



ArcGIS Enterprise Security: Securing Content

Jeff Smith and Scott MacDonald

ESRI USER CONFERENCE

GIS
INSPIRING
WHAT'S
NEXT

Why keep your content secure?

C. I. A.

Confidentiality

- Protect sensitive and secret information from improper access
- Stay aware of who has access to what content

Integrity

- Maintain the authority and consistency of your data and information
- Prevent improper editing or alteration of your content

Availability

- Keep your sites and data continuously operating
- Minimize downtime

This aspect is more covered by our high availability sessions

This morning's talk

- Item security in the ArcGIS Enterprise portal
- The role of groups in your portal
- Securely using ArcGIS Server services
- Layers of security in web maps and apps
- Distributed collaborations for trusted sharing
- Custom roles and fine-grained privileges
- Crafting your access and authentication policies

Best practices and **decision points**





Securing portal items



Stay secure while sharing items

- 360 VR Experience (.3vr)
- AppBuilder Extension (URL)
- AppBuilder widget package (.zip)–Only portal ad
- Application (URL)
- ArcGIS Desktop add-in (.esriaddin)
- ArcGIS Explorer add-in (.eaz)
- ArcGIS Explorer application configuration (.ncfg)
- ArcGIS Explorer document (.nmf)
- ArcGIS Explorer layer (.nmc)
- ArcGIS for Windows Mobile package (.wmpk)
- ArcGIS Pro add-in (.esriaddinx)
- ArcGIS Pro configuration (.proconfigX)
- ArcGlobe document (.3dd)
- ArcMap document (.mxd)



What's an item?

Everything in your portal.

Web Mapping Application	
Web Map	
Feature Layer (hosted)	
File Geodatabase	
Web Mapping Application	
Feature Layer (hosted)	
Shapefile	
Map Image Layer	



Stay secure while sharing items

Share

Share the item(s) with:

- Everyone
- 10.6.1 ArcGIS Enterprise Built-In
- These groups:
 - 1061views
 - Featured Maps and Apps
 - Public Safety Hub
 - Residential Life Department
 - Secure Content Team

These settings will replace the current settings.

OK Cancel

Portal content security is handled at the item level.

Web Mapping Application	
Web Map	
Feature Layer (hosted)	
File Geodatabase	
Web Mapping Application	
Feature Layer (hosted)	
Shapefile	
Map Image Layer	



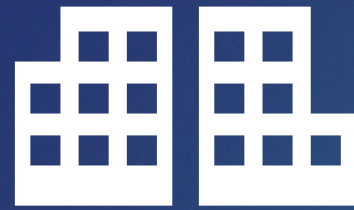
Stay secure while sharing items



Not shared



**Shared with
one or more
groups**



**Shared with
your whole
organization**



**Shared with
everyone**

**Most secure
Least access**

**Least secure
Most access**



Stay secure while sharing items

Portal items can only be shared
at the group level

Items cannot be shared with
individual users

Share

Share the item(s) with:

- Everyone
- 10.6.1 ArcGIS Enterprise Built-In
- These groups:
 - 1061views
 - Featured Maps and Apps
 - Public Safety Hub
 - Residential Life Department
 - Secure Content Team

These settings will replace the current settings.

OK Cancel



Design groups with security in mind

Home Gallery Map Scene Groups Content Organization Initial ...

Residential Life Department Edit

Overview Content Members Settings

Edit Thumbnail

R Maps and data for department employees only. Do not disseminate private information protected by FERPA law! Edit
owned by admin

Invite Users
Share

Membership Requests 0

Description Edit

Add an in-depth description of the group.

Latest Content View All Group Content

Student rooms
by admin
Updated: Jun 11, 2018

Details

Created: June 11, 2018
Viewable by:
Organization
Contributors: Members
1 1


Owner Change Owner
admin

Home Gallery Map Scene Groups Content Organization Initial ...

Secure Content Team Edit

Overview Content Members Settings

Edit Thumbnail

 For high-security items. Edit
owned by admin

Invite Users
Share

Membership Requests 0

Description Edit

Add an in-depth description of the group.

Latest Content View All Group Content

World Port Index by admin
World Port Index by admin

Details

Created: June 11, 2018
Viewable by: Only group members
Contributors: Members
5 2

Owner Change Owner
admin

Tags Edit



Design groups with security in mind

Home Gallery Map Scene Groups Content Organization

Create New Group

The group creation wizard asks four questions:

Who can view this group?

Who can join this group?

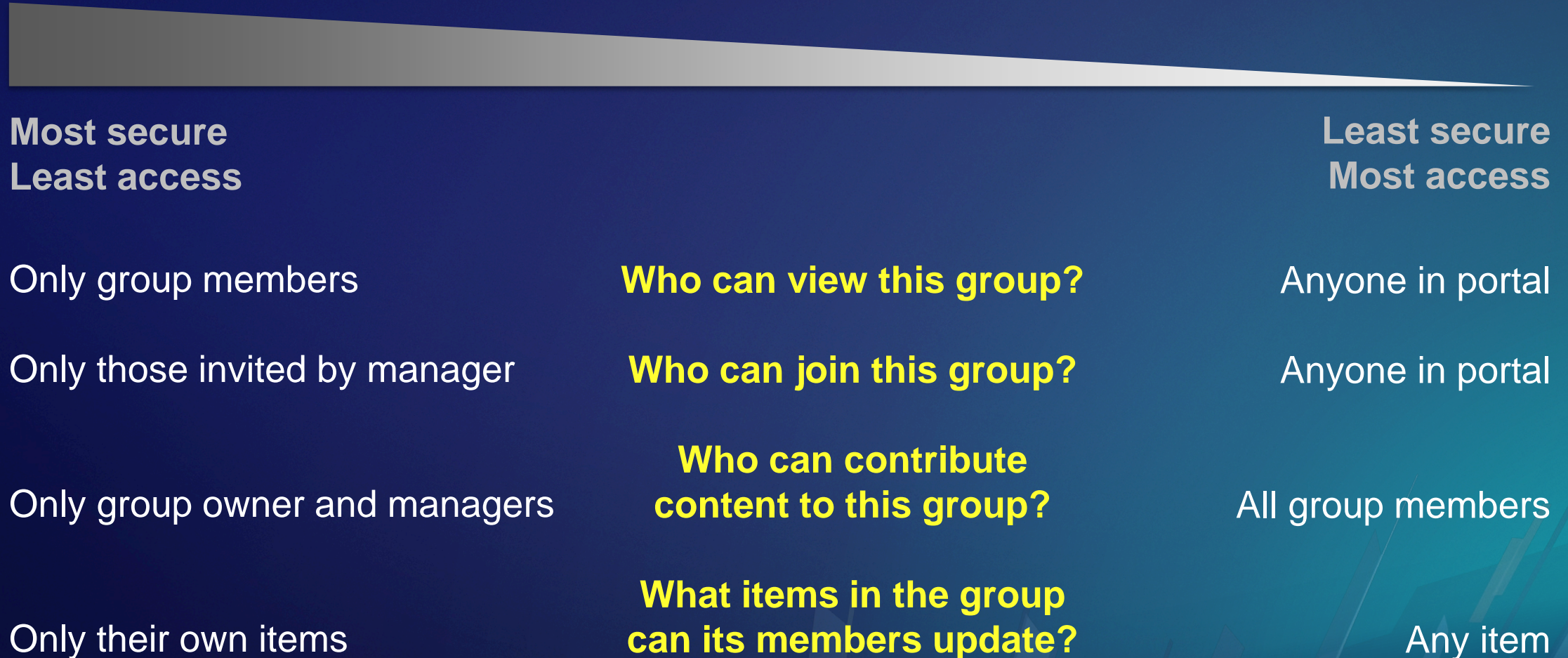
**Who can contribute
content to this group?**

**What items in the group
can its members update?**

Security decision point:
How secure do you
want your groups to
be? Do some groups
need to be more secure
than others?



Design groups with security in mind





Design groups with security in mind

Security best practice: Make rigorous use of portal groups, and only share sensitive items at the group level.



Share portal items securely

Demo



Service security



Considerations for securing map services

- **Who can view? Who can edit?**
- **Security of map service extensions controlled by map service**
 - OGC: WMS, WFS, WMTS, etc.
 - Feature Service

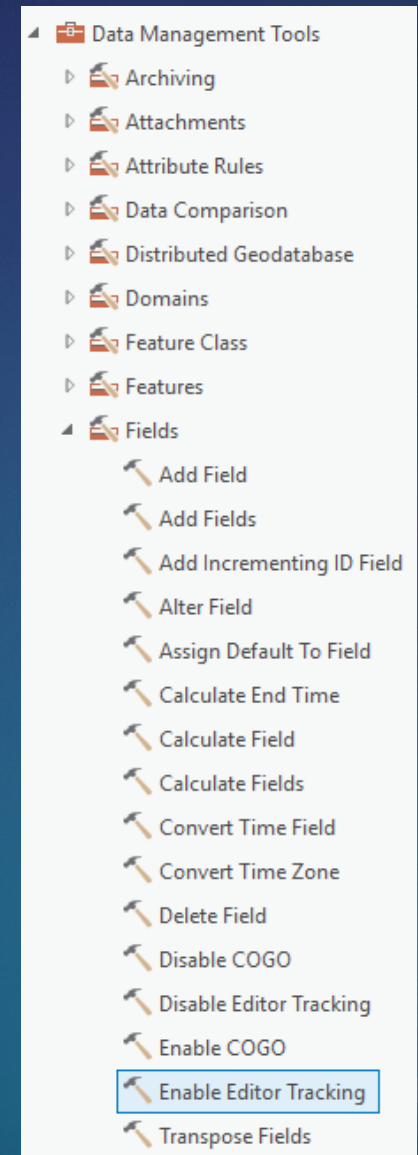


Editor tracking on feature services

Enabled before publishing a feature service from Desktop to Server

When enabled, view:

- Everyone who creates new features on the service
- Creation date of the service
- The last user to edit the service
- The last time the service was edited





Enable editor tracking on hosted feature layers

Feature Layer (hosted) Save Cancel

Editing

- Enable editing.
- 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 currently shared with: Organization

• 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)

• Who can manage edits?

- You
- Administrators
- Data curators with the appropriate privileges



Adding Secured Services

- Services become items in your portal
- **Decision point:** Should you store credentials?
 - Users will not be prompted to authenticate if you do
 - More seamless experience
 - Who will have access to this service as a portal item?



Adding Secured Services

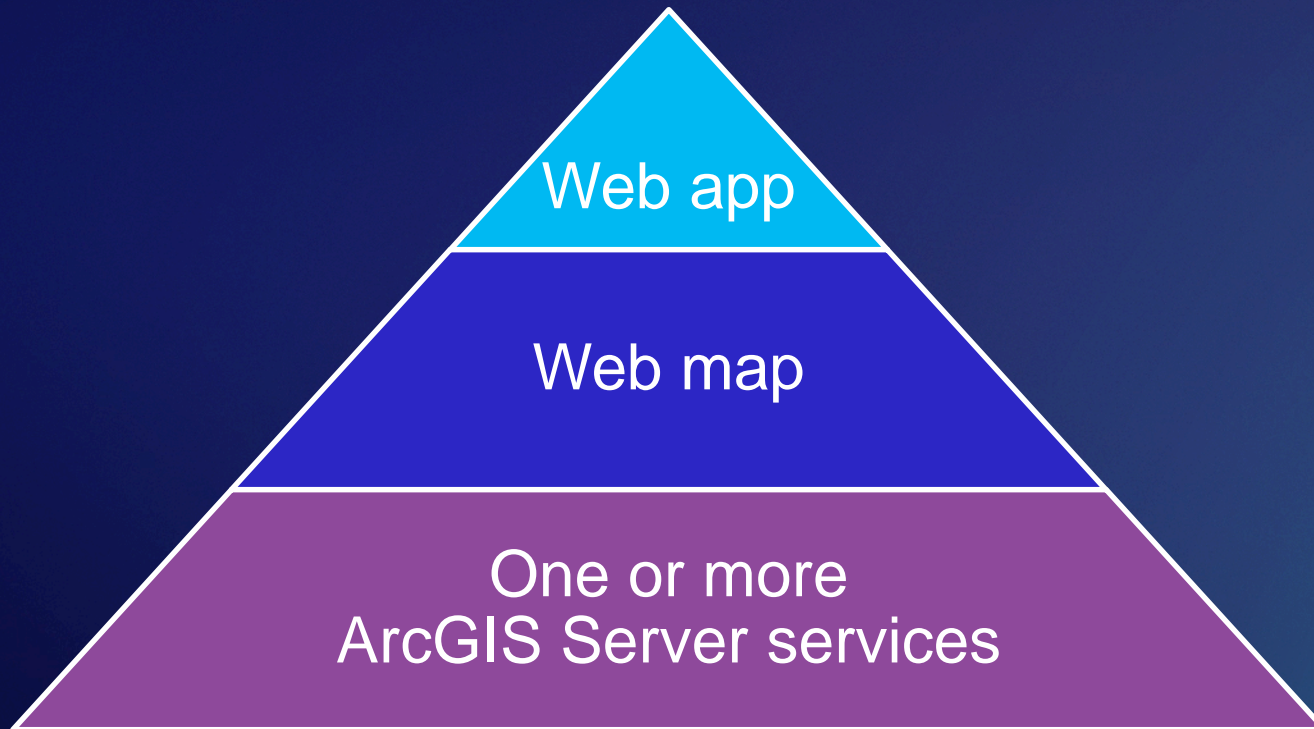
Demo



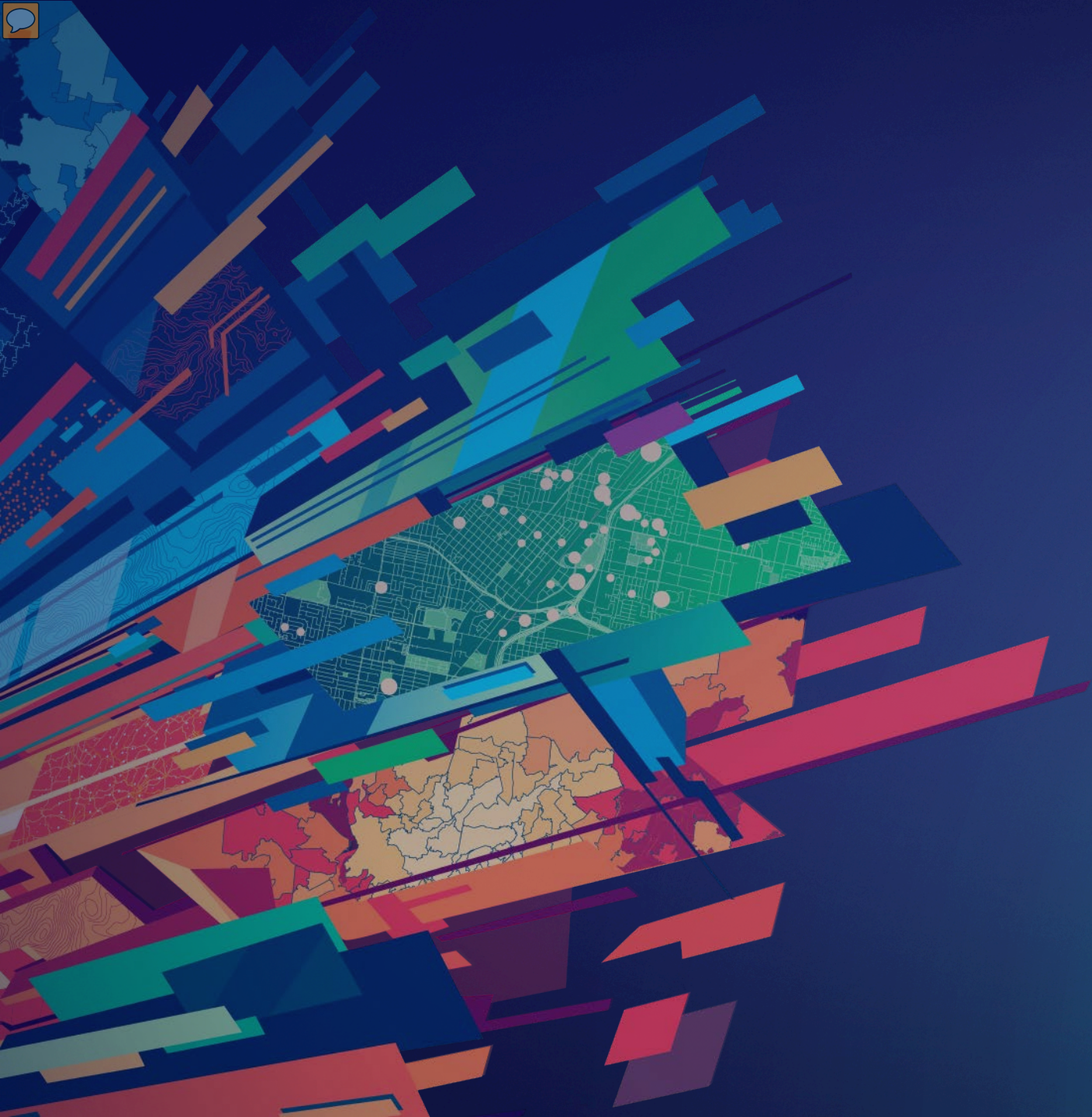
Securing web maps and web apps



The layers of a web app



**Consider
security at each
tier of this
pyramid.**



Securing Web Applications

Demo

Distributed collaborations





Distributed collaborations

- Sharing content in a secure, trusted pipeline
- Familiar access control – group sharing model
- Each participant keeps its own security settings
- Automatic synchronization schedule
- New this summer: ArcGIS Enterprise to ArcGIS Online

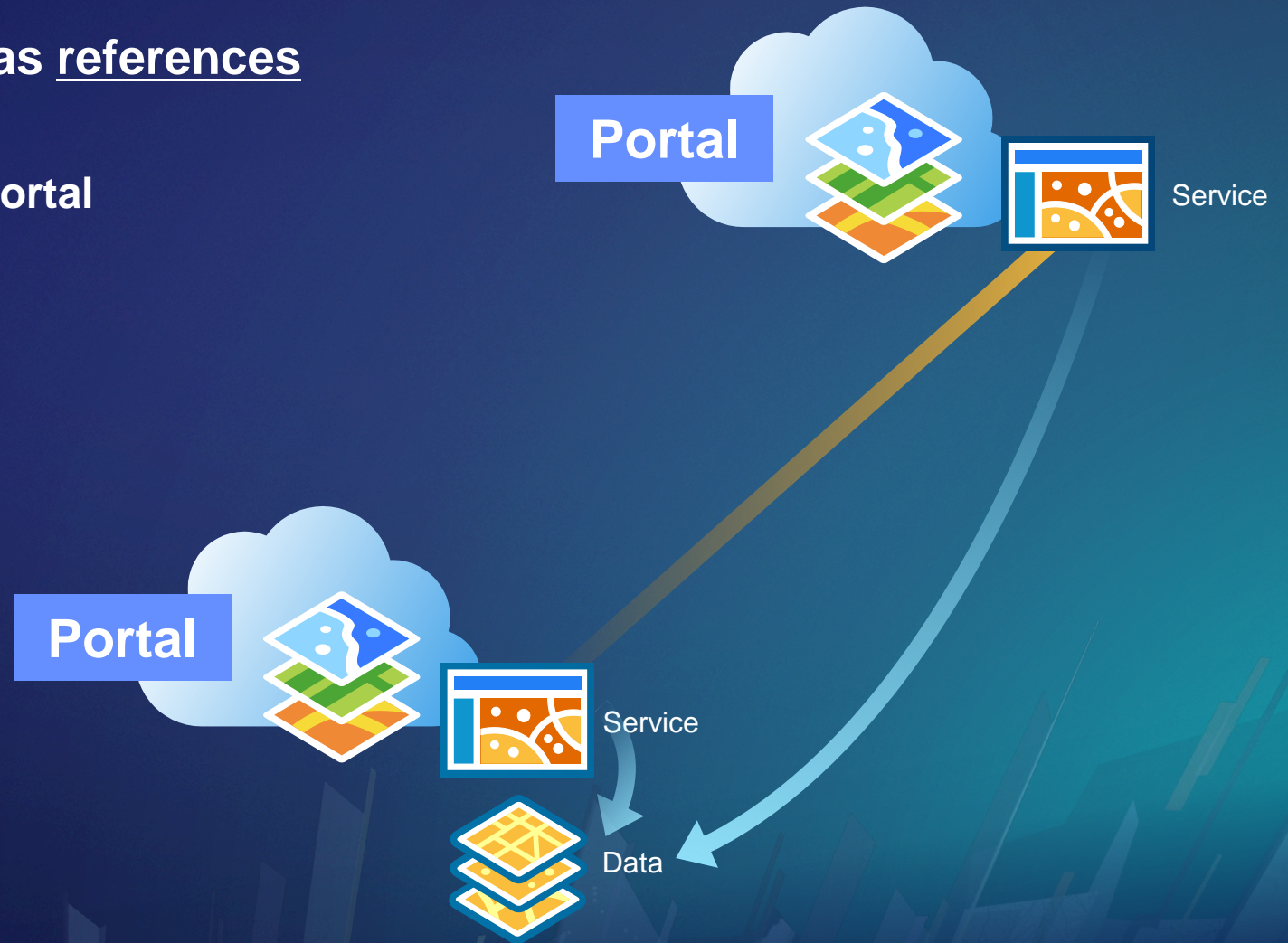




Distributed collaborations

- Sharing feature layer items as references
 - Data stays in your portal
 - Users need access to your portal

When sharing by reference, your content keeps the security settings of your portal.

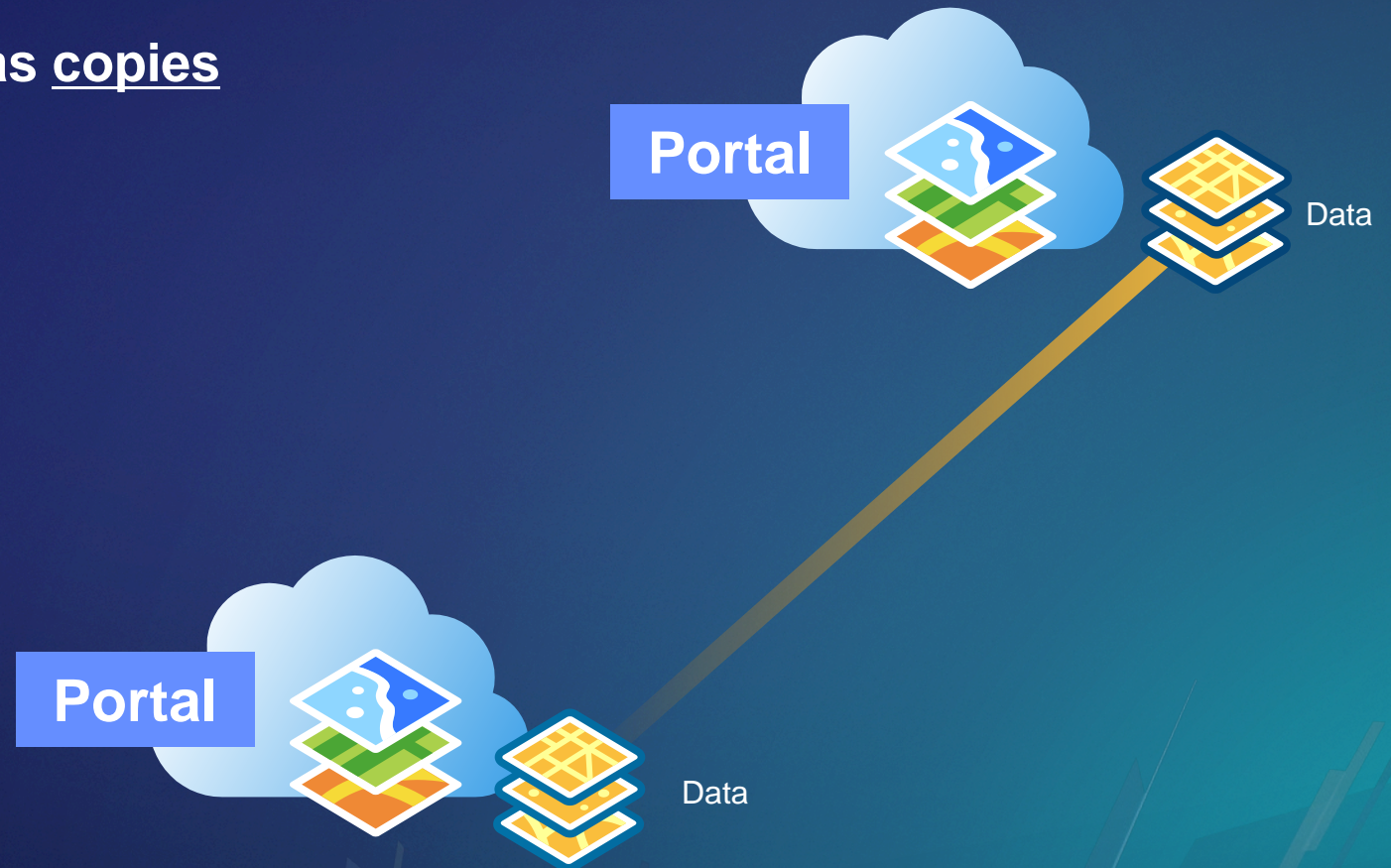




Distributed collaborations

- Sharing feature layer items as copies
 - Data is also shared
 - Recipients don't need access to your portal

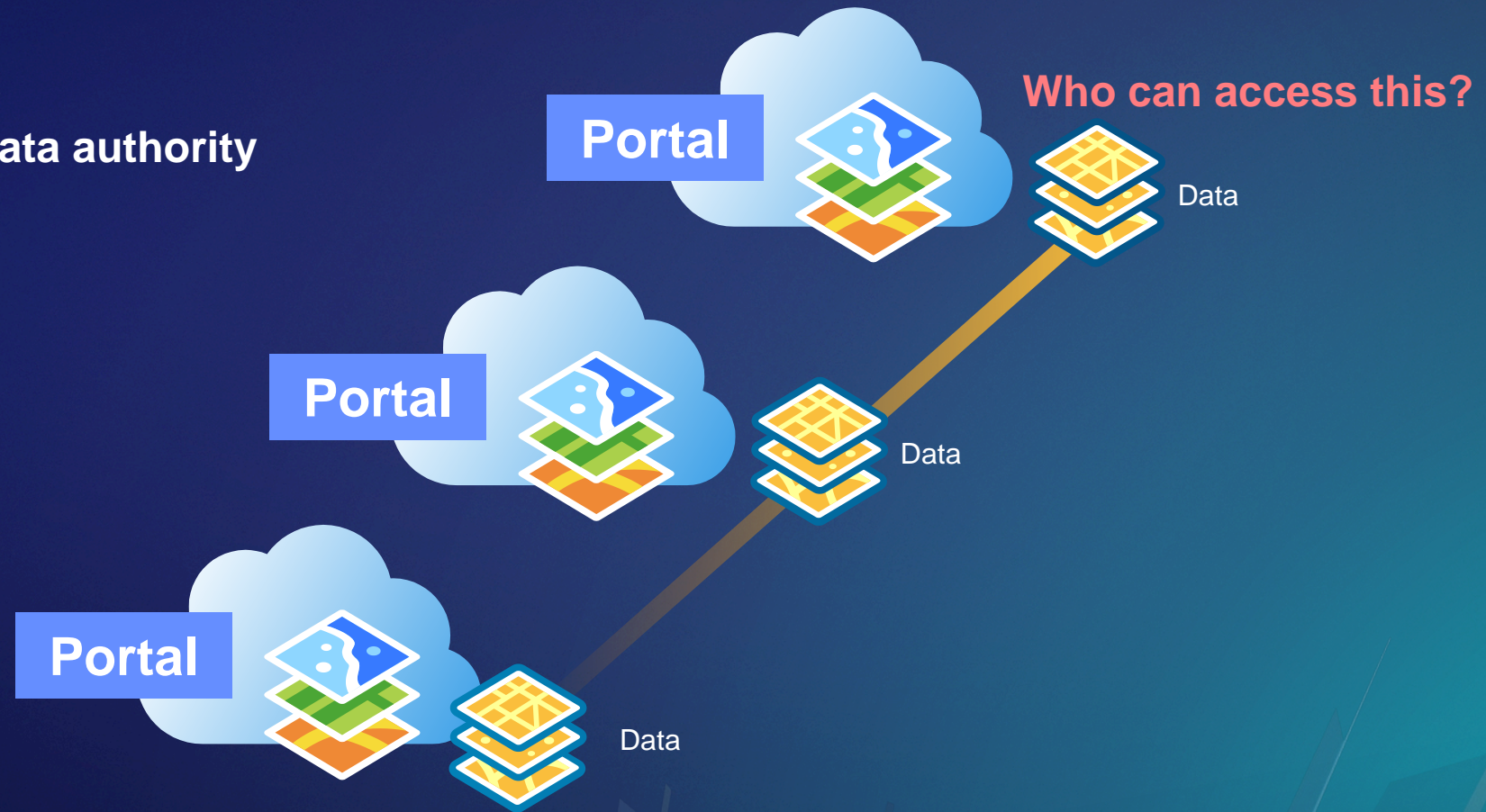
When sharing by copy, those copies of your content are subject to the other portal's settings.





Distributed collaborations

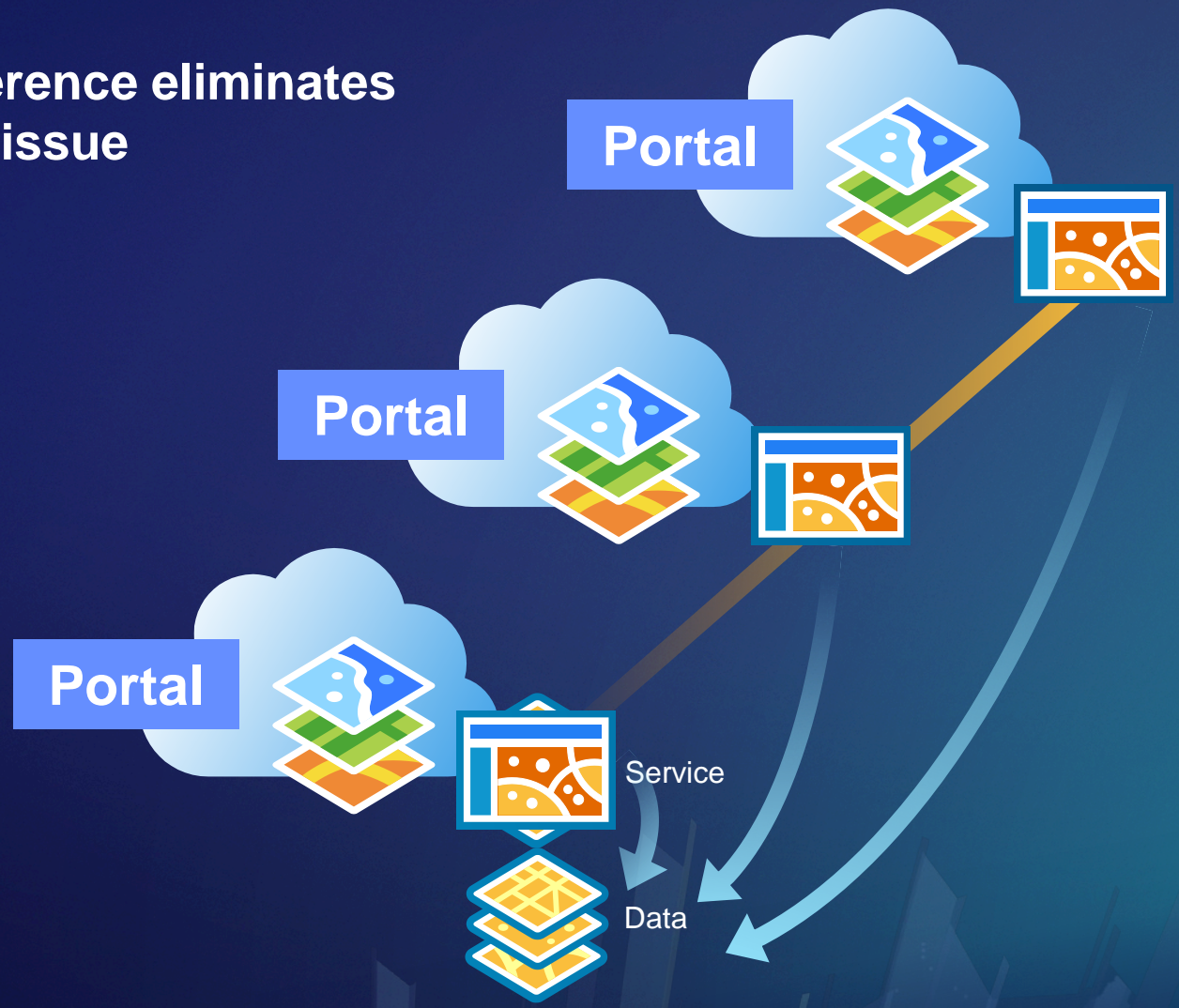
- Transitive trust
 - Risk to your data authority





Distributed collaborations

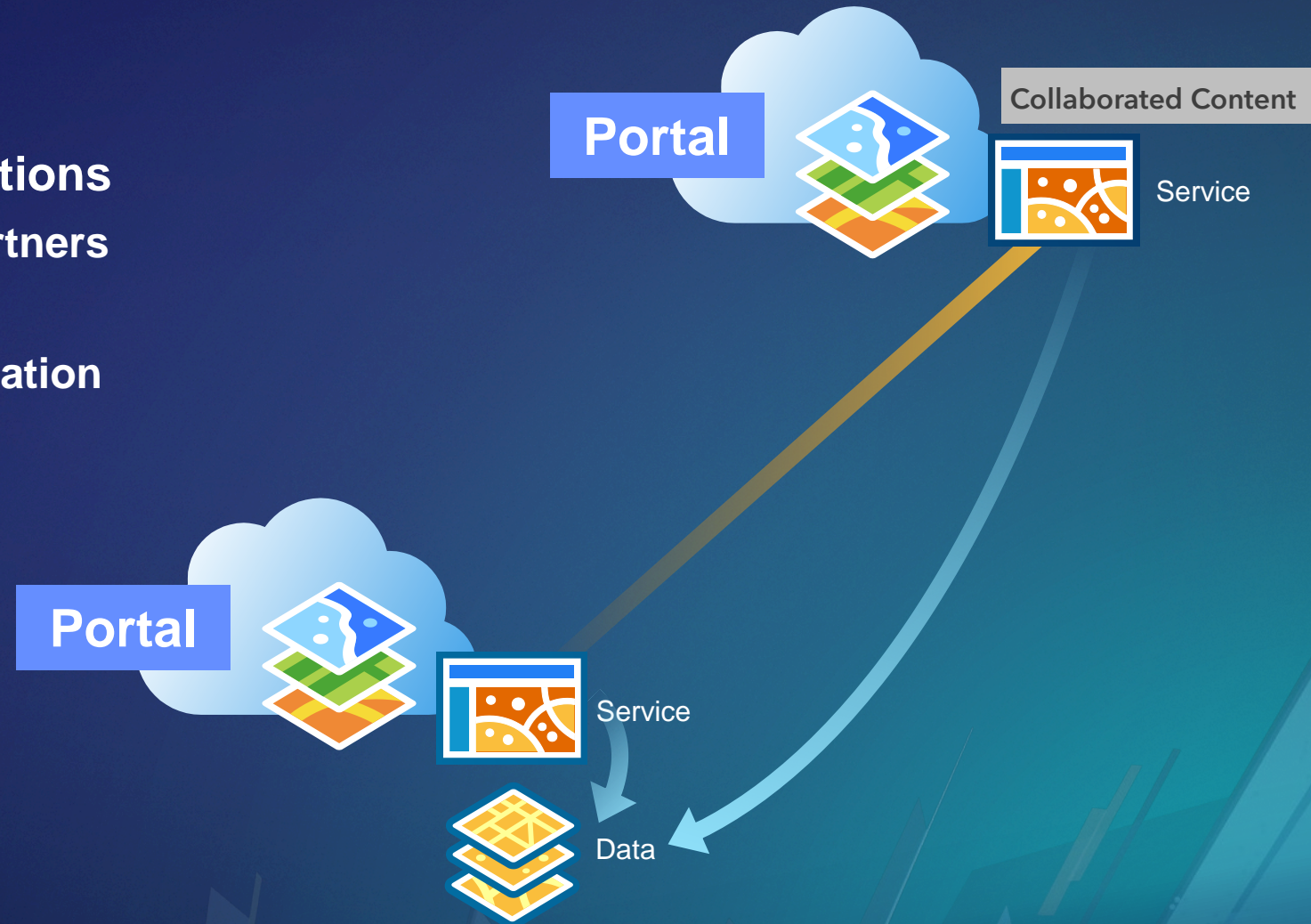
- Sharing by reference eliminates transitive trust issue





Distributed collaborations

- **Collaboration security considerations**
 - Limit collaborations to trusted partners
 - Share services instead of data
 - Establish new groups for collaboration
- **Distributed Collaboration**
Demo Theater 05
11:15 a.m. today!





Access and authentication





Secure content with encryption

- Using HTTPS prevents eavesdropping on web traffic
- If possible, enable HTTPS Only



Unsecure HTTP



SSL protocol



Secure HTTPS



Integrating enterprise authentication

Who can log in to your portal?

Built-in identity store

Users configured
within your portal

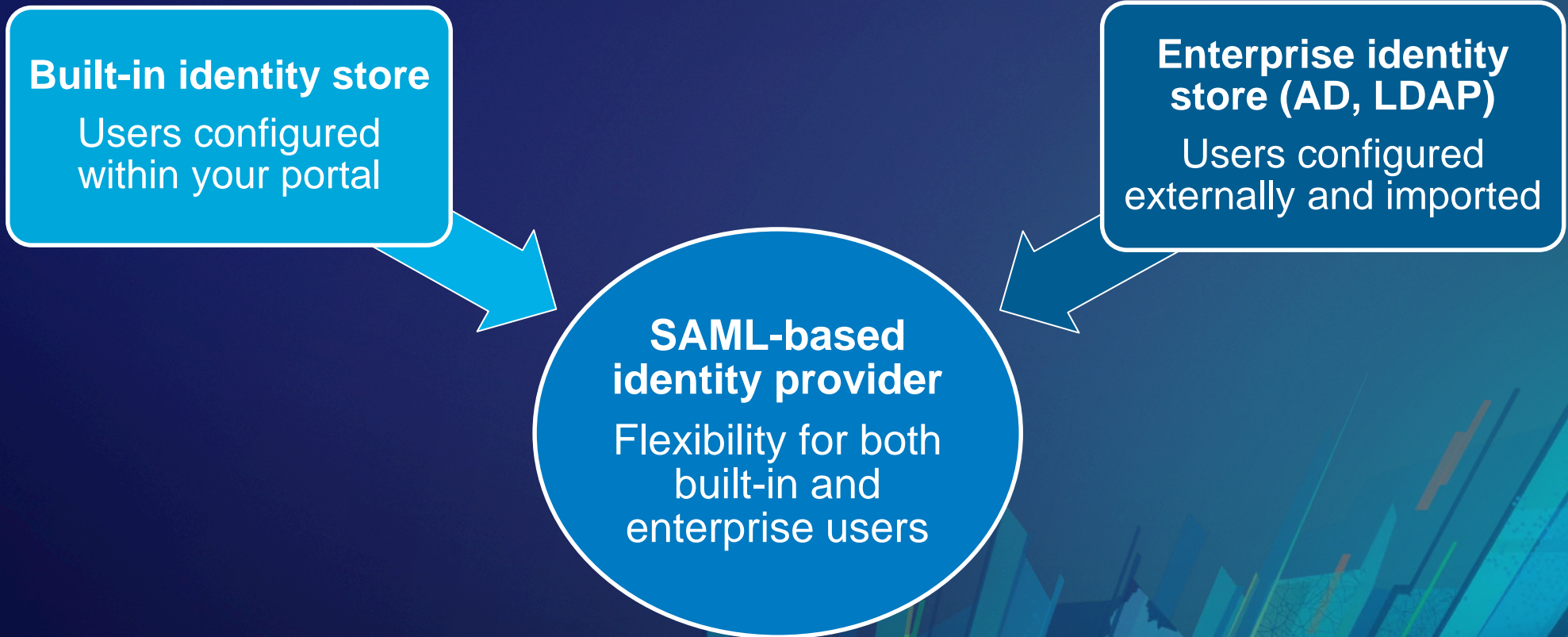
Enterprise identity store (AD, LDAP)

Users configured
externally and imported



Integrating enterprise authentication

Who can log in to your portal?





Design groups with security in mind

Who can join this group?

- By default the group manager controls the group membership
- If ArcGIS Enterprise is configured with enterprise users and groups, the group can be linked to an enterprise group
 - Facilitates group membership

Who can join this group?

- Those who request membership and are approved by a group manager
- Only those invited by a group manager
- Anyone

Who can join this group?

- Those who request membership and are approved by a group manager
- Only those invited by a group manager
- Members of an enterprise group
- Anyone

Members of an Enterprise Group

None selected

Search for Group



Anonymous access to the portal

- **If enabled**

- Don't need authentication to view first five pages of your portal (in red)
- Cannot view
- Can add public items to your map, but can't save or share

- **If disabled**

- Authentication required upon initial access of your portal
- Cannot view information about your groups or any of your content
- **This is the more secure option**

Home Gallery Map Scene **Groups** Content Organization

10.6.1 ArcGIS Enterprise Built-In

SAVE CANCEL

General
Home Page
Gallery
Map
Items
Groups
Utility Services
ArcGIS Online
Servers
Roles
Collaborations
Security

Security

Configure the security settings for your portal.

Policies

- Allow access to the portal through HTTPS only.
- Allow anonymous access to your portal.
- Allow members to edit biographical information and who can see their profile.
- Allow users to create new built-in accounts.

Sharing and Searching

- Members can share content publicly.

Password Policy



Security decision point: Do our usage patterns permit us to disable anonymous access to our portal?

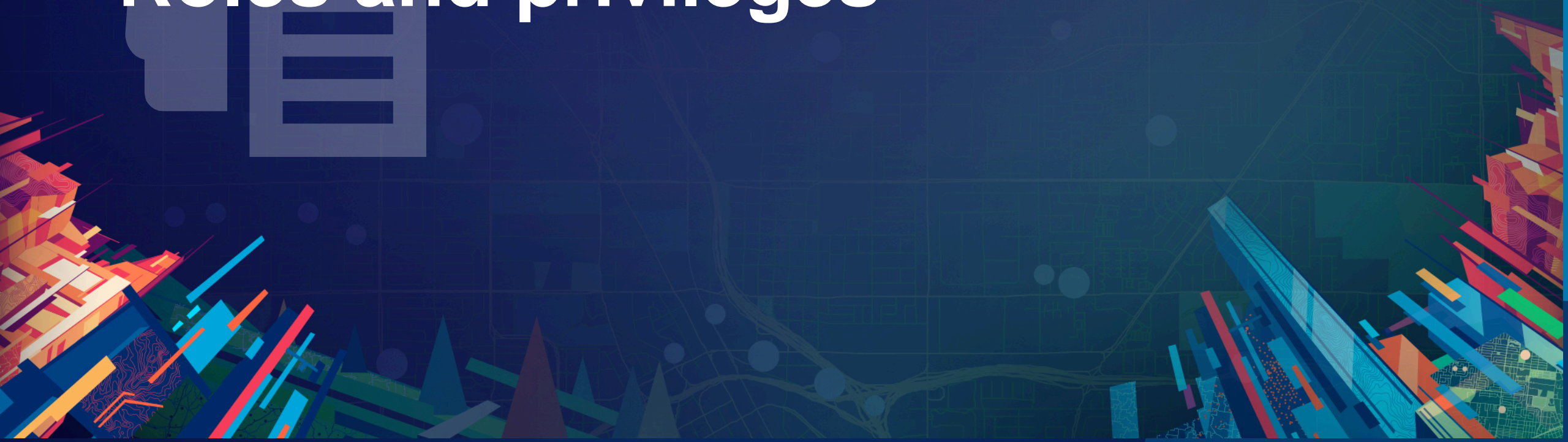


Disable anonymous access to the portal

Demo



Roles and privileges





Beyond levels 1 and 2

- **Level 1 user – Viewer only**
- **Level 2 user – Admin, Publisher, User**

- **Beyond the default roles – custom roles**
- **Defined with fine-grained privileges**
 - **List is steadily growing**



Built-in and custom roles

**General
privileges**

Members

Groups

Content

Sharing

Analysis

Features

**Admin
privileges**

Members

Groups

Content



Security best practice: Maintain a focused set of custom roles to control your users' privileges.



Define a custom role in your portal

Demo

Summary of **best practices**

- **Proactively design your portal to impart confidentiality and integrity**
- **Make rigorous use of portal groups**
- **Only share sensitive portal items at the group level**
- **Enable edit tracking on hosted feature layers**
- **Use distributed collaboration to share content with trusted partners**
- **Maintain a focused set of custom roles**
- **Make sure HTTPS encryption is standard**
- **If appropriate, disable anonymous access to your portal**

Other sessions of interest

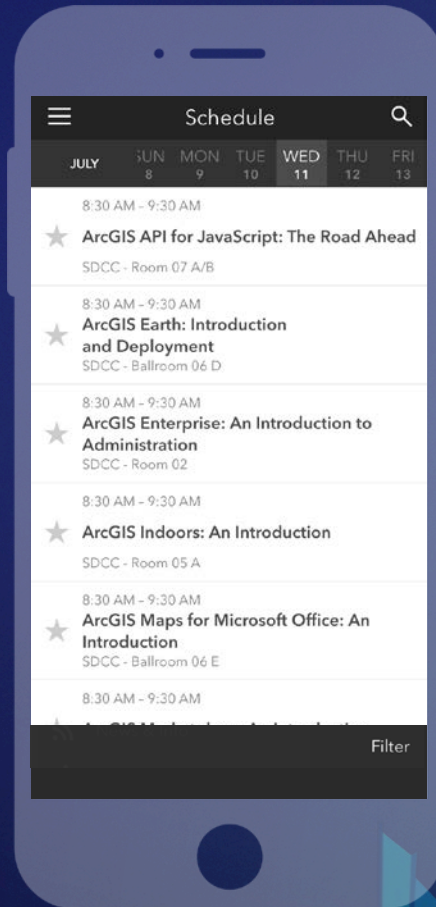
WORKSHOP	LOCATION	TIME FRAME
<ul style="list-style-type: none">• BPs for Layers and Service Types	<ul style="list-style-type: none">• Room 16 B	<ul style="list-style-type: none">• 10 – 11 a.m. today
<ul style="list-style-type: none">• Distributed Collaboration	<ul style="list-style-type: none">• Demo Theater 05	<ul style="list-style-type: none">• 11:15 a.m. – 12 noon today
<ul style="list-style-type: none">• Supporting your ArcGIS Enterprise deployment	<ul style="list-style-type: none">• Room 05 B	<ul style="list-style-type: none">• 2:30 – 3:30 p.m. today
<ul style="list-style-type: none">• SSL Considerations	<ul style="list-style-type: none">• Room 15 A	<ul style="list-style-type: none">• 2:30 – 3:30 p.m. today
<ul style="list-style-type: none">• ArcGIS Enterprise: Advanced topics in administration	<ul style="list-style-type: none">• Room 04	<ul style="list-style-type: none">• 9 – 10 a.m. Friday
<ul style="list-style-type: none">• ArcGIS Enterprise: Road Ahead	<ul style="list-style-type: none">• Ballroom 06 E	<ul style="list-style-type: none">• 9 – 10 a.m. Friday

Please take our survey on the app

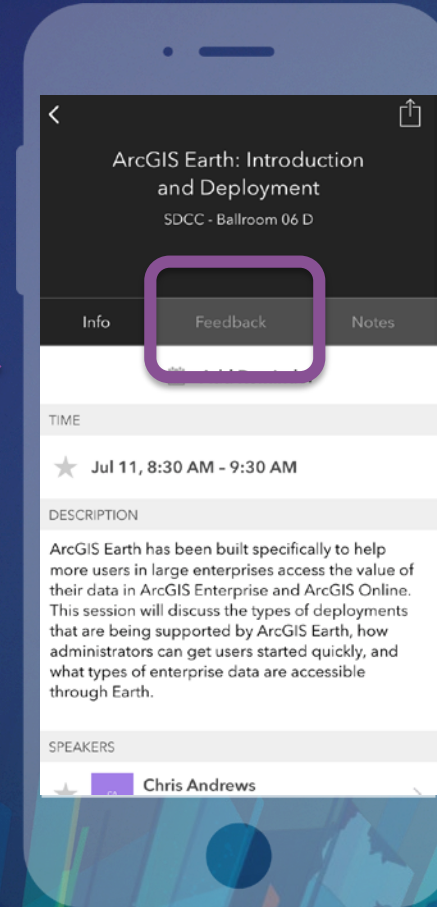
Download the Esri Events app and find your event



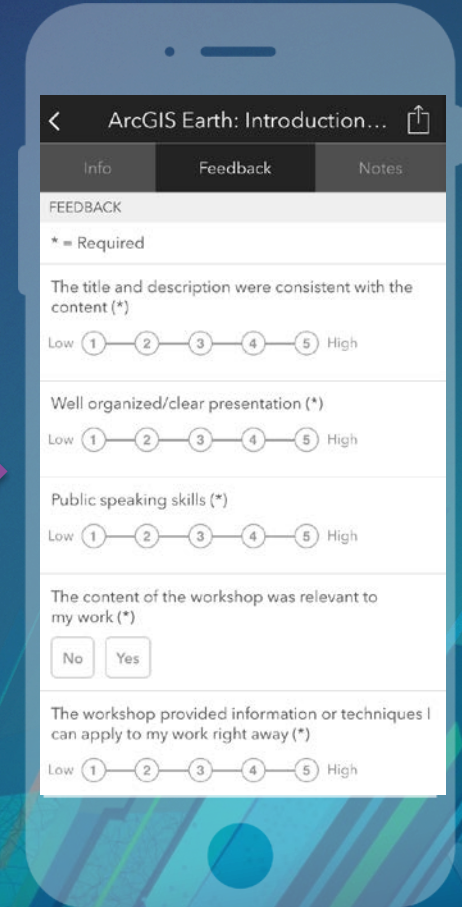
Select the session you attended



Select the Feedback tab



Complete answers and select "Submit"





esri

**THE
SCIENCE
OF
WHERE**