Understanding ArcGIS for Server Security

Thomas Shippee & Gregory Ponto
Agenda

- **Disclaimer:** Will not cover SAML or OAuth (early beta)
- Understanding role-based security in ArcGIS Server
- Configuring service security using ArcGIS Online
- Leveraging Active Directory for single sign on
Understanding role-based security in ArcGIS Server

Using a default security configuration
Role types determine privileges

GIS service management

- gisAdmin
  Type: Administrator
- gisPub
  Type: Publisher

Access to services

- parkGuide
  Type: User
- parkRanger
  Type: User
Case study: GIS team

User: Alex

gisAdmin

User: Beth

gisPub

Manage Services

Site Admin

Manage Services
Role types determine privileges

Accounts

Primary site administrator (PSA)

Roles

gisAdmin
Administrators

Joe

Sam

gisPub
Publishers

Services

Privileges

gisPub
Publishers

Services
Case study: User team

**parkRanger**
Trails
Restricted Areas

User: Rick

**parkGuide**
Trails

User: Gina
Controlling access to services

Accounts
- Rick
- Gina
- Eric

Roles
- parkRanger
- parkGuide

Permissions
- Service Root
- Secured
- Trails
- Restricted Areas
- Admin
Configuring security using ArcGIS Online

An intuitive security model
ArcGIS Online organization security

Server
- On-premises
- Cloud-based

AGOL Organization

- GIS service links
- Content
- Groups (Security)
- Subscription services (Location analytics)
- Hosted services
AGOL account privileges

Accounts

- Alex
  - Administrator
- Beth
  - Publisher
- Rick
  - User
- Gina
  - User
- Eric
  - User
- Mary
  - User
- Joe
  - Publisher
- John
  - User
- Eric
  - User
- Mary
  - User

Privileges

- Manage users
- Configure site security
- Monitor usage
- etc.

Administer Organization

Publish hosted services

Use shared services

Save/share content

csv, mpk, shp/zip
AGOL sharing options

Groups
- parkGuide
- parkRanger
- World Elevation
- AGOL Organization
- Everyone

Invited users
- Publisher
- Gina
- Rick
- Members of my Organization
- No access restrictions

Shared content
- parkRanger
  - R-Areas
  - Trails
- My Organization
  - Shared services
- Public content
  - Hosted
  - Shared services & content
- Shared content
  - csv, mpk, shp/zip
- My Organization
  - csv, mpk, shp/zip
- Everyone
  - Public content
  - csv, mpk, shp/zip
  - Shared services & content
Security for “hybrid” sharing

AGOL Organization

Pass thru URL

Groups (Security)

Server
On-premises or Cloud-based

Usr: Rick
PW: *****

ParkTrails

proxy

Embedded credential
user: ArcGIS_Online
Leveraging Active Directory for single sign on

Single sign on with an Active Directory security store
Default Security Model

- GIS services
- Web application
- GIS servers
- Web Adaptor
- Enterprise geodatabase
- ArcGIS for Server site
- Built-in security store
- HTTPS
- IDentity manager
- ArcGIS tokens
- LAN
- HTTP
- Service authorization
- GIS tier
- HTTPS
- Web server
- authentication
Active Directory / Single Sign On Model

- Enterprise geodatabase
- GIS services
- ArcGIS for Server site
- GIS servers
- Web Adaptor
  - Web Tier Authentication
  - Web Server
  - HTTPS
- Web application
  - Pass-Through
  - No Code!
- Windows
  - Active Directory
  - HTTP LAN
  - HTTPS
  - Service authorization
  - Pass-Through
  - No Code!
Active Directory / Single Sign On Model

- **ArcGIS Site Configuration**
  - Security Store = Active Directory
  - Web Tier Authentication
  - Assign Roles to Access Services

- **Web Server Configuration**
  - Use Web Adaptor
  - Set “Integrated Windows Authentication” on IIS

- **Application Code**
  - None!
Public Key Infrastructure

With an Active Directory security store
Active Directory / Single Sign On Model + PKI

GIS services

Service authorization

Enterprise geodatabase

ArcGIS for Server site

HTTPS

GIS servers

HTTPS

Web Adaptor

Web Tier Authentication

Web application

Windows

Active Directory

Client Certificate (Soft Cert)
(Smart Card)
(CAC Card)

No Code!
Active Directory / Single Sign On Model + PKI

• ArcGIS Site Configuration
  - Security Store = Active Directory
  - Web Tier Authentication
  - Assign Roles to Access Services

• Web Server Configuration
  - Use Web Adaptor
  - Set “Active Directory Client Certificate Authentication” on IIS
  - Accept client certificates

• Application Code
  - None!
Rate This Session

Your feedback is important

• Quick Link from www.esri.com/devsummit
Questions

• Session ID: 57
• Offering ID: 225

Contact info

• tshippee@esri.com
• gponto@esri.com