ArcGIS Online – A Multi-Tenant System
• Platform Security
• Deployment Architecture
• Compliance (FedRAMP/GDPR & more)
• New Security Advisor Tool
Platform Security
Andrea Rosso
Portal Information Model

Portal

Groups

Items

Members
• Your Organization
• Custom Url (yoururl.maps.arcgis.com)
• Public or Private
• All Organization Settings
Items

- **Typed**
  - 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
- Discoverable
  - No one
  - Organization
  - Everyone
- Members have a Role


Roles

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

• **Specialized Groups**
  - All members can update included items

• **Restrictions**
  - Can only be created by Admins
  - Items and Members must be in Org
  - Capability cannot be toggled

• **Use Cases**
  - Shift Operators
  - Collaborative Editing
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
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
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 Policies

- Default Password Policy
  - 8 characters with at least 1 number
- Can Customize
  - Complexity
  - History
  - Expiration
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 now supported
- One SAML IDP or SAML Federation
Application Trust Boundaries

ArcGIS Online

Esri Apps
- Geonet
- Training
- My Esri
- .....  

Trusted Apps:
- App Launcher Apps
- Marketplace Apps

Other Third Party Apps

Esri Access

Login
Admin Organization Controls

- Use only HTTPS (HSTS)
- Disable Sharing to Everyone
- Purchasers
- Admin Contacts
- Disable Bio
Administrator Controls on Members

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

• Status Reports
  - Credits
  - Content
  - Members
  - Groups
Recommendations

- HTTPS Only
- Standardized Queries Only
- Setup Admin Contacts
- MFA or your own IDP
- Don’t make Editable Feature Layers Public and Use Views
- Setup Custom Roles and restrict full Admins

- Private Orgs
  - Disable Public Sharing
  - Disable Anonymous Org Access
Deployment Architecture

Hosting Options

On-Premises
- Ready in months/years
- Behind your firewall
- You manage & certify

Esri Managed Cloud Services
- Ready in weeks
- ArcGIS Enterprise in the cloud
- Dedicated services
- Advanced Plus FedRAMP Moderate

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

Anonymous Access

... All options can be combined or separate
I want to share and process operational data with field workers.

- Rapid Deployment (SaaS)
- Low TCO
- Utilize content / Basemaps
- Data: Low Impact
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**
I want to share sensitive data internally, but provide subsets to external and public users.

**Deployment Architecture**

**User Scenario – ArcGIS Online + On-Premises**

- Rapid Deployment (SaaS)
- External Data
- SAML (Enterprise Logins)
- Internal Data
- Disconnected
- Integrated Security

**Example:** EPA’s FISMA Authorized GeoPlatform
Deployment Architecture
Registering ArcGIS Server Services in ArcGIS Online (Workflow)

ArcGIS Online

Group "TeamGreen"

AGOL Org

Hosted Services, Content
Public Dataset
Storage

ArcGIS Org Accounts
External Accounts

On-Premises ArcGIS Server
Identity Provider (IDP)
User Repository AD / LDAP

2. Enterprise Logins (SAML 2.0)

3. Request to View

Users

4. Access Service

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
Cloud Basemap Service ArcGIS Online
Browser Combines Layers

https://YourServer.com/arcgis/rest...
https://services.arcgisonline.com...
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 businesses
  - 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 Security Changes Coming

- Transport security improvement roadmap established

- *Will disrupt a number of customer’s operations* if not tested/validated ahead of transition

- Broad announcement forthcoming

- First major change is disabling TLS 1.0 & 1.1 (In alignment with PCI & FedRAMP standards)
  - Planned for December 2018 release
  - Check out our TLS guide to understand compatibility with product versions (Trust Center)
Deployment Architecture

Significant Security Changes Coming (con’t)

- Second major change is disabling HTTP for all Organizations
  - Planned for September 2019 release
  - Eliminating HTTP allows utilizing HSTS across our domain, as opposed to just specific services as currently implemented
  - Maps/services/apps with HTTP calls will break and need to be fixed
  - We’ve been adding capabilities to make the transition easier
    - Update Map Layers to HTTPS
Compliance
Compliance

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

• Product Based Initiatives
  - ArcGIS Server 10.3+ - DISA STIG
  - ArcGIS Desktop 10.1+ - USGCB
  - ArcGIS Pro 1.4.1+ - USGCB

• Service Based Initiatives
  - EMCS Advanced Plus (Single-tenant) – FedRAMP Moderate
  - ArcGIS Online (Multi-tenant) – FedRAMP Tailored Low - NEW!
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) *NEW*
Compliance

GDPR / Privacy

Esri supports GDPR and continues to advance our privacy & security practices
Compliance
GDPR - Personal Data within Online Services

• **Who owns the data**
  - The customer

• **Who is responsible for categorizing datasets?**
  - The customer

• **Are there any restrictions for processing personal dataset types?**
  - Esri recommends customers not store Sensitive Personal Data unless encrypted or pseudonymized before posting for storage – Such as with a security gateway

• **What laws govern my data?**
  - Government entities – Applicable laws of customer’s jurisdiction
  - Non-government entities – US federal law & State of California law

• **Where is my data?**
  - Online service data is stored within the United States and “adequate data privacy safeguards are in place” assured through our Privacy Shield compliance
Compliance

GDPR - Privacy Impact Assessment (PIA)

• Esri has been performing PIA’s since the early 2000’s for Online services
  - ArcGIS GDPR/Privacy Best Practices whitepaper to be released soon to help guide customers
  - We welcome assisting customers with their PIA’s as necessary

• Supplementary privacy statement created specifically for our Products & Services
  - Privacy Collection & storage of privacy information is minimized in our products
  - Online Telemetry service (EUEI) disabled by default for organizations outside the US

• Company-wide privacy improvements
  - Tracking cookies can now be disabled centrally across Esri.com & ArcGIS.com
  - When Esri is Controller of customer PI, requests handled through Privacy@esri.com
Compliance
GDPR - Cookies

• Marketing focused tracking cookies are not used across paid-for ArcGIS Online services no matter what the centralized cookie setting is
Compliance
GDPR - Protect By Design

- Esri established a formal Security Development Lifecycle in 2017
- Addresses governance structure (CISO – Products, CISO – Corporate)
- Guidelines practices based on BSIMM, OWASP, CWE/SANS
- Most rigorous security measures starting 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
- Customer datasets written/updated after March 10th, 2018 are encrypted at rest
  - Pre-existing datasets to be encrypted by end of 2018
Compliance
GDPR - Data Breach Notification

• Esri notifies customers within 72hrs of confirming their data has been breached

• Customers may report concerns directly to our PSIRT team through our Trust Center

• Support for Restriction of Processing for legal holds or otherwise
  - Online records can be identified, exported, and deleted by the customer
  - Customer org admin can disable user access or call our support team to temporarily disable org
Compliance
GDPR - Consent

• Contracts
  - Data Processing Addendum (DPA) pre-signed by Esri, ready for customers to sign and available within the Trust Center documents

• Forms
  - Forms asking for private information now require consent / awareness of privacy statement

• Cookies
  - Pages with marketing related tracking have cookie consent banners
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)

• 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

• Value to Global Organizations
  - Recognized by many organizations around the globe as a gold standard for security
  - Mapping of ISO 27001 & 15408 controls is readily available via the Trust Center
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
Compliance
Summary Across ArcGIS Online

Privacy
- TRUSTe
- GDPR
- Privacy Shield

Security
- FISMA
- FedRAMP

Answers
- cloud
- security
- alliance®
New Security Advisor Tool
Michael Young
Compliance

New AGO Advisor Tool

• Validates your org settings/usage against secure best practices

• Provides organization & user level audit log visualization

• Tool now available as Preview
  - https://arcg.is/ago-advisor

• Value immediately proven
  - Already used by customer to quickly check 8 orgs and prepare for Anonymous Hacktivist Threat
Compliance

New AGO Advisor Tool

- Considering enhancements based on user input
  - Discovery of embedded HTTP links within Services/Apps
    - To help ease HTTPS transition
  - Summarize all publicly editable services
    - This is the most common way organizations accidently leak data
  - More extensive audit log display configuration
  - Support multiple Advisor scanning policies
    - GDPR, FedRAMP, General best practices, custom
  - Validate Portal for ArcGIS deployments
  - Report generation / export capability

- The Software Security & Privacy team welcomes your ideas
  - SoftwareSecurity@Esri.com
Summary

• New 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
  - Read the TLS Guide now – Much more info to come

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

- Allow only standard SQL queries.
  - Enforce parametrized queries by default to reduce the likelihood of SQL injection vulnerabilities
  - Aligns in aligning with OWASP security industry best practices
- Do not allow anonymous access to your organization unless required
- Do not allow members to share content outside the organization unless required
- For more information, see Configure security settings in the ArcGIS Online Help.
Please Take Our Survey on the App

1. Download the Esri Events app and find your event
2. Select the session you attended
3. Scroll down to find the feedback section
4. Complete answers and select “Submit”

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