

Federal GIS Conference 2014

February 10–11, 2014 | Washington DC



Securing ArcGIS Services

James Cardona

Agenda

- Security in the context of ArcGIS for Server
- Background concepts
- Access
- Securing web services
- Encryption
- Authentication
- 10.2: Understanding standardized queries
- Summary



How to configure

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

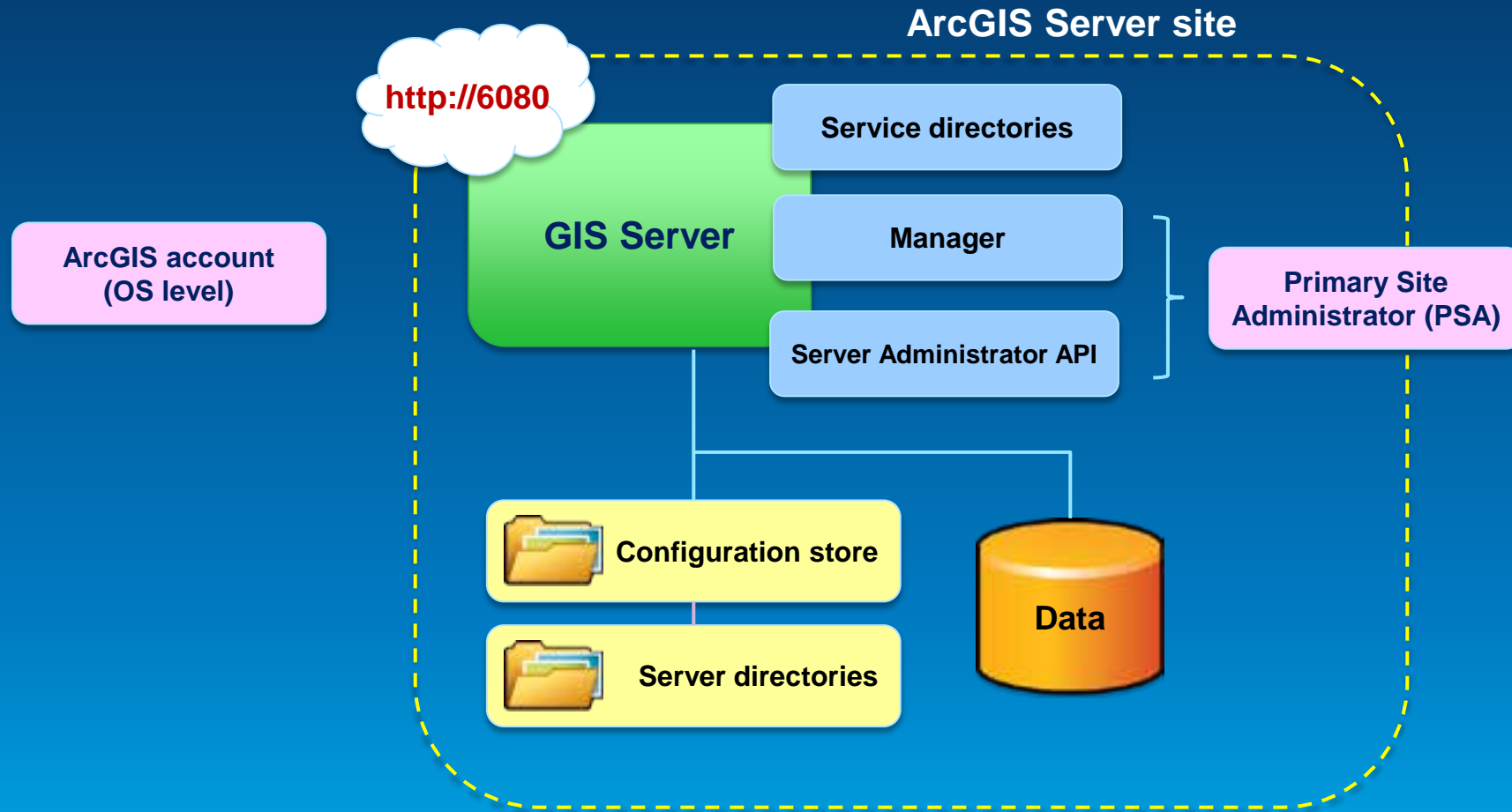
ArcGIS Server Help Documentation Security Links

[Server for Linux Security Help](#)

[Server for Windows Security Help](#)



ArcGIS for Server 10.2 Architecture



Limit “Run As” account to minimal privileges

Windows

- Access to data / software
- Run as service
- No administrative privileges
- Does not need “Allow log on locally”

Linux

- Upgrade to 10.1+, root not needed
- Access to data / software
- No administrative access.

Limit ArcGIS Server file access

- Lock down ArcGIS Server directories.

Config-store

- Run As
- GIS Admins

Directories

- Run As

Install Directory

- Run As
- GIS Admins

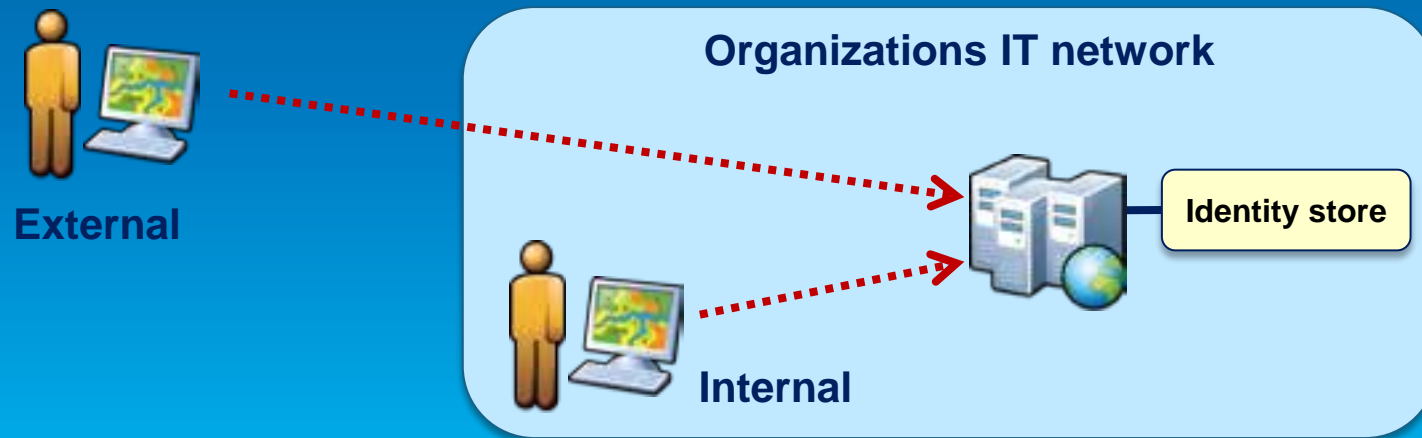
ArcGIS for Server Access

- **User** – Valid login to access Server site
- **Role** – Grouping of users
 - 3 types
 1. Administrators – Full admin control
 2. Publishers – Publish web services
 3. Users – View web services
- **Identity store** – Defines your users and roles



ArcGIS for Server: User considerations

- Where are you users coming from?
 - Determines which type of identity store you should use
- Intranet = Windows Active Directory or LDAP
- Internet = 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, or
 - Managed by my organization's IT Dept
- May affect where you define your 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

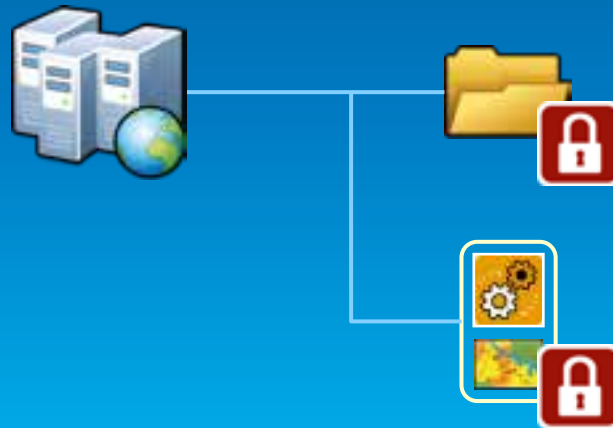
Demo

ArcGIS Server Manager
Show users and roles



Securing GIS Web Services

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



Considerations for Server Publishers

- **Publisher considerations**
 - **Limit web service capabilities**
 - **Ownership-based access control for web editing**
 - **Dynamic workspaces**

Documentation links

- [Configuring services help](#)
- [Ownership based access control help](#)
- [Dynamic layers and workspaces help](#)



Demo



ArcGIS Server Manager
Show how to secure a service

Show how to set capabilities on a
service

Encryption / HTTPS

- HTTPS encrypts content sent/received.
- HTTPS requires certificates.
 - Statement of identity, statement of trust, public key.

General Details

This certificate has been verified for the following uses:
SSL Server Certificate

Issued To
Common Name (CN) www.amazon.com
Organization (O) Amazon.com, Inc.
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 6B:66:AE:56:5F:D0:3F:7D:1E:2B:C0:BD:4A:F3:3C:66

Issued By
Common Name (CN) VeriSign Class 3 Secure Server CA - G3
Organization (O) VeriSign, Inc.
Organizational Unit (OU) VeriSign Trust Network

Validity
Issued On 5/16/2013
Expires On 5/18/2014

Fingerprints
SHA1 Fingerprint 8B:01:07:3E:AA:6B:27:91:71:8D:15:07:67:CB:9C:D0:9E:A6:13:C2
MD5 Fingerprint 63:7C:DC:3F:E9:FB:5F:F8:22:13:32:20:8A:1C:4E:40

Certificate Fields

Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Subject's Public Key
Extensions

Field Value

Modulus (2048 bits):
b7 5c 95 8f c9 d9 68 5c 2b 64 13 30 b0 8a 82 49
ff 60 ab 07 b7 50 de fd 33 4d a8 cb a0 78 a8 41
bb 83 55 6b e5 41 cc f9 36 41 33 8e 71 7e 22 01
cc ab 07 3c d5 34 15 5f 66 88 66 fe e7 e4 dc 4e
00 37 32 79 a5 11 11 14 b3 3f 1f ec 65 ea f9 c1
3c cb 94 d3 ee 27 a4 46 13 4e 40 a4 e5 a2 35 87
04 ea e8 35 11 38 81 b8 5a e7 5c 95 ec d1 e8 a2
c1 e0 12 b6 68 89 27 07 3a d2 61 d0 9f 71 0d c1

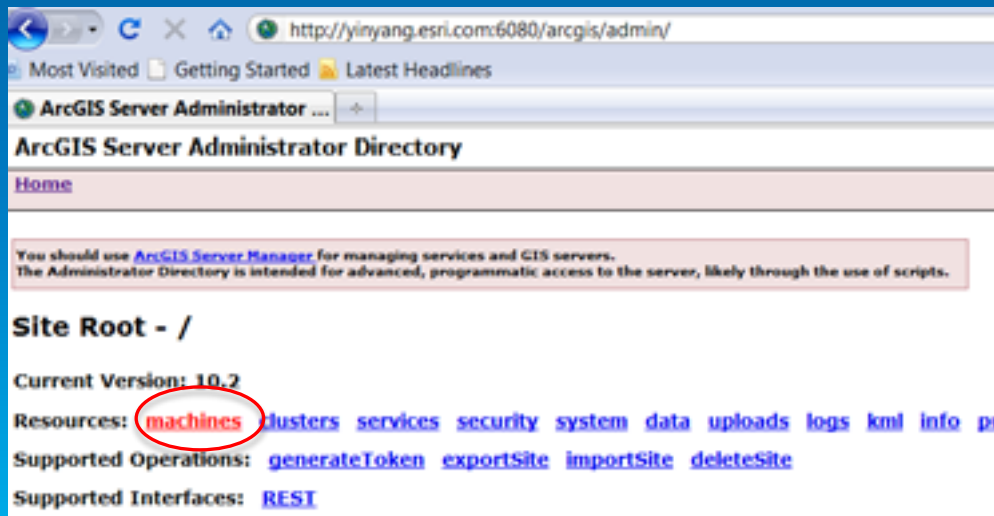
Encryption / HTTPS

- **HTTPS not enabled by default in ArcGIS Server.**
 - Recommend enabling it.
- **ArcGIS Server comes with a self-signed certificate.**
 - Self-signed means that no trusted authority vouches for the server.
 - In many organizations – not a problem, users don't directly access ArcGIS Server.
 - Can replace with a certificate trusted by a certifying authority (CA).

Using a CA-signed certificate

Log into Admin Directory

Click on machines



Using a CA-signed certificate

- Click on the machine you are interested in.
- Click on sslcertificates.



The screenshot displays the ArcGIS Server Administrator Directory interface. The browser title is "Machine - YINYANG.ESRI.COM". The page title is "ArcGIS Server Administrator Directory". The breadcrumb navigation is "Home > machines > YINYANG.ESRI.COM". The main heading is "Machine - YINYANG.ESRI.COM".

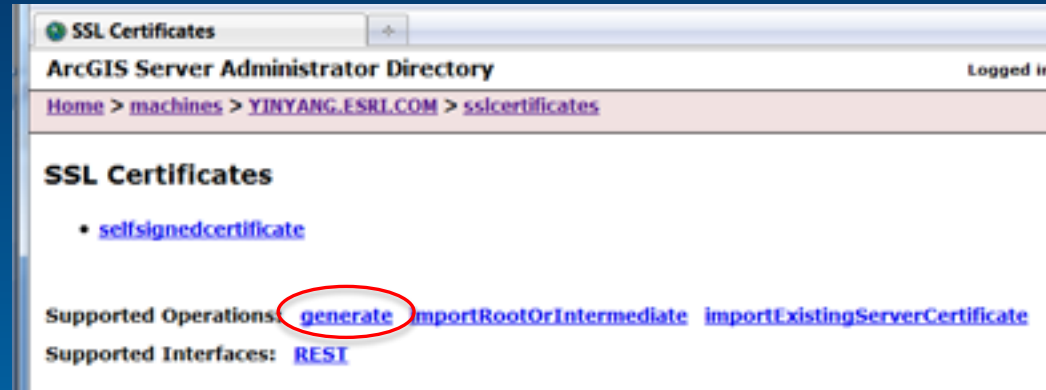
Under the "Server Machine Properties" section, the following details are listed:

Name:	YINYANG.ESRI.COM
Admin URL:	http://yinyang.esri.com:6080/arcgis/admin
Platform:	Linux-amd64-2.6.32.12-0.7-default
Server Start Time:	2013-06-16T01:25:14,96
Web server maximum heap size (in MB):	-1
Web server SSL Enabled :	false
Web server SSL Certificate:	SelfSignedCertificate
App server maximum heap size (in MB):	256
SOC maximum heap size (in MB):	64
Synchronize:	false

Below the properties section is a "+ Ports" section which is currently collapsed.

At the bottom, the "Resources" section includes links for "status", "sslcertificates", "edit", "start", "stop", and "unregister". The "sslcertificates" link is circled in red. The "Supported Interfaces" section lists "REST".

Using a CA-signed certificate



- Can see the automatically generated certificate.
- Operations
 - generate creates a new one
 - importRootOrIntermediate to trust CA's
 - importExistingServerCertificate brings in an existing certificate and the private key (advanced)
- We'll pick generate.

Using a CA-signed certificate

Before

The screenshot shows the 'Operation - generateSelfSignedCertificate' web form. The 'Self Signed Certificate Parameters' section contains the following fields:

Alias:*	<input type="text"/>
Key Algorithm:	RSA
Key Size:	1024
Signature Algorithm:	SHA1withRSA
Common Name:*	YINYANG.ESRI.COM
Organizational Unit:	<input type="text"/>
Organization:*	<input type="text"/>
City or Locality:	<input type="text"/>
State or Province:	<input type="text"/>
Country Code (Two letter Country code ex: US):	<input type="text"/>
Validity (In days):	90
Subject Alternative Name :	<input type="text"/>

At the bottom, the 'Format' dropdown is set to 'HTML' and a 'Generate' button is visible.

After

The screenshot shows the 'Operation - generateSelfSignedCertificate' web form after configuration. The 'Self Signed Certificate Parameters' section contains the following fields:

Alias:*	yinyang.esri.com
Key Algorithm:	RSA
Key Size:	1024
Signature Algorithm:	SHA1withRSA
Common Name:*	YINYANG.ESRI.COM
Organizational Unit:	Development
Organization:*	Esri
City or Locality:	Redlands
State or Province:	California
Country Code (Two letter Country code ex: US):	US
Validity (In days):	730
Subject Alternative Name :	<input type="text"/>

The 'Alias:*' field is circled in red. At the bottom, the 'Format' dropdown is set to 'HTML' and a 'Generate' button is visible.

Using a CA-signed certificate

ArcGIS Server Administrator Directory

Home > machines > YINYANG.ESRI.COM > sslcertificates

SSL Certificates

[yinyang.esri.com](#)
• [selfsignedcertificate](#)

Supported Operations: [generate](#) [importRootOrIntermediate](#) [importExist](#)

Supported Interfaces: [REST](#)

Certificate - yinyang.esri.com

Certificate Information

Alias name: yinyang.esri.com
Creation date: Jul 8, 2013
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: O=Esri, CN=YINYANG.ESRI.COM, OU=Development, L=Redlands, ST=California, C=US
Issuer: O=Esri, CN=YINYANG.ESRI.COM, OU=Development, L=Redlands, ST=California, C=US
Serial number: 229c8658
Valid from: Mon Jul 08 22:19:02 CEST 2013 until: Wed Jul 08 22:19:02 CEST 2015
Certificate fingerprints:
MD5: 86:EC:EE:26:73:84:23:47:B5:31:52:3E:85:C1:46:1B
SHA1: A7:5C:EC:07:61:92:80:B1:E3:85:45:3D:E0:08:B3:DE:A4:83:68:93
SHA256: 4D:d7:9E:B9:30:3D:A1:31:69:C7:63:03:88:15:62:79:BF:81:E0:74:BB:81:DD:AA:EB:DD:02:B2:A7:4D:
Signature algorithm name: SHA1withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 6E 5D 70 71 40 EC 3B 2B BC AB 24 C1 55 F5 DF 73 n]pq@:;+...\$U...s
0010: 7E 80 E1 0E
]
]

Supported Operations: [generateCSR](#) [export](#) [delete](#) [importSignedCertificate](#)

Supported Interfaces: [REST](#)

Import Root Certificate

ArcGIS Server Administrator Directory

Home > machines > YINYANG.ESRI.COM > sslcertificates > yinyang.esri.com

Import Signed Certificate For : yinyang.esri.com

Import CA Certificate

Signed Certificate:

Format: [HTML](#)

Using a CA-signed certificate

ArcGIS Server Administrator Directory
Home > machines > YINYANG.ESRI.COM

Machine - YINYANG.ESRI.COM

Server Machine Properties

Name:	YINYANG.ESRI.COM
Admin URL:	http://yinyang.esri.com:6080/arcgis/admin
Platform:	Linux-amd64-2.6.32.12-0.7-default
Server Start Time:	2013-06-16T01:25:14,96
Web server maximum heap size (in MB):	-1
Web server SSL Enabled :	false
Web server SSL Certificate:	SelfSignedCertificate
App server maximum heap size (in MB):	256
SOC maximum heap size (in MB):	64
Synchronize:	false

+ Ports

Resources: [status](#) [sslcertificates](#)

Supported Operations: [edit](#) [start](#) [stop](#) [unregister](#)

Supported Interfaces: [REST](#)

ArcGIS Server Administrator Directory
Home > machines > YINYANG.ESRI.COM > edit

Operation - edit

Warning
A change in the web server's heap size will cause the web server to be restarted.

Server Machine Properties

Machine name:*	YINYANG.ESRI.COM
Admin URL:*	http://yinyang.esri.com:6080/arcgis/admin
Web server maximum heap size (in MB):	-1
Web server SSL Certificate :	yinyang.esri.com
App server maximum heap size (in MB):	256
SOC maximum heap size (in MB):	64

Ports

JMXPort:	4000
OpenEJBPort:	4001
NamingPort:	4002
DerbyPort:	4003

Format: HTML

Save Edits

Demo

Enabling HTTPS

ArcGIS Server Administrator Directory

Home > security > config

Security/Config

Security Configuration

Protocol:	HTTP Only
Security for virtual directories enabled:	True
Authentication tier:	WEB_ADAPTER
Authentication mode:	WEB_ADAPTER_AUTHENTICATION
Web adaptor shared secret:	Your secret will expire yearly ago

User Store Configuration

Type:	WINDOWS
adminUserPassword:	ll/1shgpyk/
adminUser:	asworld/admin

Role Store Configuration

Type:	WINDOWS
adminUserPassword:	ll/1shgpyk/
adminUser:	asworld/admin

Supported Operations: [HTTPS](#) [UPDATE](#)

Supported Interfaces: [HTTPS](#)

ArcGIS Server Administrator Directory

Home > security > config > update

Operation - update

Warning
Changing Protocol will cause the web server to be restarted.

Security Configuration

Protocol:	HTTPS Only
Virtual directories security enabled:	<input type="checkbox"/>
Authentication tier:	WEB_ADAPTER
Web adaptor shared secret:	Your secret will expire yearly ago

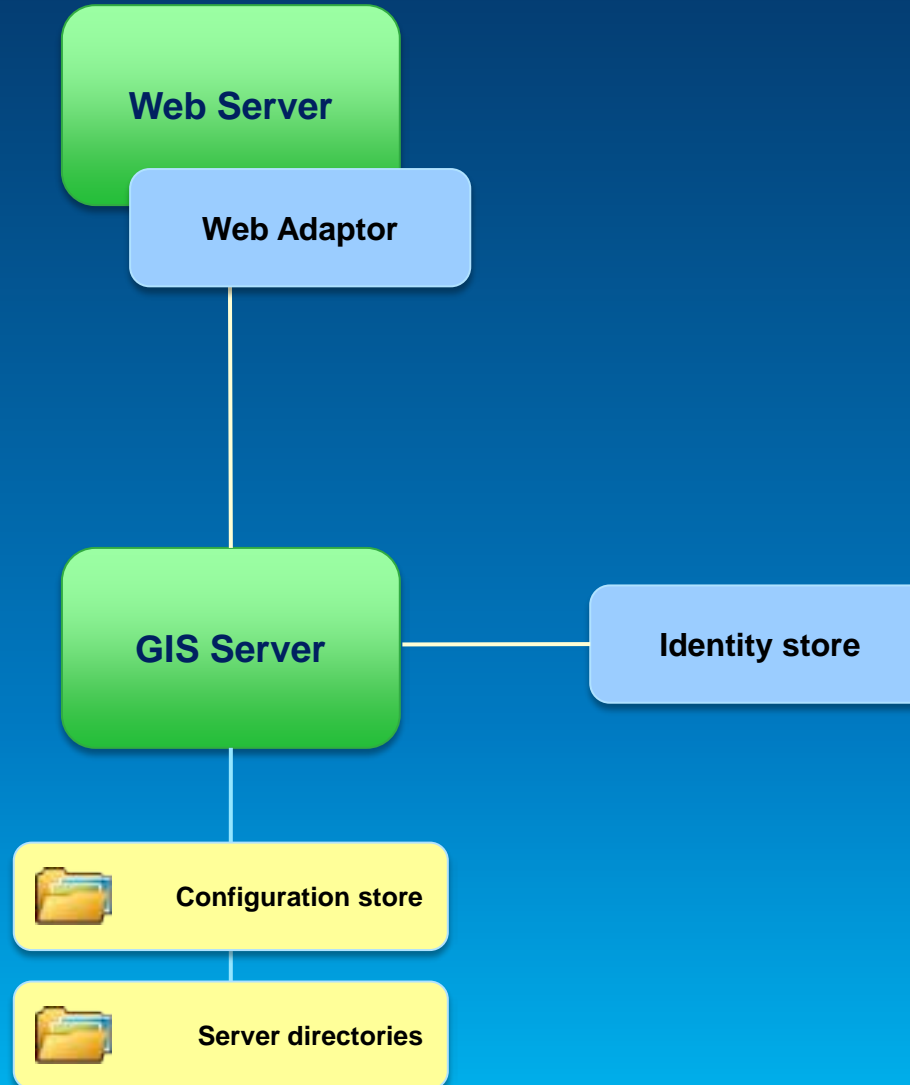
Authentication Tier / Method

- **Authentication**
 - Check and verify user identity
- **2 options**
 1. **GIS Tier**
 - Uses tokens to authenticate
 2. **Web Tier**
 - **Uses HTTP Authentication**
 - Basic, Digest, Integrated Windows, Client certificates, Custom



Server Architecture - Security

- ArcGIS Server site
- + Identity store
- + 3rd party web server
- + Web Adaptor



ArcGIS for Server – Web Adaptor

- Enables Server to work with 3rd party web server
- Leverage web server features
- Provides more flexibility to control site access
- Conceptually like a reverse proxy

Documentation links

- [About ArcGIS Web Adaptor](#)

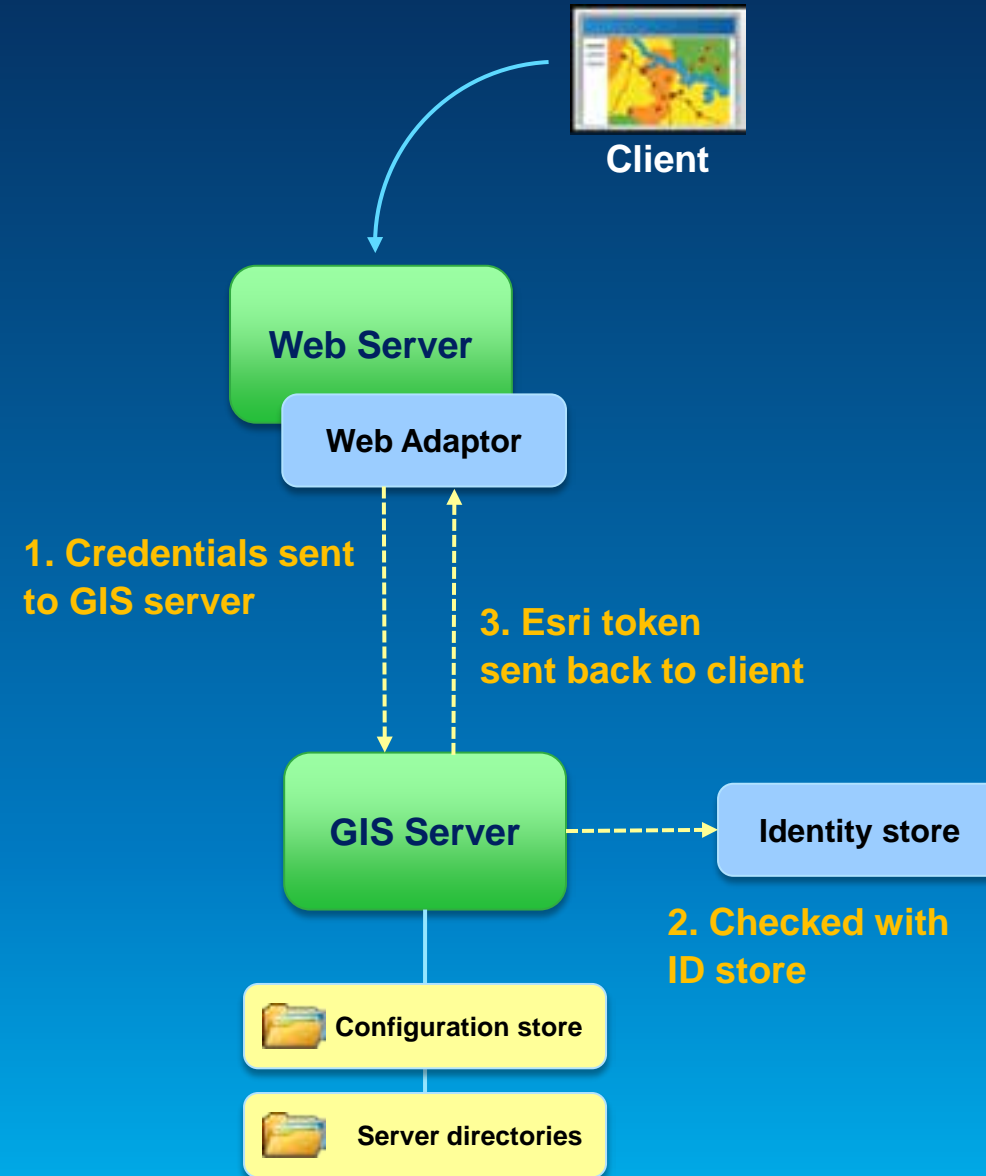


GIS Tier Authentication

- GIS Server checks credentials
- **Token**
 - Unique identifier sent from Server to client to identify an interaction session

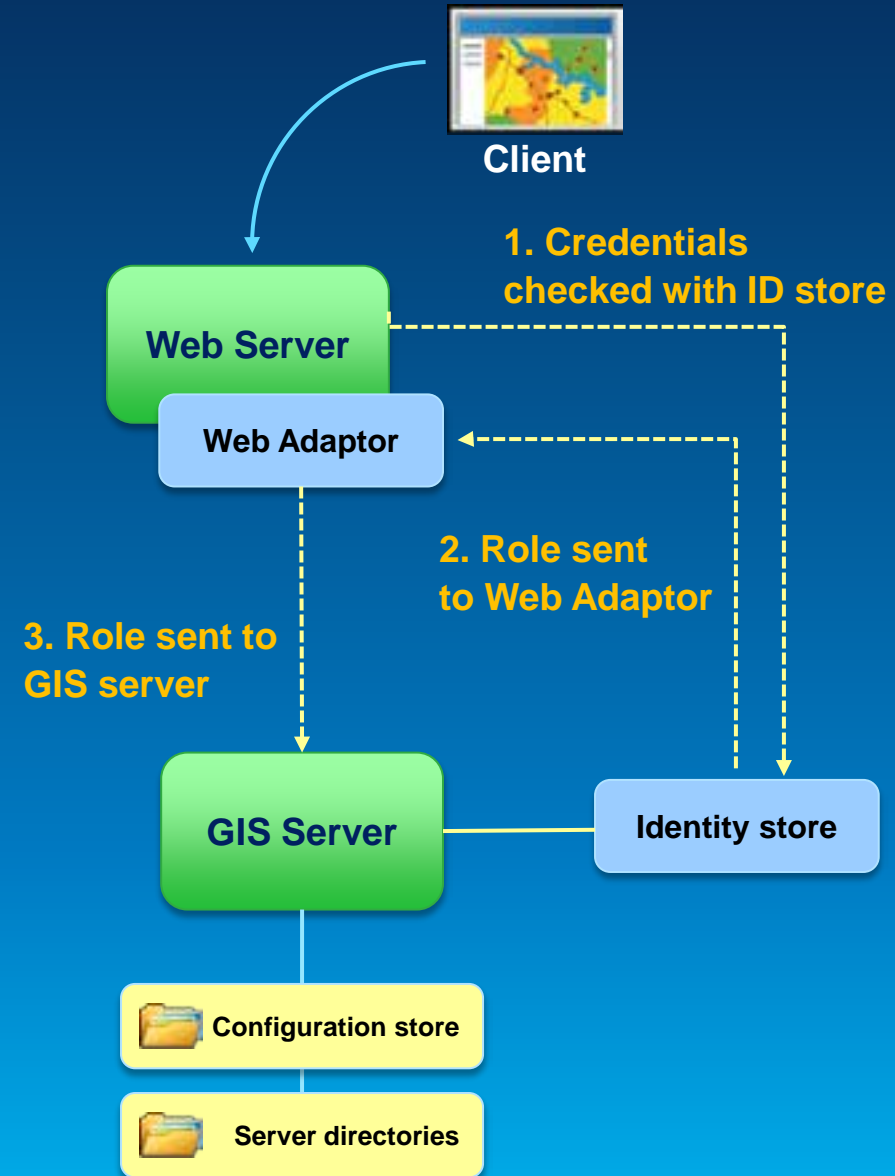
Documentation links

- [About ArcGIS Server Tokens](#)



Web Tier Authentication

- Must use Web Adaptor
- HTTP authentication



GIS Tier vs. Web Tier Authentication

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

Demo

ArcGIS Server Manager
Set up authentication in wizard

Show IIS configuration of
Web Adaptor



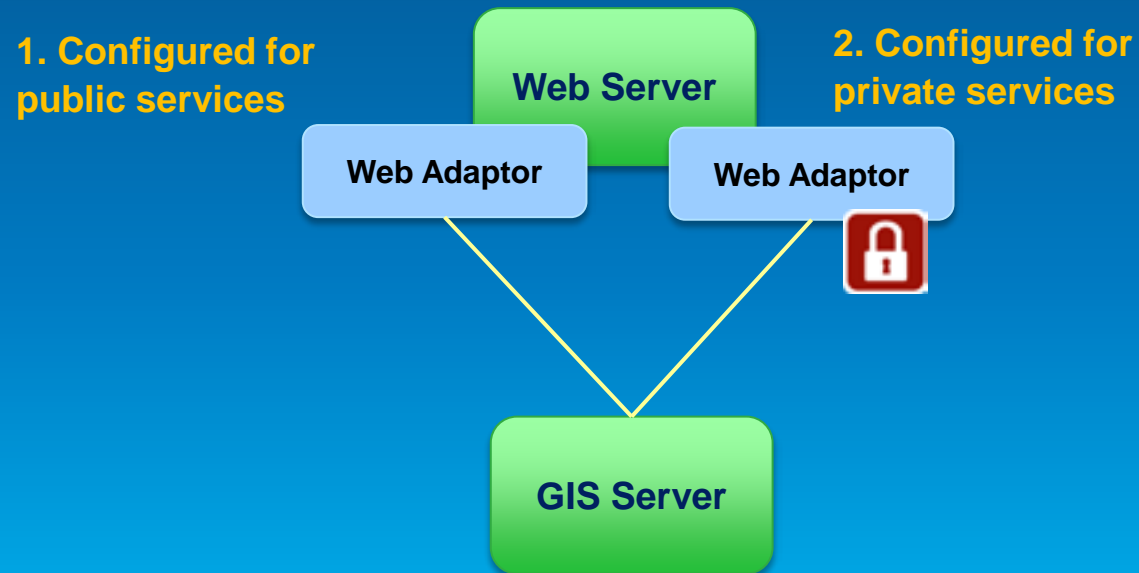
Supporting Public and Private Services

- How do I access public (anonymous) services?
- Web Server blocks me



Supporting Public and Private Services

- Use Web tier authentication
- Configure 2 Web Adaptors for the Server site



Standardized queries

- **Prior to 10.2, query syntax unique for each database**
- **Led to two problems**
 - **Software passes through queries directly to database scanning for malicious attacks. Hard to prevent many creative SQL injection attacks.**
 - **Hard for developers to write query code.**

Standardized queries

- **10.2 introduces standardized queries**
 - Same syntax against all databases (FGDB syntax)
 - Each query parsed and prepared before sending to the database.
 - Stronger defense against SQL injection attacks.
 - Easier to write queries.

Standardized queries

- This could be a breaking change for custom applications.
- Things likely to break:
 - Date queries
 - Using non-SQL standard functions specific to a database
 - Putting non-where-clause syntax into where clause (such as group by).

Standardized queries

- **What can you do if things break?**
 - **Recommended: update your applications to use new syntax.**
 - **Disable standardized queries. Not recommended for security reasons. Puts your Server at risk.**

Further Recommendations

Disable the
primary site
administrator

- Prevents backdoor attacks

Disable services
directory

- Prevents XSS attacks

Block Admin Calls
on web adaptor

- Limits attack vectors



Questions



Understanding our world.