



Esri International Developer Summit  
Palm Springs, CA

# Securing ArcGIS for Server

David Cordes, Raj Padmanabhan

# Agenda

- **Security in the context of ArcGIS for Server**
- **User and Role Considerations**
- **Identity Stores**
- **Authentication**
- **Securing web services**
- **Protecting against attacks**
- **Summary**

# ArcGIS for Server Security

- **Protecting your ArcGIS Server site and its web services**
- **Control who has access**
  - Integrate with your organization's IT infrastructure
- **Define what valid users can do**
  - Permissions



# ArcGIS for Server Access: Authorization

- **User** – Valid login to access Server site
- **Role** – Grouping of users

1. Administrators – Full admin control



2. Publishers – Publish web services



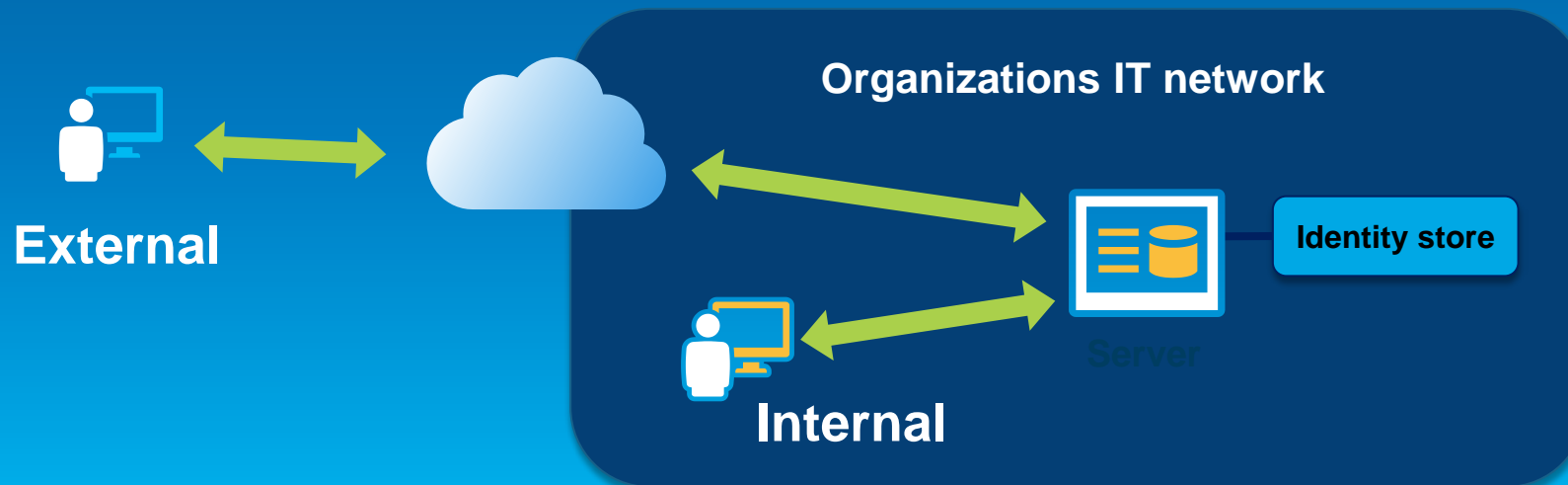
3. Users – view web services



- **Identity Store** – Repository for user and role information

# ArcGIS for Server: User considerations

- **Where are you users coming from?**
  - Determines which type of identity store you should use
- **Internal : Windows Active Directory, LDAP or custom**
- **External : Built-in or custom**



# ArcGIS for Server: Role considerations

- **How much control do I have on my ArcGIS Server site?**
- **Managed by me, within my Dept**
  - Built-in roles
- **Managed by my organization's IT Dept**
  - External, enterprise defined roles

# ArcGIS for Server: Identity store

- **Identity store** – Defines your users and roles
- 3 different options
  1. **Built-in** (default)
  2. **Register with an enterprise identity store**
    - Windows Active Directory
    - LDAP
  3. **Mixed mode**
    - Users from enterprise identity store
    - Roles from built-in store

# Demo

## ArcGIS Server Manager User and role management





# Authentication Tier / Method

- **Authentication**

- Check and verify user identity

- **Authentication options**

1. **GIS Tier**

- Uses ArcGIS Tokens to authenticate

2. **Web Tier**

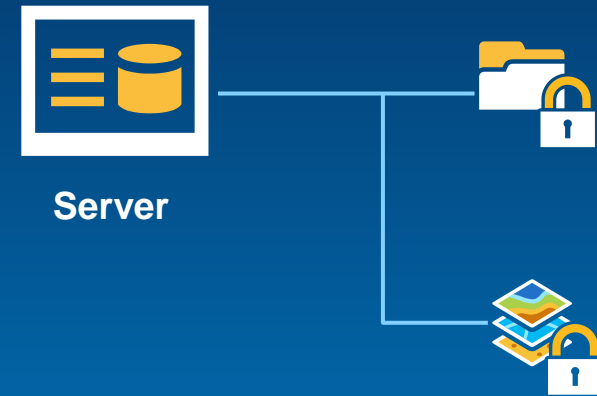
- Uses Integrated Windows authentication, Client certificates, Basic, Digest, etc

## GIS Tier vs. Web Tier Authentication

	GIS Tier / Token	Web Tier / HTTP Auth
<b>Default</b>	Yes	No
<b>Public / anonymous possible</b>	Yes	No
<b>Clients Supporting</b>	Esri	All, including OGC
<b>Requirements</b>	Enable SSL	Web Adaptor(s) required Basic – require SSL Digest – special setup IWA – Windows only

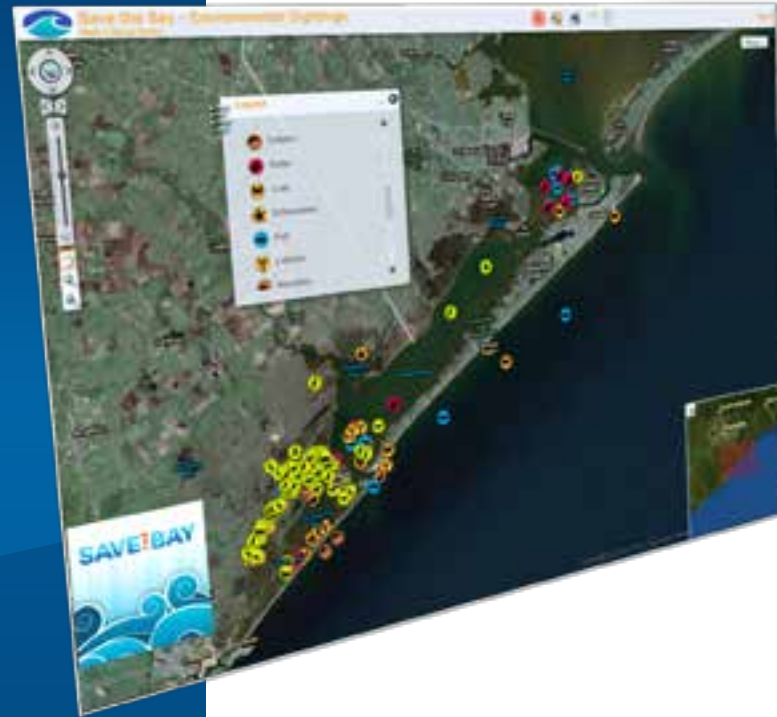
# Securing GIS Web Services

- Set permissions for roles on
  - A Folder
  - Individual services
- Administrators / Publishers grant permissions
- All new services are public by default
  - Anonymous access
- Can specify whether folders require HTTPs



# Demo

ArcGIS Server Manager  
How to secure a service  
Accessing a secured service



# Supporting Public and Private Services

- **How do I host public (anonymous) services with web tier authentication?**
- **Configure 2 Web Adaptors for the same Server site**
  - **web adaptor 1: authenticated access**
  - **web adaptor 2: anonymous access**

# Demo

Public and private services

# Protecting Against Attacks

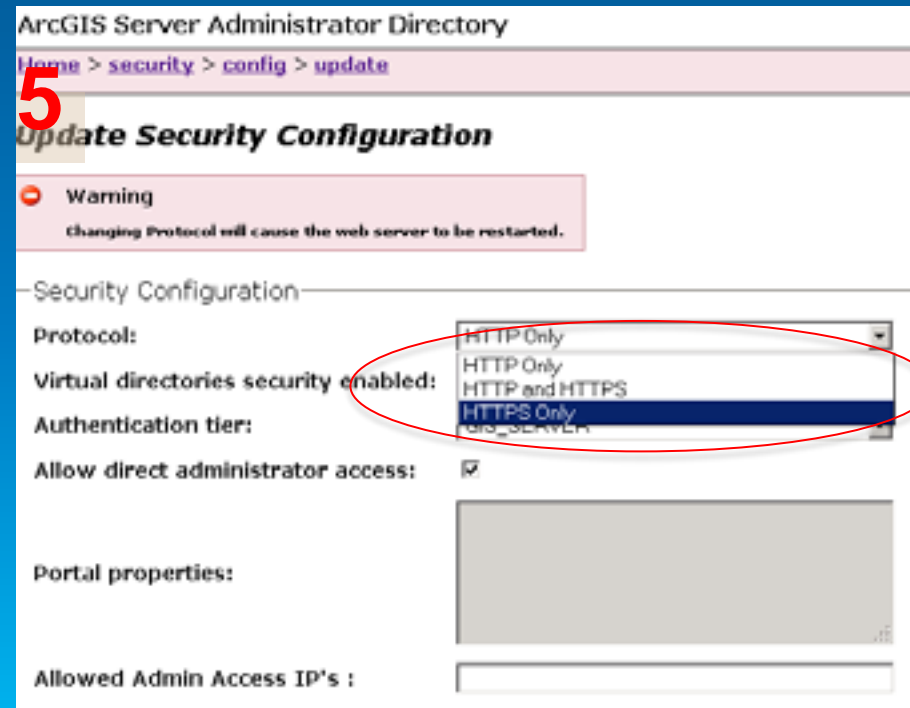
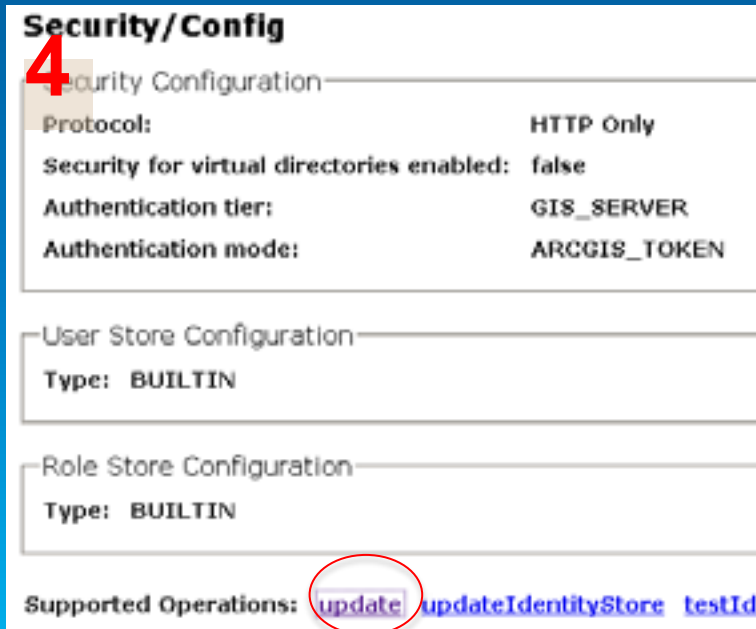
David Cordes

# Preventing Snooping

- **HTTPS**
  - **Between Server and web adaptor/proxy**
  - **Between web adaptor/proxy and client**
  - **Easy to configure**
- **Lock down your directories**
  - **Config-store**
  - **Output directories**
  - **No permissions to anyone except ArcGIS Server account**



# Enabling HTTPS – Click by click



# Preventing Cross-Site Scripting Attacks

- **Bad Guy gets you to click on a link for reputable site**
- **Bad Guy gets you to do bad things with your credentials**
- **Four recommendations**
  - **Use latest software**
  - **Disable Services Directory in Server**
  - **Disable Portal directory in Portal**
  - **Log out when done**

# Preventing Cross-Site Request Forgery (CSRF)

- **Bad Guy gets you to go to their site**
- **Bad Guy gets you to do bad things with your credentials**
- **ArcGIS Server (10.1 SP1+) automatically protects against CSRF admin operations**
- **Recommendations**
  - **Upgrade to 10.1 SP1 or later**
  - **Configure cross-domain access (<http://bit.ly/1fnhj29>)**
  - **Configure shorter-lived tokens**

# Disabling Services Directory

Home > system > handlers > rest > servicesdirectory > edit

## Edit Services Directory

Edit Services Directory

Services Directory Enabled :

AllowedOrigins : my-web-server.esri.com

Javascript API URL : http://serverapi.arcgisonline.com/jsapi/arcgi

Javascript API SDK URL : http://help.arcgis.com/en/webapi/javascript/

Javascript API CSS URL : http://serverapi.arcgisonline.com/jsapi/arcgi

Javascript API CSS2 URL : http://serverapi.arcgisonline.com/jsapi/arcgi

ArcGIS.com Map Text : ArcGIS.com Map

ArcGIS.com URL : http://www.arcgis.com/home/webmap/viewe

Format: HTML

Save

Navigation Path in Admin Directory

Enabling/disabling – easy as a click

Bonus: limit which web servers can access  
Your services

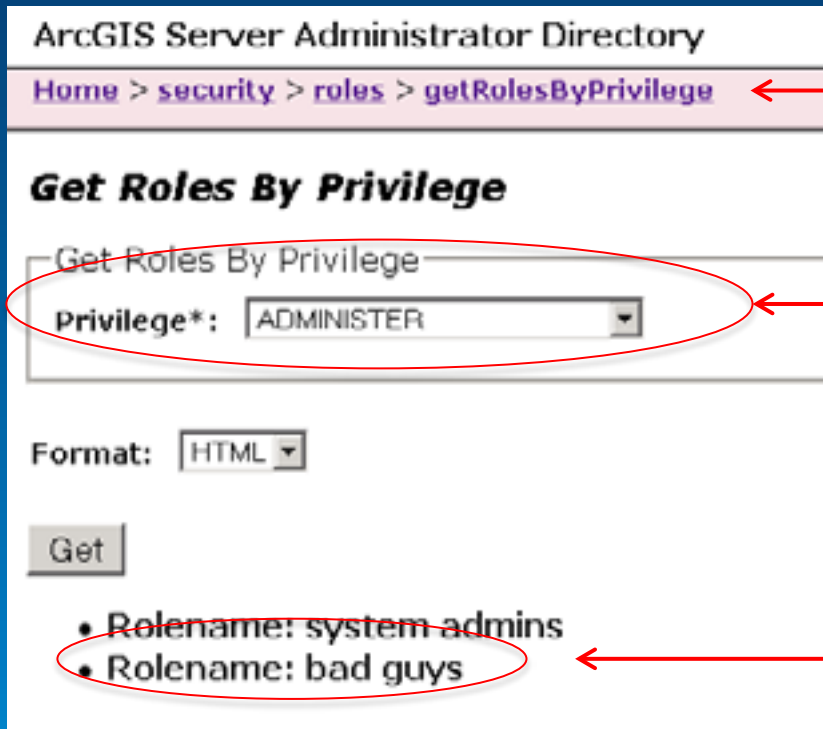
# Preventing SQL Injection Attacks

- **Bad guy uses normal access to find holes in your database**
  - To modify data
  - Grant greater permissions to himself
  - Execute code on your machine
- **If you use an enterprise database, you're at risk**
- **Recommendation:**
  - Latest DBMS upgrade
  - Follow DBMS vendor best practices
  - Upgrade to ArcGIS Server 10.2 or greater
  - Validate inputs in custom apps

# Escalation of Privileges Attacks

- **Bad guy is able to upgrade his privileges**
  - In ArcGIS Server
  - In your domain
- **Recommendations**
  - Using enterprise groups (not built-in groups)
  - 10.2+, use admin API to list admins/publishers to detect changes

# Checking Privileges



Navigation Path

Home > security > roles > getRolesByPrivilege

Check to see which roles have administer privilege

Uh oh!

# Denial-of-Service Attacks

- **Bad guy is able to shut your ArcGIS Server down by sending lots of requests**
- **Most attacks observed in wild are still through low-level network protocols**
- **Recommendations**
  - **Secure services**
  - **Set wait and usage time outs**



# Setting Time-outs

ArcGIS Server Manager

Services Site Security Logs

Manage Services OGC Services KML Network Links Sharing

Editing: [Site \(root\)](#) > SampleWorldCities [Help](#) [Save and Restart](#) [Cancel](#)

General  
Parameters  
Capabilities  
**Pooling**  
Processes  
Caching  
Item Description

**Specify Number of Instances**

Minimum number of instances per machine:

Maximum number of instances per machine:

**Specify Service Timeouts**

The maximum time a client can use a service:  seconds

The maximum time a client will wait to get a service:  seconds

The maximum time an idle instance can be kept running:  seconds

# Summary

- **Secure your services**
  - Can use your organization's logins
  - Can use your organization's groups
- **Protecting yourself from attack**
  - Attacks are becoming the norm, not the exception
  - Esri working harder, smarter to protect you
  - Upgrade, don't be scared of minor releases
  - Educate yourself – read doc, attend these sessions

# Survey

- <http://www.esri.com/events/devsummit/session-rater>
- Enter: “Securing ArcGIS for Server”
- 10 seconds
- Comments really welcome

**FYI: Slides for this presentation are available at:**

[\*\*http://1drv.ms/1fnkpTK\*\*](http://1drv.ms/1fnkpTK)



Understanding our world.