



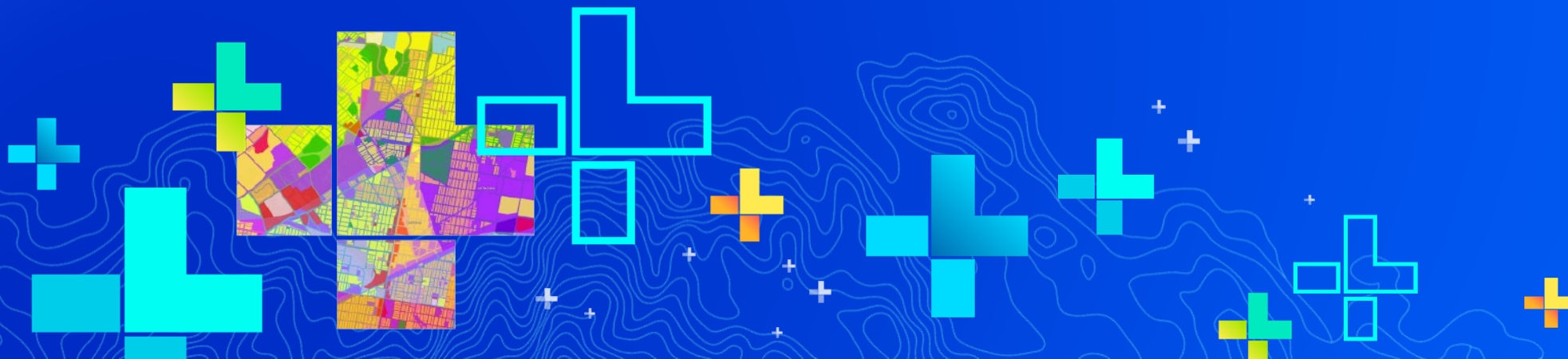
ArcGIS Online: An Introduction to Security, Privacy, and Compliance

Andrea Rosso

Michael Young

Paul Ross

SEE
WHAT
OTHERS
CAN'T



ArcGIS Online Security

You

- App Configuration
- Access
- Credentials
- Roles, Privileges
- Sharing
- Authentication Options
- Password Policy
- Personal Information
- Tracking Usage

Esri

- Software Design & Security
- Privacy
- Secure Operations
- Certifications/Compliance
- Customer Communication
- Customer Data
- OS, Network, Firewall Config

Infrastructure
Partners

- Compute
- Storage
- Database
- Network
- Physical Security

Agenda

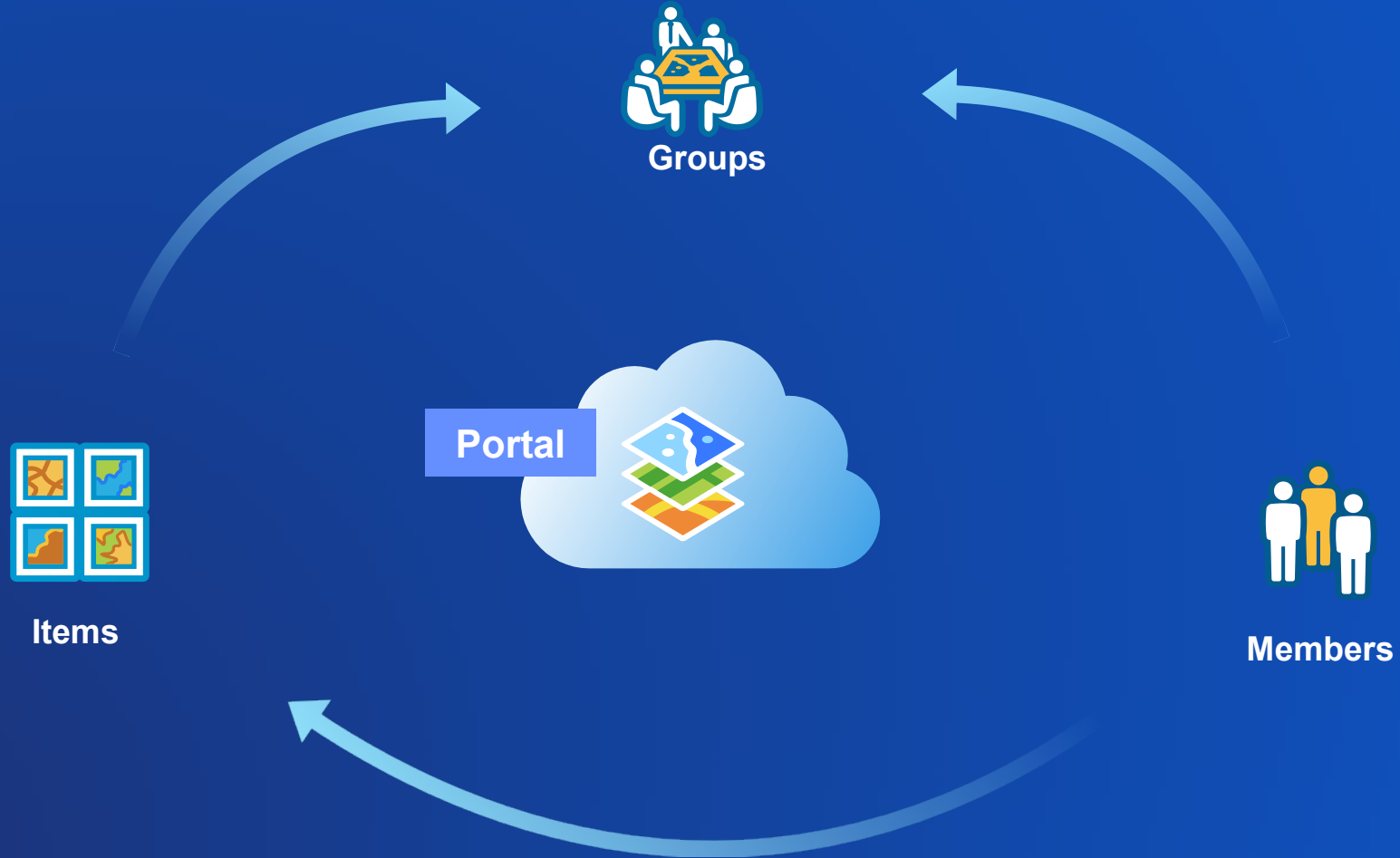
- **Platform Security**
- **Deployment Architecture**
- **Compliance**
- **Security Advisor Tool**

Platform Security

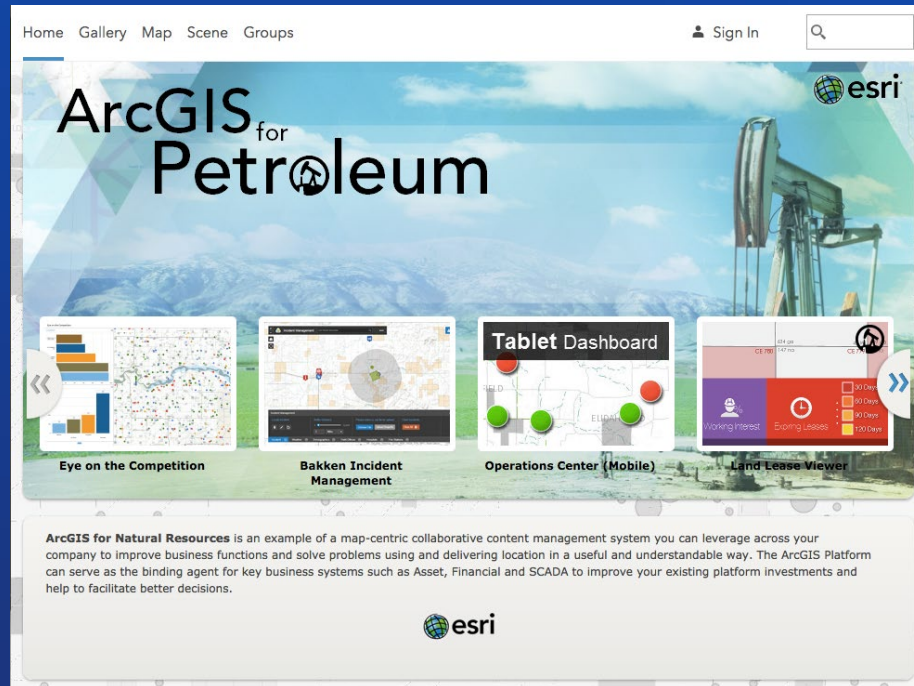
Andrea Rosso



Portal Information Model













Portal



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

Items

1 - 5 of 5 in uc2018sec Sort by: Date Modified ▾ ↓

<input type="checkbox"/>	Title			Modified
<input type="checkbox"/>	 Store Closures	CSV	 ★ ...	Jul 6, 2018
<input type="checkbox"/>	 Buildings	Web Scene	 ★ ...	Jul 6, 2018
<input type="checkbox"/>	 Hazards	Feature Layer (hosted)	 ★ ...	Jul 6, 2018
<input type="checkbox"/>	 Schools	Shapefile	 ★ ...	Jul 6, 2018
<input type="checkbox"/>	 USA Zip Codes	Layer Package	 ★ ...	Jul 6, 2018

- **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

<input type="checkbox"/>	Member	Last login	User type	Role
<input type="checkbox"/>	 Al Dente al_EsriSecPres	Never	Viewer	Viewer
<input type="checkbox"/>	 Barbara Seville barbara_EsriSecPres	Never	Viewer	Viewer
<input type="checkbox"/>	 Marsha Mellow nmarsha_EsriSecPres	Never	Viewer	Viewer
<input type="checkbox"/>	 randall williams EsriSecPresentations	Never	Creator	Administrator
<input type="checkbox"/>	 Randall Williams randall_williams_EsriSecPres	Never	Creator	Publisher

Roles

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

Create a new role Save role Discard

Role name

Description

Privilege compatibility
View | View and edit | View, edit, create and manage

Compatible with Creator user type

Role privileges
Import settings from an existing role or template Toggle all on Collapse all

General Privileges

<input type="checkbox"/> Members [-]	<input type="checkbox"/> Groups [-]	<input type="checkbox"/> Content [-]
<input type="checkbox"/> View	<input type="checkbox"/> Create, update, and delete <input type="checkbox"/> Join organizational groups <input type="checkbox"/> Join external groups <input type="checkbox"/> View groups shared with organization	<input type="checkbox"/> Create, update, and delete <input type="checkbox"/> Publish hosted feature layers <input type="checkbox"/> Publish hosted tile layers <input type="checkbox"/> Publish hosted scene layers <input type="checkbox"/> View content shared with organization
<input type="checkbox"/> Sharing [-]	<input type="checkbox"/> Premium Content [-]	<input type="checkbox"/> Features [-]
<input type="checkbox"/> Share with groups <input type="checkbox"/> Share with organization <input type="checkbox"/> Share with public <input type="checkbox"/> Make groups visible to organization <input type="checkbox"/> Make groups visible to public <input type="checkbox"/> Make groups available to Open Data	<input type="checkbox"/> Geocoding <input type="checkbox"/> Network Analysis <input type="checkbox"/> Spatial Analysis <input type="checkbox"/> GeoEnrichment <input type="checkbox"/> Demographics <input type="checkbox"/> Elevation Analysis	<input type="checkbox"/> Edit <input type="checkbox"/> Edit with full control

Administrative Privileges

<input type="checkbox"/> Members [-]	<input type="checkbox"/> Groups [-]	<input type="checkbox"/> Content [-]
<input type="checkbox"/> View all <input type="checkbox"/> Update <input type="checkbox"/> Delete <input type="checkbox"/> Invite	<input type="checkbox"/> View all <input type="checkbox"/> Update <input type="checkbox"/> Delete <input type="checkbox"/> Reassign ownership	<input type="checkbox"/> View all <input type="checkbox"/> Update <input type="checkbox"/> Delete <input type="checkbox"/> Reassign ownership

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?

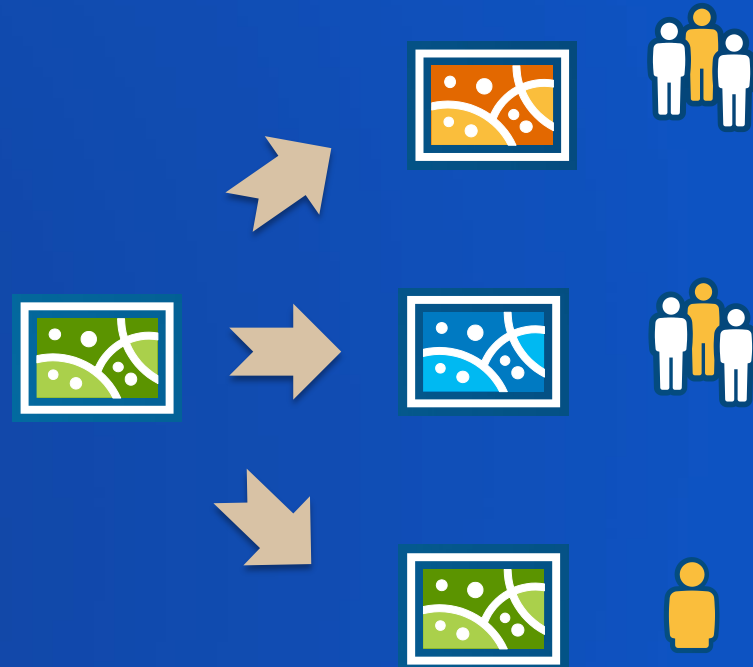
- You
- Administrators
- Data curators with the appropriate privileges

Export Data

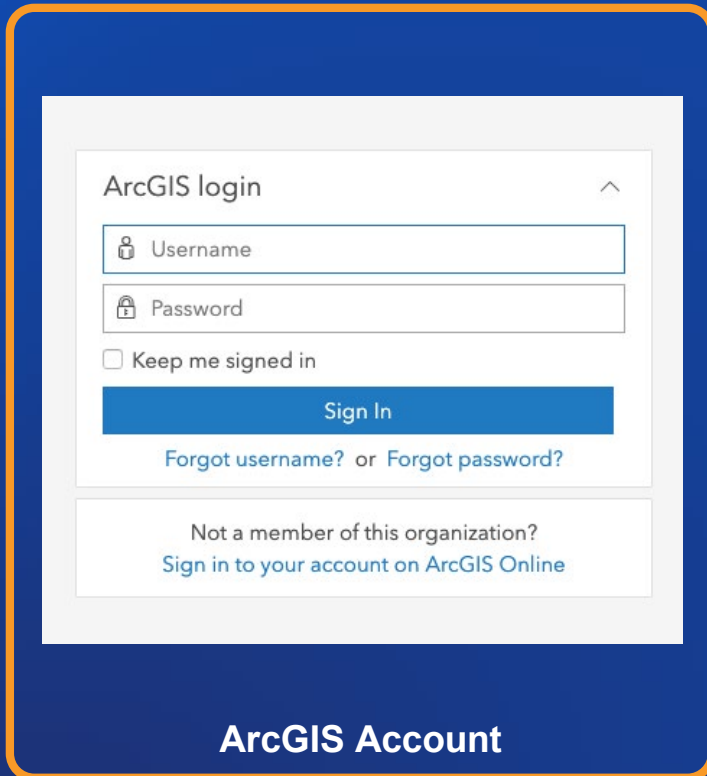
- Allow others to export to different formats.

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



Authentication Options – ArcGIS Accounts



ArcGIS login

Username

Password

Keep me signed in

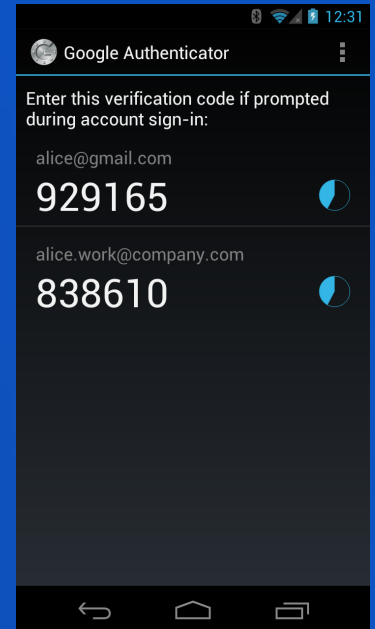
Sign In

[Forgot username?](#) or [Forgot password?](#)

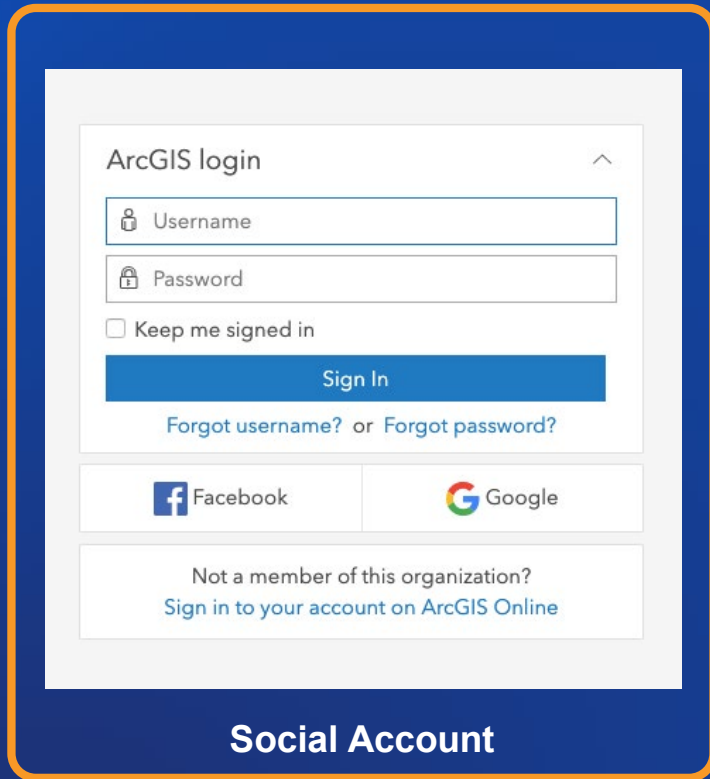
Not a member of this organization?
[Sign in to your account on ArcGIS Online](#)

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

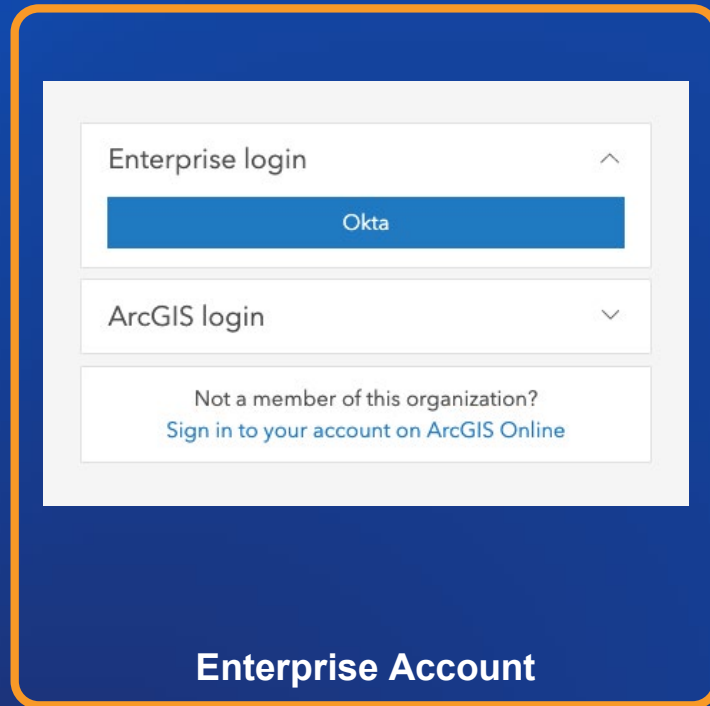


Authentication Options – Social Accounts

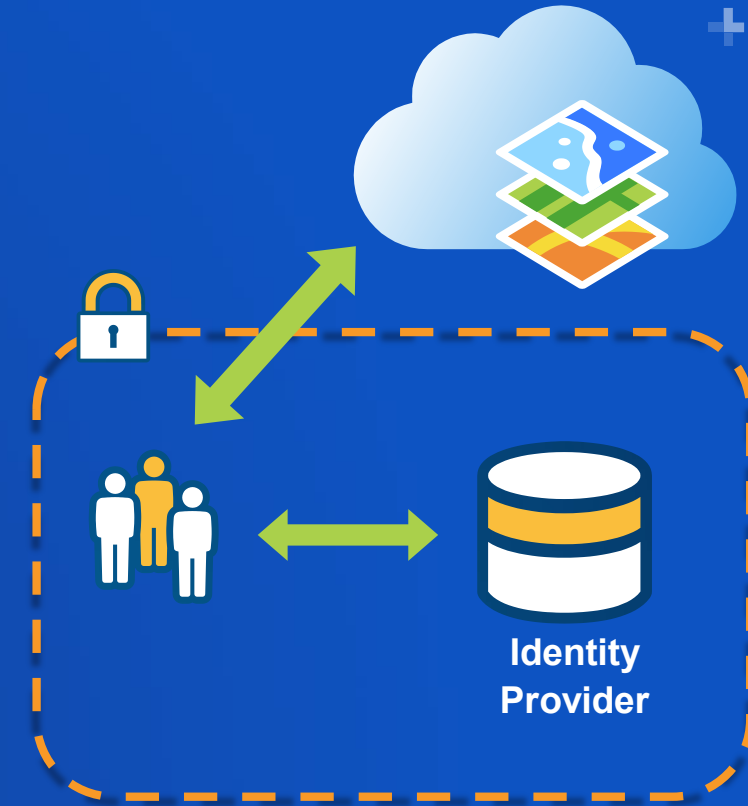


- Facebook Logins
- Google Logins
- By Invitation
- Social Login maps to unique username in Organization
- Requires an email
- Sign out doesn't sign out of your Social login

Authentication Options – Enterprise Accounts



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




Admin Organization Controls

- **HTTPS and HSTS**
- **Disable Sharing to Everyone**
- **Disable Bio**
- **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.

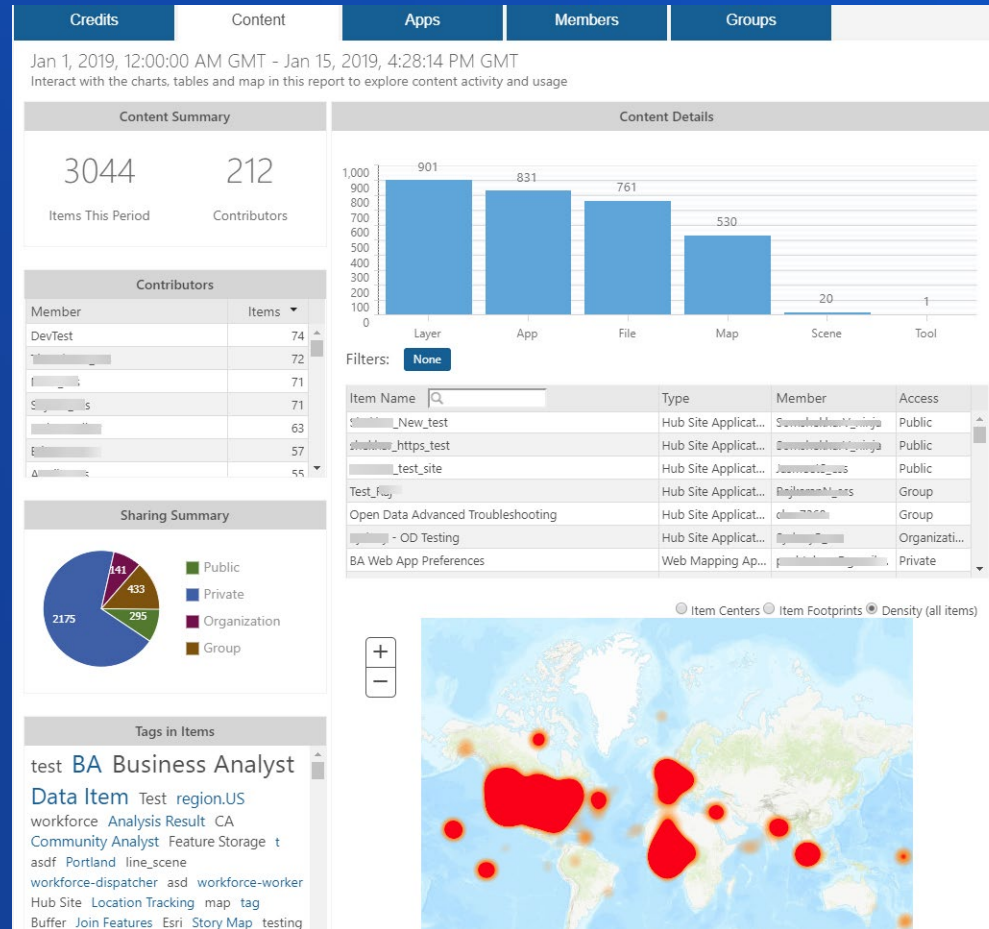
Sharing and Searching



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

Keeping Track of Usage – Status Dashboard

- Credits
- Content
- Apps
- Members
- Groups



Keeping Track of Usage – Activity Log

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

The screenshot shows a software interface with a 'Download activity log' button highlighted in yellow. Below it, a modal dialog box is open, titled 'Download activity log'. The dialog contains the following information:

- Subscription ID:** 5725037879
- Feature:** Standard
- System Health:** All systems OK
- Created:** Jul 18, 2011
- Renewal Date:** Aug 2, 2011

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

Configuration options in the dialog:

- Start date:** 1/15/2019
- Start time:** 12:00 AM
- Maximum number of events:** 100

At the bottom right, there are two buttons: 'Download CSV' and 'Cancel'.

Keeping Track of Usage – Activity Log

Activity Log Example

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	id	idType	orgId	owner	actor	ip	action	created	created_utc	request	reqId	clientId	data						
1		u	WI7Y1m9			198.1	login	1546318814111	1/1/2019 5:00	/sharing/rest/oauth2/token	1c47a745646f4b09b73588	arcgisprodesktop							
2		u	WI7Y1m9			198.1	login	1546318823182	1/1/2019 5:00	/sharing/rest/generateToken	98813591834540c0a51fe3	ref.http://www.arcgis.com							
3	1	i	WI7Y1m			198.1	add	1546318835306	1/1/2019 5:00	/sharing/rest/portals/self/collaborations/6f6e43014379efc4391ab04811f67963c54			{"name": "462beeb8-8f5f-4de9-a3e8-12ac9bb18566.crpK"}						
4	1	i	WI7Y1m			198.1	update	1546318836441	1/1/2019 5:00	/sharing/rest/portals/self/collaborations/6f6e43014379efc4391ab04811f67963c54	ded006c5d37141eab37b785648d1b595		{}						
5	1	i	WI7Y1m			198.1	delete	1546318836573	1/1/2019 5:00	/sharing/rest/portals/self/collaborations/6f6e43014379efc4391ab04811f67963c54	ded006c5d37141eab37b785648d1b595								
6		u	WI7Y1m9			198.1	login	1546318844809	1/1/2019 5:00	/sharing/oauth2/token	775dbaaa946b4732a6e2c	arcgisprodesktop							
7		u	WI7Y1m9			198.1	login	1546318883084	1/1/2019 5:01	/sharing/rest/oauth2/token	e84901650b224843a000e1	arcgisprodesktop							
8	s	u	WI7Y1m9		sha	198.1	login	1546318884280	1/1/2019 5:01	/sharing/rest/oauth2/token	c8f258ab762047ec96499a	arcgisprodesktop							
9		u	WI7Y1m9			198.1	login	1546318909201	1/1/2019 5:01	/sharing/rest/oauth2/token	75ea048523d244cba8679f	arcgisprodesktop							
10		u	WI7Y1m9			198.1	login	1546318911806	1/1/2019 5:01	/sharing/rest/oauth2/token	0c4344ae46a34adbb373f	arcgisprodesktop							
11	ke	u	WI7Y1m9		N	198.1	login	1546318912175	1/1/2019 5:01	/sharing/rest/oauth2/token	c559e94e791c473b9347ef	arcgisprodesktop							
12	ss	u	WI7Y1m9		S	198.1	login	1546318922605	1/1/2019 5:02	/sharing/rest/oauth2/token	28e802ac80504432a89a2e	arcgisprodesktop							
13		u	WI7Y1m9			198.1	login	1546318928810	1/1/2019 5:02	/sharing/rest/oauth2/token	3c2e550f50a340be817d50	arcgisprodesktop							
14		u	WI7Y1m9			198.1	login	1546318947471	1/1/2019 5:02	/sharing/rest/oauth2/token	c5f8da08875e404b857148	arcgisprodesktop							
15		u	WI7Y1m9			198.1	login	1546319018444	1/1/2019 5:03	/sharing/rest/oauth2/token	f452ac8c9978458491cd4d	arcgisprodesktop							
16		u	WI7Y1m9			198.1	login	1546319028396	1/1/2019 5:03	/sharing/rest/oauth2/token	50fa0f678ce04248aa80c3	arcgisprodesktop							
17	oc	cp	WI7Y1m9			198.1	update	1546319037463	1/1/2019 5:03	/sharing/rest/portals/self/collaborations/2219275c50ee6024146b3a8ae770fbabdf			{"portalId": "8bd218ff-7966-42fa-a87f-cdaec47a178", "role": "Guest", "status": "Active"}						
18	7	i	WI7Y1m			198.1	add	1546319053392	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/22182041a8a17c546e48504c28f3e7e08c6			{"name": "b3ca94ec-211a-44cc-a758-1651a77ea8a7.crpK"}						
19	7	i	WI7Y1m			198.1	update	1546319055641	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/2219e9f5d67dffb44d9b10577a311c70da7			{}						
20	7	i	WI7Y1m			198.1	delete	1546319055739	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/2219e9f5d67dffb44d9b10577a311c70da7									
21	9	i	WI7Y1m			198.1	add	1546319077690	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221acc827b3c34e42c28ab04bc8c6585144			{"name": "46c1ca9d-d2de-4363-a1aa-ae09cd1513ae.crpK"}						
22	b	i	WI7Y1m			198.1	update	1546319079507	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221b597a0249734401088d2cf1b3ab7e36f									
23	b	i	WI7Y1m			198.1	update	1546319079584	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221b597a0249734401088d2cf1b3ab7e36f									
24	b	i	WI7Y1m			198.1	update	1546319080313	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221b597a0249734401088d2cf1b3ab7e36f			{}						
25	9	i	WI7Y1m			198.1	delete	1546319080519	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221b597a0249734401088d2cf1b3ab7e36f									
26	9	i	WI7Y1m			198.1	delete	1546319080519	1/1/2019 5:04	/sharing/rest/portals/self/collaborations/221b597a0249734401088d2cf1b3ab7e36f									
27		u	WI7Y1m9			198.1	login	1546319096183	1/1/2019 5:04	/sharing/generateToken	0b56e228b2c24175a4d19	ref.http://www.arcgis.com							
28		u	WI7Y1m9			198.1	login	1546319125446	1/1/2019 5:05	/sharing/oauth2/token	88fff571a3f64ea59a0c7ce	drone2map							
29		u	WI7Y1m9			203.1	login	1546319136761	1/1/2019 5:05	/sharing/rest/oauth2/token	4e64fd0cf3ca485e97b6a7	arcgisprodesktop							
30		u	WI7Y1m9			198.1	login	1546319185690	1/1/2019 5:06	/sharing/rest/oauth2/token	7509bce05c794d5a9f707c	arcgisprodesktop							

Recommendations

- **Setup Admin Contacts**
- **Use MFA or your own IDP**
- **Don't share Editable Feature Layers to Everyone and Use Views**
- **Setup Custom Roles and restrict full Admins**

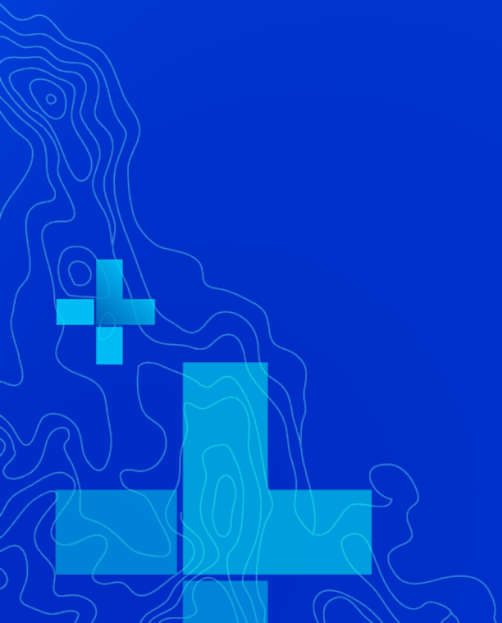
- **Older Organizations**
 - **HTTPS Only**
 - **Standardized Queries Only**

- **Private Organizations**
 - **Disable Public Sharing**
 - **Disable Anonymous Org Access**



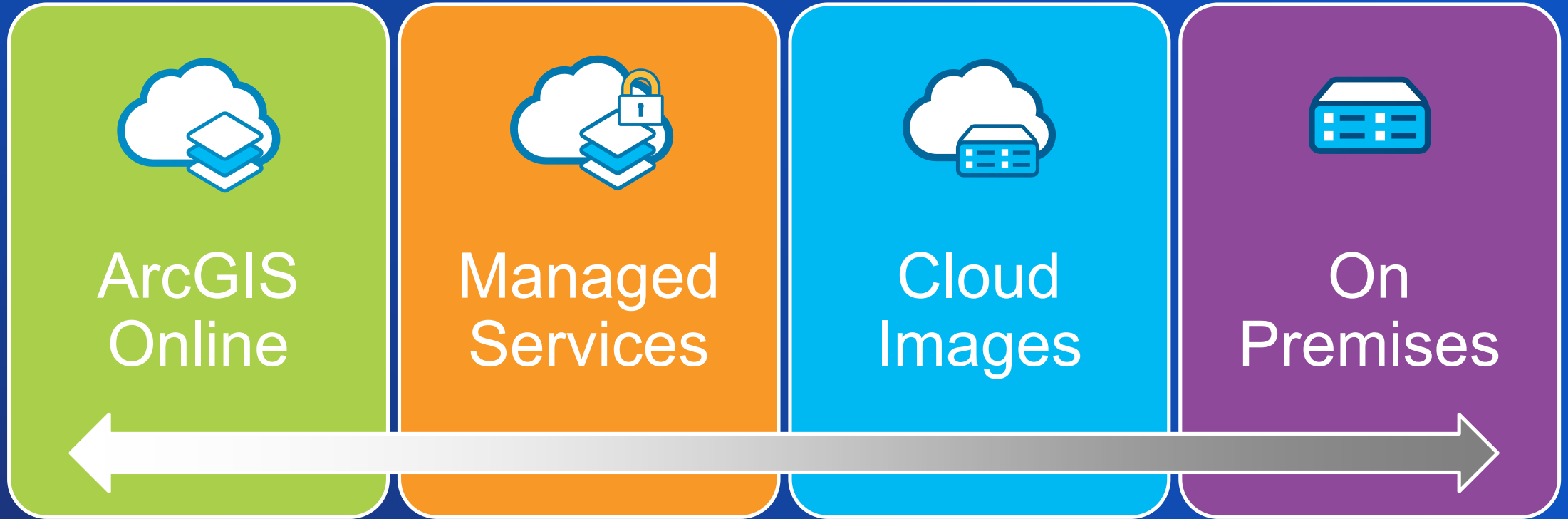
Deployment Architecture

Michael Young



Deployment Architecture

Options



Deployment Architecture

Responsibility

Responsibility	ArcGIS On-Premises	ArcGIS Cloud Images	EMCS Advanced+ <i>FedRAMP Moderate</i>	ArcGIS Online <i>FedRAMP Tailored Low</i>
Data Classification & Accountability	Customer Managed	Customer Managed	Customer Managed	Customer Managed
Client & End-Point Protection	Customer Managed	Customer Managed	Esri Managed	Esri Managed
Identity and Access Management	Customer Managed	Customer Managed	Shared (Customer/Esri)	Shared (Customer/Esri)
Application Level Controls	Customer Managed	Customer Managed	Shared (Customer/Esri)	Shared (Customer/Esri)
Network Controls	Customer Managed	Customer Managed	Shared (Customer/Esri)	Shared (Customer/Esri)
Physical Security	Customer Managed	Cloud Provider Managed	Cloud Provider Managed	Cloud Provider Managed

Customer Managed



Cloud Provider Managed

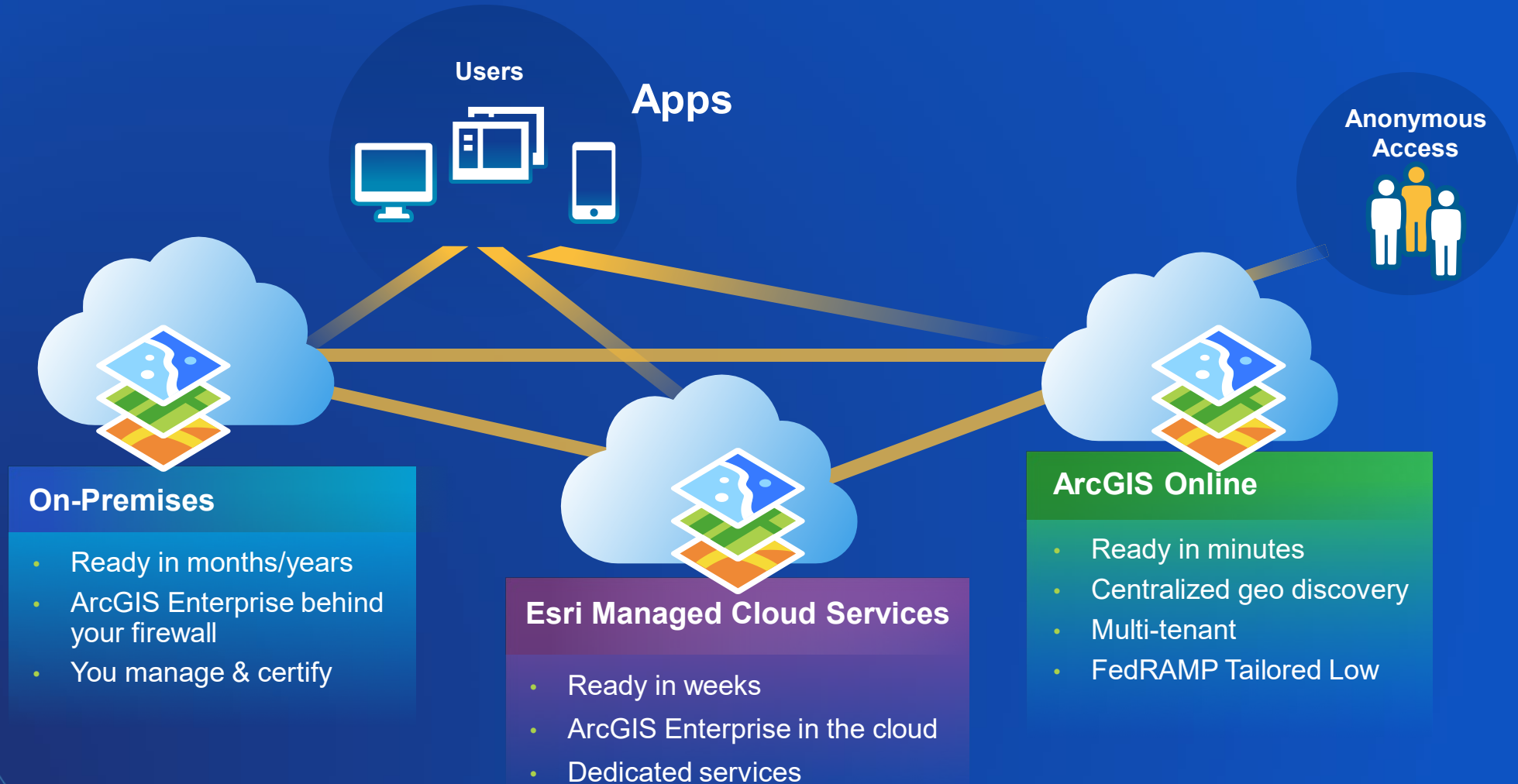


Esri Managed



Deployment Architecture

Hosting Options



... 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.

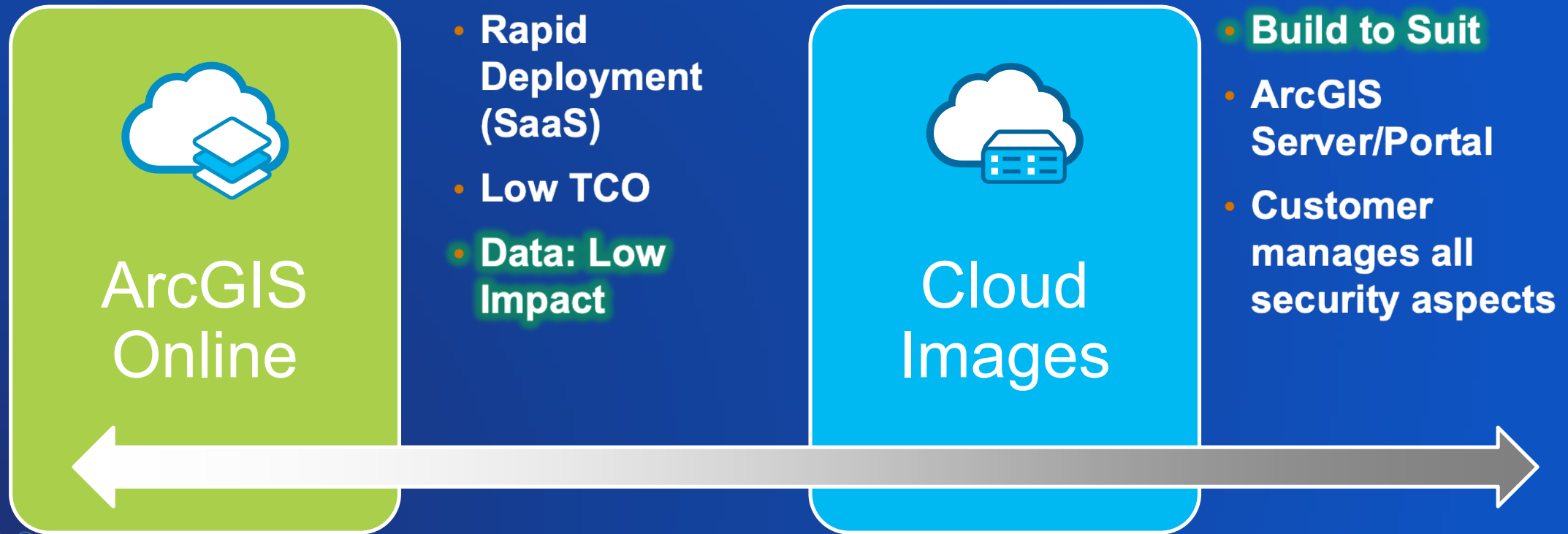


- Rapid Deployment (SaaS)
- Low TCO
- Utilize content / Basemaps
- **Data: Low Impact**

Deployment Architecture

User Scenario – ArcGIS Online + Cloud Images

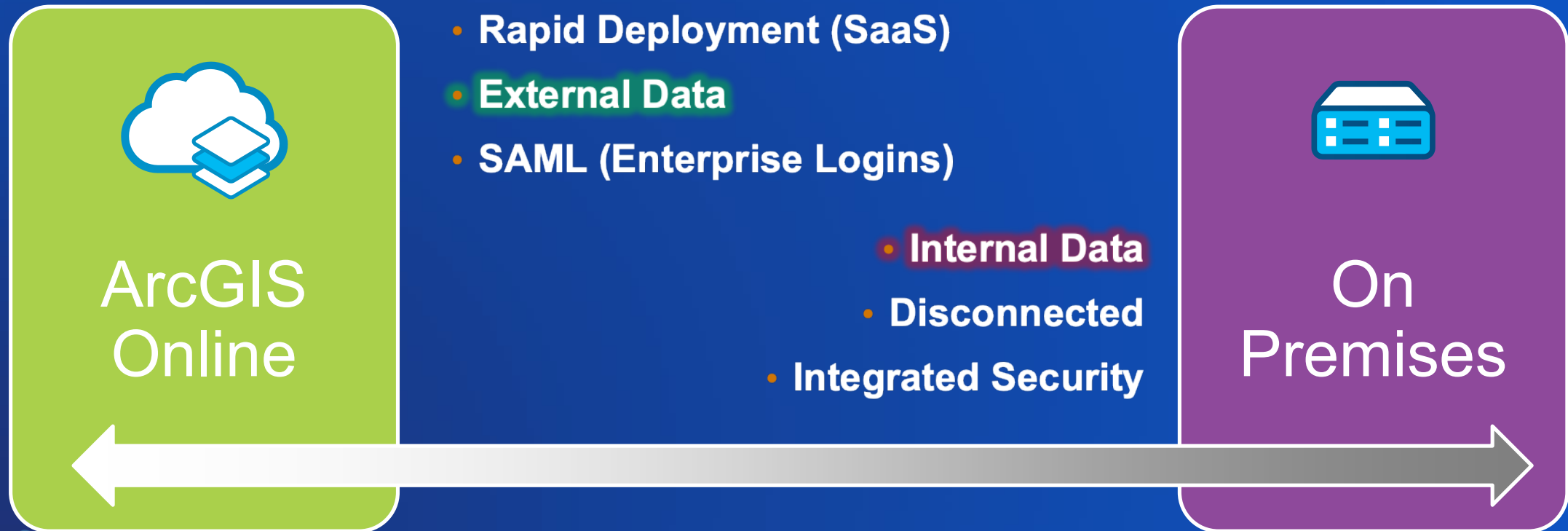
I need to pilot a solution that requires basemaps and some ArcGIS Server specific features.



Deployment Architecture

User Scenario – ArcGIS Online + On-Premises

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



Example: EPA's FISMA Authorized GeoPlatform

Deployment Architecture

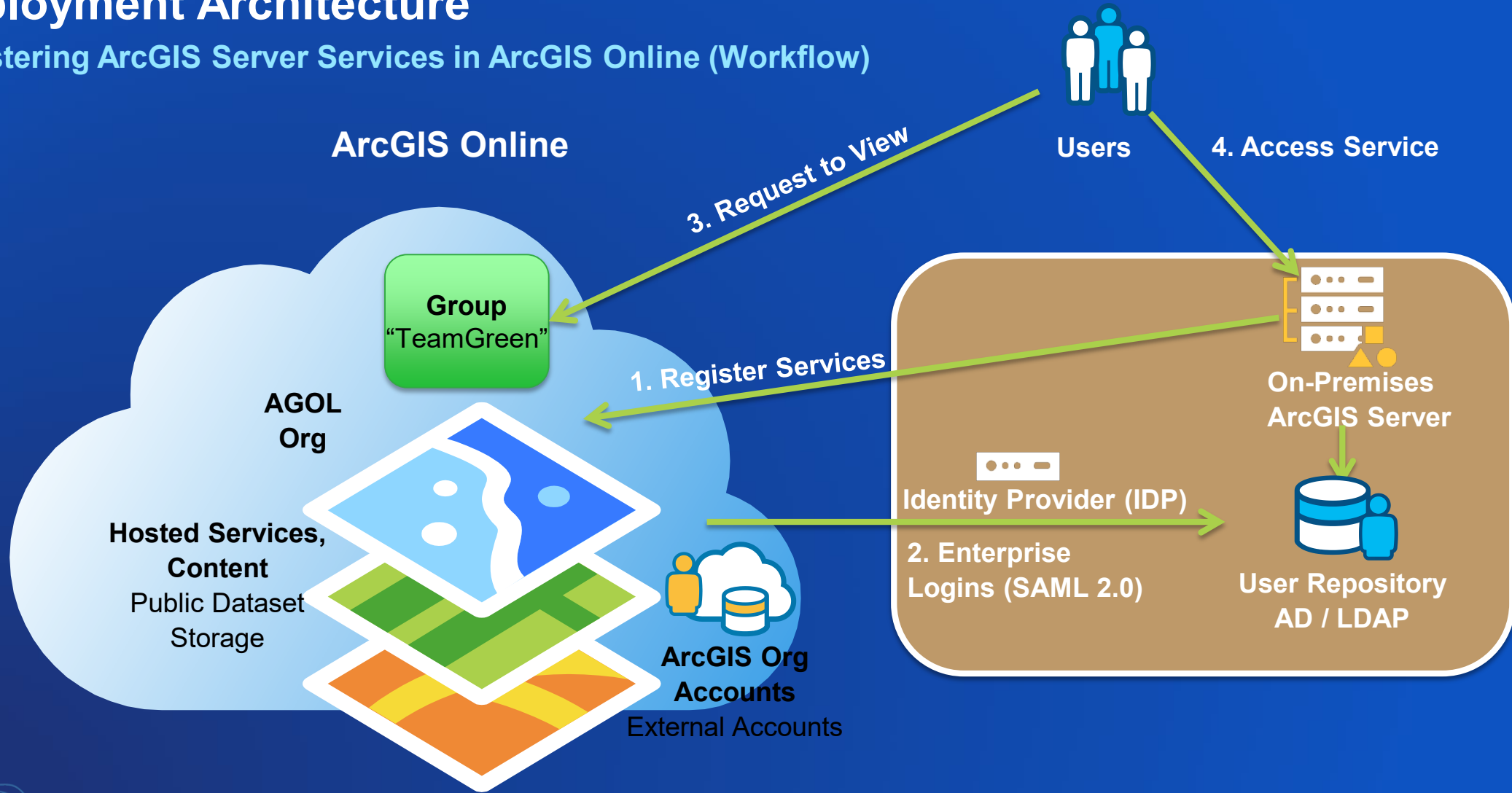
Registering ArcGIS Server Services in ArcGIS Online

- **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)



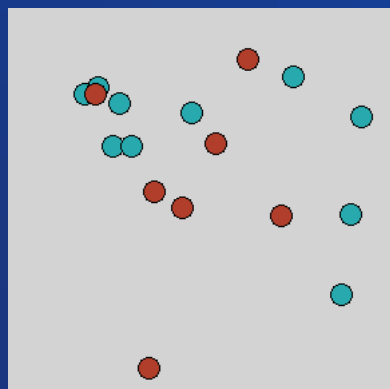
Segment sensitive data internally and public data in cloud

Deployment Architecture

Registering ArcGIS Server Services in ArcGIS Online

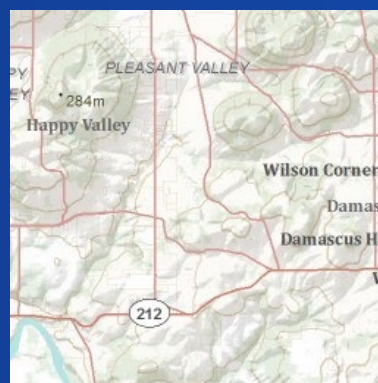
- Where are internal and cloud datasets combined?
 - At the browser
 - The browser makes separate requests for information to multiple sources and does a “mash-up”
 - Token security with TLS or even a VPN connection could be used between the device browser and on-premises system

On-Premises Operational
Layer Service



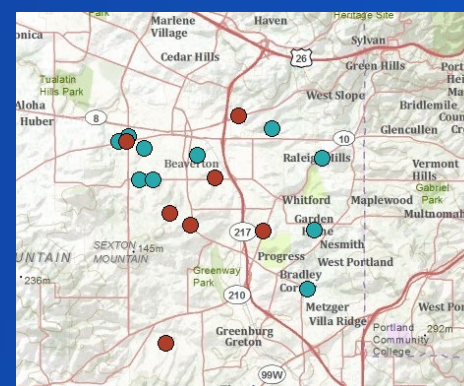
<https://YourServer.com/arcgis/rest...>

Cloud Basemap Service
ArcGIS Online



<https://services.arcgisonline.com...>

Browser Combines Layers

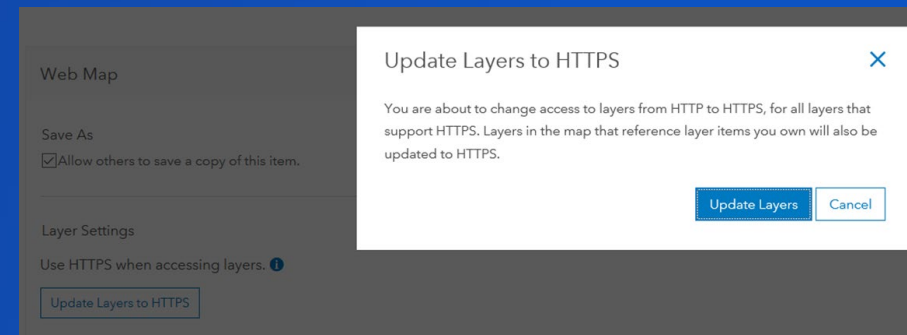


Deployment Architecture

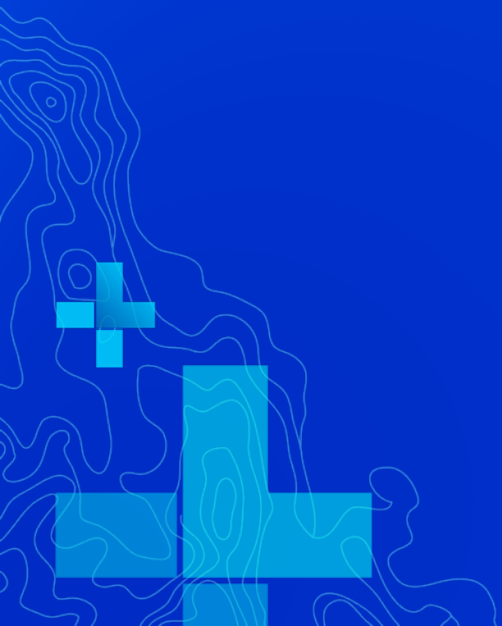
Significant Security Change Coming



- **TLS 1.2 only was enforced in 2019**
- ***In 2020 all ArcGIS Online organizations will have HTTPS only enforced***
 - Allows utilizing HSTS across domain, as opposed to specific services
- **Customers utilizing HTTP only services with ArcGIS Online and external HTTP services need to begin preparing now**
 - Maps/services/apps with HTTP calls will break and need to be fixed
 - Capabilities to make the transition easier
 - Update Map Layers to HTTPS
 - HTTP Checker added to AGO Security Advisor tool



Compliance



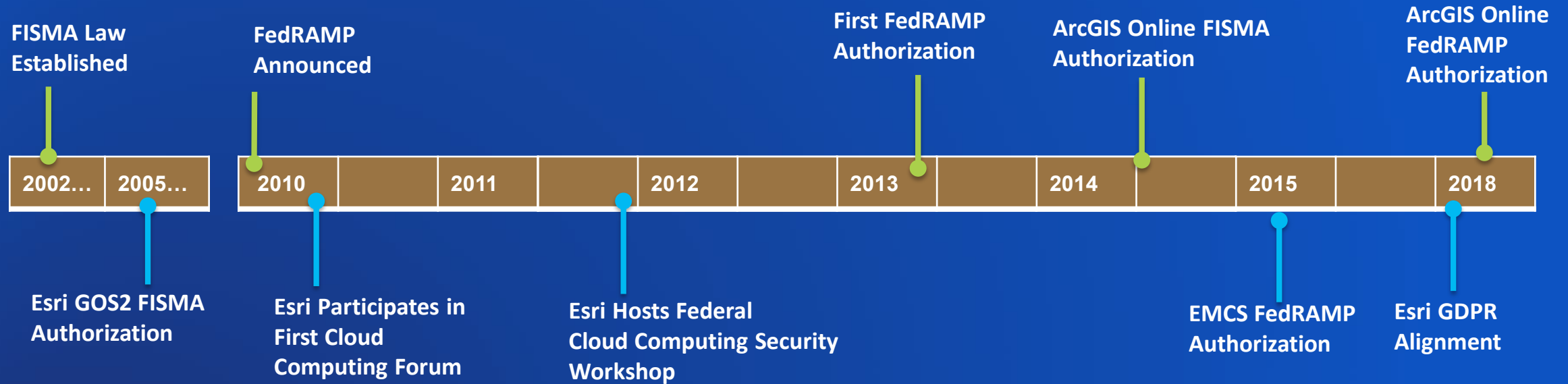
Compliance

- **Milestones**
- **Cloud Infrastructure Providers**
- **Privacy Assurance / GDPR**
- **Security Assurance / FedRAMP**



Compliance

Milestones



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



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)**
 - Stronger privacy assurance
- **California Consumer Privacy Act (CCPA)**
 - Currently working on ensuring alignment by enforcement 1/1/2020



Compliance

Protect By Design

- Esri established a formal Security Development Lifecycle 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 now encrypted at rest



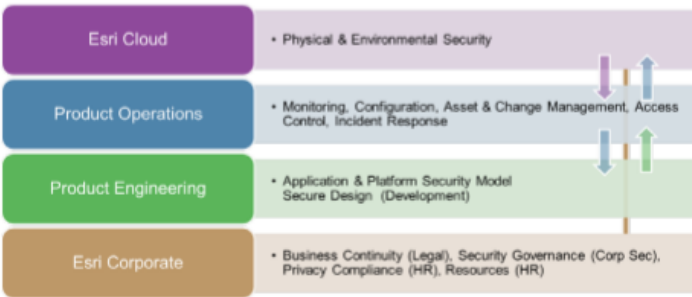
Esri Software Security and Privacy

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.



Functional Area	Security Responsibilities
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 Agency FedRAMP Tailored Low authorization-to-operate (ATO)**
 - Referred to as a Low-Impact Software as a Service (Li-SaaS)
 - Standardizes US government security authorization process for cloud products and services
- **Value to All Organizations**
 - Recognized by many organizations around the globe as a gold standard for security
 - Mapping of ISO 27001 & 15408 controls available via Trust Center
 - Ensures annual 3rd party assessments

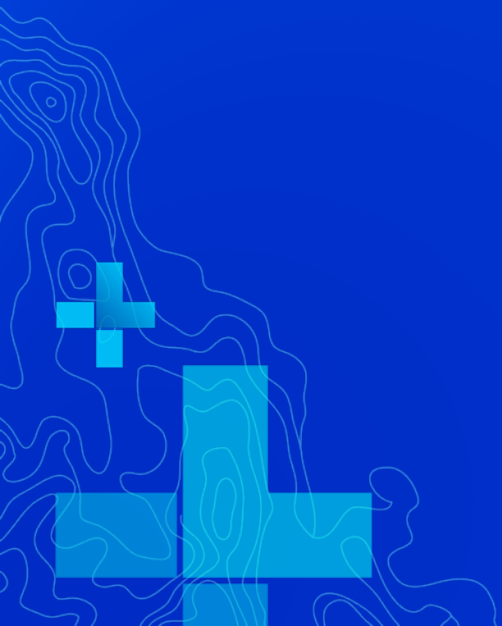


Compliance

Summary Across ArcGIS Online



Security Advisor Tool

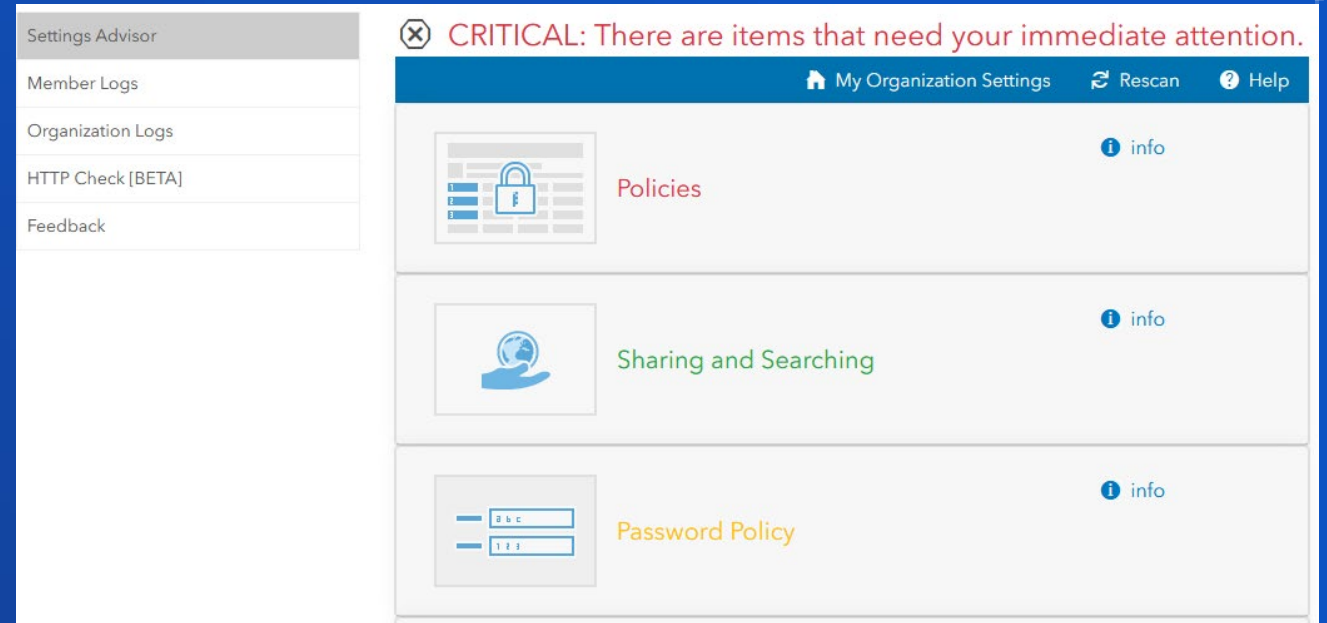
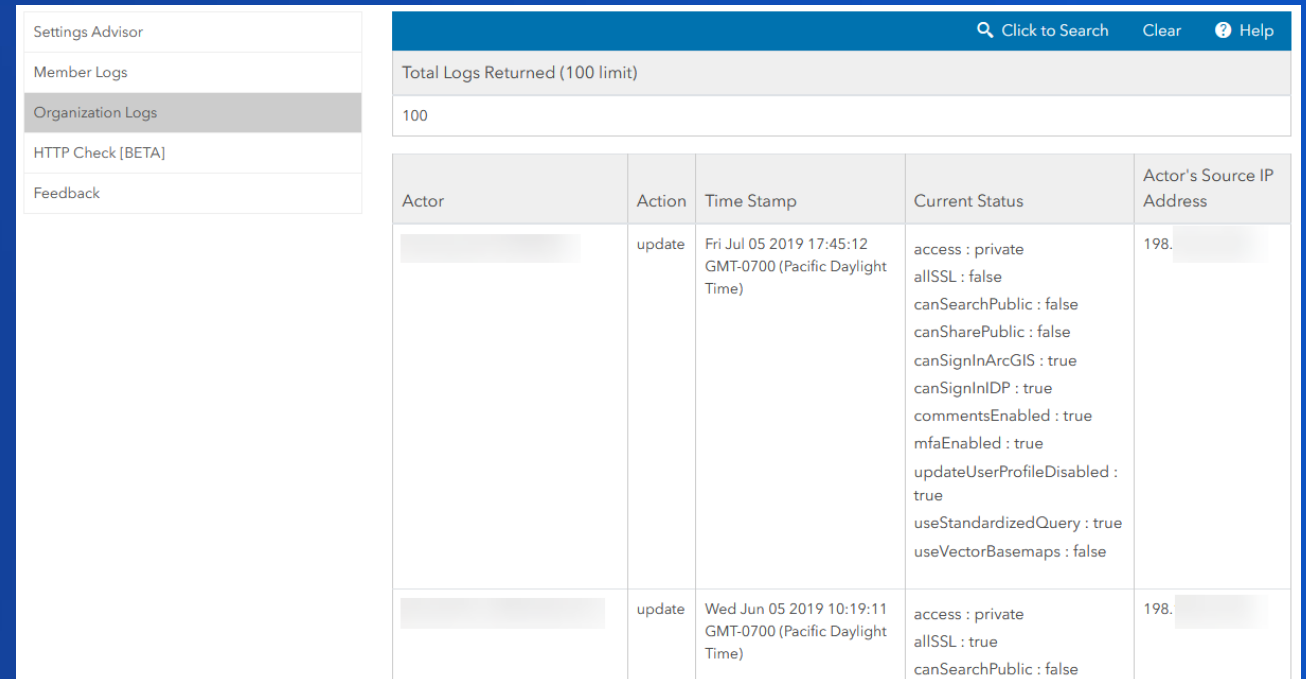


AGO Security Advisor Tool

- Launch from ArcGIS Trust Center



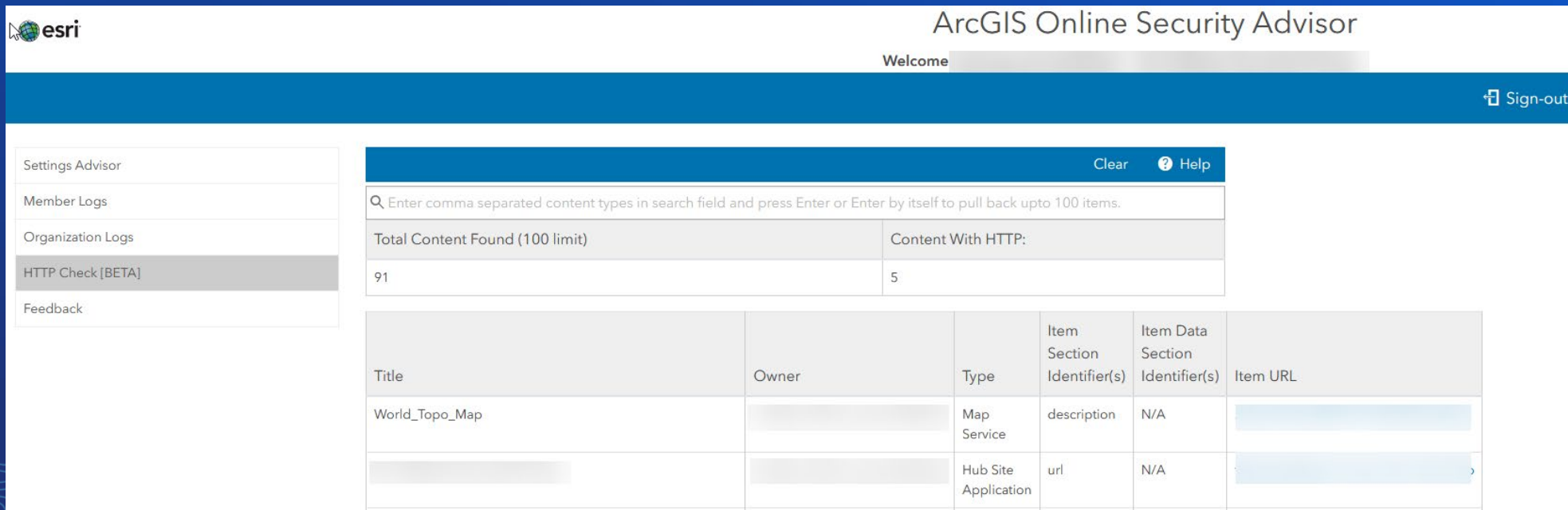
- Validate settings/usage against secure best practices
- GUI for organization & user level audit log visualization
 - SoftwareSecurity@Esri.com

A screenshot of the Security Advisor dashboard. On the left is a sidebar menu with items: Settings Advisor, Member Logs, Organization Logs, HTTP Check [BETA], and Feedback. The main content area has a red banner at the top that says "CRITICAL: There are items that need your immediate attention." Below the banner are three cards: "Policies" (with a padlock icon), "Sharing and Searching" (with a globe icon), and "Password Policy" (with a password field icon). Each card has an "info" link.A screenshot of the Security Advisor audit log. The sidebar menu is the same as in the previous screenshot, but "Organization Logs" is selected. The main content area shows a search bar with "Click to Search", "Clear", and "Help" buttons. Below the search bar, it says "Total Logs Returned (100 limit)" and "100". A table displays the log entries with columns: Actor, Action, Time Stamp, Current Status, and Actor's Source IP Address.

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

- **Version 2.0 released this week - New HTTP Checker feature**
 - Helps ease HTTPS enforcement in 2020 for customers with HTTP still enabled
 - Flags any HTTP references within your org



The screenshot displays the ArcGIS Online Security Advisor interface. The top navigation bar includes the Esri logo, the title "ArcGIS Online Security Advisor", a "Welcome" message, and a "Sign-out" button. A left-hand sidebar contains navigation options: "Settings Advisor", "Member Logs", "Organization Logs", "HTTP Check [BETA]" (which is highlighted), and "Feedback". The main content area features a search bar with a "Clear" and "Help" button. Below the search bar, a summary table shows search results:

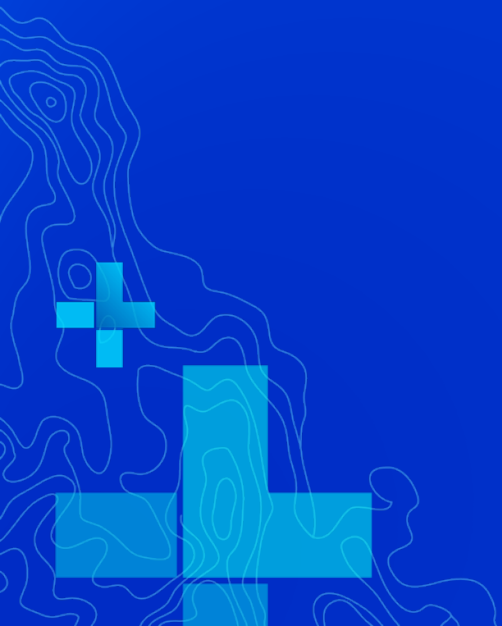
Total Content Found (100 limit)	Content With HTTP:
91	5

Below the summary table is a detailed table of content items with the following columns: Title, Owner, Type, Item Section Identifier(s), Item Data Section Identifier(s), and Item URL.

Title	Owner	Type	Item Section Identifier(s)	Item Data Section Identifier(s)	Item URL
World_Topo_Map		Map Service	description	N/A	
		Hub Site Application	url	N/A	

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

Summary



Summary

- **FedRAMP Tailored Low authorization and GDPR 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](https://trust.arcgis.com)**
 - **In-depth Cloud Security Alliance (CSA) answers readily available**
 - **Security best practice validation tool**



Summary

Want to learn more?

ArcGIS Trust Center

Overview

Security

Privacy

Compliance

Documents

Launch Security Advisor

Search ArcGIS Trust Center



Security / Cloud

Overview

Cloud

Cloud options

ArcGIS Online capabilities

ArcGIS Online guidance

Esri Managed Cloud Services

Enterprise

Desktop

Mobile

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.

In this topic

[Report a Security Concern](#)

[Application security settings](#)

[Authentication](#)

[Authorization](#)

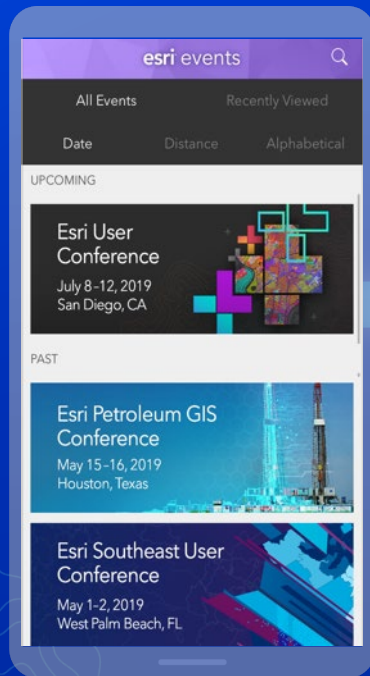
[Encryption](#)

[Logging and Auditing](#)

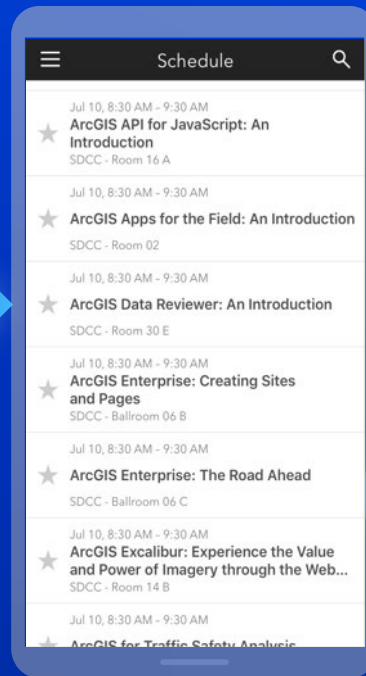
[Related content](#)

Please Share Your Feedback in the App

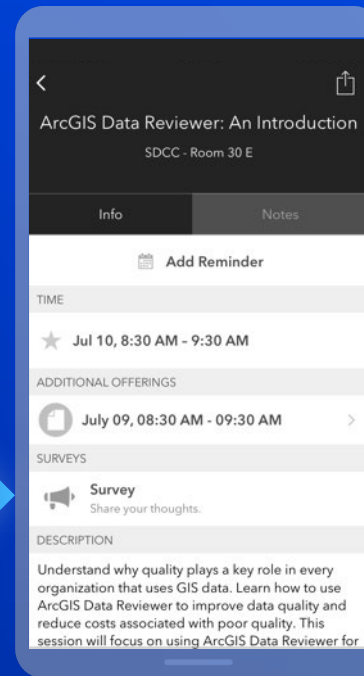
Download the Esri Events app and find your event



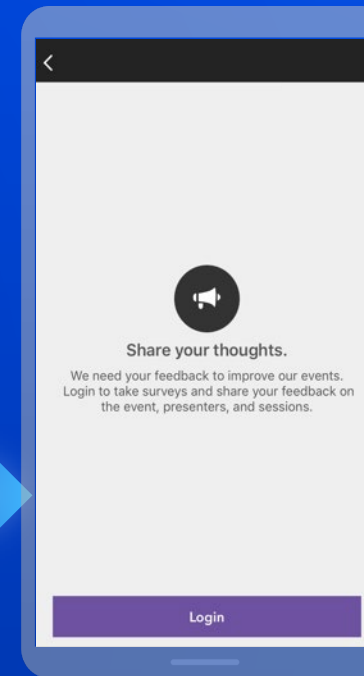
Select the session you attended



Scroll down to "Survey"



Log in to access the survey



Complete the survey and select "Submit"

