ArcGIS Online: A Security, Privacy & Compliance Overview

Andrea Rosso – Lead Architect
Michael Young – CISO Products
ArcGIS Online – A Multi-Tenant System
Agenda

- Platform Security
- Deployment Architecture
- Compliance
Platform Security
Andrea Rosso
Portal Information Model

Portal

Groups

Items

Users
- Your Organization
- Custom URL (yoururl.maps.arcgis.com)
- Public or Private
Items

- Typed
  - Web Map
  - Services
  - Data
  - ...

- Private by default

- Can Share to
  - Groups
  - Organization
  - Everyone/Public
Users

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

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

- Contain Items and Users
- Users 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 Users must be within 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

• Custom Roles can have Edit or Edit with full control privileges
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 Account

Social Account

Enterprise Account
Enterprise Identities

• 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 Online identities with Enterprise Identities
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
- Users setup their own Multi-factor
Password Policies

• Default Password Policy
  - 8 characters with at least 1 number

• Can Customize
  - Complexity
  - History
  - Expiration
Admin Organization Controls

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

- Trusted Servers
- Allow Portal Access
- Allow Origins
Administrator Controls on Users

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

• Status Reports
  - Credits
  - Content
  - Members
  - Groups
Deployment Architecture
Michael Young
Deployment Architecture

Responsibility

**On-premises**
- ArcGIS Server
- OS/DB/Network
- Security Infrastructure
- Virtual / Physical Servers

**Cloud Images**
- ArcGIS Server
- OS/DB/Network
- Cloud Infrastructure (IaaS)

**Managed Services**
- ArcGIS Server
- OS/DB/Network
- Cloud Infrastructure (IaaS)

**ArcGIS Online**
- ArcGIS Online
- OS/DB/Network
- Cloud Infrastructure (IaaS)

**FedRAMP Moderate**
- Security Infrastructure by default

**FISMA Low**
- Security Infrastructure

---

**Customer Responsibility**

**Esri Responsibility**

**CSP Responsibility**
Deployment Architecture

Hosting Options

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

Esri Managed Cloud Services
- Ready in days
- All ArcGIS capabilities at your disposal in the cloud
- Dedicated services
- FedRAMP Moderate

ArcGIS Online
- Ready in minutes
- Centralized geo discovery
- Multi-tenant
- FISMA 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.

ArcGIS Online

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

Cloud Images

- 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.

**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
User Scenario - ArcGIS Online + On-Premises w/Collaboration

- Starting with 10.5.1 Collaboration was enhanced to connect ArcGIS Online with ArcGIS Enterprise
- Allows for a greater flow of data and maps between the two systems
- Search and discover data and maps through a single home system, no matter how it is physically spread out and maintained across different departments within your organization
- Currently provided as part of the early adopter program
Deployment Architecture
ArcGIS Online FISMA Authorized Use Cases

- **Use Case 1 - Public Dissemination**
  - Publish tiles for fast, scalable visualizations
  - Share information with the public
  - Can be used for mashing up services with external non-SSL sites

- **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
Using ArcGIS Online for Public Dissemination

• Pros
  - Variable user loads handled by ArcGIS Online
  - Public information Segmented from Sensitive
  - Internal users have SSO experience w/IWA

• Cons
  - Internal users access ArcGIS Online with separate logins
  - Partners do not have an SSO experience
  - External publishing workflow is needed
Deployment Architecture
Using Both ArcGIS Online & Portal On-Premises

- **Pros**
  - Same scalability and segmentation benefits for public services
  - Portal & Server Federation provide employee SSO

- **Cons**
  - Overhead of internal Portal management / hardware
  - Separate workflows for Portal and ArcGIS Online
  - New ArcGIS Online / Portal collaboration capabilities in 10.5.1 can offset this con
Deployment Architecture

Using Multiple ArcGIS Online Orgs for Segmentation (Private/Public)

• Pros
  - ArcGIS Online operates as a central discovery portal
  - Mobile users / Collector App access ArcGIS Online directly
  - Enterprise logins utilized for employee SSO experience

• Cons
  - Two separate ArcGIS Online orgs to manage
  - Partner logins managed within ArcGIS Online
  - No SSO experience for Partners
Managed Services

Deployment Architecture
User Scenario - ArcGIS Online + Managed Services

I want to share sensitive internal data, but provide subsets to external and public users. I also don’t want to have to manage servers/infrastructure.

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

Example: US Census utilizes Managed Services Adv Plus offering for Public information
Deployment Architecture

Esri Managed Cloud Services

Active/Active Redundant across two Cloud Data Centers

- Web Application Firewall
  - WAF
- ArcGIS for Portal
- ArcGIS Server
- Relational Database
  - Intrusion Detection
    - IDS / SIEM
  - Centralized Management
    - Backup, CM, AV, Patch, Monitor
- File Servers
  - Bastion Gateway
    - MFA
  - Authentication/Authorization
    - LDAP, DNS, PKI
- Cloud Infrastructure
  - Hypervisor, TCP/IP, Network ACLs, Routing, Storage, Hardware

Legend
- Customer
- Application
- Cloud Provider
- Security
Deployment Architecture
Common ArcGIS Online Questions

1. Where is my data?
   - All ArcGIS Online customer data resides within US Data centers on US soil

2. Is my information encrypted?
   - Organization administrator can force TLS encryption for all communications
   - ArcGIS Online does not encrypt customer data at rest

3. Is my data locked into ArcGIS Online?
   - No, customer can download data back to their organization via shapefiles, CSVs, or original publication package

4. How do I know if ArcGIS Online was affected by the latest major Internet vulnerability?
   - Trust.ArcGIS.com announcements
   - Answers to all of the above questions and more available
Compliance

- Milestones
- Esri Corporate
- Cloud Infrastructure Providers
- Products and Services
- Solution Guidance
Esri has actively participated in hosting and advancing secure compliant solutions for over a decade.
Compliance

Corporate

- ISO 27001
  - Esri’s Corporate Security Charter

- Privacy Assurance
  - EU-U.S. Privacy Shield self-certified
    - General Esri Privacy Statement
    - Products & Services Privacy Statement Supplement
  - TRUSTed cloud certified
  - General Data Protection Regulation (GDPR)
    - Active alignment project in place for May 2018 deadline
Compliance
Cloud Infrastructure Providers

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

Cloud Infrastructure Security Compliance
Compliance
Product, Service, Solution

• Product Based Initiatives
  - ArcGIS Server 10.3+ - DISA STIG
  - ArcGIS Desktop 9.3+ - USGCB
  - ArcGIS Pro 1.4.1+ - USGCB

• Service Based Initiatives
  - ArcGIS Online (Multi-tenant) - FISMA Low
  - EMCS Advanced Plus (Single-tenant) - FedRAMP Moderate

• Solution Based Guidance
  - CJIS- Law enforcement - Started
  - HIPAA – Healthcare - Future
Compliance
FedRAMP

- New FedRAMP Tailored Low Authorization Program being released August 2017
- Program targeted for SaaS offerings hosted on FedRAMP authorized cloud infrastructure providers
  - Great fit for ArcGIS Online
  - Advancements made during this authorization include
    - Incorporating cloud-specific security control guidance of FedRAMP beyond FISMA
    - Shifts from NIST 800-53 Rev 3 security controls to Rev 4 (current release)
    - Incorporate ArcGIS Online capabilities from both AWS and MS Azure such as Hosted Feature Services
  - Goal is to complete ArcGIS Online authorization before end of 2017
- Details on new Tailored Low program: https://tailored.fedramp.gov/policy/
Compliance
Summary Across ArcGIS Online

Privacy
- TRUSTe
- Privacy Shield

Compliance
- FISMA Authorization & Accreditation
- FedRAMP

Answers
- cloud security alliance®

Trust.ArcGIS.com
Compliance
Validation Tool

- Checklist validates your org settings/usage against secure best practice recommendations

- Audit log provides a summary of user actions

- Tool in beta form at this time and looking for feedback

- Interested? SecureSoftware@Esri.com
Summary

• ArcGIS Online security capabilities continue to advance

• Utilizes World-Class Cloud Infrastructure Providers

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

• Upcoming ArcGIS Online FedRAMP Tailored Agency Authorization
  - Cross-cloud provider authorization Azure/AWS
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
Please take our Survey
Your feedback allows us to help maintain high standards and to help presenters

Find your event in the Esri Events App

Find the session you want to review

Scroll down to the bottom of the session

Answer survey questions and submit