

# Secured Services Best Practices on ArcGIS for Server

Patrick Jackson & Harrold Sompotan

# Agenda

- **Security Store types(Built-in vs. AD or LDAP stores)**
- **Modes of authentication(GIS/Web Tier)**
- **Selecting the right Authentication Tier**
- **SSL Encryption**
- **Other considerations**

# ArcGIS for Server identity store types:

- Built-in Store
  - Create users and groups within ArcGIS Server
- Windows Active Directory
- LDAP store
  - Leverage the existing security store
- Other common security stores used:
  - SQL server Store
  - Custom ASP.NET providers
  - Portal for ArcGIS Federation

# GIS Tier authentication

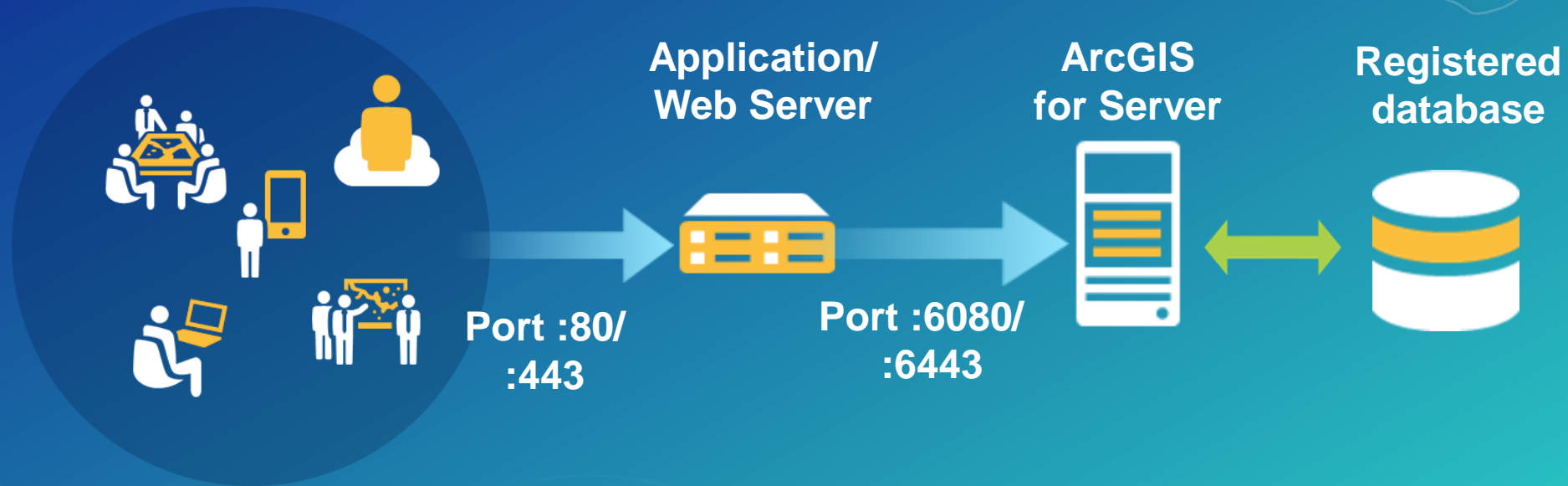
Authenticated using Esri's token-based authentication mechanism.  
The web adaptor can be used or can be omitted.





# Web Tier authentication

- **ArcGIS Server delegates authentication to the web server such as Microsoft IIS, Apache, etc.**
- **Requires the use of the Web Adaptor.**



# Determining the best authentication tier

## GIS Tier authentication

- Both public and internal access required
- Services primarily consumed by clients built using ArcGIS Web APIs
- Token based support for printing secure services



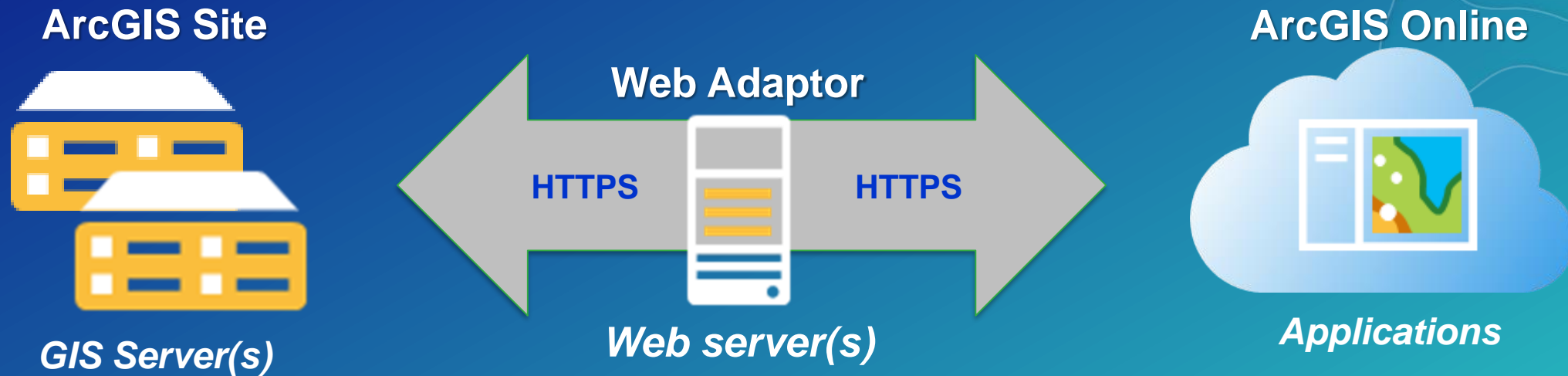
# Determining the best authentication tier (cont.)

## Web Tier authentication

- Internal user access only.
- SSO(Single Sign On) requirement
- No support for Print Services



# Encryption



- ✓ **HTTPS end to end**
  - ✓ Valid SSL certificate
  - ✓ SSL Cert on Web Adaptor
  - ✓ Not required on AGS



# Other considerations when setting up secured services

- **Disable the PSA (Primary Site Administrator)**
- **Limit access to the ArcGIS Server directories**
- **Encrypt the ArcGIS Server directories**



# Demo

Setting up ArcGIS Server with Windows Domain and Built in Roles



## ArcGIS Server Manager

Enter your ArcGIS Server username and password:

Username:

Password:

Login





# Demo

Setting up LDAP and Built in Roles



## ArcGIS Server Security

ArcGIS Server security determines who can administer the GIS server, who can publish to the GIS server, and who can use the services.

General ArcGIS Server security settings are displayed below. To change the accounts recognized by ArcGIS Server and set their permissions, click the Users and Roles links above. To set access rules for a service, use the Services > Manage Services page.

### Configuration Settings

User Store:

Role Store:

Authentication Tier:

Authentication Mode:

#### Primary Site Administrator

Username:

#### Token Settings

Lifespan of Short-lived Token:

Lifespan of Long-lived Token:

### Security Configuration Wizard

## Enterprise Store Type

You have chosen to use users from your existing directory. These users will be managed by ArcGIS Server.

Choose your Enterprise store type:

☐ Windows Domain

☒ LDAP

### Configuration Settings

User Store:

Role Store:

Authentication Tier:

Authentication Mode:

#### Primary Site Administrator

Username:

#### Token Settings

Lifespan of Short-lived Token:

Lifespan of Long-lived Tokens:

### Security Configuration Wizard

## LDAP User Store

Host name:

Port:

Base DN:

URL:

RDN attribute:

Administrator's DN:

Password:

Test Connection

Back

Next

Cancel



## Configuration Settings

User Store:

Role Store:

Authentication Tier:

Authentication Mode:

## Primary Site Administrator

Username:

## Token Settings

Lifespan of Short-lived Token:

Lifespan of Long-lived Token:

## Security Configuration Wizard



Connection to server

## LDAP User Store

Host name:

Port:

Base DN:

URL:

RDN attribute:

Administrator's DN:

Password:

Test Connection

```
C:\Windows\System32\cmd.exe

WHOAMI /FQDN
WHOAMI /LOGONID
WHOAMI /USER
WHOAMI /USER /FO LIST
WHOAMI /USER /FO CSU
WHOAMI /GROUPS
WHOAMI /GROUPS /FO CSU /NH
WHOAMI /PRIV
WHOAMI /PRIV /FO TABLE
WHOAMI /USER /GROUPS
WHOAMI /USER /GROUPS /PRIV
WHOAMI /ALL
WHOAMI /ALL /FO LIST
WHOAMI /ALL /FO CSU /NH
WHOAMI /?

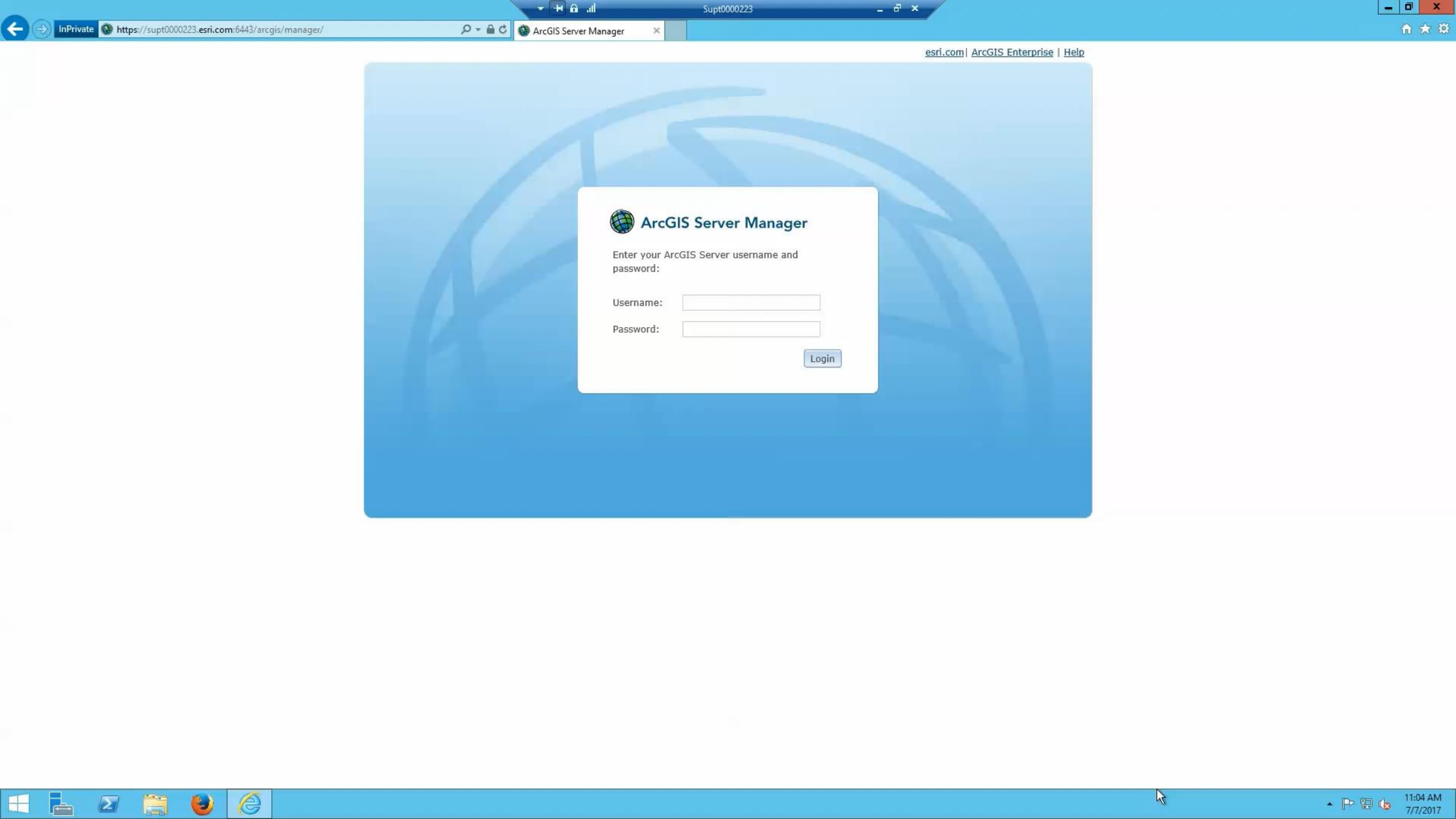
C:\windows\system32>whoami /fqdn
CN=demo,OU=Users,OU=Managed,DC=uc,DC=esri,DC=com
```

Host name	Your Servers Hostname
Port	389 normally
Base DN	The distinguished name (DN) of the node in the directory server under which user information is maintained. (ou=users,ou=arcgis,dc=mydomain,dc=com)
URL	This is created automatically based on the hostname and Base DN
RDN attribute	The relative distinguished name (RDN) attribute for user entries in the LDAP server. (For the DN "cn=john,ou=users,ou=arcgis,dc=mydomain,dc=com" the RDN is "cn=john" and the RDN attribute is cn.)
Administrator's DN	The easiest way to get this for AD is to do a whoami /FQDN. (uid=admin,ou=administrators,dc=mydomain,dc=com)

**\*\*It is recommended that you specify an administrator account with a password that does not expire.**

# Demo

Securing a service in Server Manager



## ArcGIS Server Manager

Enter your ArcGIS Server username and password:

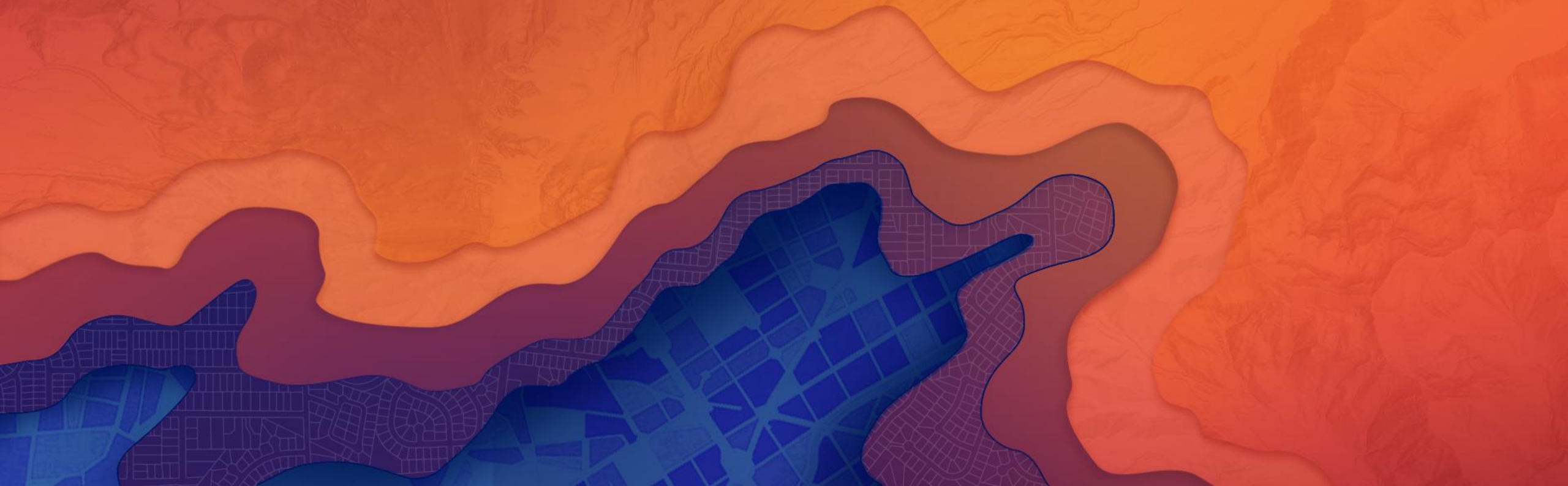
Username:

Password:

Login



# Questions?

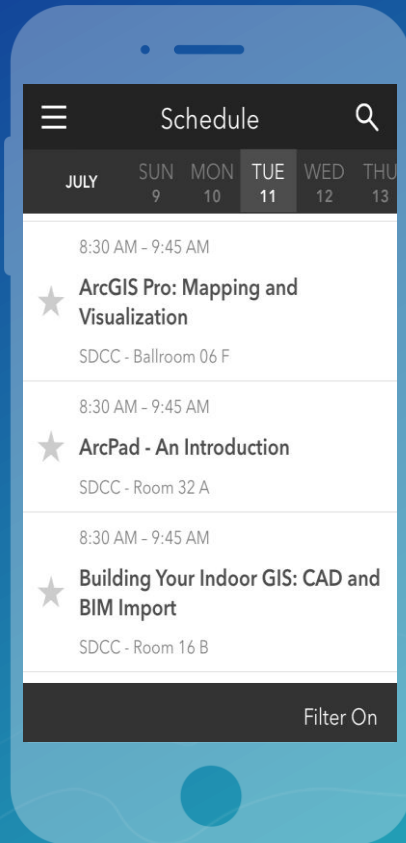


# Please Take Our Survey on the Esri Events App!

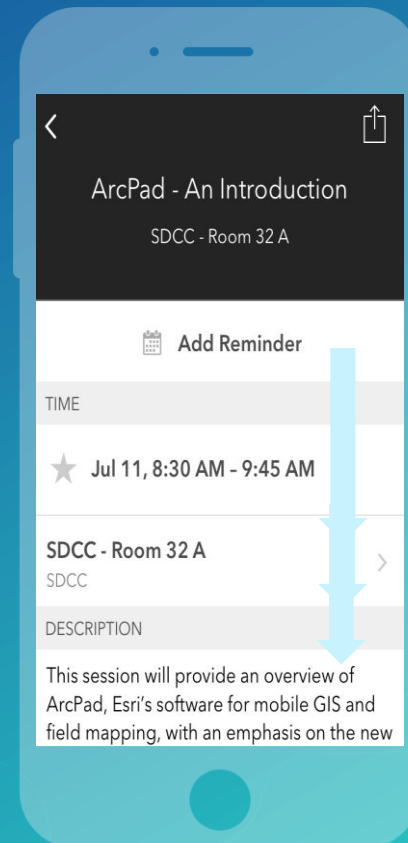
**Download the Esri Events app and find your event**



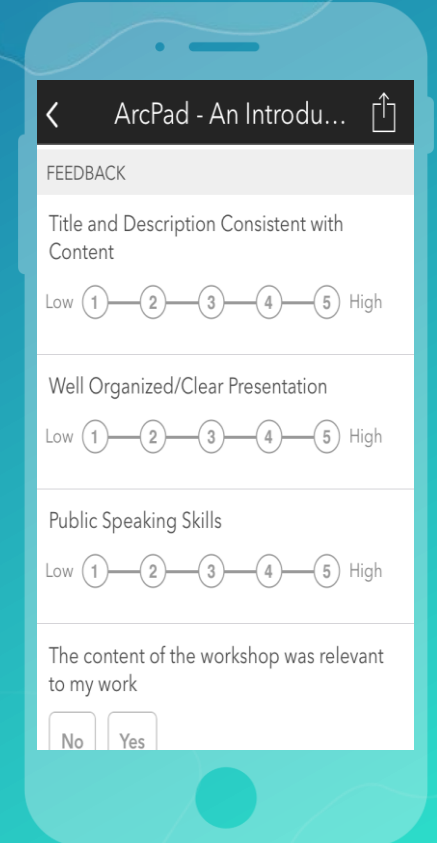
**Select the session you attended**



**Scroll down to find the survey**



**Complete Answers and Select "Submit"**







esri

THE  
SCIENCE  
OF  
WHERE