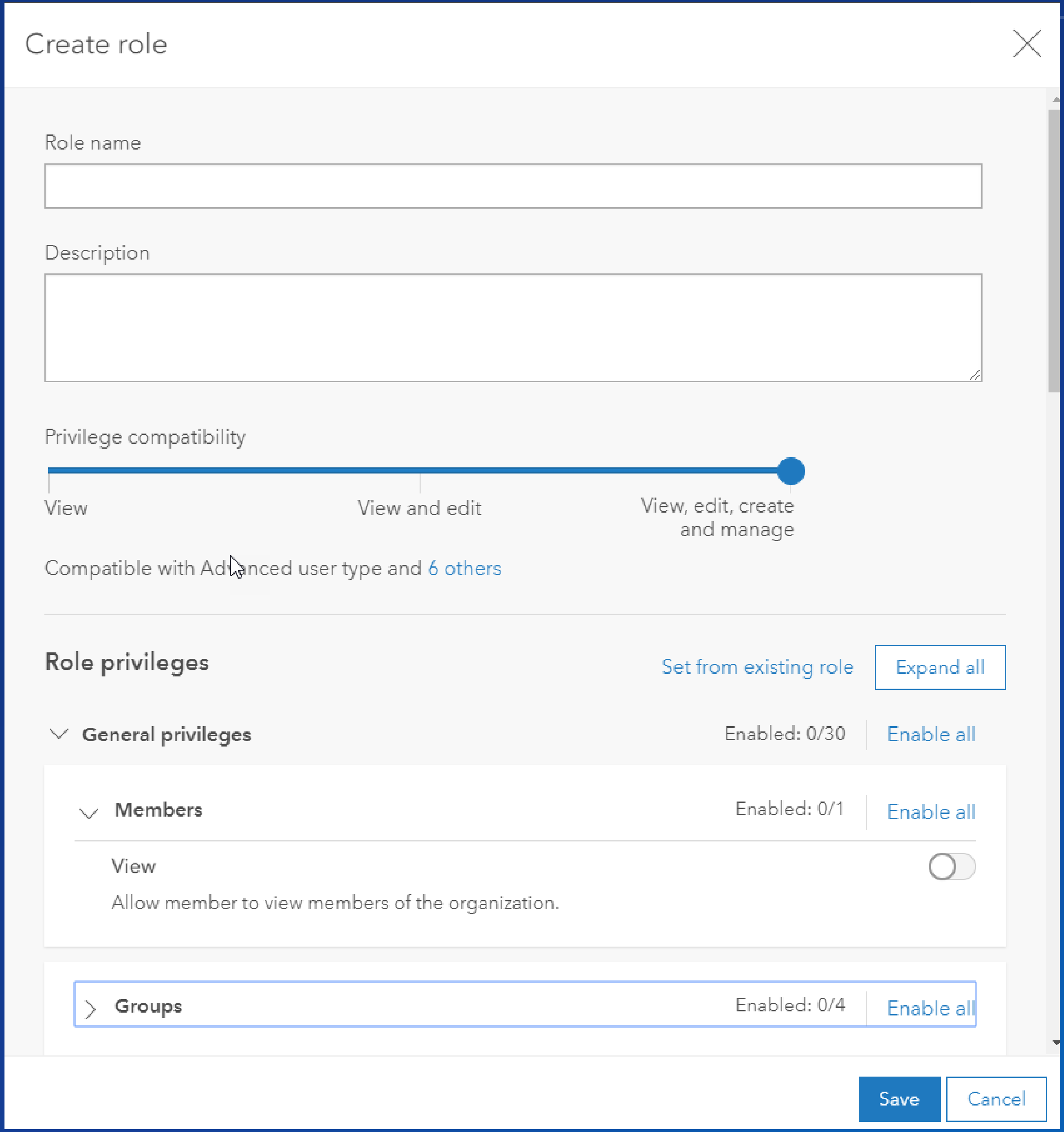


□	Member	Last login ▼	User type	Role	
□	AD Al Dente al_EsriSecPres	Never	Viewer	Viewer ▼	•••
□	BS Barbara Seville barbara_EsriSecPres	Never	Viewer	Viewer ▼	•••
□	MM Marsha Mellow nmarsha_EsriSecPres	Never	Viewer	Viewer ▼	•••
□	RW randall williams EsriSecPresentations	Never	Creator	Administrator ▼	•••
□	RW Randall Williams randall_williams_EsriSecPres	Never	Creator	Publisher ▼	•••

Roles

Roles define privilege levels

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



Create role

Role name

Description

Privilege compatibility

View — View and edit — View, edit, create and manage

Compatible with Advanced user type and 6 others

Role privileges

General privileges Enabled: 0/30

Members Enabled: 0/1

View

Allow member to view members of the organization.

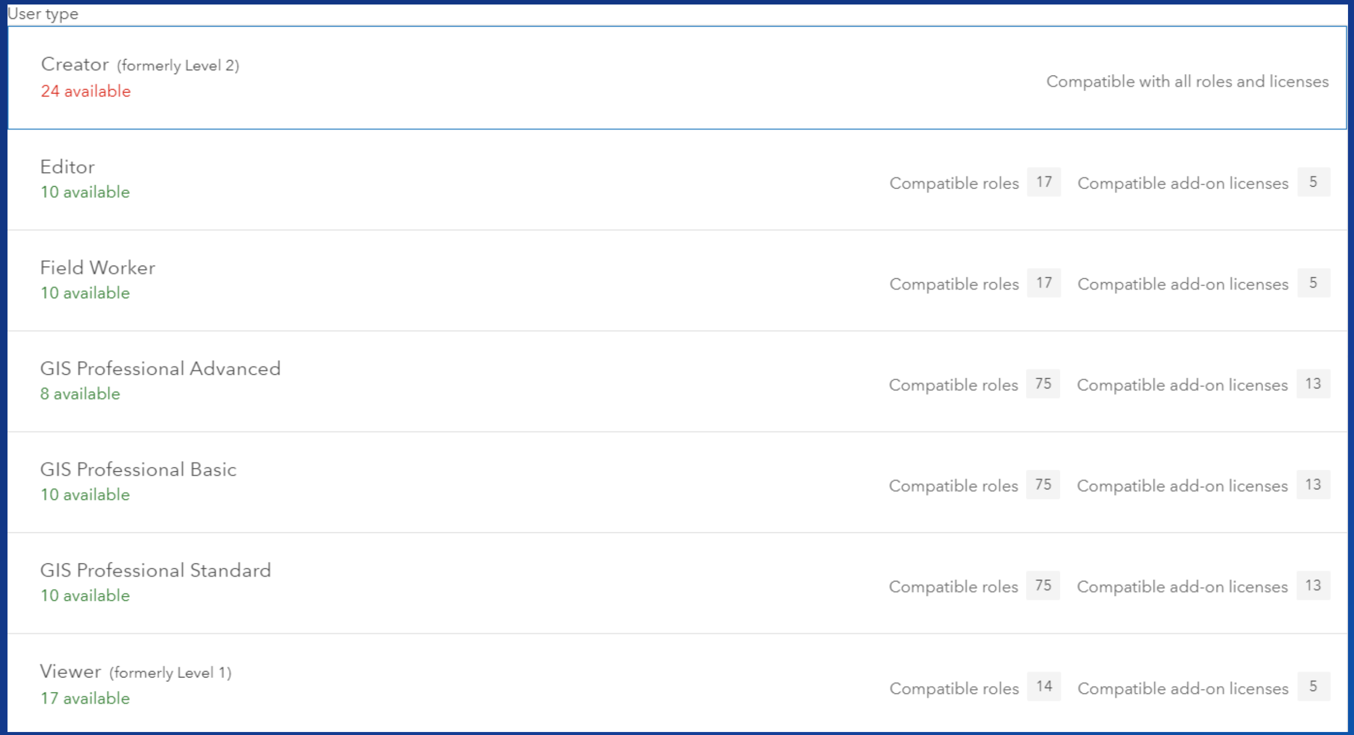
Groups Enabled: 0/4

User Types

Access to content and capabilities

- User Types
  - GIS Professional
  - Creator (formerly Level 2)
  - Field Worker
  - Editor
  - Viewer

- Available user types are dependent upon assigned role



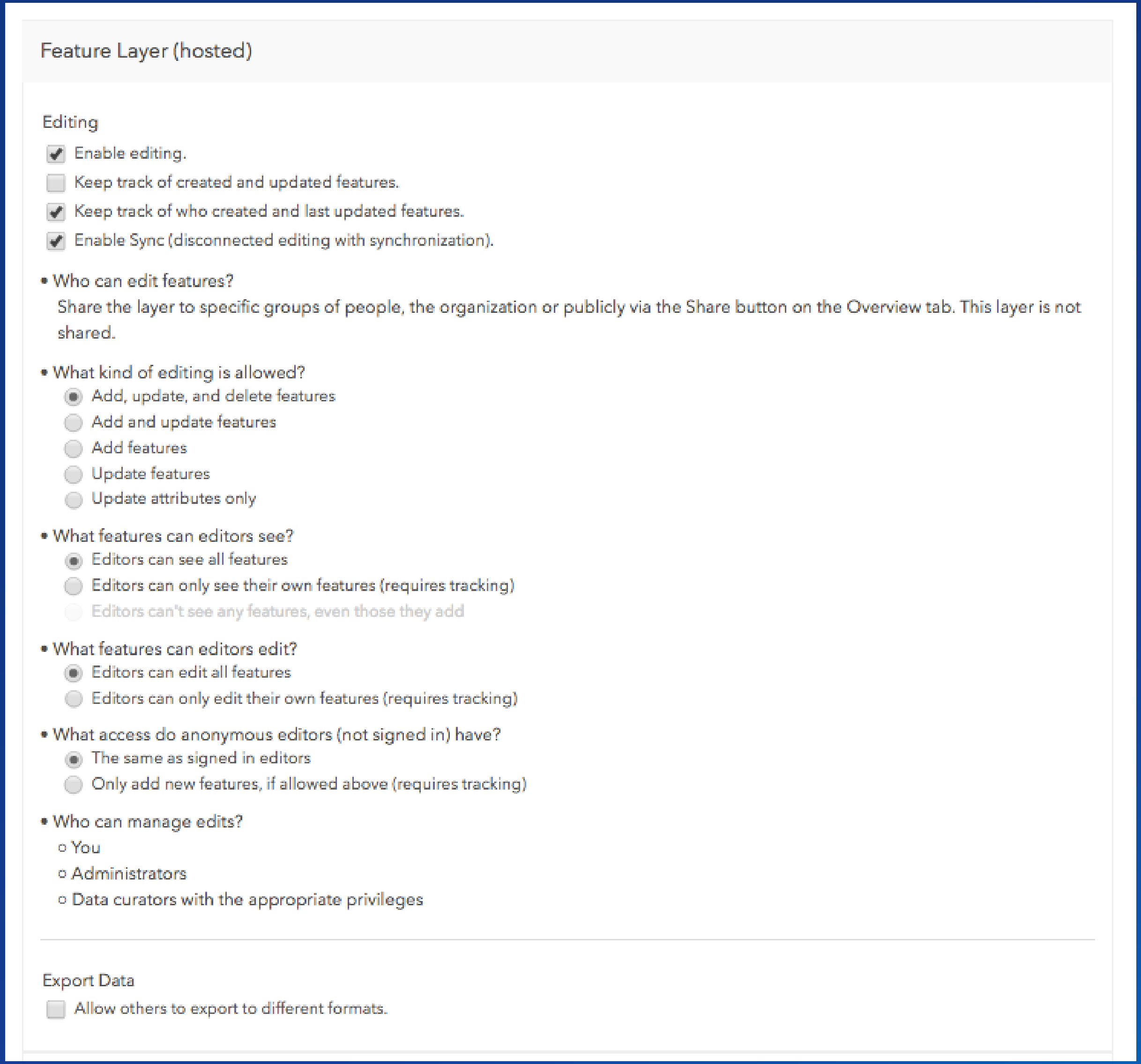
User type		
Creator (formerly Level 2) 24 available	Compatible with all roles and licenses	
Editor 10 available	Compatible roles 17	Compatible add-on licenses 5
Field Worker 10 available	Compatible roles 17	Compatible add-on licenses 5
GIS Professional Advanced 8 available	Compatible roles 75	Compatible add-on licenses 13
GIS Professional Basic 10 available	Compatible roles 75	Compatible add-on licenses 13
GIS Professional Standard 10 available	Compatible roles 75	Compatible add-on licenses 13
Viewer (formerly Level 1) 17 available	Compatible roles 14	Compatible add-on licenses 5

Groups

- Contain Items and Members
- Members have access to items in group
- Group owners can share items to their own groups
- Groups can be visible to:
  - No one (private)
  - Organization
  - Everyone
  - Items do not inherit visibility
- Groups with Update Capabilities

Feature Layer 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



Feature Layer (hosted)

Editing

☑ Enable editing.

□ Keep track of created and updated features.

☑ Keep track of who created and last updated features.

☑ Enable Sync (disconnected editing with synchronization).

- Who can edit features?

  Share the layer to specific groups of people, the organization or publicly via the Share button on the Overview tab. This layer is not shared.

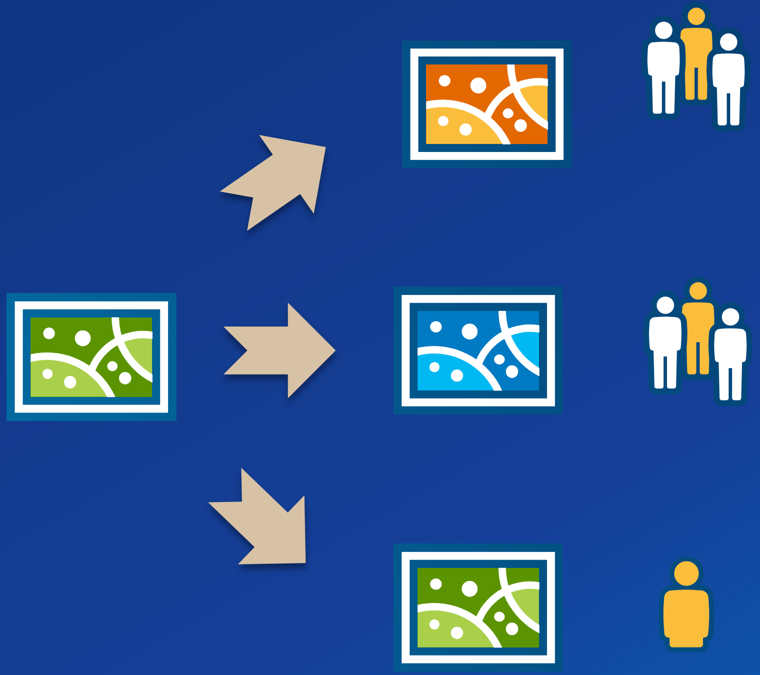
- What kind of editing is allowed?
  - ● Add, update, and delete features
  - ○ Add and update features
  - ○ Add features
  - ○ Update features
  - ○ Update attributes only
- What features can editors see?
  - ● Editors can see all features
  - ○ Editors can only see their own features (requires tracking)
  - ○ Editors can't see any features, even those they add
- What features can editors edit?
  - ● Editors can edit all features
  - ○ Editors can only edit their own features (requires tracking)
- What access do anonymous editors (not signed in) have?
  - ● The same as signed in editors
  - ○ Only add new features, if allowed above (requires tracking)
- Who can manage edits?
  - You
  - Administrators
  - Data curators with the appropriate privileges

Export Data

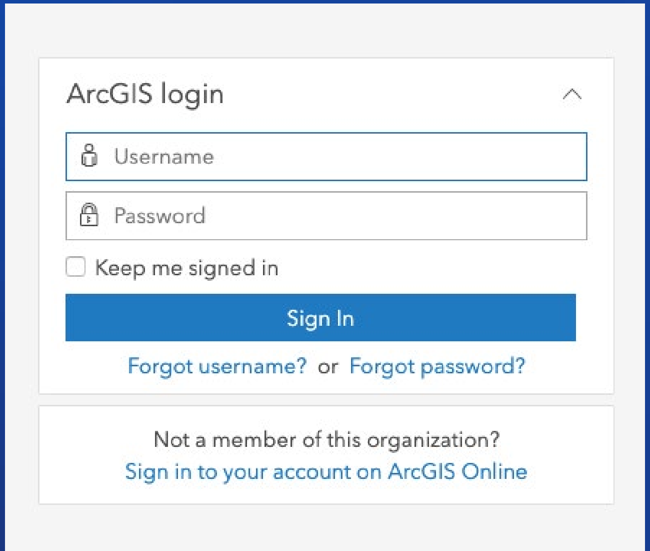
□ Allow others to export to different formats.

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 Accounts



ArcGIS login

Username

Password

□ Keep me signed in

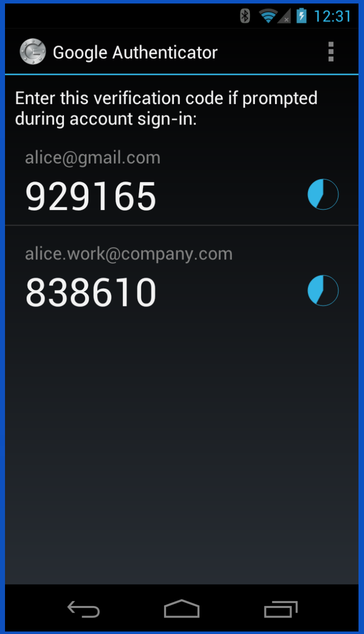
Sign In

Forgot username? or Forgot password?

Not a member of this organization?
Sign in to your account on ArcGIS Online

ArcGIS Account

- 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
  - Members setup their own Multi-factor
- Password Policy
  - Default Password Policy
    - 8 characters with at least 1 number
    - Weak passwords validation
  - Can Customize
    - Complexity
    - History
    - Expiration



12:31

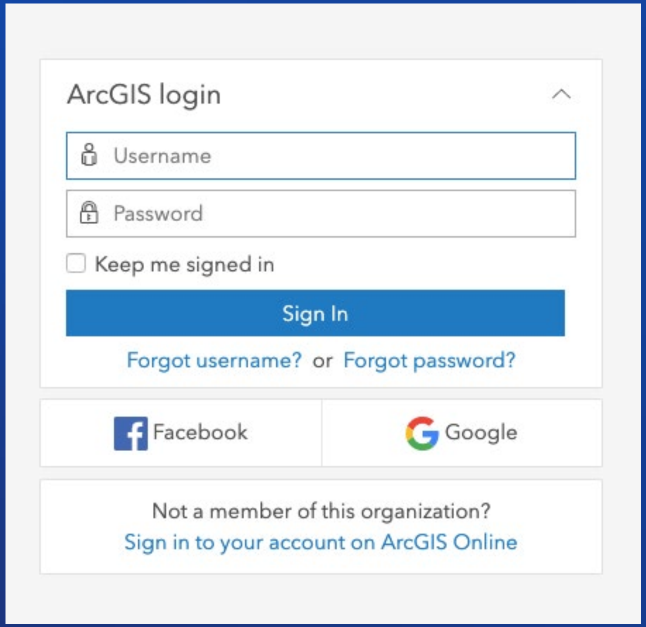
Google Authenticator

Enter this verification code if prompted during account sign-in:

alice@gmail.com
929165

alice.work@company.com
838610

Authentication Options – Social Accounts



ArcGIS login

Username

Password

□ Keep me signed in

Sign In

Forgot username? or Forgot password?

Facebook

Google

Not a member of this organization?

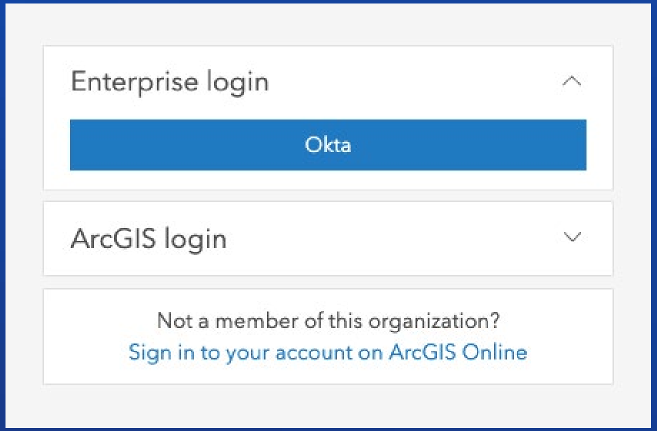
Sign in to your account on ArcGIS Online

Social Account

- Facebook Logins
- Google Logins

- By Invitation
- Login maps to unique username in Organization
- Requires an email
- Sign out doesn't sign out of your Social login

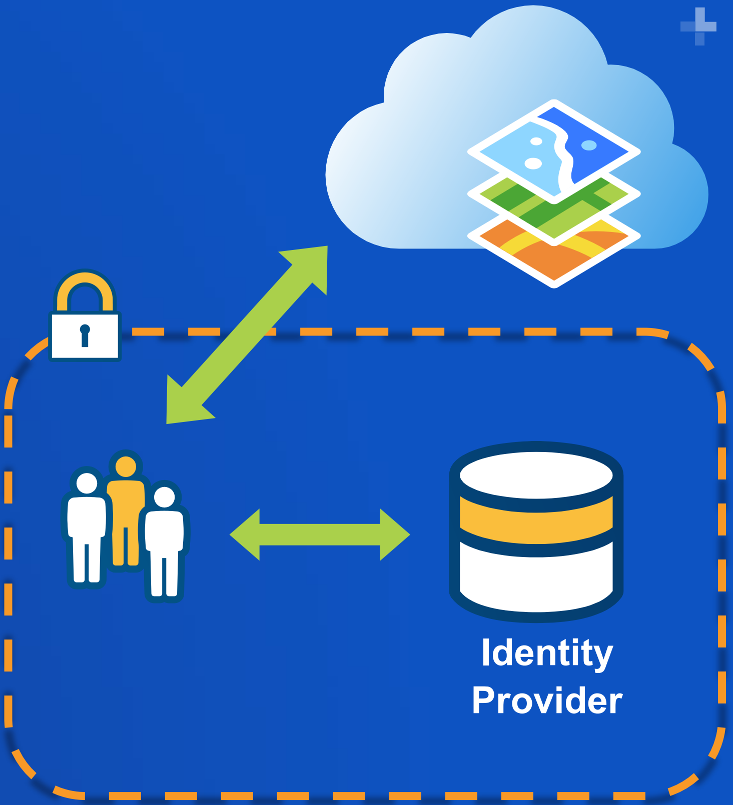
Authentication Options – Enterprise Accounts



Not a member of this organization?
Sign in to your account on ArcGIS Online

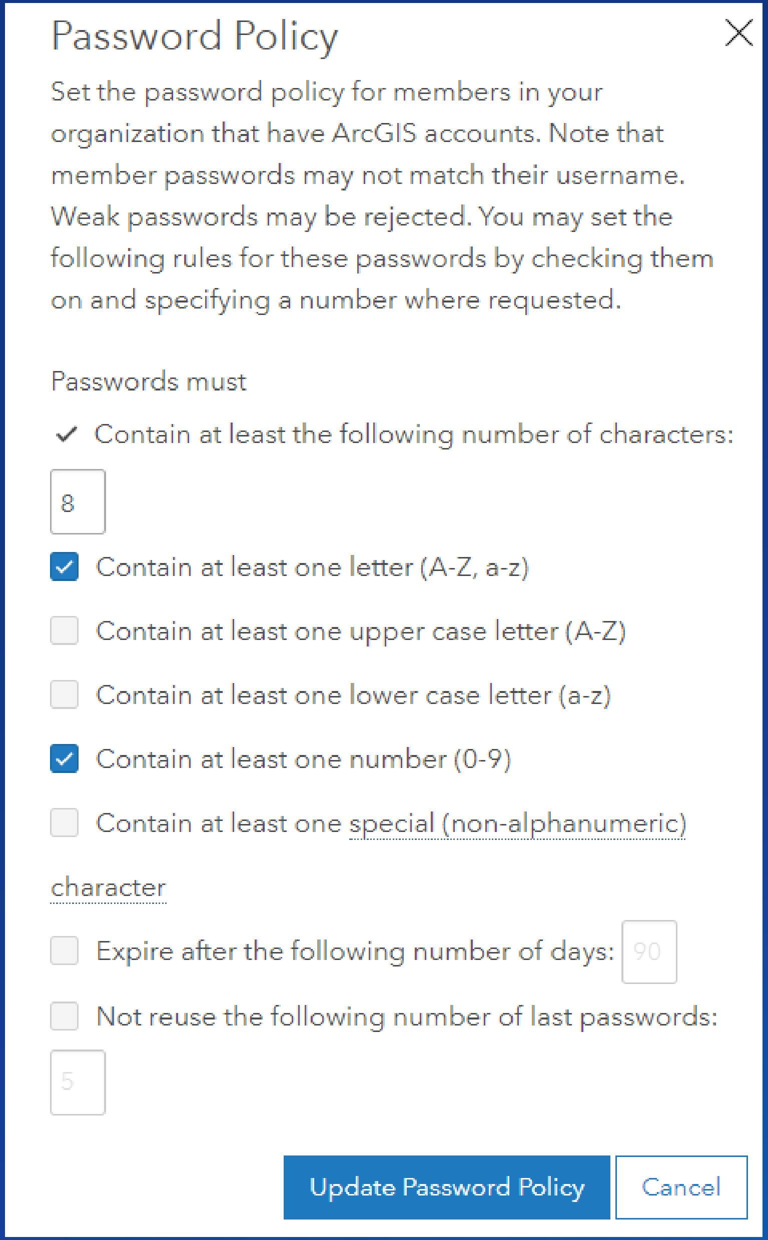
Enterprise Account

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



Password Polices

- Default Password Policy
  - 8 characters with at least 1 number
  - May not match username
  - Weak passwords may be rejected
- Can Customize
  - Complexity
  - History
  - Expiration



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: 8

☑ 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)

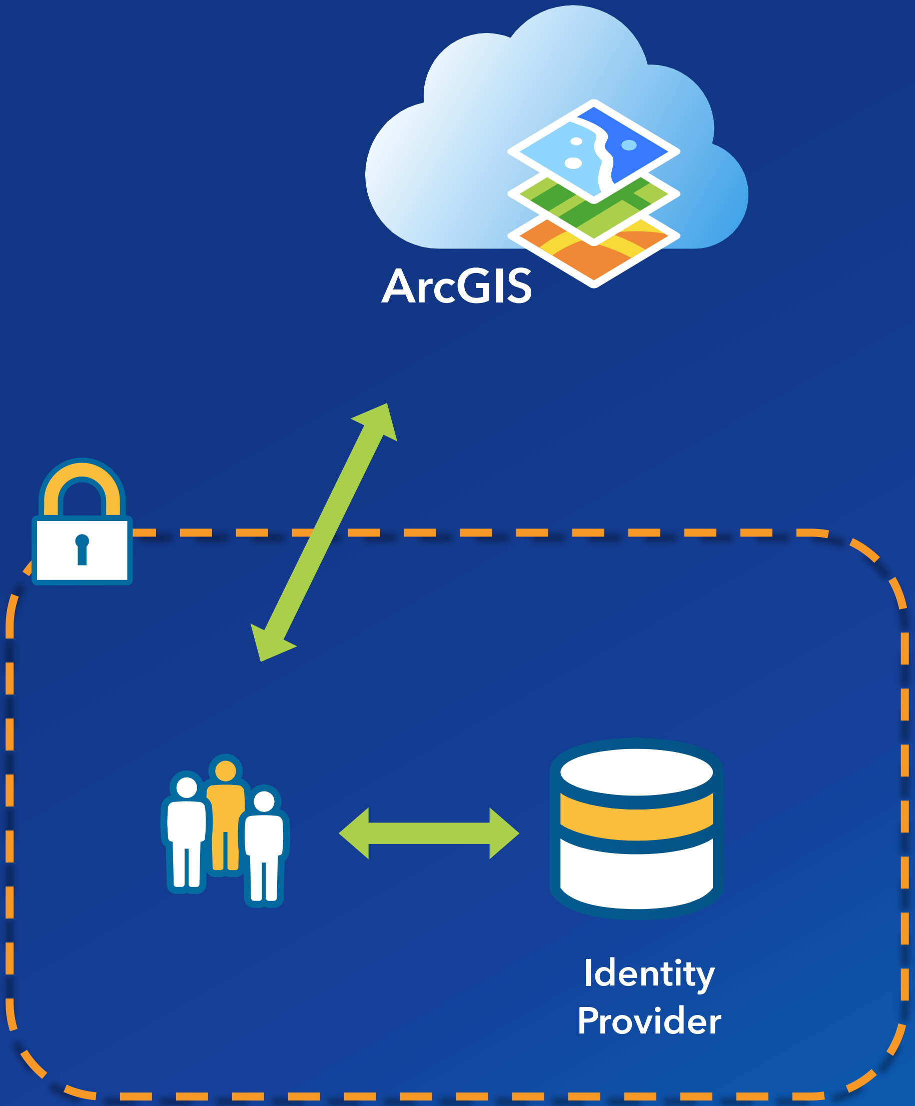
☐ Contain at least one special (non-alphanumeric) character

☐ Expire after the following number of days: 90

☐ Not reuse the following number of last passwords: 5

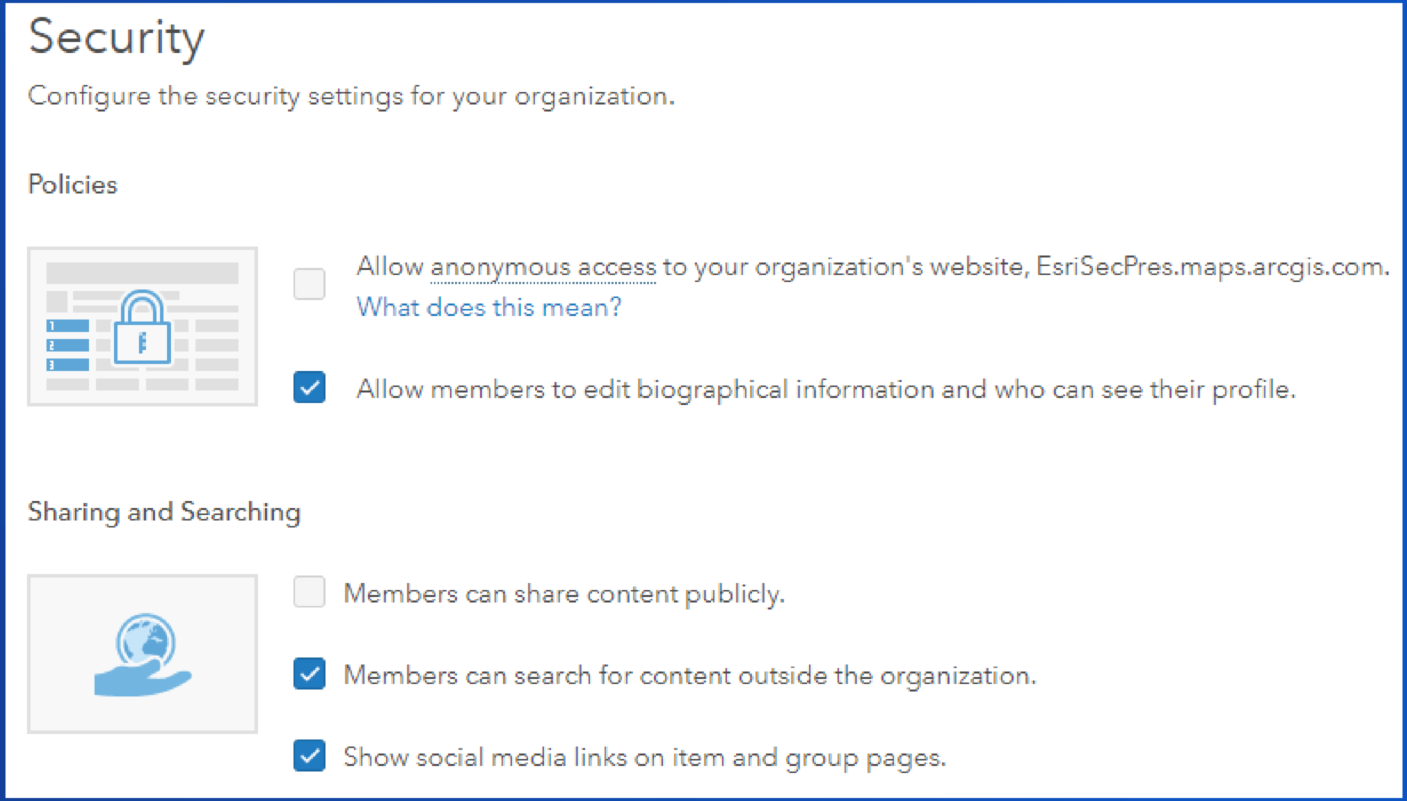
Enterprise Identities

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



Admin Organization Controls

- Disable Sharing to Everyone
- Disable Bio or Profile
- Disable Comments
- Setup Admin Contacts
- Setup Purchasers



Security

Configure the security settings for your organization.

Policies

☐ Allow anonymous access to your organization's website, EsriSecPres.maps.arcgis.com.
What does this mean?

☑ Allow members to edit biographical information and who can see their profile.

Sharing and Searching

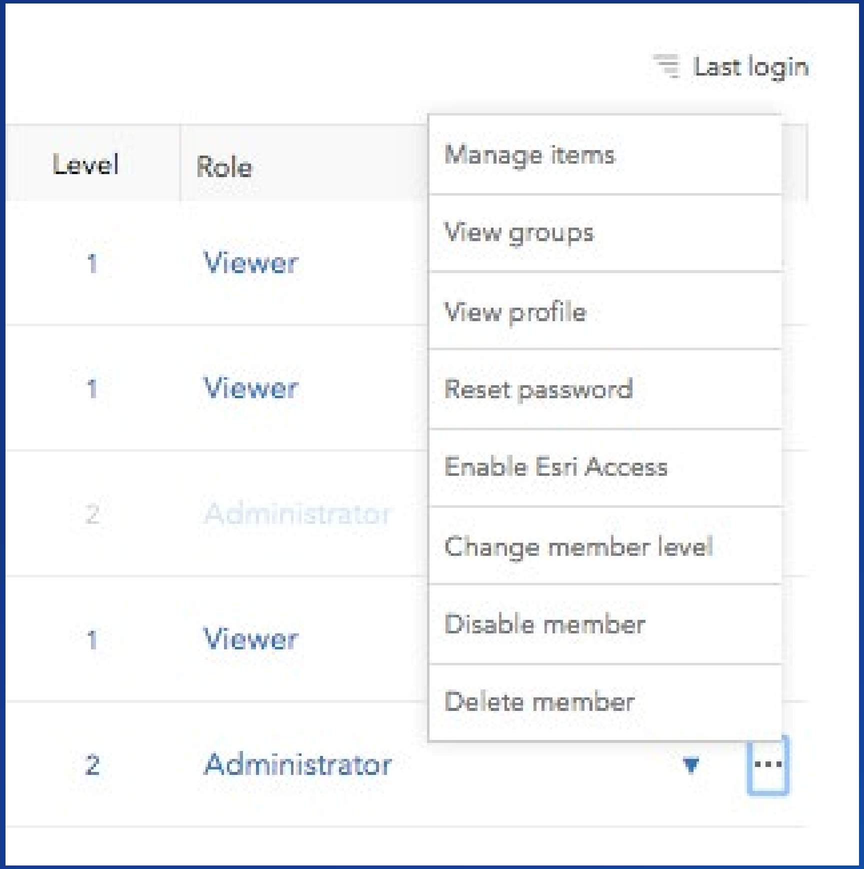
☐ Members can share content publicly.

☑ Members can search for content outside the organization.

☑ Show social media links on item and group pages.

Administrator Controls on Members

- Admins can
  - Manage Items, Groups, Profile
  - Disable Members
  - Delete Members
  - Reset Member’s Password
  - Change Role
  - Enable Esri Access

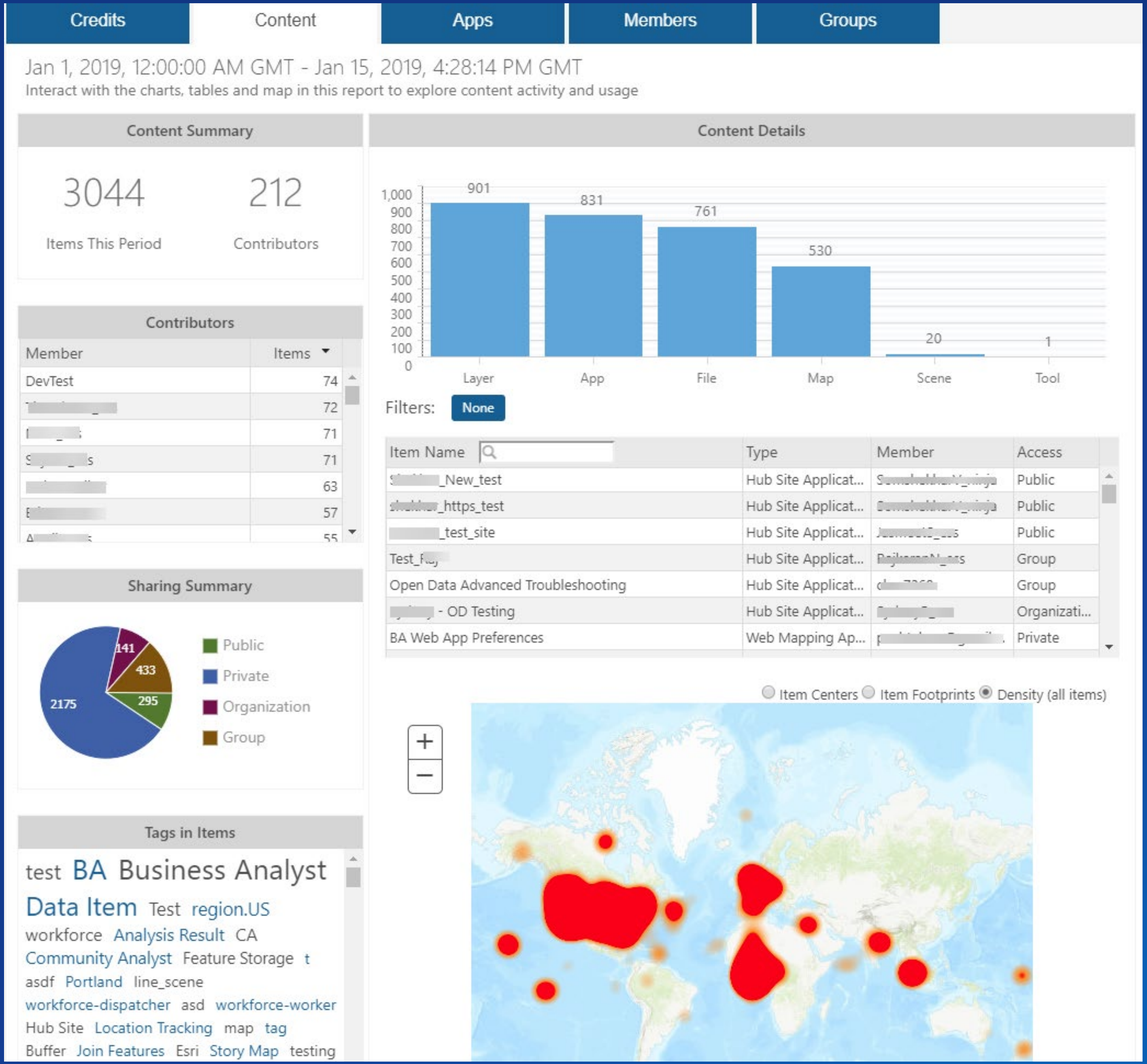


Last login

Level	Role
1	Viewer
1	Viewer
2	Administrator
1	Viewer
2	Administrator

Keeping Track of Usage

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



Jan 1, 2019, 12:00:00 AM GMT - Jan 15, 2019, 4:28:14 PM GMT

Interact with the charts, tables and map in this report to explore content activity and usage

Content Summary

3044 Items This Period

212 Contributors

Contributors

Member	Items ▾
DevTest	74
[redacted]	72
[redacted]	71
[redacted]	71
[redacted]	63
[redacted]	57
[redacted]	55

Sharing Summary

Tags in Items

test BA Business Analyst Data Item Test region.US workforce Analysis Result CA Community Analyst Feature Storage t asdf Portland line_scene workforce-dispatcher asd workforce-worker Hub Site Location Tracking map tag Buffer Join Features Esri Story Map testing

Content Details

Filters: None

Item Name 🔍	Type	Member	Access
[redacted]_New_test	Hub Site Applicat...	[redacted]	Public
[redacted]_https_test	Hub Site Applicat...	[redacted]	Public
[redacted]_test_site	Hub Site Applicat...	[redacted]	Public
Test_[redacted]	Hub Site Applicat...	[redacted]	Group
Open Data Advanced Troubleshooting	Hub Site Applicat...	[redacted]	Group
[redacted] - OD Testing	Hub Site Applicat...	[redacted]	Organizati...
BA Web App Preferences	Web Mapping Ap...	[redacted]	Private

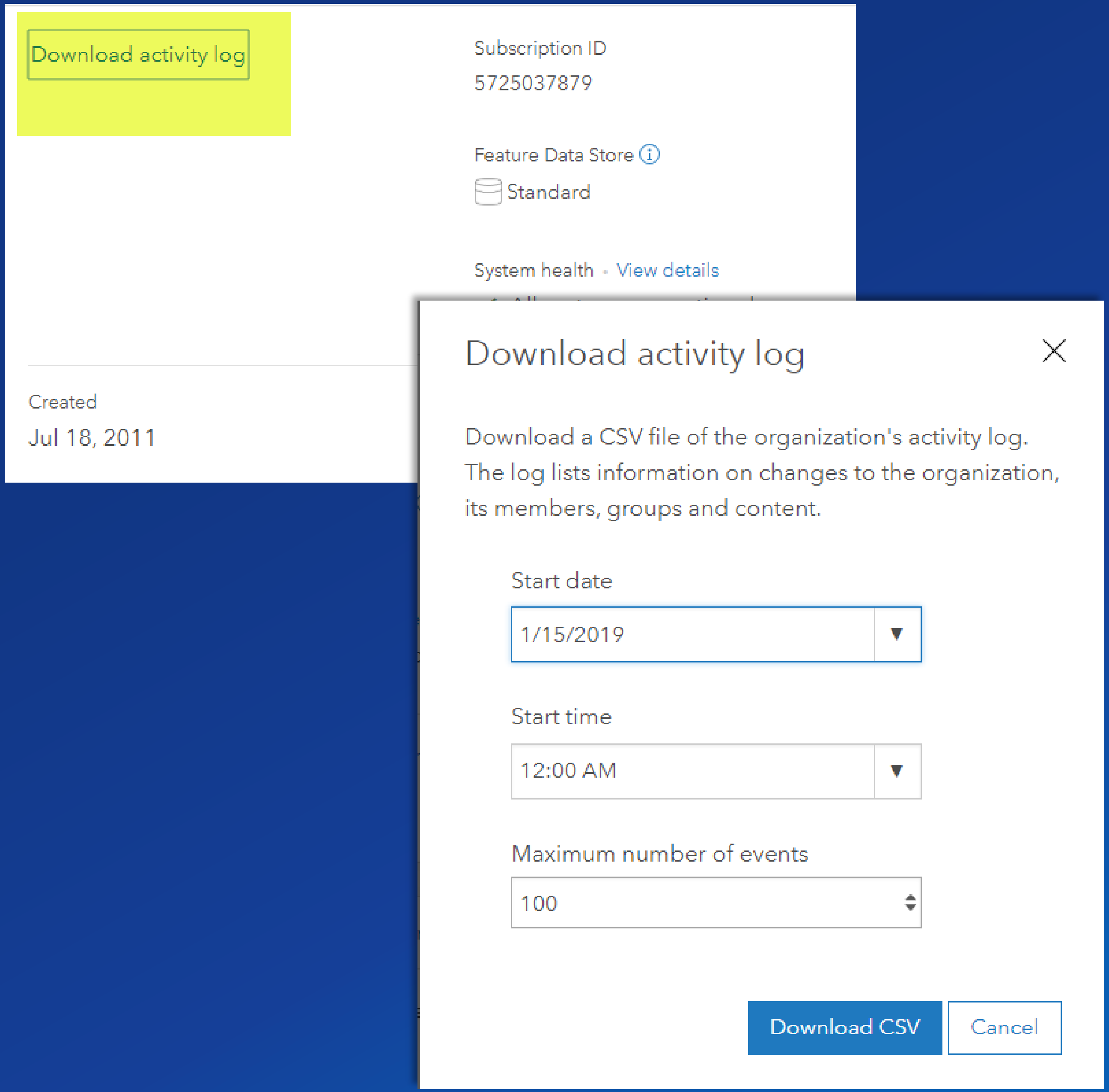
○ Item Centers ○ Item Footprints ● Density (all items)

Keeping Track of Usage

Activity Log

Helps answer questions like:

- What was affected?
- Who did it?
- What did they do?
- When did they do it?
- Where was it done from?



Subscription ID
5725037879

Feature Data Store
Standard

System health · View details

Created
Jul 18, 2011

Download activity log

Download a CSV file of the organization's activity log. The log lists information on changes to the organization, its members, groups and content.

Start date: 1/15/2019

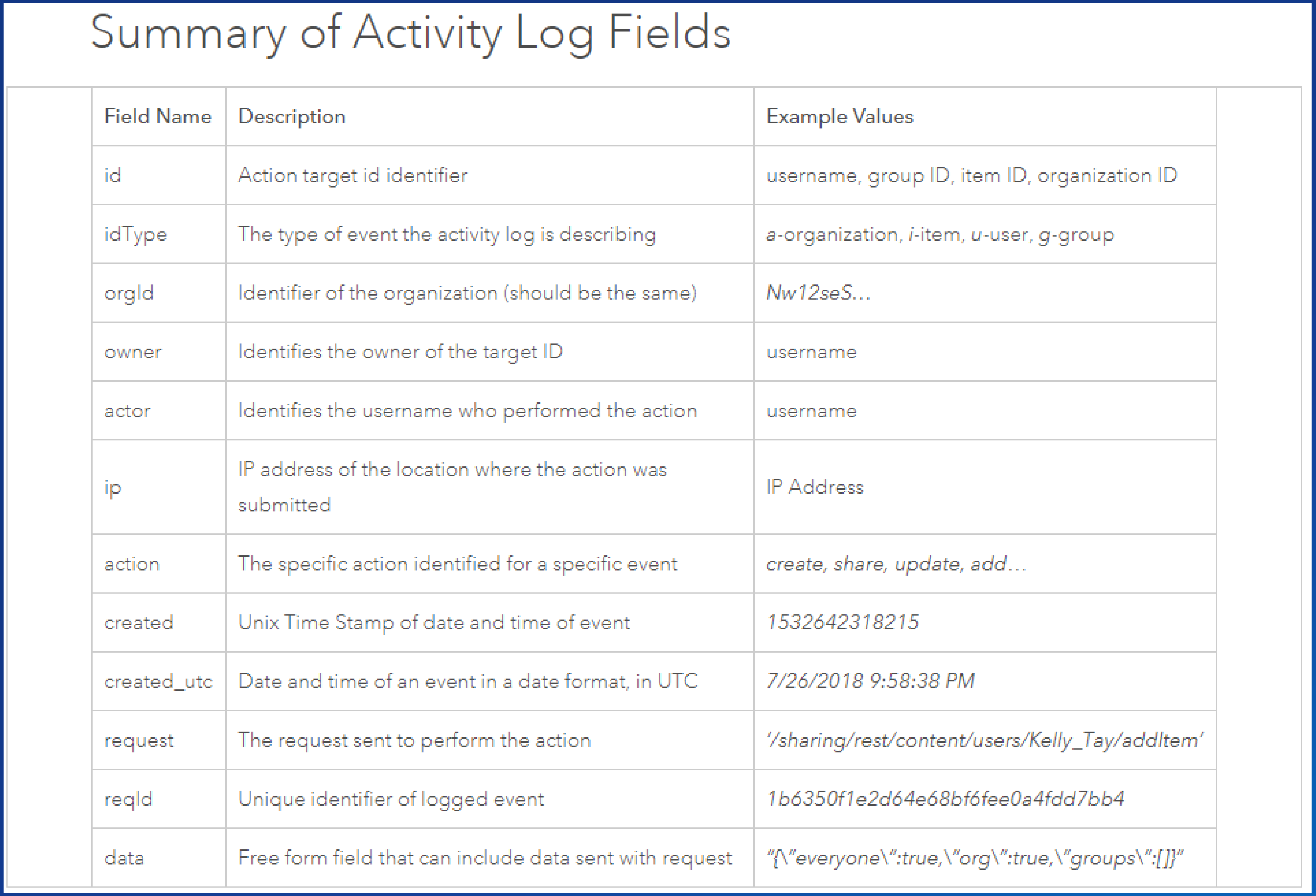
Start time: 12:00 AM

Maximum number of events: 100

Keeping Track of Usage

Activity Log

- What – idType
  - Organization
  - Item
  - User
  - Group
- Who
  - Id
  - Owner
  - actor
- Action
  - Request
  - Data
- When
  - UTC and Epoch
- From Where
  - IP address

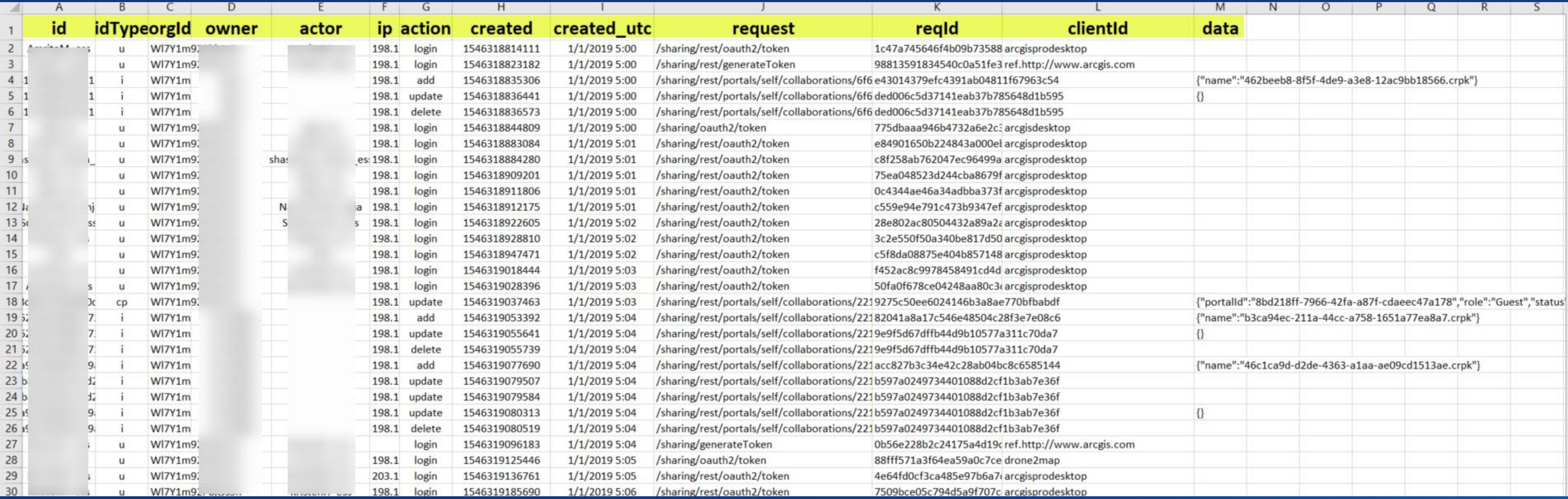


Summary of Activity Log Fields

Field Name	Description	Example Values
id	Action target id identifier	username, group ID, item ID, organization ID
idType	The type of event the activity log is describing	*a*-organization, *i*-item, *u*-user, *g*-group
orgId	Identifier of the organization (should be the same)	*Nw12seS…*
owner	Identifies the owner of the target ID	username
actor	Identifies the username who performed the action	username
ip	IP address of the location where the action was submitted	IP Address
action	The specific action identified for a specific event	*create, share, update, add…*
created	Unix Time Stamp of date and time of event	*1532642318215*
created_utc	Date and time of an event in a date format, in UTC	*7/26/2018 9:58:38 PM*
request	The request sent to perform the action	*'/sharing/rest/content/users/Kelly_Tay/addItem'*
reqId	Unique identifier of logged event	*1b6350f1e2d64e68bf6fee0a4fdd7bb4*
data	Free form field that can include data sent with request	*"{\"everyone\":true,\"org\":true,\"groups\":[]}"*

Keeping Track of Usage

Activity Log Example



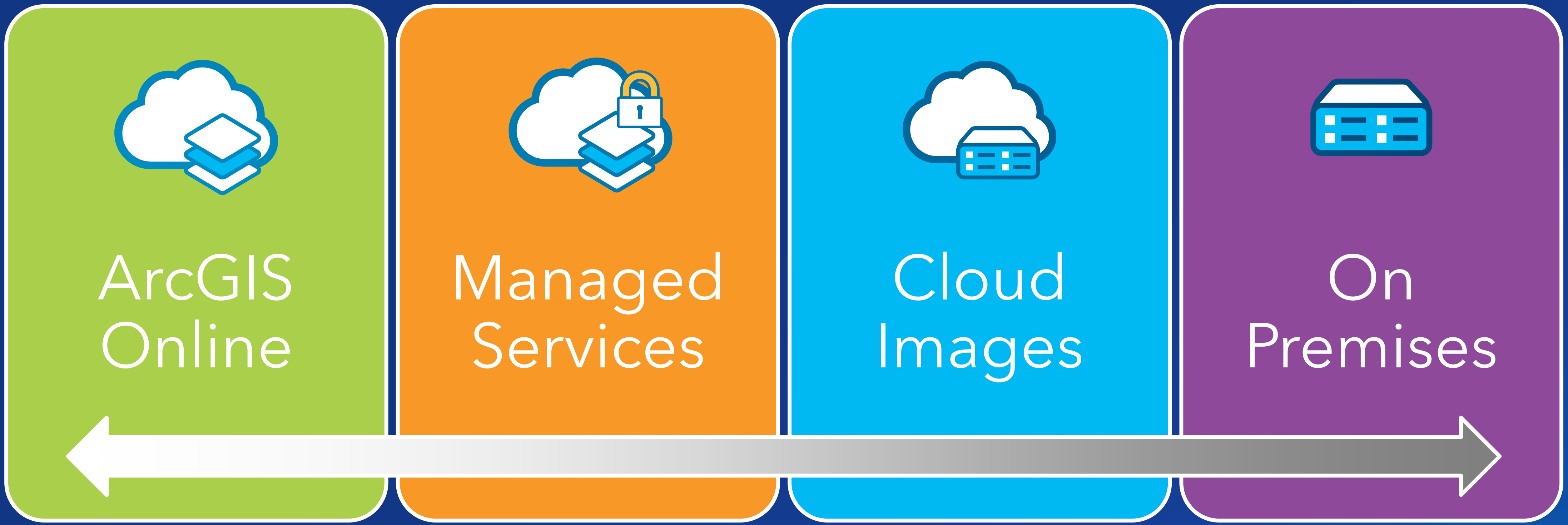
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	**id**	**idType**	**orgId**	**owner**	**actor**	**ip**	**action**	**created**	**created_utc**	**request**	**reqId**	**clientId**	**data**
2	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318814111	1/1/2019 5:00	/sharing/rest/oauth2/token	1c47a745646f4b09b73588	arcgisprodesktop	
3	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318823182	1/1/2019 5:00	/sharing/rest/generateToken	98813591834540c0a51fe3	ref.http://www.arcgis.com	
4	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	add	1546318835306	1/1/2019 5:00	/sharing/rest/portals/self/collaborations/6f6	e43014379efc4391ab04811f67963c54		{"name":"462beeb8-8f5f-4de9-a3e8-12ac9bb18566.crpk"}
5	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	update	1546318836441	1/1/2019 5:00	/sharing/rest/portals/self/collaborations/6f6	ded006c5d37141eab37b785648d1b595		{}
6	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	delete	1546318836573	1/1/2019 5:00	/sharing/rest/portals/self/collaborations/6f6	ded006c5d37141eab37b785648d1b595		
7	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318844809	1/1/2019 5:00	/sharing/oauth2/token	775dbaaa946b4732a6e2c	arcgisdesktop	
8	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318883084	1/1/2019 5:01	/sharing/rest/oauth2/token	e84901650b224843a000e	arcgisprodesktop	
9	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318884280	1/1/2019 5:01	/sharing/rest/oauth2/token	c8f258ab762047ec96499a	arcgisprodesktop	
10	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318909201	1/1/2019 5:01	/sharing/rest/oauth2/token	75ea048523d244cba8679f	arcgisprodesktop	
11	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318911806	1/1/2019 5:01	/sharing/rest/oauth2/token	0c4344ae46a34adbba373f	arcgisprodesktop	
12	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318912175	1/1/2019 5:01	/sharing/rest/oauth2/token	c559e94e791c473b9347ef	arcgisprodesktop	
13	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318922605	1/1/2019 5:02	/sharing/rest/oauth2/token	28e802ac80504432a89a2	arcgisprodesktop	
14	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318928810	1/1/2019 5:02	/sharing/rest/oauth2/token	3c2e550f50a340be817d50	arcgisprodesktop	
15	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546318947471	1/1/2019 5:02	/sharing/rest/oauth2/token	c5f8da08875e404b857148	arcgisprodesktop	
16	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546319018444	1/1/2019 5:03	/sharing/rest/oauth2/token	f452ac8c9978458491cd4d	arcgisprodesktop	
17	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546319028396	1/1/2019 5:03	/sharing/rest/oauth2/token	50fa0f678ce04248aa80c3	arcgisprodesktop	
18	[redacted]	cp	WI7Y1m9	[redacted]	[redacted]	198.1	update	1546319037463	1/1/2019 5:03	/sharing/rest/portals/self/collaborations/221	9275c50ee6024146b3a8ae770bfbabdf		{"portalId":"8bd218ff-7966-42fa-a87f-cdaeec47a178","role":"Guest","status
19	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	add	1546319053392	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221	82041a8a17c546e48504c28f3e7e08c6		{"name":"b3ca94ec-211a-44cc-a758-1651a77ea8a7.crpk"}
20	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	update	1546319055641	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221	9e9f5d67dffb44d9b10577a311c70da7		{}
21	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	delete	1546319055739	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221	9e9f5d67dffb44d9b10577a311c70da7		
22	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	add	1546319077690	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221	acc827b3c34e42c28ab04bc8c6585144		{"name":"46c1ca9d-d2de-4363-a1aa-ae09cd1513ae.crpk"}
23	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	update	1546319079507	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221	b597a0249734401088d2cf1b3ab7e36f		
24	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	update	1546319079584	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221	b597a0249734401088d2cf1b3ab7e36f		
25	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	update	1546319080313	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221	b597a0249734401088d2cf1b3ab7e36f		{}
26	[redacted]	i	WI7Y1m	[redacted]	[redacted]	198.1	delete	1546319080519	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221	b597a0249734401088d2cf1b3ab7e36f		
27	[redacted]	u	WI7Y1m9	[redacted]	[redacted]		login	1546319096183	1/1/2019 5:04	/sharing/generateToken	0b56e228b2c24175a4d19	ref.http://www.arcgis.com	
28	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546319125446	1/1/2019 5:05	/sharing/oauth2/token	88fff571a3f64ea59a0c7ce	drone2map	
29	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	203.1	login	1546319136761	1/1/2019 5:05	/sharing/rest/oauth2/token	4e64fd0cf3ca485e97b6a7	arcgisprodesktop	
30	[redacted]	u	WI7Y1m9	[redacted]	[redacted]	198.1	login	1546319185690	1/1/2019 5:06	/sharing/rest/oauth2/token	7509bce05c794d5a9f707c	arcgisprodesktop	

Deployment Architecture

Michael Young

Deployment Architecture

Options



ArcGIS Online

Managed Services

Cloud Images

On Premises

Deployment Architecture

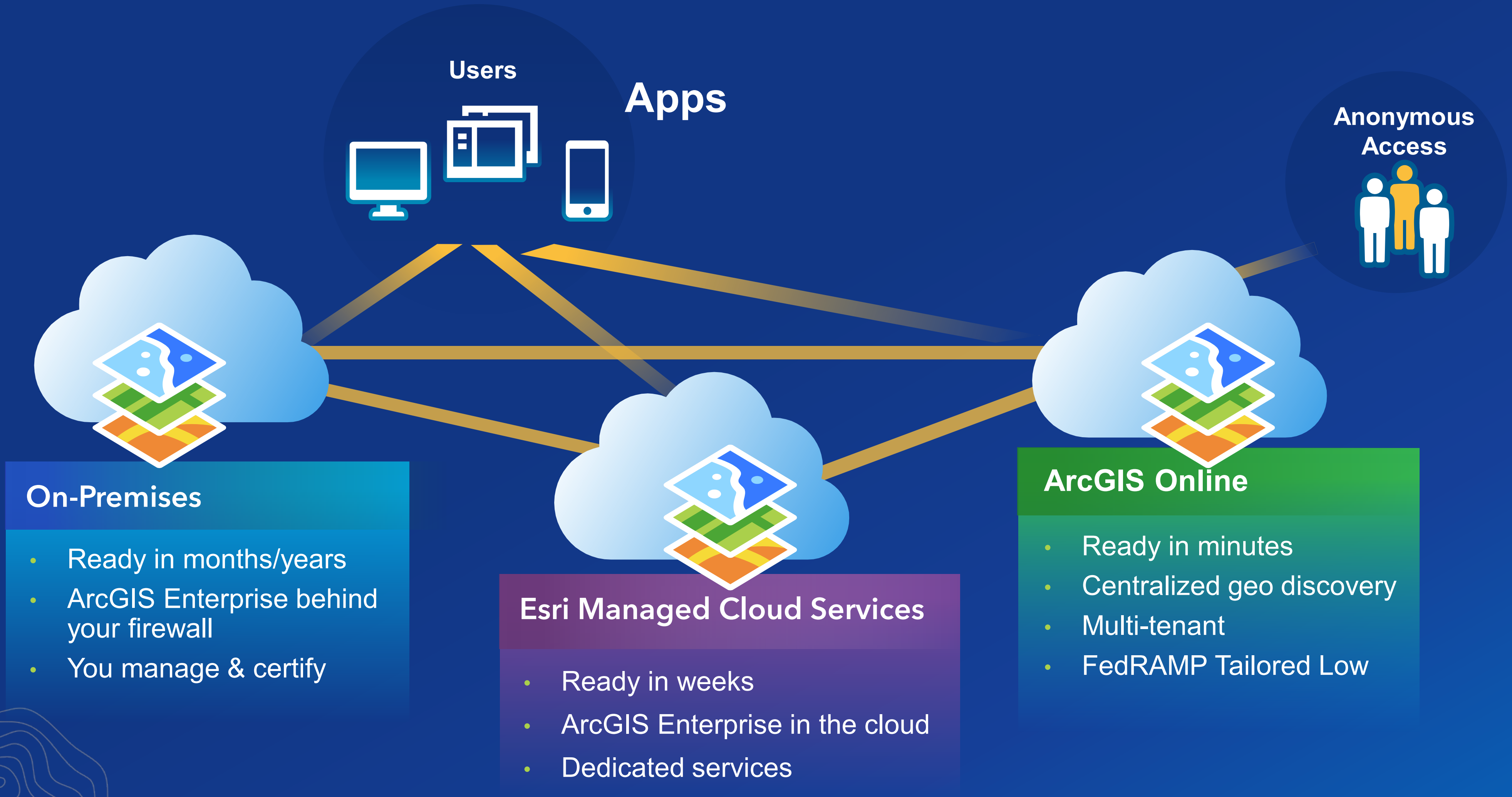
Responsibility

Responsibility	ArcGIS On-Premises	ArcGIS Cloud Images	EMCS Advanced+ *FedRAMP* *Moderate*	ArcGIS Online *FedRAMP* *Tailored Low*
Data Classification &Accountability	🟧	🟧	🟧	🟧
Client & End-Point Protection	🟧	🟧	🟦	🟦
Identity and Access Management	🟧	🟧	🟦/🟧	🟦/🟧
Application Level Controls	🟧	🟧	🟦/🟧	🟦/🟧
Network Controls	🟧	🟧	🟦/🟩	🟦/🟩
Physical Security	🟧	🟩	🟩	🟩

Customer Managed 🟧 Cloud Provider Managed 🟩 Esri Managed 🟦

Deployment Architecture

Hosting Options



On-Premises

- Ready in months/years
- ArcGIS Enterprise behind your firewall
- You manage & certify

Esri Managed Cloud Services

- Ready in weeks
- ArcGIS Enterprise in the cloud
- Dedicated services

ArcGIS Online

- Ready in minutes
- Centralized geo discovery
- Multi-tenant
- FedRAMP Tailored Low

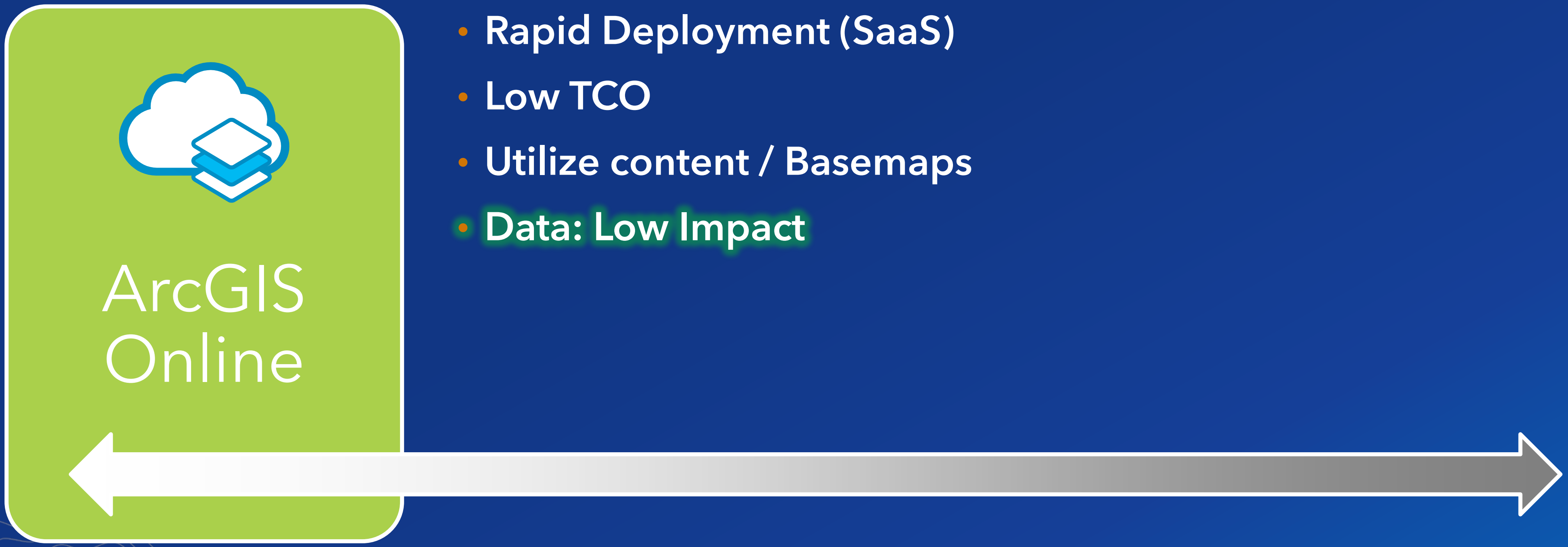
. . . All options can be combined or separate

Deployment Architecture

User Scenario – ArcGIS Online Alone

I want to share and process operational data with field workers.

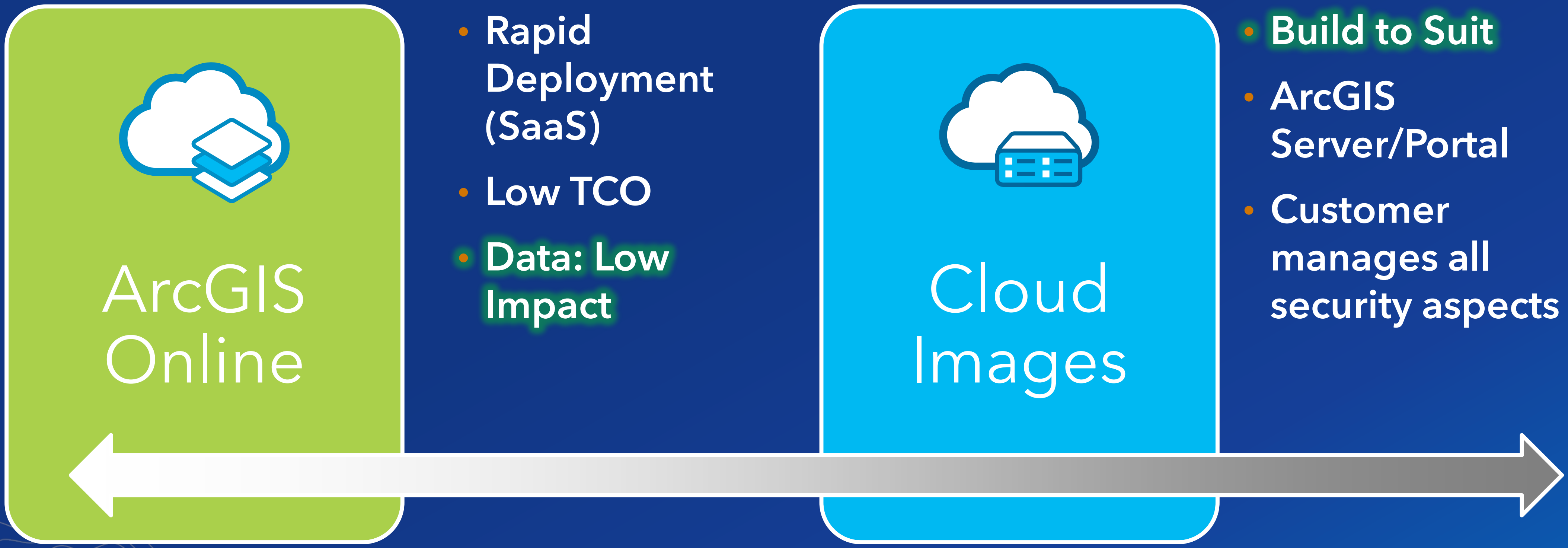
- Rapid Deployment (SaaS)
- Low TCO
- Utilize content / Basemaps
- Data: Low Impact



Deployment Architecture

User Scenario – ArcGIS Online + Cloud Images

I need to pilot a solution that requires basemaps and some ArcGIS Server specific features.



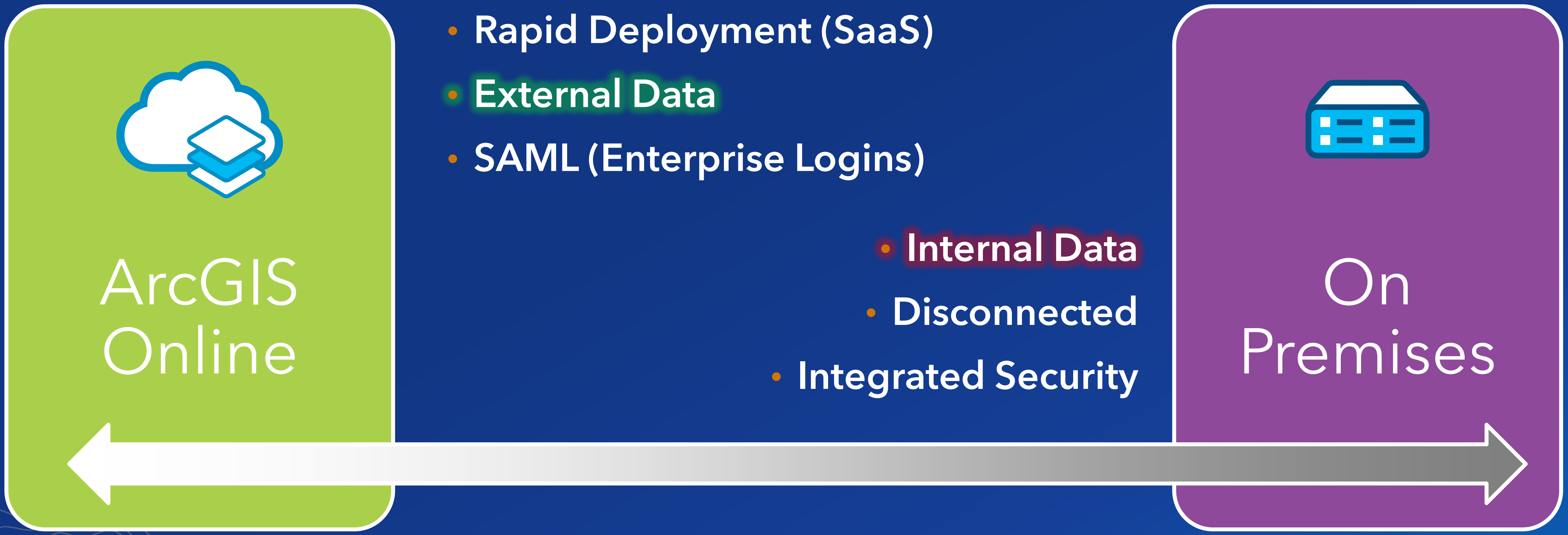
- Rapid Deployment (SaaS)
- Low TCO
- Data: Low Impact

- Build to Suit
- ArcGIS Server/Portal
- Customer manages all security aspects

Deployment Architecture

User Scenario – ArcGIS Online + On-Premises

I want to share sensitive data internally, but provide subsets to external and public users.



ArcGIS Online

- Rapid Deployment (SaaS)
- External Data
- SAML (Enterprise Logins)

- Internal Data
- Disconnected
- Integrated Security

On Premises

***Example**: EPA's FISMA Authorized GeoPlatform*

Deployment Architecture

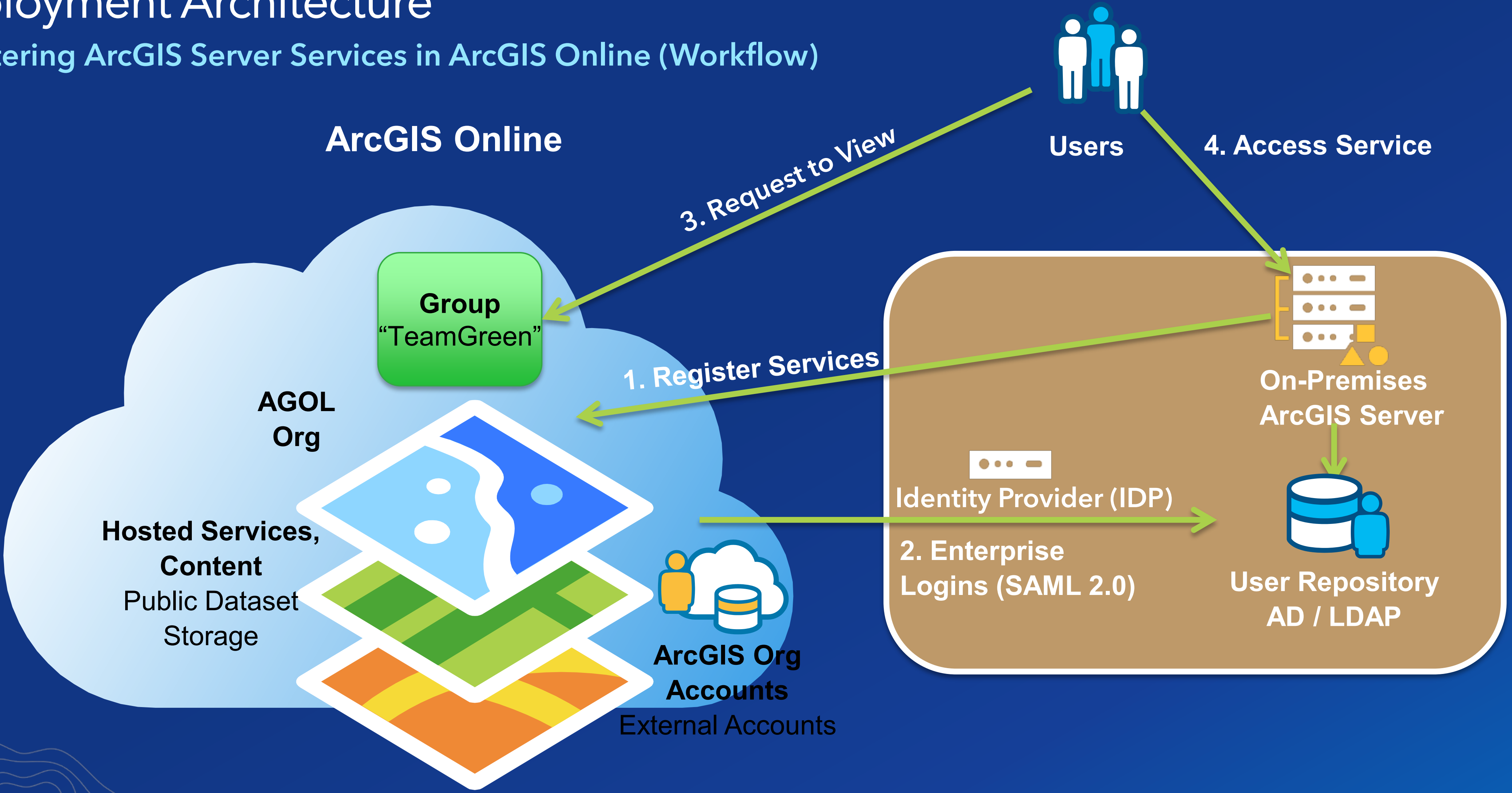
Registering ArcGIS Server Services in ArcGIS Online

- **Common for large enterprises**
  - **Primary reason**
    - **Data Segmentation / Prevent storing sensitive data in the cloud**

- **What is stored in ArcGIS Online? – Service Metadata**
  - **Username & password -** Default, not saved
  - **Initial extent -** Adjust to a less specific area
  - **Name & tags -** Address with organization naming convention
  - **IP Address -** Utilize DNS names within URL's
  - **Thumbnail image –** Replace with any image as appropriate

Deployment Architecture

Registering ArcGIS Server Services in ArcGIS Online (Workflow)



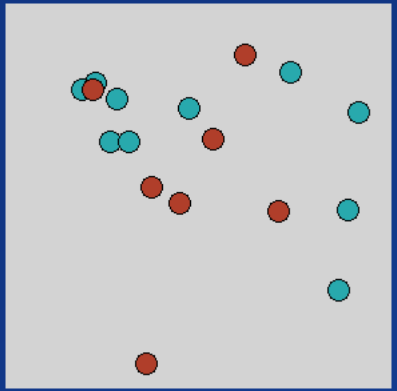
Segment sensitive data internally and public data in cloud

Deployment Architecture

Registering ArcGIS Server Services in ArcGIS Online

- **Where are internal and cloud datasets combined?**
  - At the browser
  - The browser makes separate requests for information to multiple sources and does a "mash-up"
  - Token security with TLS or even a VPN connection could be used between the device browser and on-premises system

On-Premises Operational Layer Service



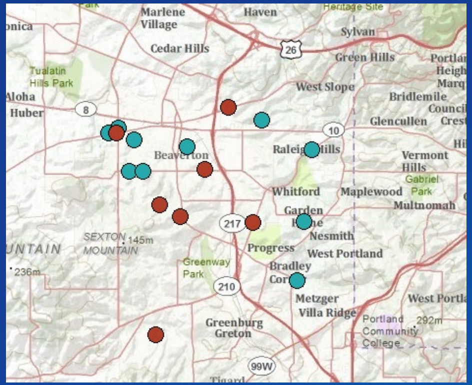
https://YourServer.com/arcgis/rest...

Cloud Basemap Service ArcGIS Online

PLEASANT VALLEY
284m
Happy Valley
Wilson Corner
Damasc
Damascus He
212

https://services.arcgisonline.com...

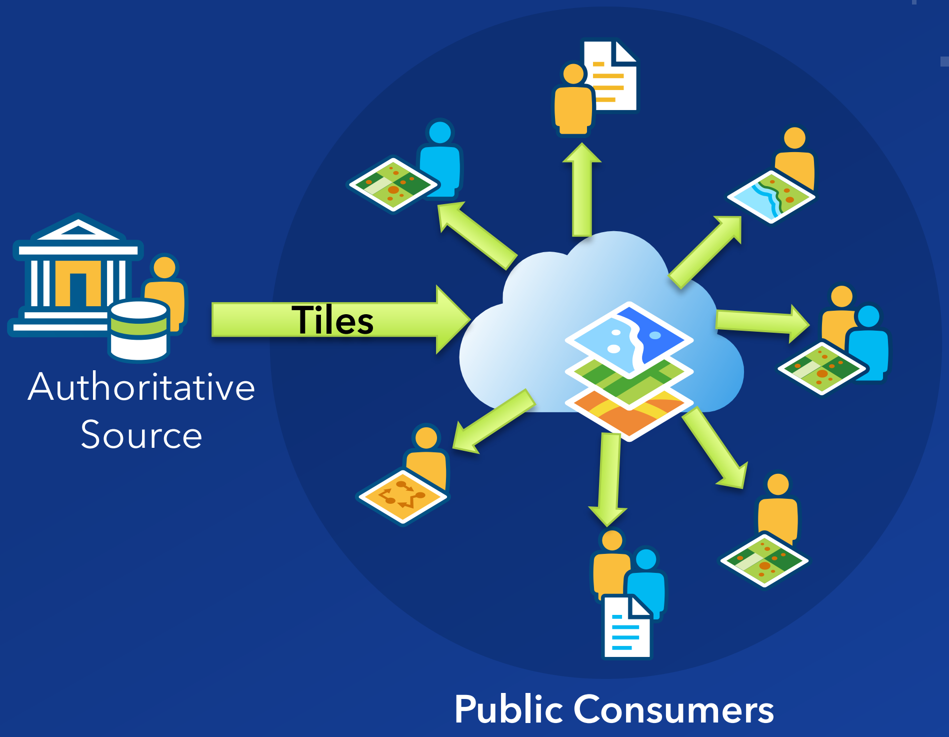
Browser Combines Layers



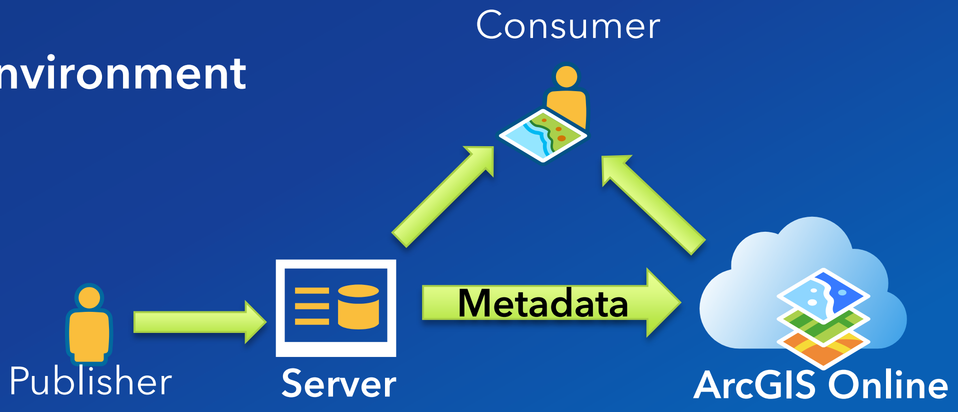
Deployment Architecture

ArcGIS Online FedRAMP Authorized Use Cases

- Use Case 1 – Public Dissemination
  - Publish tiles for fast, scalable visualizations
  - Share information with the public
  - Works well with new "Authoritative" content label



- Use Case 2 – Share operational data within or between organizations
  - Register ArcGIS Server Services in ArcGIS Online
  - Sensitive data stored on premises or other authorized environment
  - ArcGIS Online operates as a discovery portal
  - Utilize Enterprise Logins



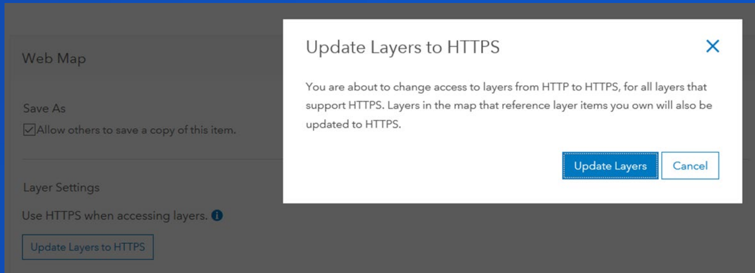
Deployment Architecture

Significant ArcGIS Online Security Change Coming

- TLS 1.2 only was enforced in 2019

- *September 15, 2020 HTTPS Only Enforced*
  - Ensures your organization meets Binding Operational Directives for HSTS

- If your organization currently allows for HTTP you need to prepare now
  - HTTP calls will be redirected to HTTPS
  - If a client can't redirect to HTTPS it will fail (eg. old Java scripts / some Python scripts)
    - ArcGIS Enterprise deployments without HTTPS option will have mixed content failures with ArcGIS Online layers
  - Capabilities to make the transition easier
    - Update Map Layers to HTTPS
    - HTTP Checker added to AGO Security Advisor tool



Web Map

Save As

☑ Allow others to save a copy of this item.

Layer Settings

Use HTTPS when accessing layers.

Update Layers to HTTPS

You are about to change access to layers from HTTP to HTTPS, for all layers that support HTTPS. Layers in the map that reference layer items you own will also be updated to HTTPS.

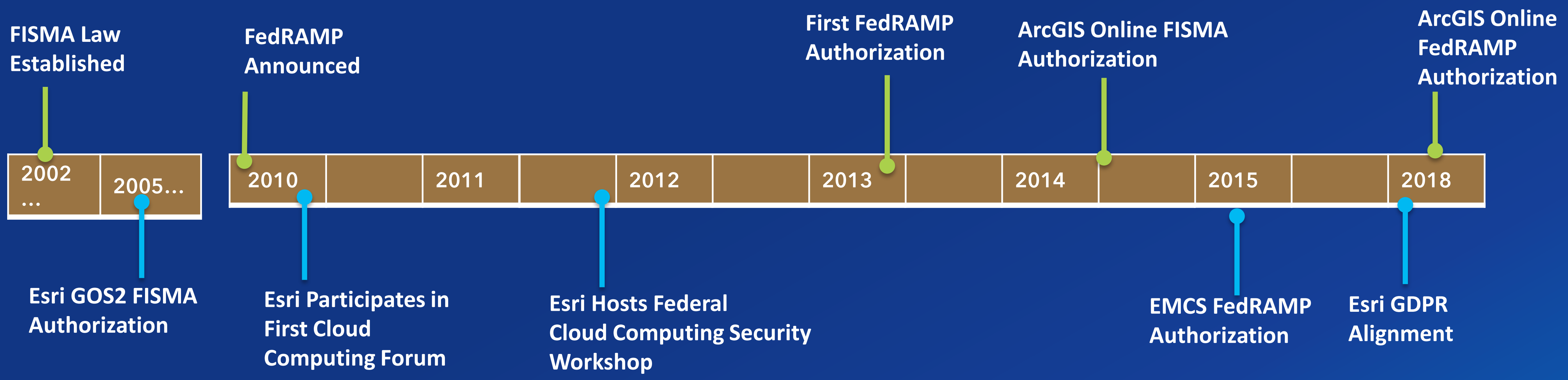
Compliance

Compliance

- Milestones
- Cloud Infrastructure Providers
- Products and Services
- Privacy Assurance / GDPR / CCPA
- Security Assurance / FedRAMP

Compliance

Milestones



FISMA Law Established

FedRAMP Announced

First FedRAMP Authorization

ArcGIS Online FISMA Authorization

ArcGIS Online FedRAMP Authorization

2002 … | 2005… | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2018

Esri GOS2 FISMA Authorization

Esri Participates in First Cloud Computing Forum

Esri Hosts Federal Cloud Computing Security Workshop

EMCS FedRAMP Authorization

Esri GDPR Alignment

Esri has actively participated in hosting and advancing secure compliant solutions for over a decade

Compliance

Cloud Infrastructure Providers

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

Cloud Infrastructure Security Compliance

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

Information Security Management System
ISO
27001
Certified

Compliance

Products & Services

- Product Based Initiatives
  - ArcGIS Server 10.3+ - DISA STIG
  - ArcGIS Desktop 9.3+ - USGCB
  - ArcGIS Pro 1.4.1+ - USGCB
- Service Based Initiatives
  - EMCS Advanced Plus (Single-tenant) – FedRAMP Moderate
  - ArcGIS Online (Multi-tenant) – FedRAMP Tailored Low
- Details for obtaining our FedRAMP packages available
  - https://www.fedramp.gov/accessing-csps-fedramp-materials-omb-max/
  -

Compliance

Privacy Assurance

- EU-U.S. Privacy Shield self-certified
  - General Esri Privacy Statement
  - Products & Services Privacy Statement Supplement

- TRUSTe
  - Provides privacy certification and dispute resolution

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
  - Stronger privacy assurance / DPA

- Up next – ArcGIS Online HIPAA Geocoding Service

Privacy Shield

TRUSTe
Certified Privacy

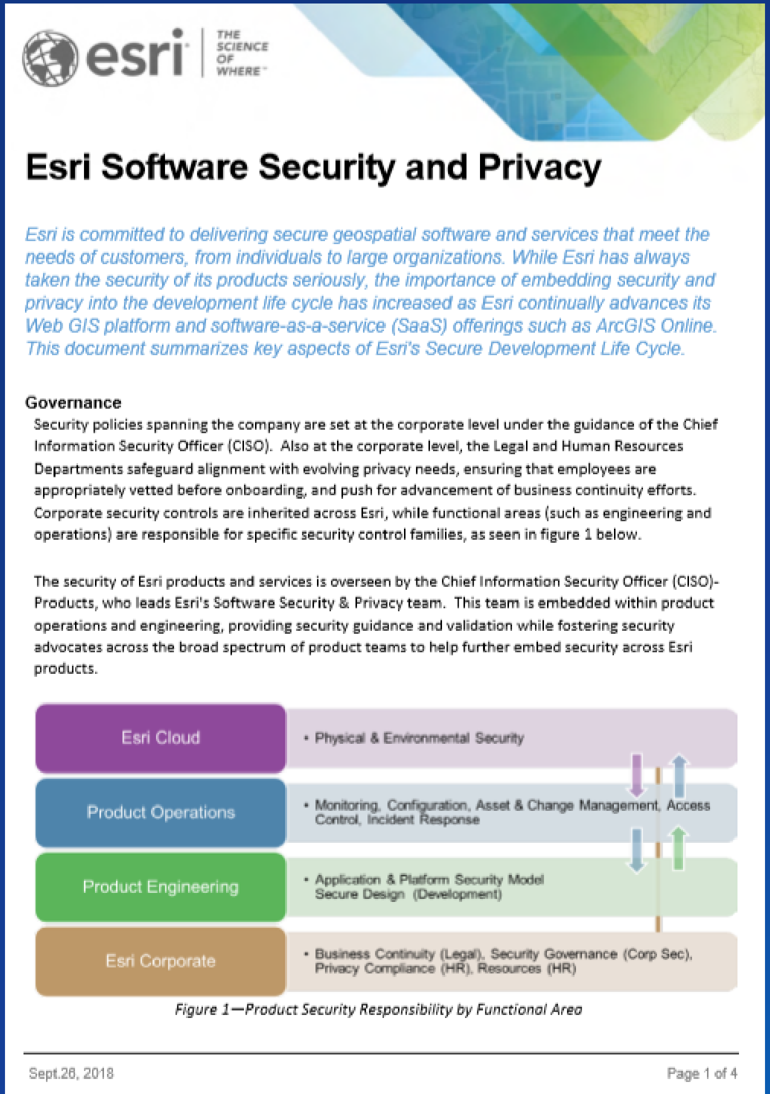
GDPR

CALIFORNIA
CONSUMER
PRIVACY ACT

Compliance

Protect By Design

- Esri established a formal Security Development Lifecyle in 2017
- Addresses governance structure (CISO – Products, CISO – Corporate)
- Guideline practices based on BSIMM, OWASP, CWE/SANS
- Most rigorous security measures with ArcGIS Enterprise & Online
- Static, Dynamic, and Component Analysis + 3rd party testing
- Product Security Incident Response Team (PSIRT) established
- FedRAMP Tailored Low Authorization drives continuous monitoring
- ArcGIS Online customer datasets are encrypted at rest and in transit



esri | THE SCIENCE OF WHERE

Esri Software Security and Privacy

Esri is committed to delivering secure geospatial software and services that meet the needs of customers, from individuals to large organizations. While Esri has always taken the security of its products seriously, the importance of embedding security and privacy into the development life cycle has increased as Esri continually advances its Web GIS platform and software-as-a-service (SaaS) offerings such as ArcGIS Online. This document summarizes key aspects of Esri's Secure Development Life Cycle.

Governance

Security policies spanning the company are set at the corporate level under the guidance of the Chief Information Security Officer (CISO). Also at the corporate level, the Legal and Human Resources Departments safeguard alignment with evolving privacy needs, ensuring that employees are appropriately vetted before onboarding, and push for advancement of business continuity efforts. Corporate security controls are inherited across Esri, while functional areas (such as engineering and operations) are responsible for specific security control families, as seen in figure 1 below.

The security of Esri products and services is overseen by the Chief Information Security Officer (CISO)-Products, who leads Esri's Software Security & Privacy team. This team is embedded within product operations and engineering, providing security guidance and validation while fostering security advocates across the broad spectrum of product teams to help further embed security across Esri products.

Esri Cloud	• Physical & Environmental Security
Product Operations	• Monitoring, Configuration, Asset & Change Management, Access Control, Incident Response
Product Engineering	• Application & Platform Security Model Secure Design (Development)
Esri Corporate	• Business Continuity (Legal), Security Governance (Corp Sec), Privacy Compliance (HR), Resources (HR)

Figure 1—Product Security Responsibility by Functional Area

Sept.26, 2018 Page 1 of 4

See Esri Software Security & Privacy overview in Trust Center documents

Compliance

FedRAMP

- ArcGIS Online received an Agency FedRAMP Tailored Low authorization-to-operate (ATO) on June 28, 2018

- Authorization known as a Low-Impact Software as a Service (Li-SaaS)
  - Ensures annual 3rd party assessments

- Value to US Government Agencies
  - FedRAMP standardizes way US government agencies perform security authorizations for cloud products and services, shifting the authorization process from years/months to weeks/days

Compliance

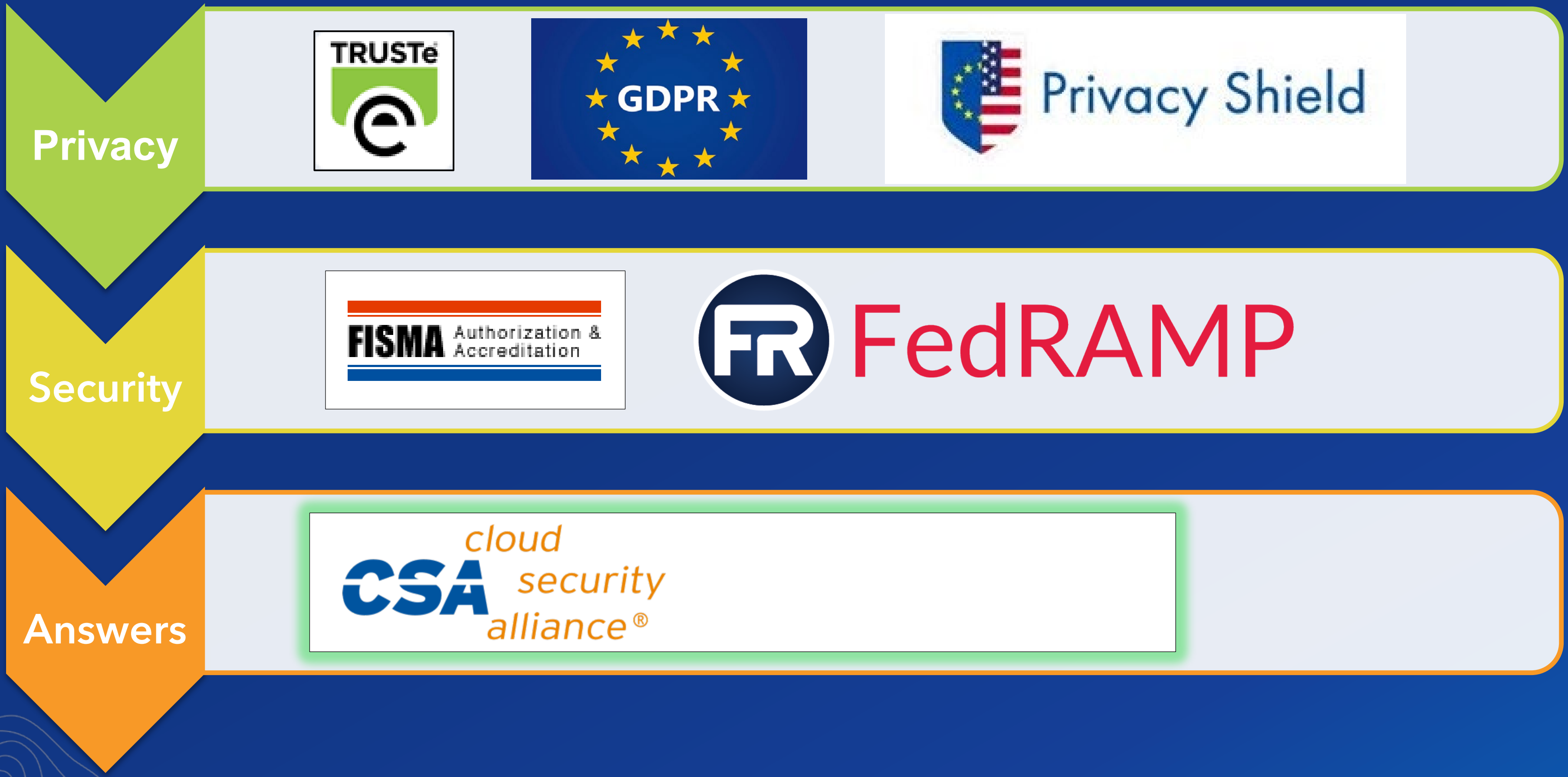
FedRAMP Alignment

- A Customer Responsibility Matrix (CRM) details recommended Organization settings to align with FedRAMP guidelines (summarized below)
  - Enable the HTTPS Only Security Policy
  - Enable Allow only Standard SQL Queries
  - Disable Security Policy allowing members to edit biographical information
  - Enable SAML v2.0 Enterprise Logins
  - Disable Social logins (w/exception for Google business accounts)
  - Add relevant domains for Allow Origins
  - Enable using Esri vector basemaps under Settings/Map/Basemap Gallery

The CRM is available as part of the AGO FedRAMP Package

Compliance

Summary Across ArcGIS Online


Privacy
TRUSTe
GDPR
Privacy Shield
Security
FISMA Authorization & Accreditation
FR FedRAMP
Answers
CSA cloud security alliance®

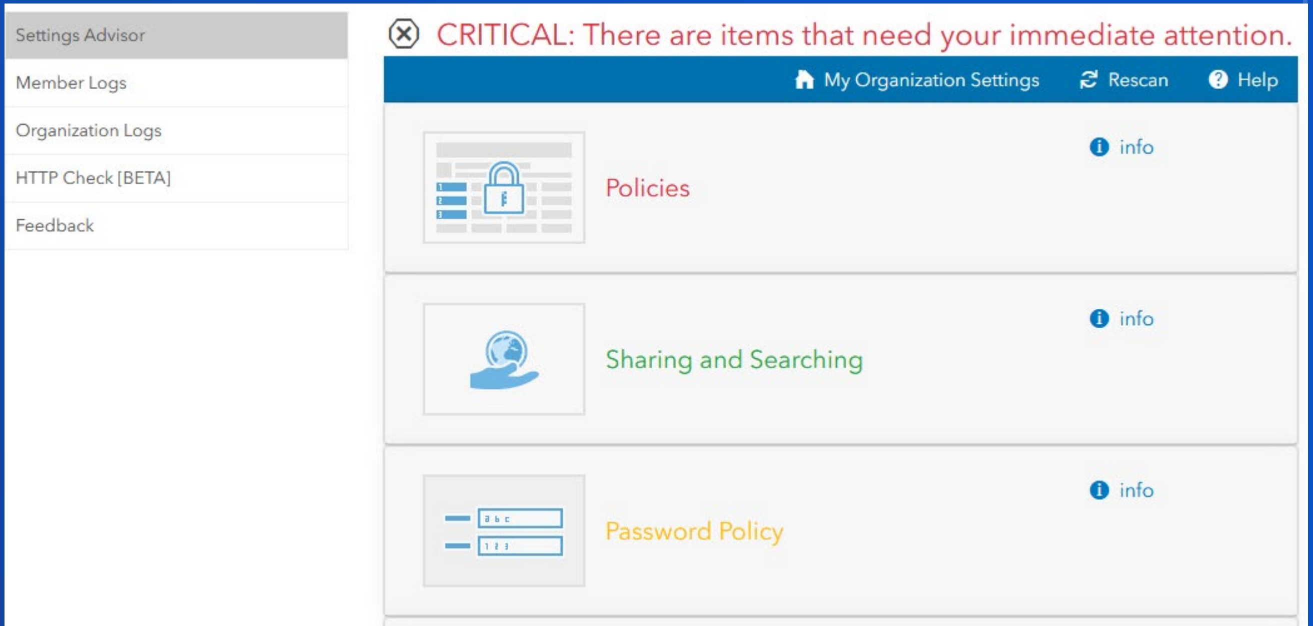
Trust.ArcGIS.com

Easing Security & Privacy Validation

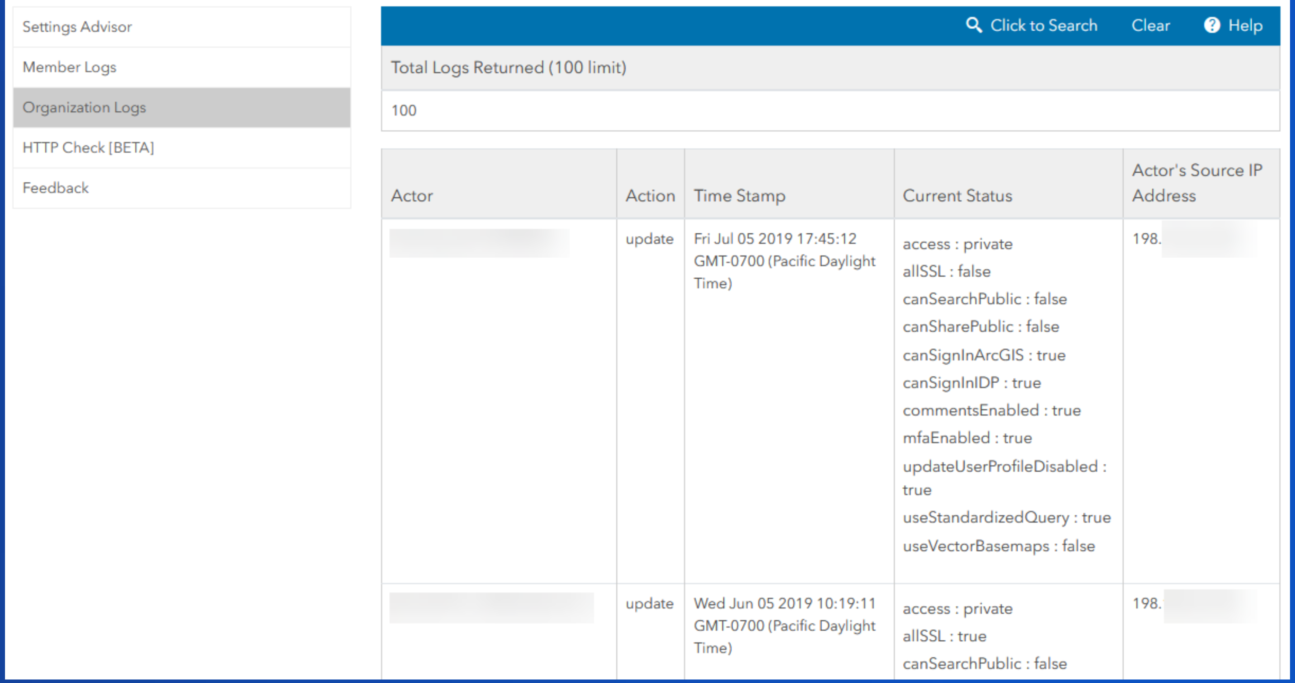
AGO Security Advisor Tool

- **Launch from ArcGIS Trust Center**

- **Validate settings/usage against secure best practices**
- **GUI for organization & user level audit log visualization**



CRITICAL: There are items that need your immediate attention.



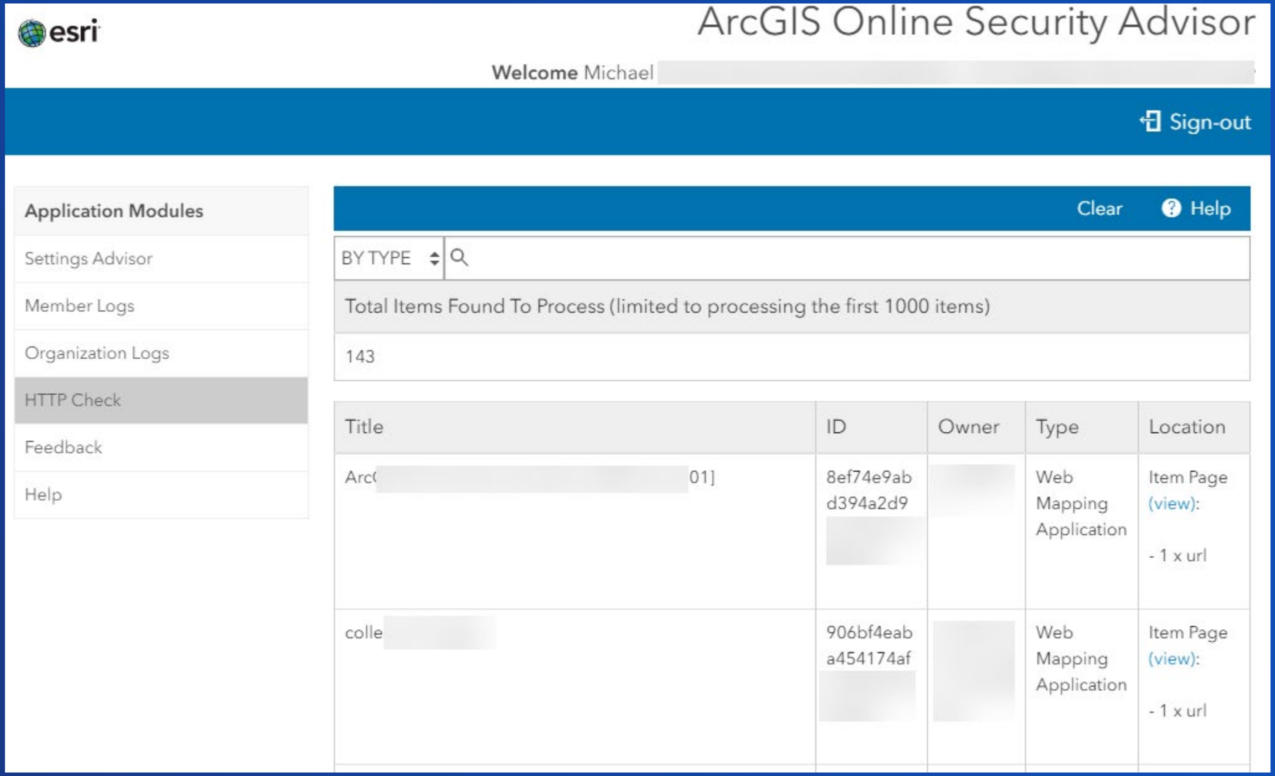
Total Logs Returned (100 limit)

100

Actor	Action	Time Stamp	Current Status	Actor's Source IP Address
[redacted]	update	Fri Jul 05 2019 17:45:12 GMT-0700 (Pacific Daylight Time)	access : private allSSL : false canSearchPublic : false canSharePublic : false canSignInArcGIS : true canSignInIDP : true commentsEnabled : true mfaEnabled : true updateUserProfileDisabled : true useStandardizedQuery : true useVectorBasemaps : false	198.[redacted]
[redacted]	update	Wed Jun 05 2019 10:19:11 GMT-0700 (Pacific Daylight Time)	access : private allSSL : true canSearchPublic : false	198.[redacted]

AGO Security Advisor Tool

- **New HTTP Checker feature**
  - **Helps ease HTTPS enforcement for customers with HTTP *still* enabled**
  - **Flags any HTTP references within your org**



esri

ArcGIS Online Security Advisor

Welcome Michael [redacted]

Application Modules

- Settings Advisor
- Member Logs
- Organization Logs
- HTTP Check
- Feedback
- Help

Total Items Found To Process (limited to processing the first 1000 items)

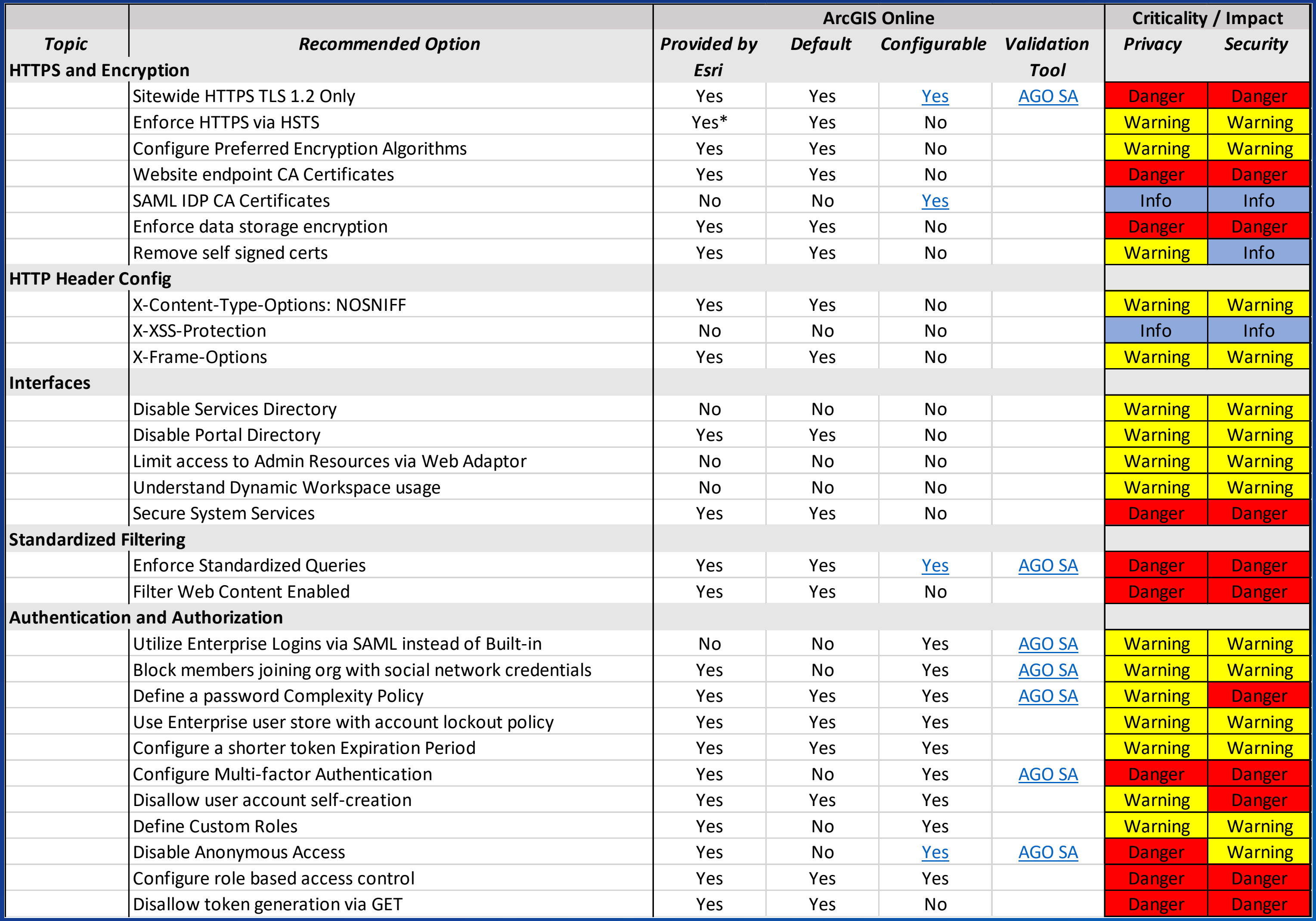
143

Title	ID	Owner	Type	Location
Arc[redacted]01]	8ef74e9ab d394a2d9 [redacted]	[redacted]	Web Mapping Application	Item Page (view): - 1 x url
colle[redacted]	906bf4eab a454174af [redacted]	[redacted]	Web Mapping Application	Item Page (view): - 1 x url

Python HTTP Checker will be released for more advanced needs/Enterprise validation

Additional Security & Privacy Guidance Coming

- Upcoming ArcGIS privacy paper lays out the relative security and privacy impact of application settings
  - Guidance for ArcGIS Enterprise and ArcGIS Online
  - Highlights which ones checked by Security Advisor
  - Privacy check will be added to Security Advisor tool
- Final policy recommendations will be based on incorporating feedback from customers like you!



		ArcGIS Online				Criticality / Impact	
Topic	*Recommended Option*	*Provided by Esri*	*Default*	*Configurable*	*Validation Tool*	*Privacy*	*Security*
HTTPS and Encryption							
	Sitewide HTTPS TLS 1.2 Only	Yes	Yes	Yes	AGO SA	Danger	Danger
	Enforce HTTPS via HSTS	Yes*	Yes	No		Warning	Warning
	Configure Preferred Encryption Algorithms	Yes	Yes	No		Warning	Warning
	Website endpoint CA Certificates	Yes	Yes	No		Danger	Danger
	SAML IDP CA Certificates	No	No	Yes		Info	Info
	Enforce data storage encryption	Yes	Yes	No		Danger	Danger
	Remove self signed certs	Yes	Yes	No		Warning	Info
HTTP Header Config							
	X-Content-Type-Options: NOSNIFF	Yes	Yes	No		Warning	Warning
	X-XSS-Protection	No	No	No		Info	Info
	X-Frame-Options	Yes	Yes	No		Warning	Warning
Interfaces							
	Disable Services Directory	No	No	No		Warning	Warning
	Disable Portal Directory	Yes	Yes	No		Warning	Warning
	Limit access to Admin Resources via Web Adaptor	No	No	No		Warning	Warning
	Understand Dynamic Workspace usage	No	No	No		Warning	Warning
	Secure System Services	Yes	Yes	No		Danger	Danger
Standardized Filtering							
	Enforce Standardized Queries	Yes	Yes	Yes	AGO SA	Danger	Danger
	Filter Web Content Enabled	Yes	Yes	No		Danger	Danger
Authentication and Authorization							
	Utilize Enterprise Logins via SAML instead of Built-in	No	No	Yes	AGO SA	Warning	Warning
	Block members joining org with social network credentials	Yes	No	Yes	AGO SA	Warning	Warning
	Define a password Complexity Policy	Yes	Yes	Yes	AGO SA	Warning	Danger
	Use Enterprise user store with account lockout policy	Yes	Yes	Yes		Warning	Warning
	Configure a shorter token Expiration Period	Yes	Yes	Yes		Warning	Warning
	Configure Multi-factor Authentication	Yes	No	Yes	AGO SA	Danger	Danger
	Disallow user account self-creation	Yes	Yes	Yes		Warning	Danger
	Define Custom Roles	Yes	No	Yes		Warning	Warning
	Disable Anonymous Access	Yes	No	Yes	AGO SA	Danger	Warning
	Configure role based access control	Yes	Yes	Yes		Danger	Danger
	Disallow token generation via GET	Yes	Yes	No		Danger	Danger

Summary

Summary

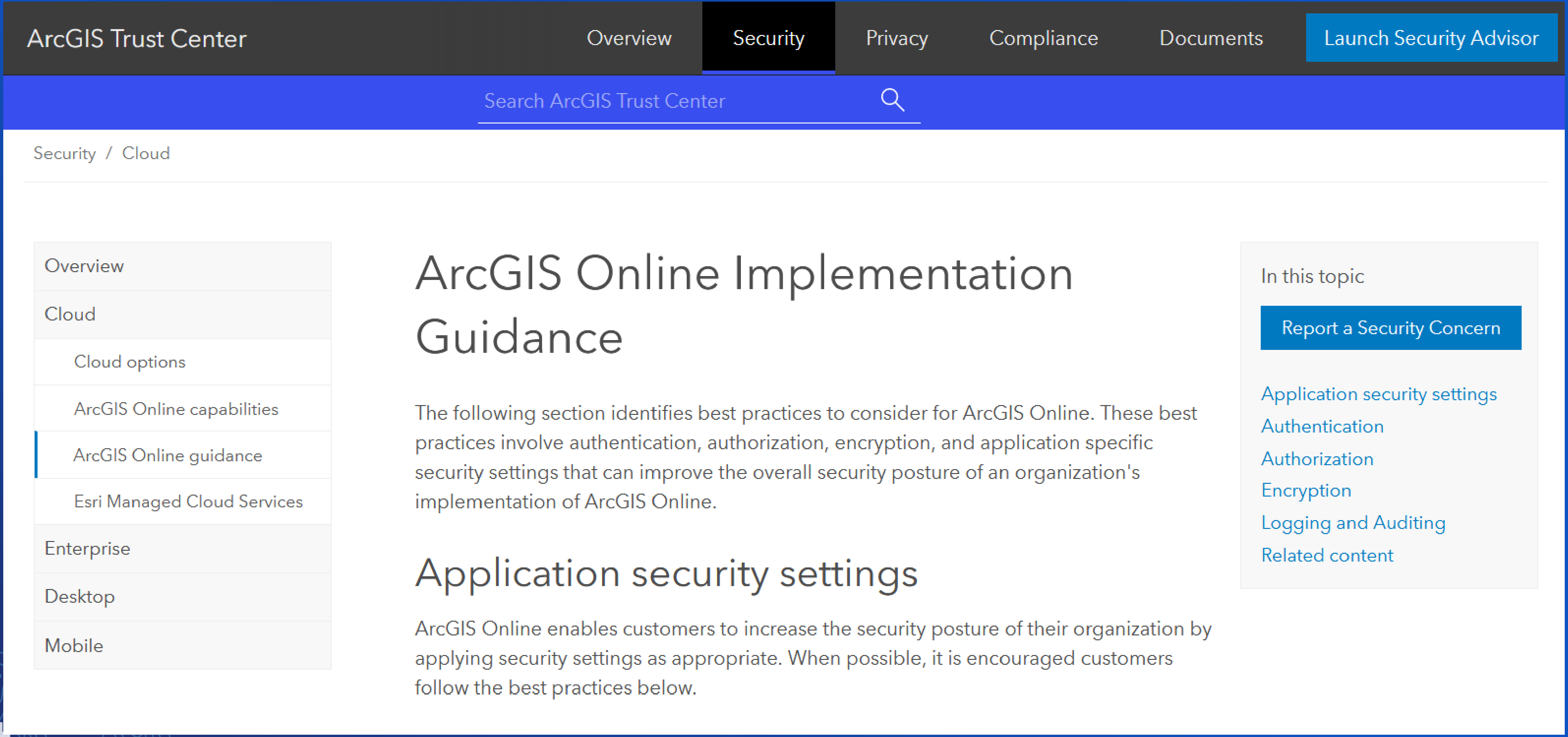
- FedRAMP, GDPR and CCPA alignment ensure ArcGIS Online security & privacy capabilities continue to advance

- Significant security advancements are coming that could directly affect your operations
  - HTTPS Only enforced in 2020

- Extensive security, privacy, compliance, and status info available
  - Trust Center - Trust.ArcGIS.com
  - In-depth Cloud Security Alliance (CSA) answers readily available
  - Security best practice validation tool

Summary

Want to learn more?



ArcGIS Online Implementation Guidance

The following section identifies best practices to consider for ArcGIS Online. These best practices involve authentication, authorization, encryption, and application specific security settings that can improve the overall security posture of an organization's implementation of ArcGIS Online.

Application security settings

ArcGIS Online enables customers to increase the security posture of their organization by applying security settings as appropriate. When possible, it is encouraged customers follow the best practices below.

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 *September 15, 2020*
- What does this mean for you?
  - After 9/15/20 all HTTP requests to ArcGIS Online will be redirected to HTTPS
  - Clients limited to HTTP only will fail (for example scheduled clear-text Python script calls)
  - HTTP only ArcGIS Enterprise deployments may have issues accessing ArcGIS Online services
- What do you need to do?
  - Validate your ArcGIS Online org utilizes HTTPS only immediately
  - Launch AGO Security Advisor tool to check your org settings @ Trust.ArcGIS.com
  - If HTTP enabled, use tool to discover HTTP references and change to HTTPS
  - Enforce HTTPS only for your orgs ASAP and validate clients/scripts can use HTTPS
  - Keep an eye out for additional announcements and support guidance pages

Questions?

esri

esri | THE SCIENCE OF WHERE

2019 ESRI
FEDERAL GIS CONFERENCE
WASHINGTON, DC