esri

THE
SCIENCE
OF
WHERE

ArcGIS Enterprise Security: Advanced

Gregory Ponto & Jeff Smith

Agenda

- Focus: Security best practices for ArcGIS Enterprise

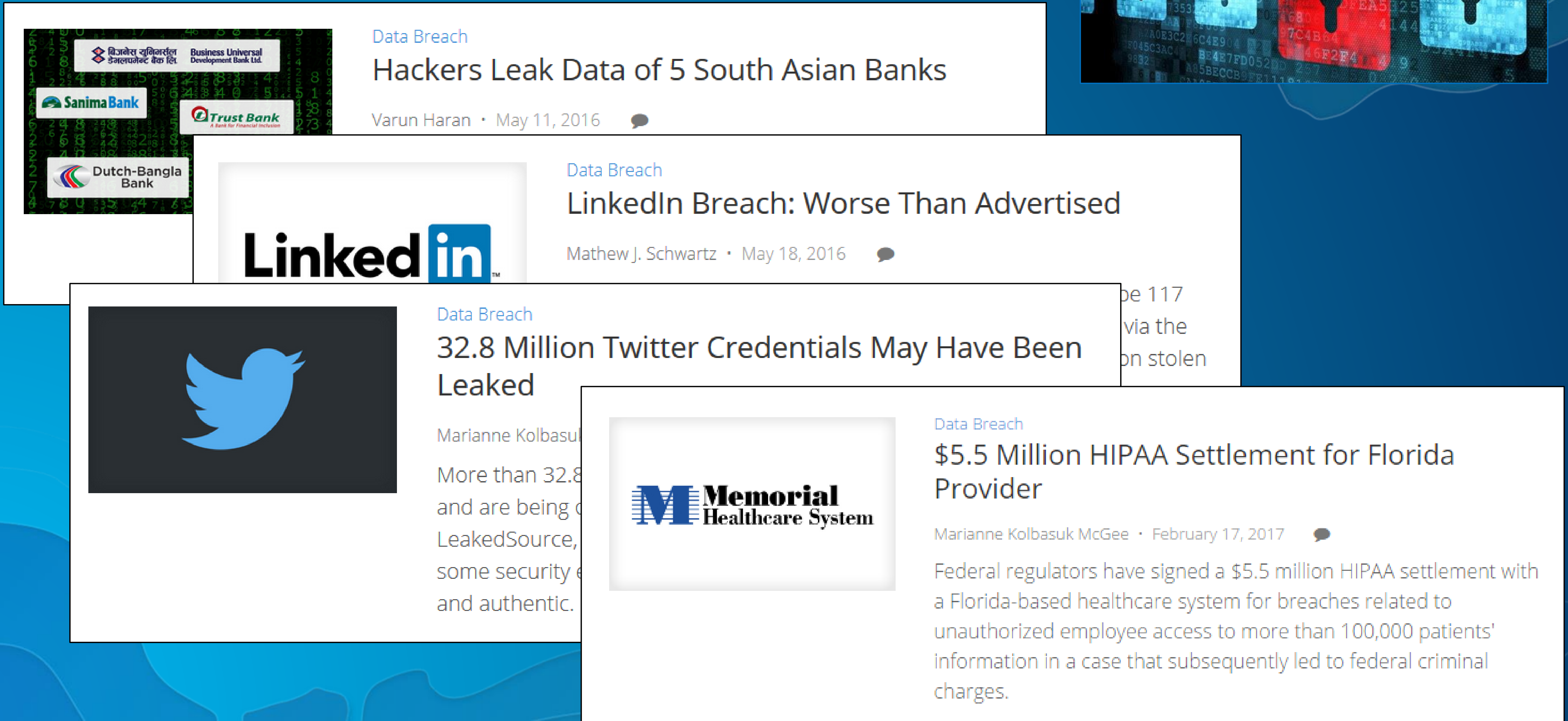
- ArcGIS Server
- Portal for ArcGIS
- 10.5.x Features

Strongly Recommend:

Knowledge of ArcGIS Server and Portal for ArcGIS

Security is Important

http://www.databreachtoday.com/news



Data Breach

Hackers Leak Data of 5 South Asian Banks

Varun Haran • May 11, 2016

बिजनेस युनिभर्सल डेभलपमेन्ट बैंक लि.
Business Universal Development Bank Ltd.
Sanima Bank
Trust Bank
A Bank for Financial Inclusion
Dutch-Bangla Bank

Data Breach

LinkedIn Breach: Worse Than Advertised

Mathew J. Schwartz • May 18, 2016

be 117
via the
on stolen

Data Breach

32.8 Million Twitter Credentials May Have Been Leaked

Marianne Kolbasu

More than 32.8
and are being
LeakedSource,
some security
and authentic.

Data Breach

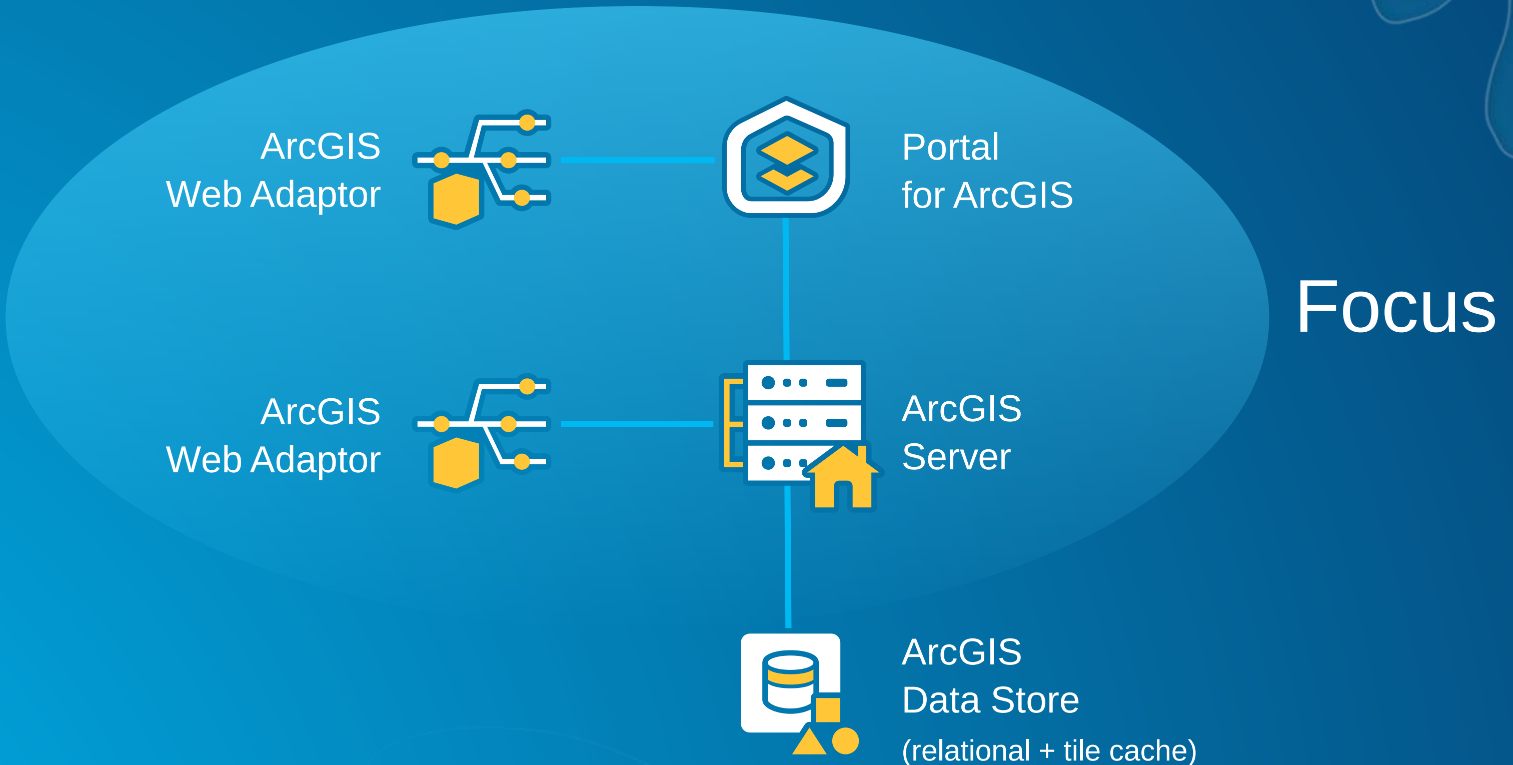
$5.5 Million HIPAA Settlement for Florida Provider

Marianne Kolbasuk McGee • February 17, 2017

Federal regulators have signed a $5.5 million HIPAA settlement with a Florida-based healthcare system for breaches related to unauthorized employee access to more than 100,000 patients' information in a case that subsequently led to federal criminal charges.

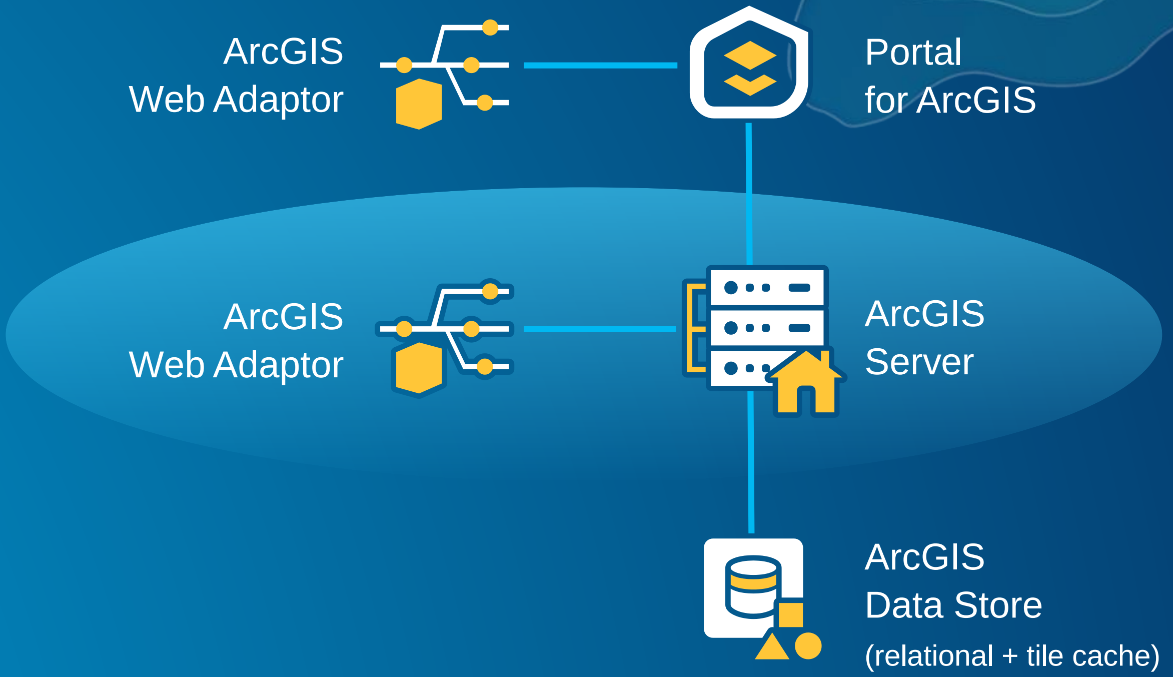
ArcGIS Enterprise

Logical Architecture



Agenda

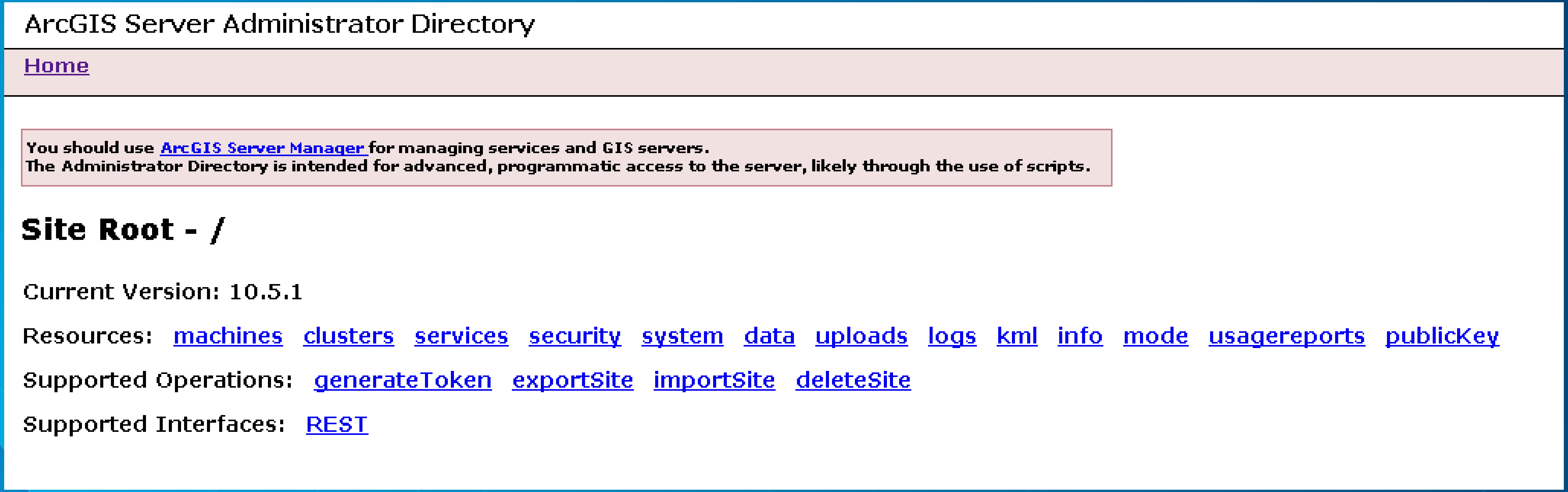
- GIS Server
  - Enable and use HTTPS
  - Disable services directory
  - Restrict cross domain requests
  - Restrict file permissions
  - Disable PSA account
  - Scan Server script
- Portal for ArcGIS
- Advanced options



Review: ArcGIS Server Administrator Directory

`https://localhost:6443/arcgis/admin`

- Web App, provides interface into an ArcGIS Server site
- Many security settings enabled via this interface



ArcGIS Server Administrator Directory

Home

You should use ArcGIS Server Manager for managing services and GIS servers.
The Administrator Directory is intended for advanced, programmatic access to the server, likely through the use of scripts.

Site Root - /

Current Version: 10.5.1

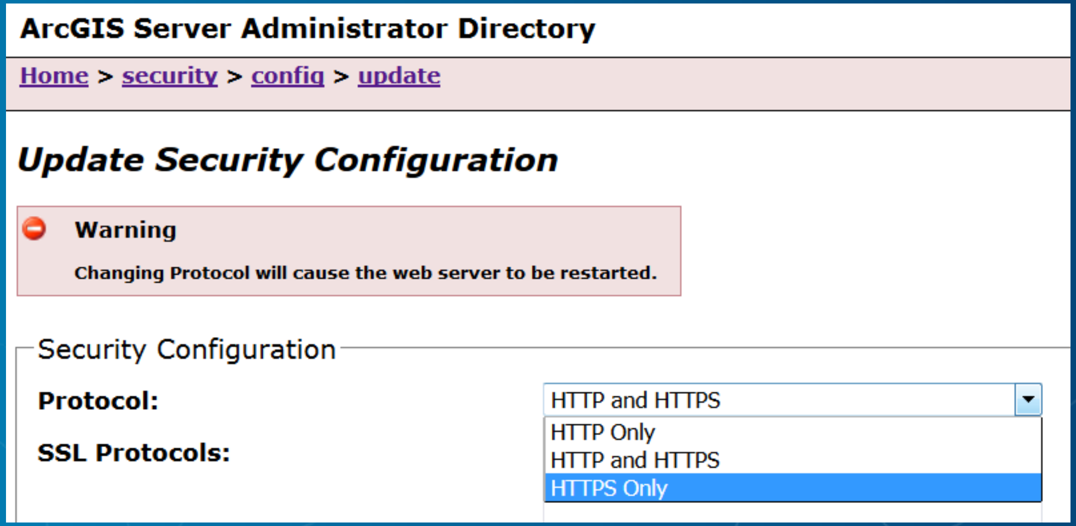
Resources: machines clusters services security system data uploads logs kml info mode usagereports publicKey

Supported Operations: generateToken exportSite importSite deleteSite

Supported Interfaces: REST

Enable and Use HTTPS

- HTTPS – *Hypertext Transfer Protocol Secure*
- Initial step in creating a secure environment should always be to encrypt traffic
- Protects against a simple network sniffer
- Enabled by default in 10.4+
- Recommended to restrict to HTTPS only if possible
- ArcGIS Server Admin Directory
  - `Security > config > update`



ArcGIS Server Administrator Directory

Home > security > config > update

Update Security Configuration

Warning

Changing Protocol will cause the web server to be restarted.

Security Configuration

Protocol: HTTP and HTTPS

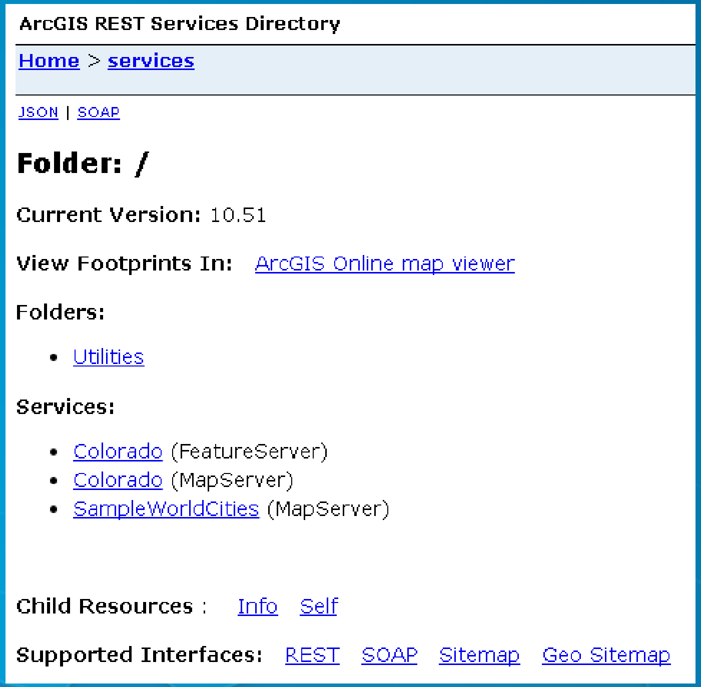
SSL Protocols:

Disable the Services Directory

- ArcGIS Services Directory exposes GIS web services
  - http://localhost/ArcGIS/rest
- Recommend to NOT expose GIS web services on Production Servers

REST

Before



ArcGIS REST Services Directory

Home > services

JSON | SOAP

Folder: /

Current Version: 10.51

View Footprints In: ArcGIS Online map viewer

Folders:

- Utilities

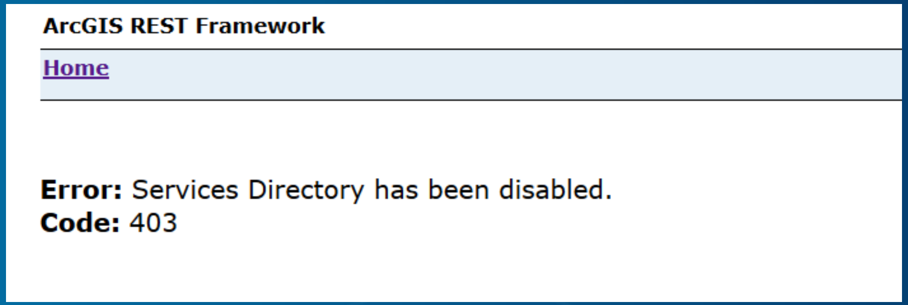
Services:

- Colorado (FeatureServer)
- Colorado (MapServer)
- SampleWorldCities (MapServer)

Child Resources : Info Self

Supported Interfaces: REST SOAP Sitemap Geo Sitemap

After



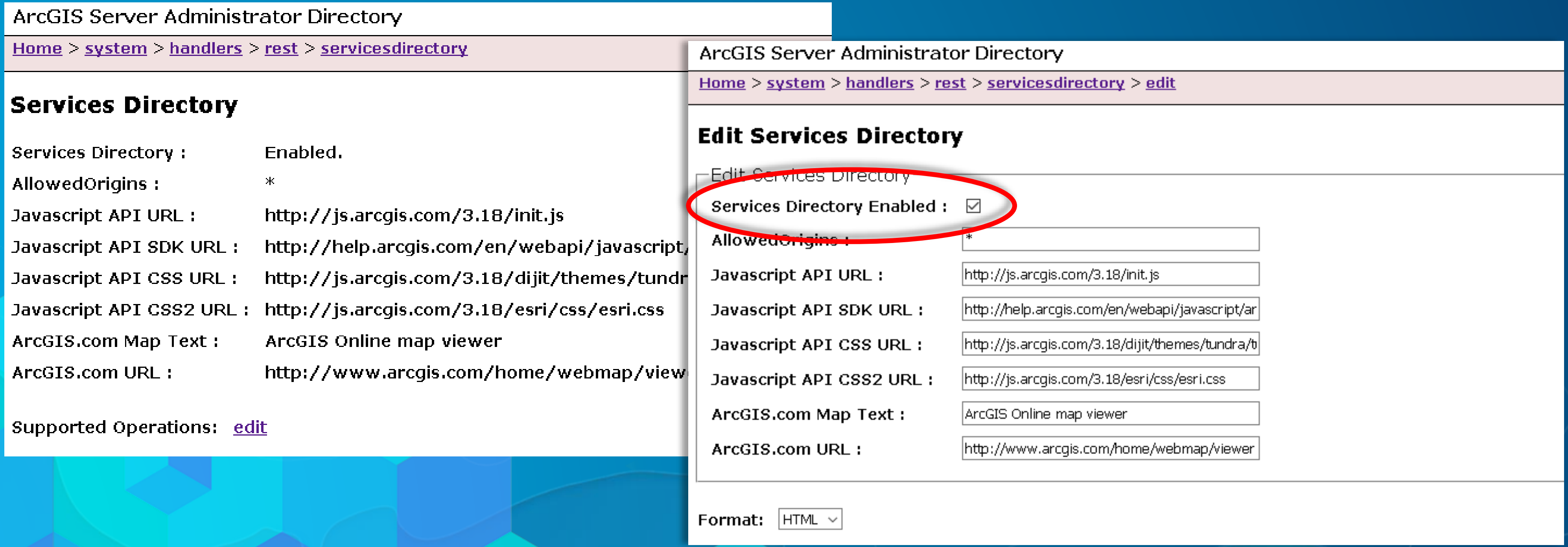
ArcGIS REST Framework

Home

Error: Services Directory has been disabled.
Code: 403

How to Disable the Services Directory

- Server Administrator Directory
  - `System > Handlers > Rest > Servicesdirectory > edit`
  - Uncheck *Services Directory Enabled* option
- Help topic: [Disable the Services Directory]()



ArcGIS Server Administrator Directory

Home > system > handlers > rest > servicesdirectory

Services Directory

Services Directory :	Enabled.
AllowedOrigins :	*
Javascript API URL :	http://js.arcgis.com/3.18/init.js
Javascript API SDK URL :	http://help.arcgis.com/en/webapi/javascript/
Javascript API CSS URL :	http://js.arcgis.com/3.18/dijit/themes/tundr
Javascript API CSS2 URL :	http://js.arcgis.com/3.18/esri/css/esri.css
ArcGIS.com Map Text :	ArcGIS Online map viewer
ArcGIS.com URL :	http://www.arcgis.com/home/webmap/view

Supported Operations: edit

ArcGIS Server Administrator Directory

Home > system > handlers > rest > servicesdirectory > edit

Edit Services Directory

Edit Services Directory

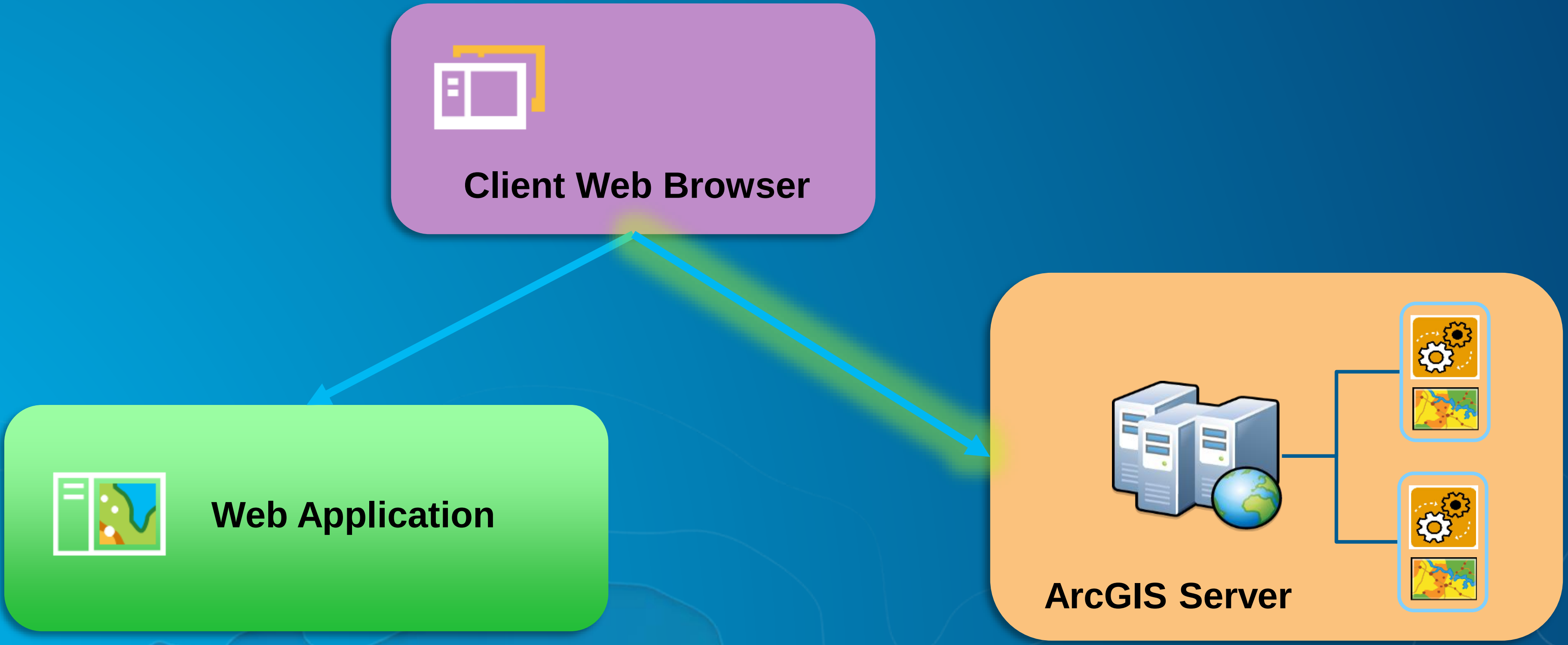
Services Directory Enabled :	☑
AllowedOrigins :	*
Javascript API URL :	http://js.arcgis.com/3.18/init.js
Javascript API SDK URL :	http://help.arcgis.com/en/webapi/javascript/ar
Javascript API CSS URL :	http://js.arcgis.com/3.18/dijit/themes/tundra/t
Javascript API CSS2 URL :	http://js.arcgis.com/3.18/esri/css/esri.css
ArcGIS.com Map Text :	ArcGIS Online map viewer
ArcGIS.com URL :	http://www.arcgis.com/home/webmap/viewer

Format: HTML

Restrict Cross-Domain (CORS) Requests

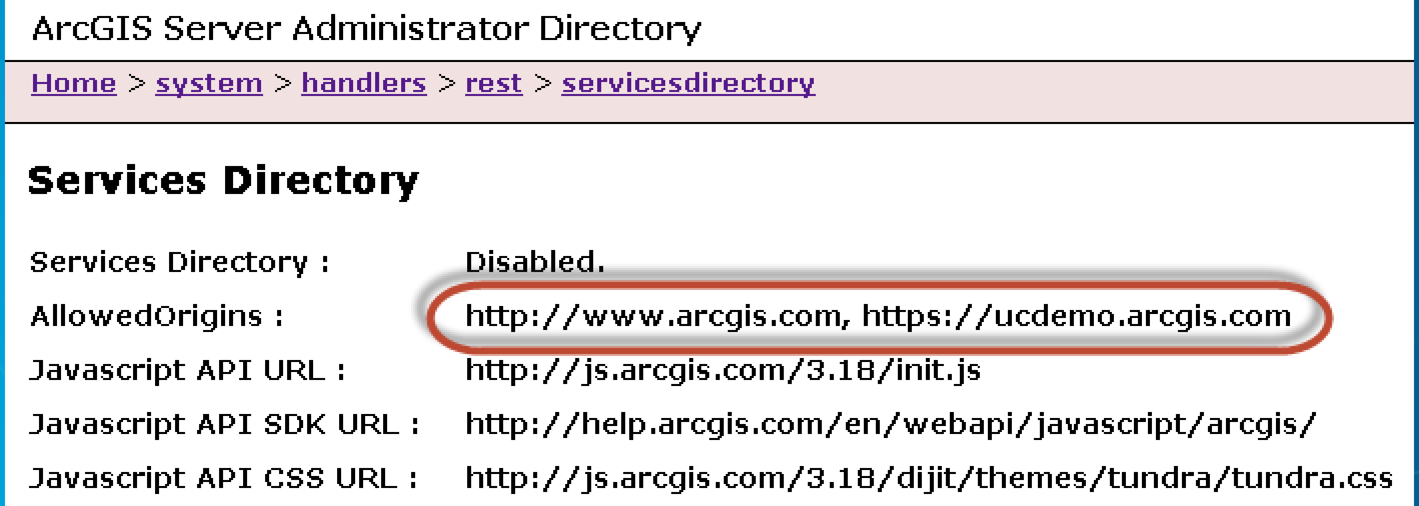
server.arcgis.com > Search “cross-domain requests”

- By default, ArcGIS Server allows cross-domain requests so that client apps can invoke its services from any domain



How to Restrict Cross-Domain Requests

- For JavaScript, a common method used to make cross domain requests is called a CORS request (cross origin resource sharing)
- These can be restricted in the Server Administrator Directory
  - `system > handlers > rest > servicesdirectory > edit`
  - `AllowOrigins` field: specify a comma-separated list of domain names that are allowed to make CORS requests to access your web services



ArcGIS Server Administrator Directory

Home > system > handlers > rest > servicesdirectory

Services Directory

Services Directory :	Disabled.
AllowedOrigins :	http://www.arcgis.com, https://ucdemo.arcgis.com
Javascript API URL :	http://js.arcgis.com/3.18/init.js
Javascript API SDK URL :	http://help.arcgis.com/en/webapi/javascript/arcgis/
Javascript API CSS URL :	http://js.arcgis.com/3.18/dijit/themes/tundra/tundra.css

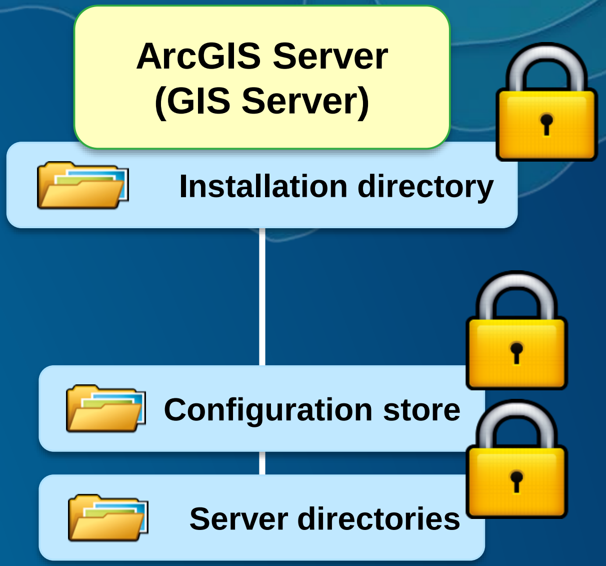
Demo

Restrict Cross-Domain Requests

Restrict File Permissions

- Recommend restrict file and folder permissions on
  - ArcGIS Server installation directory
  - Configuration store
  - Server directories

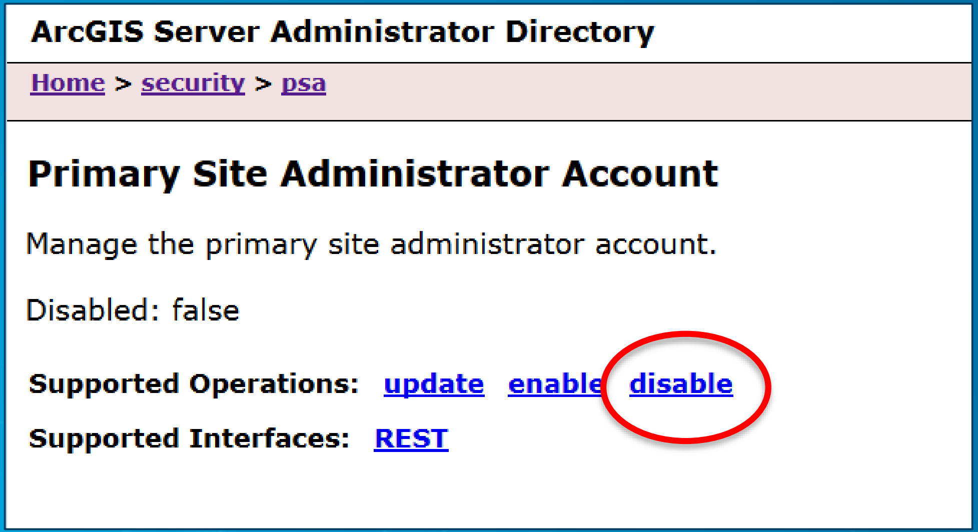
  to the ArcGIS Server account



- Your organization may require that additional accounts have access
  - Warning: Any account with write access to the configuration store can change ArcGIS Server settings

Disable Primary Site Administrator (PSA) Account

- Recommend disable the PSA account to remove an alternate method of administering ArcGIS Server outside of your enterprise users
- Access the Server Administrator Directory
  - `Security > PSA > disable`



ArcGIS Server Administrator Directory

Home > security > psa

Primary Site Administrator Account

Manage the primary site administrator account.

Disabled: false

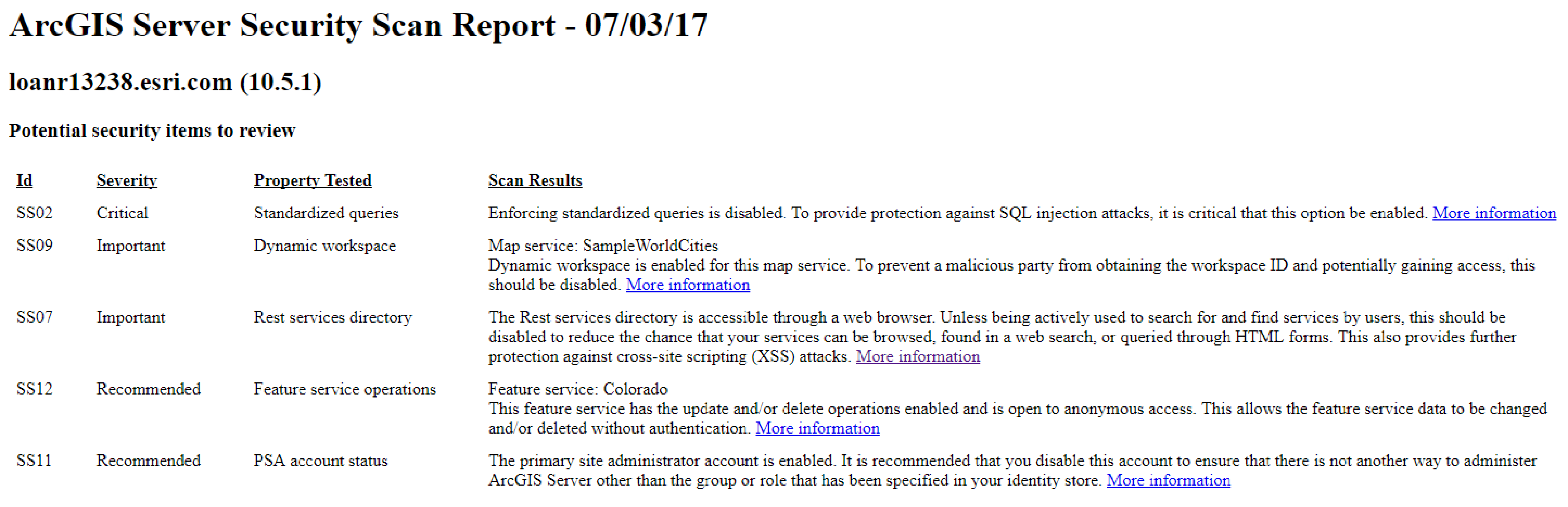
Supported Operations: update enable disable

Supported Interfaces: REST

PSA account

Scan GIS Server for Security Checks

- `serverScan.py` is a script in the Server installation directory
  - Located: `<install directory>\ArcGIS\Server\tools\admin`
- Script checks for security settings → generates a report that makes recommendations to improve security



ArcGIS Server Security Scan Report - 07/03/17

loanr13238.esri.com (10.5.1)

Potential security items to review

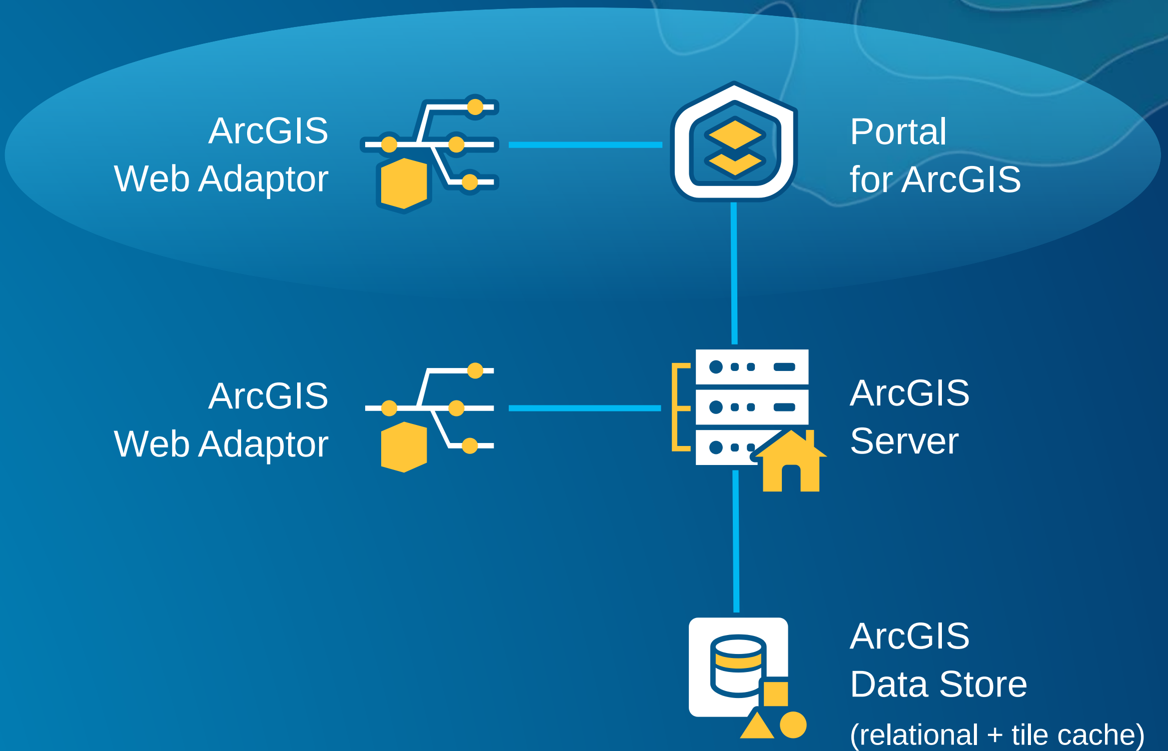
Id	Severity	Property Tested	Scan Results
SS02	Critical	Standardized queries	Enforcing standardized queries is disabled. To provide protection against SQL injection attacks, it is critical that this option be enabled. More information
SS09	Important	Dynamic workspace	Map service: SampleWorldCities Dynamic workspace is enabled for this map service. To prevent a malicious party from obtaining the workspace ID and potentially gaining access, this should be disabled. More information
SS07	Important	Rest services directory	The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks. More information
SS12	Recommended	Feature service operations	Feature service: Colorado This feature service has the update and/or delete operations enabled and is open to anonymous access. This allows the feature service data to be changed and/or deleted without authentication. More information
SS11	Recommended	PSA account status	The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your identity store. More information

Demo

Run *serverScan.py*
Security Check

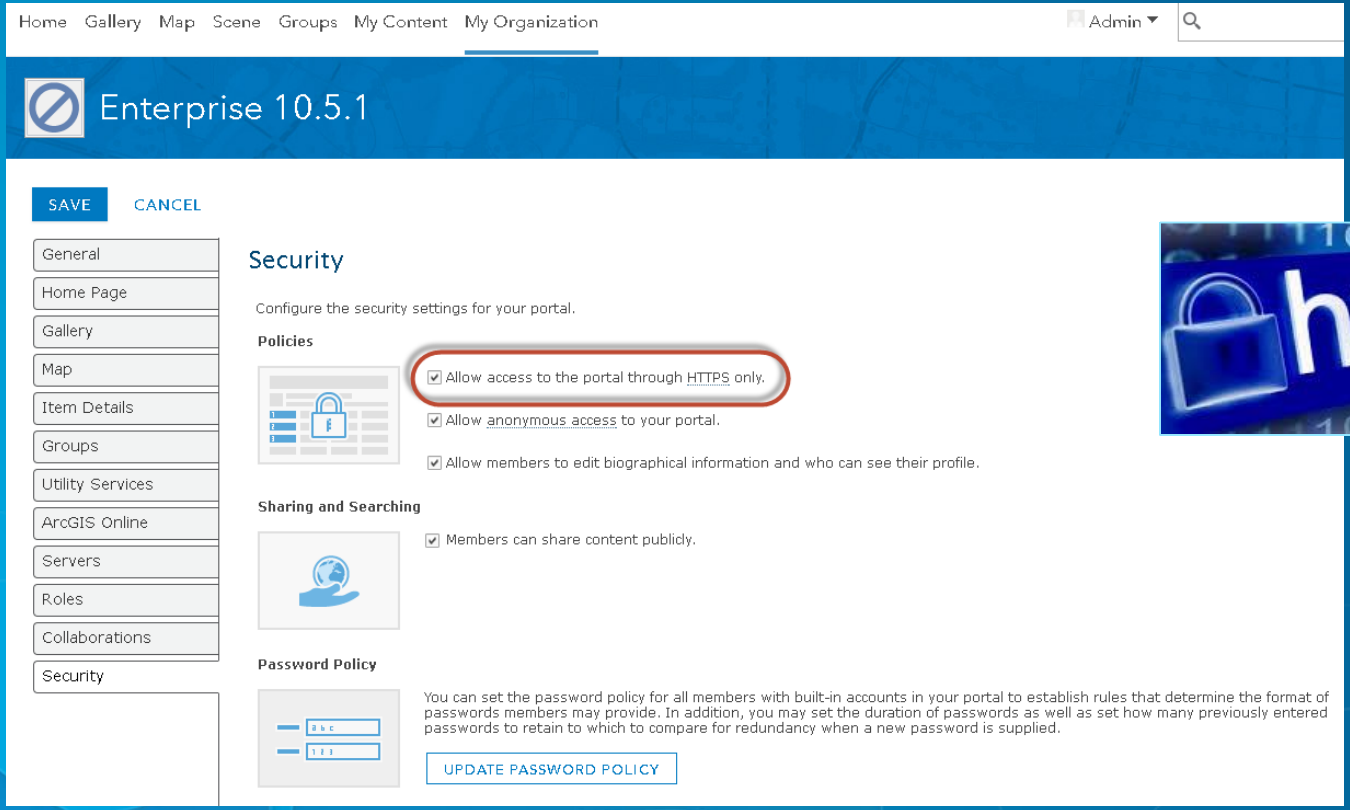
Agenda

- GIS Server
- Portal for ArcGIS
  - Enforce HTTPS Communication only
  - Disable ArcGIS Portal Directory
  - Restrict proxies
  - Disable the 'Create Account'
  - Trusted servers list
  - Scan Portal script
- Advanced options



Enable HTTPS Communication

- Enforce HTTPS so that all communication in your portal is sent using HTTPS
- Configure your portal and the web server hosting ArcGIS Web Adaptor to only allow communication through HTTPS



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.

Sharing and Searching

☑ Members can share content publicly.

Password Policy

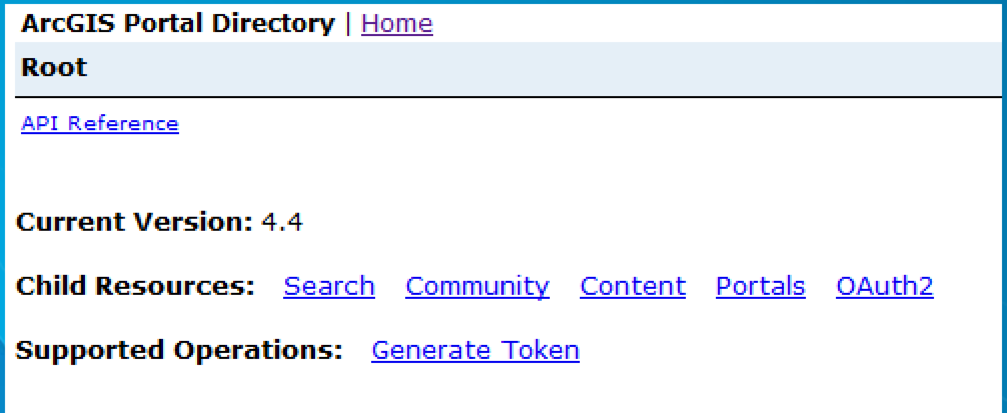
You can set the password policy for all members with built-in accounts in your portal to establish rules that determine the format of passwords members may provide. In addition, you may set the duration of passwords as well as set how many previously entered passwords to retain to which to compare for redundancy when a new password is supplied.

Disable ArcGIS Portal Directory (Production Servers)

`https://<machinename>.domain.com/arcgis/sharing`

- Provides a browsable HTML-based representation of all of Portal items
  - services, web maps, and content
- Recommend disable this to reduce the chance that your items can be browsed, found in a web search, or queried through HTML forms

Before



ArcGIS Portal Directory | Home

Root

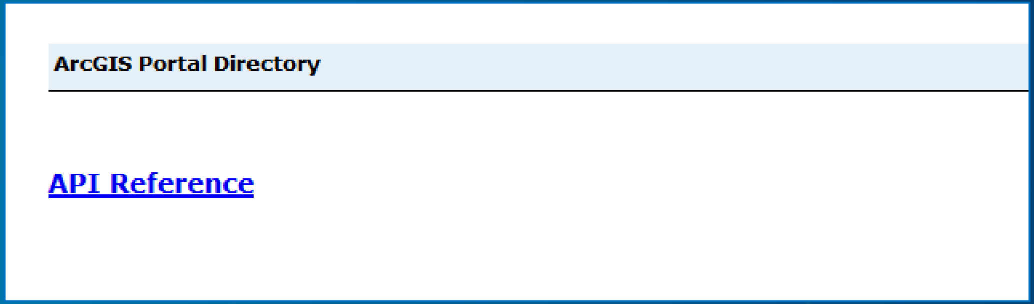
API Reference

Current Version: 4.4

Child Resources: Search Community Content Portals OAuth2

Supported Operations: Generate Token

After

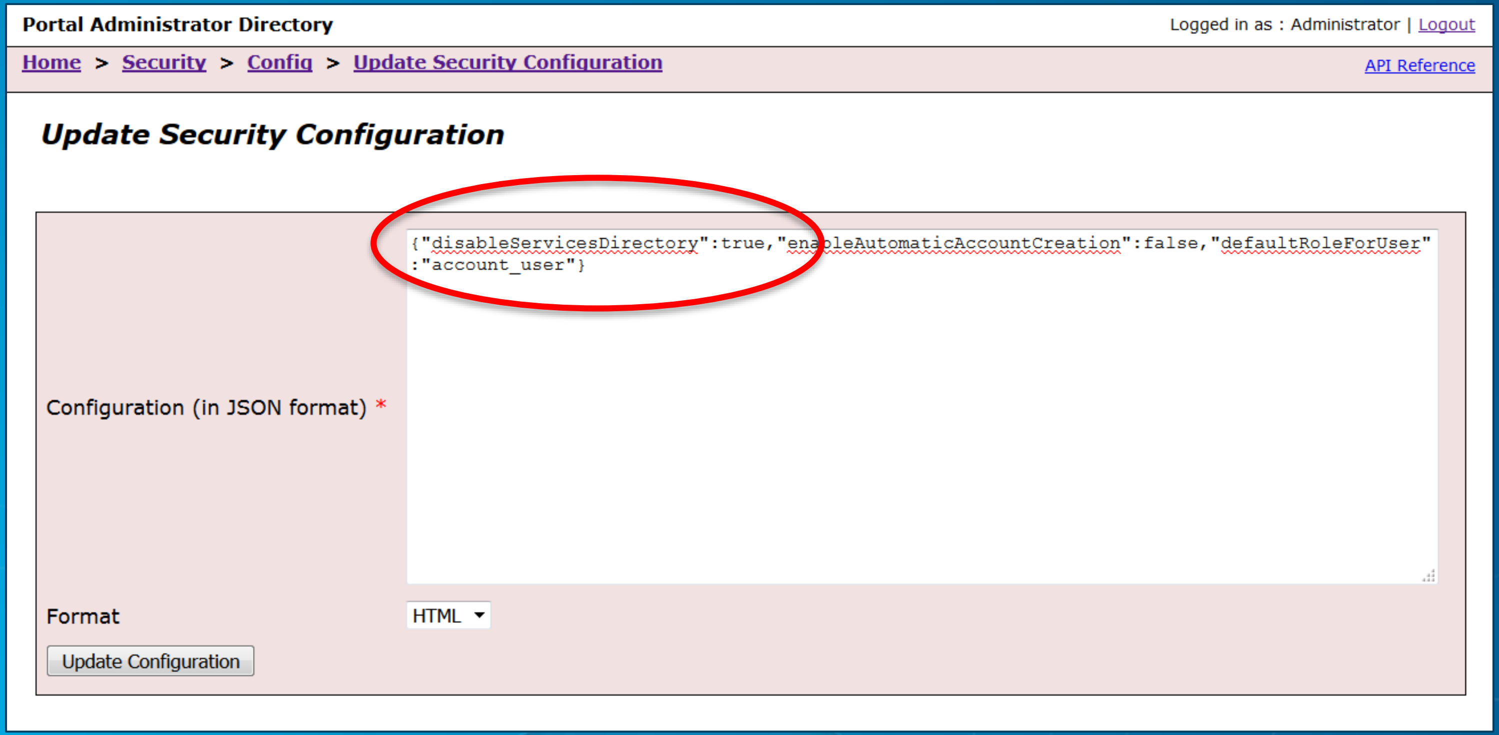


ArcGIS Portal Directory

API Reference

How to Disable ArcGIS Portal Directory

- Access the Portal Administrator Directory
  - `Security > Config > Update Security Configuration`
  - Set property = `'true'`



Portal Administrator Directory

Logged in as : Administrator | Logout

Home > Security > Config > Update Security Configuration

API Reference

Update Security Configuration

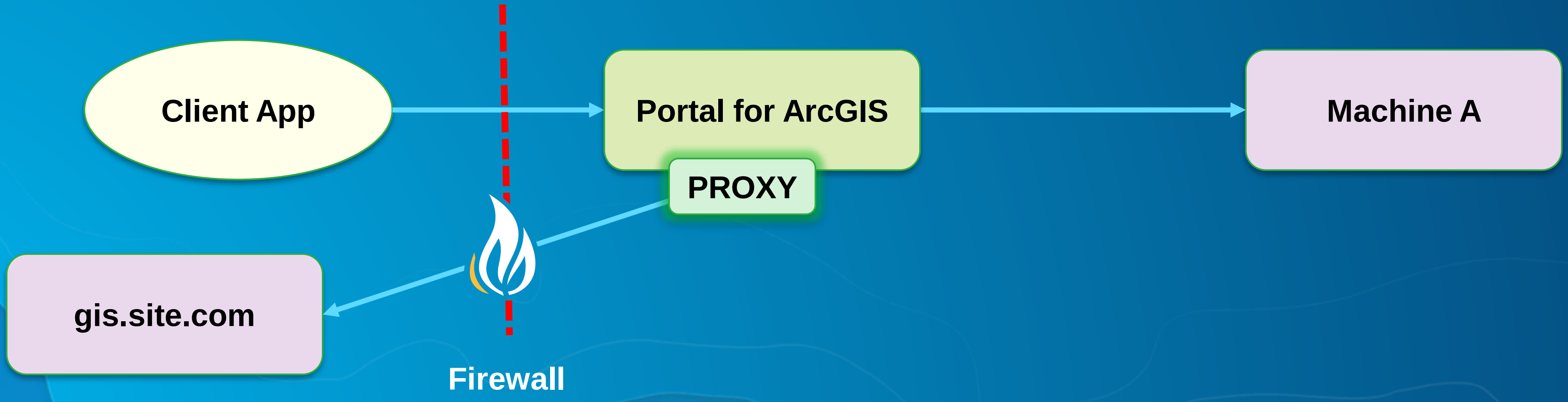
Configuration (in JSON format) *

```
{"disableServicesDirectory":true,"enableAutomaticAccountCreation":false,"defaultRoleForUser"
:"account_user"}
```

Format: HTML

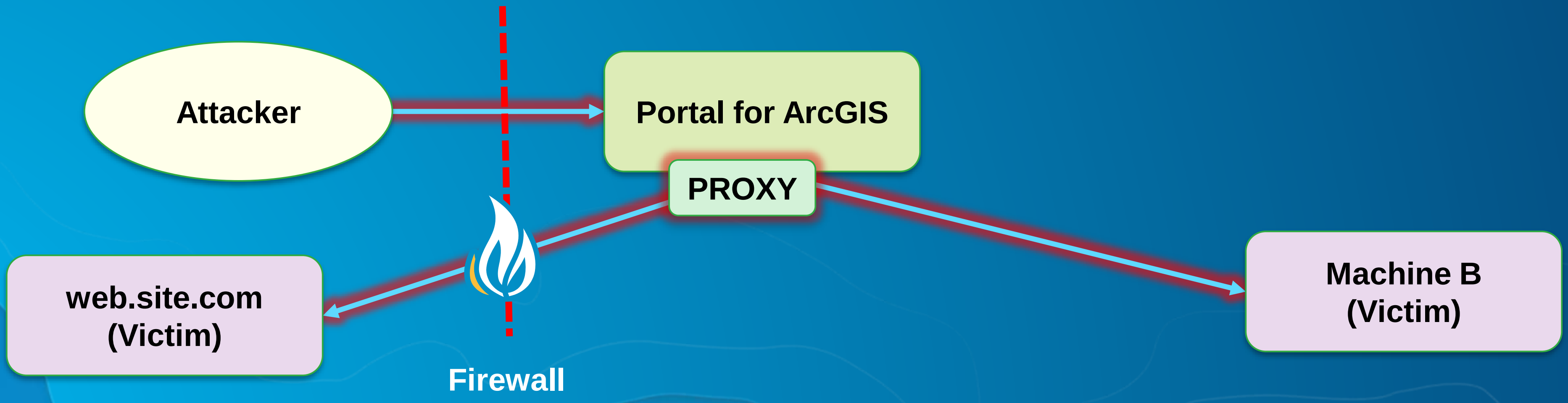
Restrict Proxy Hosts

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on a different machine
  - Storing credentials (Single Sign On)
  - OGC Services
  - Non-CORS Systems



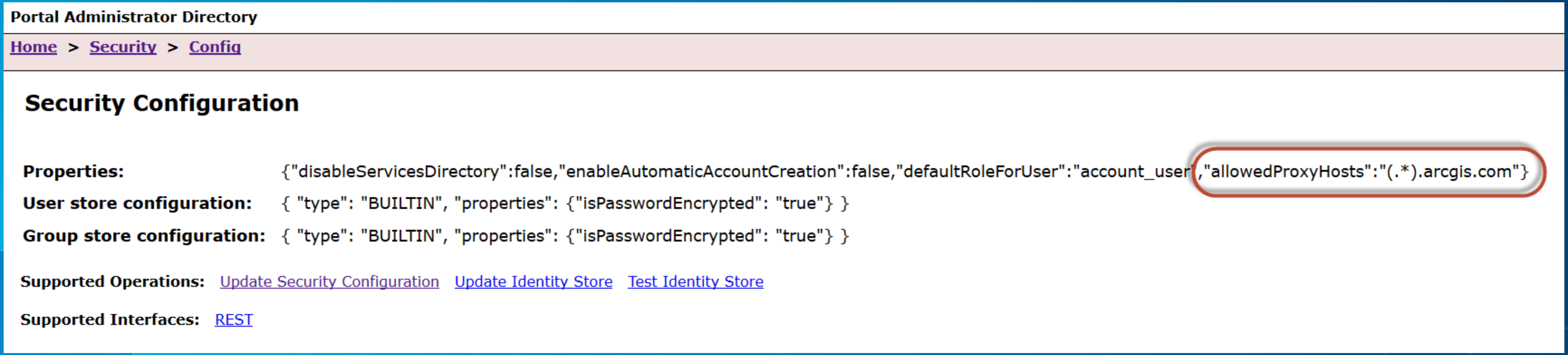
Restrict Proxy Hosts

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on a different machine
- By default the portal's proxy is open
  - Your Portal can be used to launch attacks against internal and external targets



How to Restrict Proxies

- Access the Portal Administrator Directory
  - `Security > Config > Update Security Configuration`
  - For Configuration field, add the `allowedProxyHosts` property and specify the list of approved addresses



Portal Administrator Directory

Home > Security > Config

Security Configuration

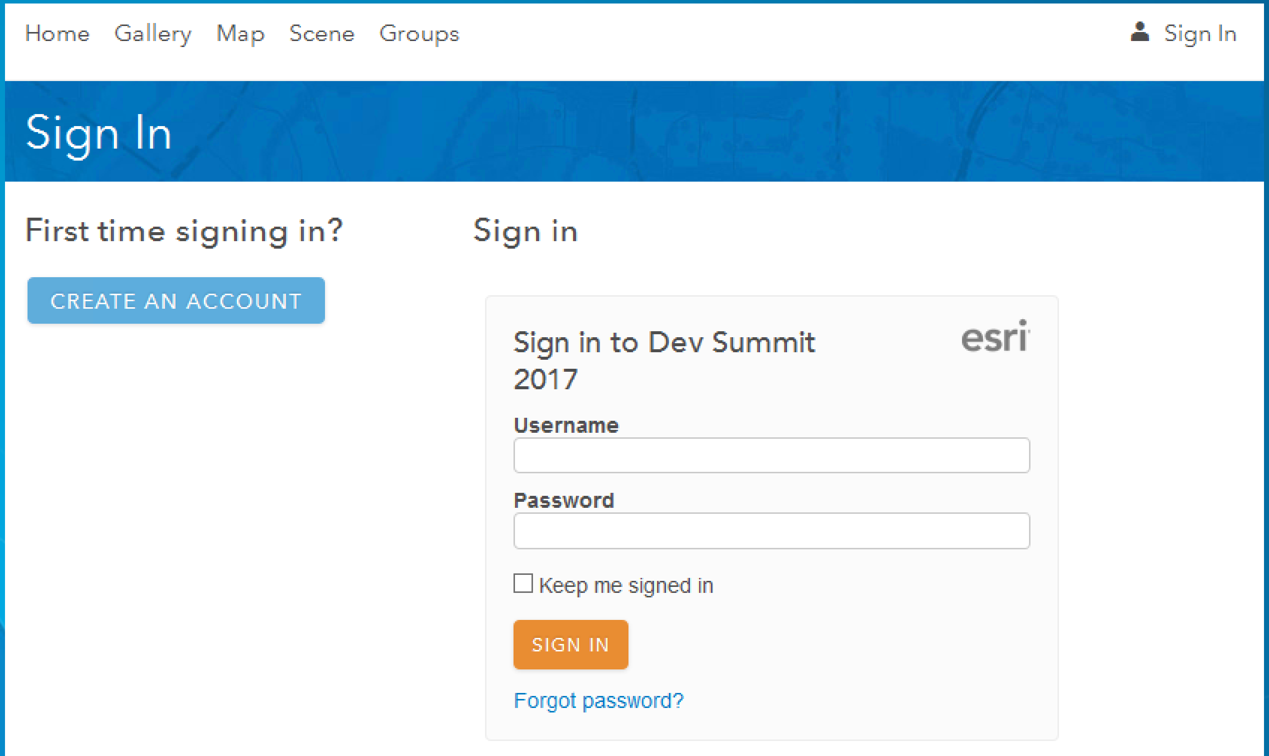
Properties:	{"disableServicesDirectory":false,"enableAutomaticAccountCreation":false,"defaultRoleForUser":"account_user","allowedProxyHosts":"(.*).arcgis.com"}
User store configuration:	{ "type": "BUILTIN", "properties": {"isPasswordEncrypted": "true"} }
Group store configuration:	{ "type": "BUILTIN", "properties": {"isPasswordEncrypted": "true"} }

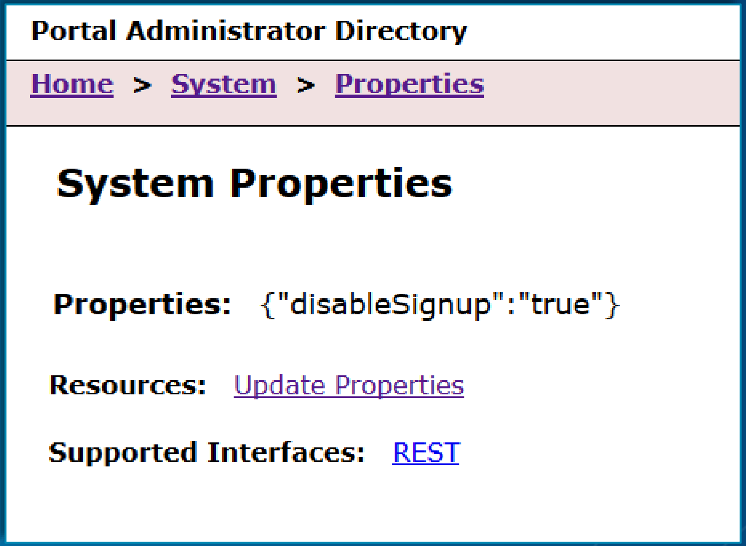
Supported Operations: Update Security Configuration Update Identity Store Test Identity Store

Supported Interfaces: REST

Disable ‘Create Account’ on Login Page

- **Recommend disable ability to create a new Portal account**
- **Access Portal Administrator Directory**
  - `System > Properties`





Portal Administrator Directory

Home > System > Properties

System Properties

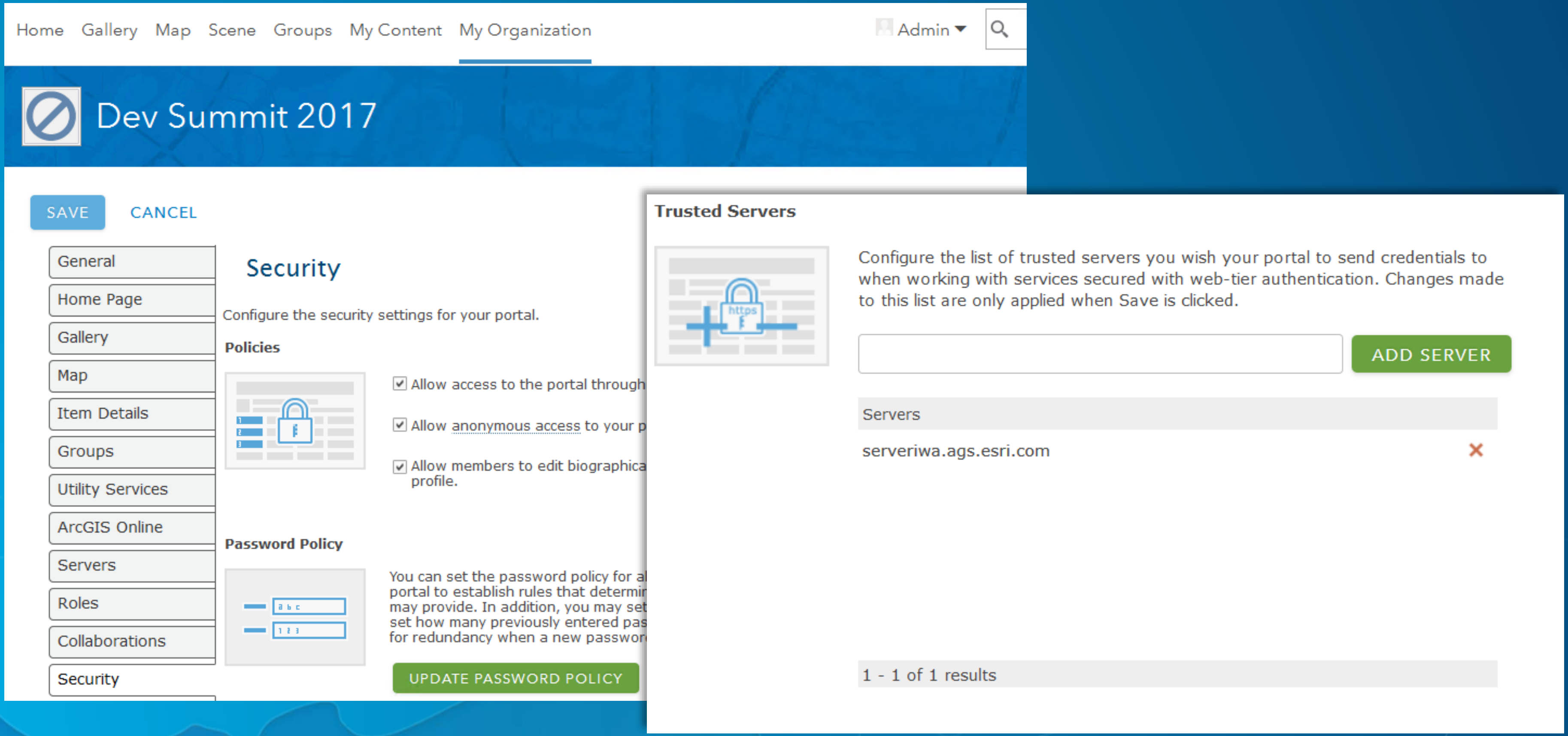
Properties: {"disableSignup":"true"}

Resources: Update Properties

Supported Interfaces: REST

Trusted Servers List in Portal

- **Configure list of trusted servers that work with Portal for ArcGIS**
- **`My Organization > Edit settings > Security`**



Security

Configure the security settings for your portal.

Policies

☑ Allow access to the portal through

☑ Allow anonymous access to your p

☑ Allow members to edit biographica profile.

Password Policy

You can set the password policy for al portal to establish rules that determir may provide. In addition, you may set set how many previously entered pas for redundancy when a new passwor

UPDATE PASSWORD POLICY

Trusted Servers

Configure the list of trusted servers you wish your portal to send credentials to when working with services secured with web-tier authentication. Changes made to this list are only applied when Save is clicked.

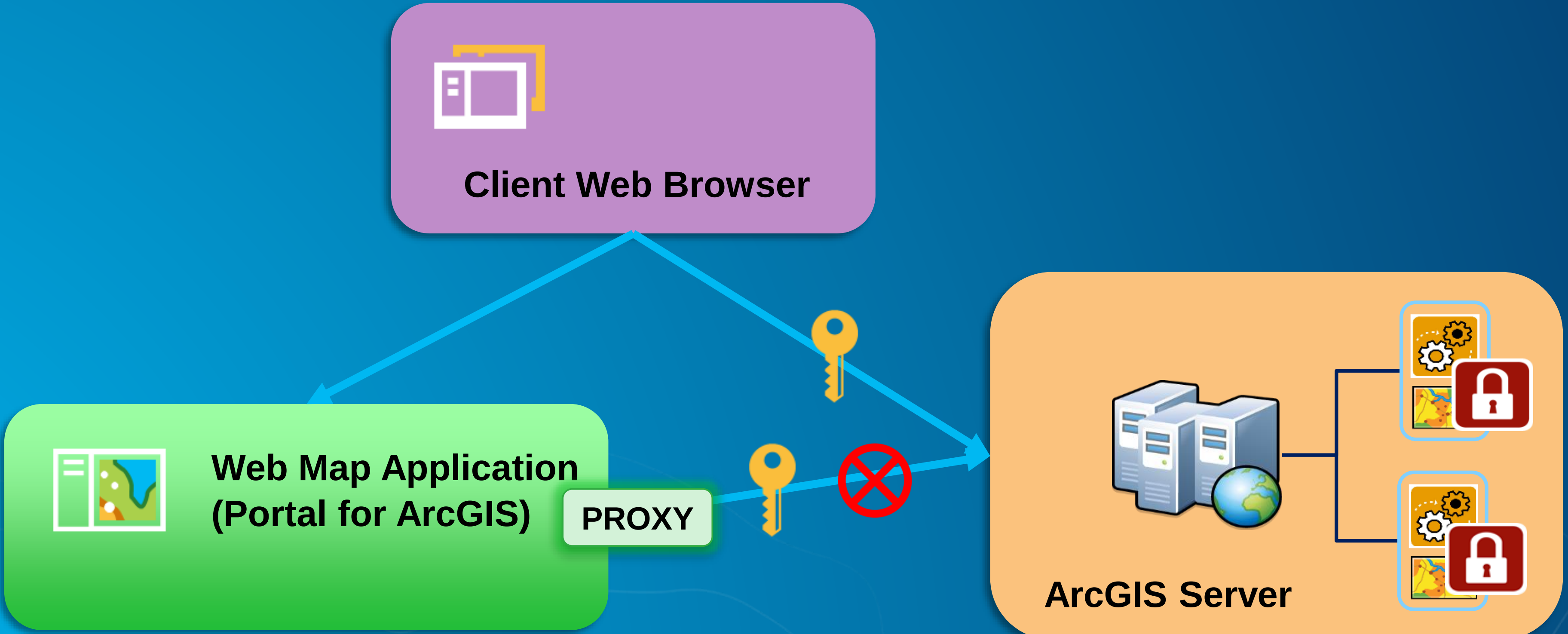
ADD SERVER

Servers
serveriwa.ags.esri.com ✕

1 - 1 of 1 results

Trusted Servers in Portal

- A list of servers to where credentials will be passed when making a CORS request to access secured resources

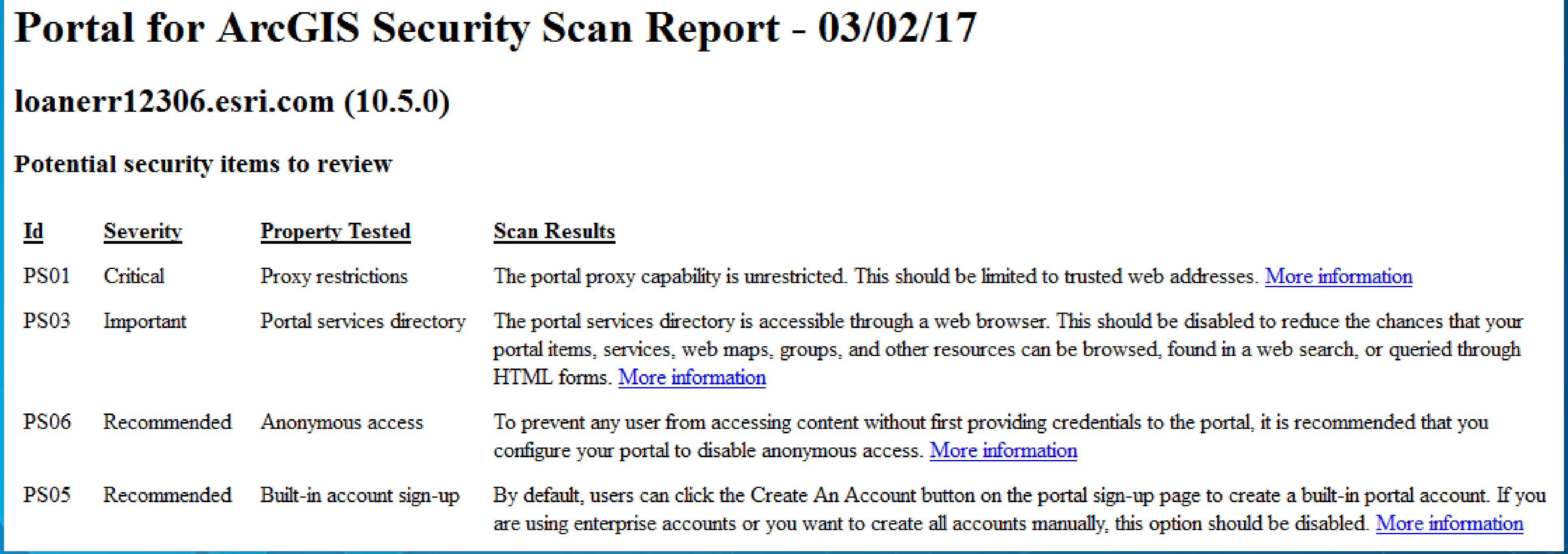


Demo

Trusted Servers in Portal for ArcGIS

Scan Portal for Security Checks

- `portalScan.py` is a script in the Portal installation directory
  - Location: `<install_directory>\ArcGIS\Portal\tools\security`
- When you run the script, it checks for security settings → generates a report that makes recommendations to improve security



Portal for ArcGIS Security Scan Report - 03/02/17

loanerr12306.esri.com (10.5.0)

Potential security items to review

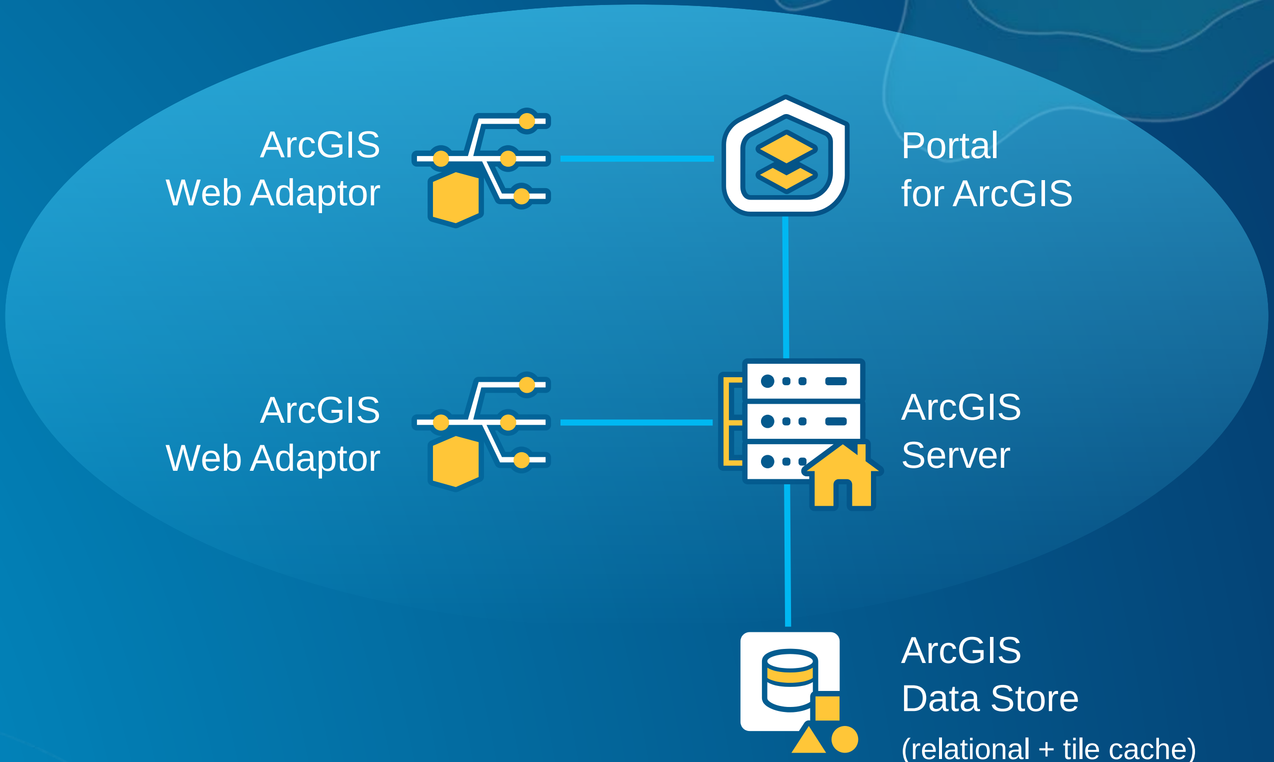
Id	Severity	Property Tested	Scan Results
PS01	Critical	Proxy restrictions	The portal proxy capability is unrestricted. This should be limited to trusted web addresses. More information
PS03	Important	Portal services directory	The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. More information
PS06	Recommended	Anonymous access	To prevent any user from accessing content without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information
PS05	Recommended	Built-in account sign-up	By default, users can click the Create An Account button on the portal sign-up page to create a built-in portal account. If you are using enterprise accounts or you want to create all accounts manually, this option should be disabled. More information

Demo

Run *portalScan.py* Security Check

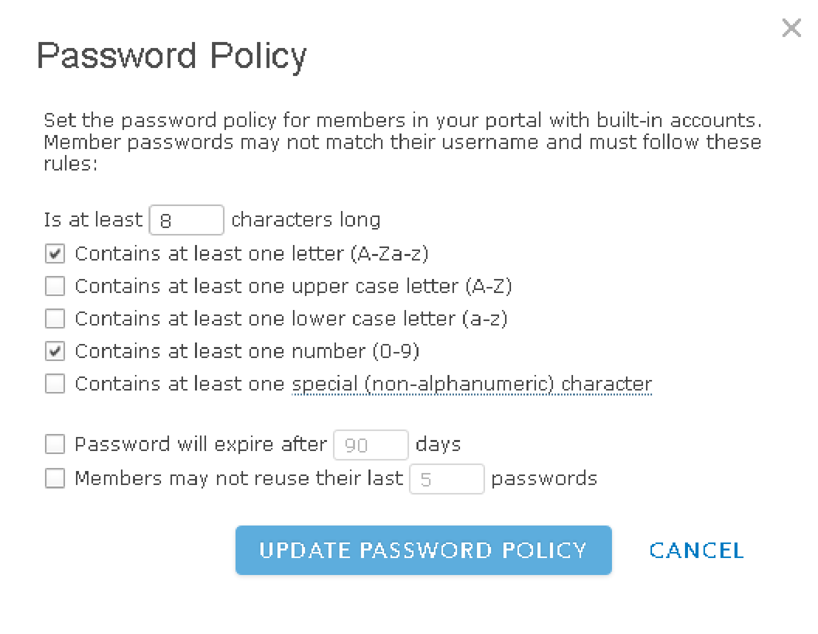
Agenda

- GIS Server
- Portal for ArcGIS
- Advanced Topics



Password settings for Portal (long passwords, complex, etc)

- **Portal > My Organization > Edit Settings > Security > Update Password Policy**



Password Policy

Set the password policy for members in your portal with built-in accounts. Member passwords may not match their username and must follow these rules:

Is at least 8 characters long

☑ Contains at least one letter (A-Za-z)

☐ Contains at least one upper case letter (A-Z)

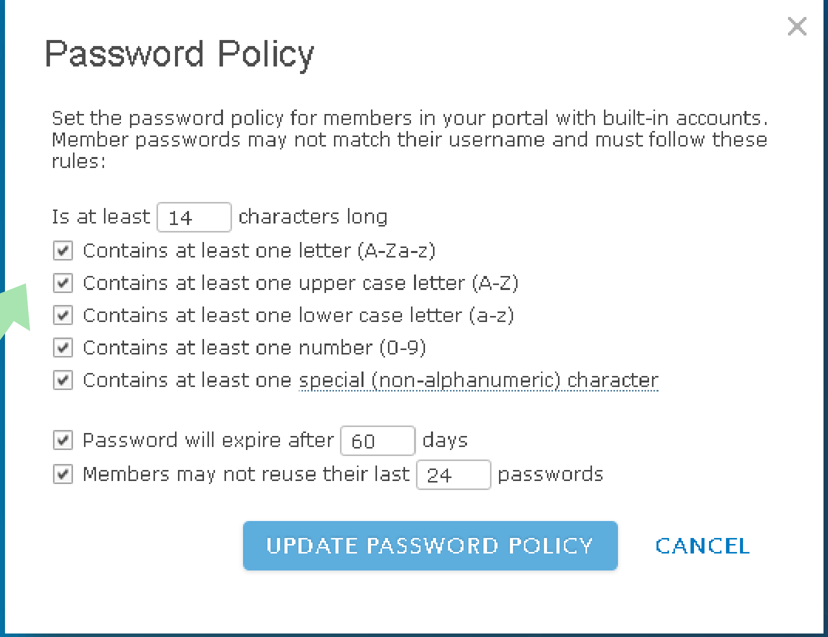
☐ Contains at least one lower case letter (a-z)

☑ Contains at least one number (0-9)

☐ Contains at least one special (non-alphanumeric) character

☐ Password will expire after 90 days

☐ Members may not reuse their last 5 passwords



Password Policy

Set the password policy for members in your portal with built-in accounts. Member passwords may not match their username and must follow these rules:

Is at least 14 characters long

☑ Contains at least one letter (A-Za-z)

☑ Contains at least one upper case letter (A-Z)

☑ Contains at least one lower case letter (a-z)

☑ Contains at least one number (0-9)

☑ Contains at least one special (non-alphanumeric) character

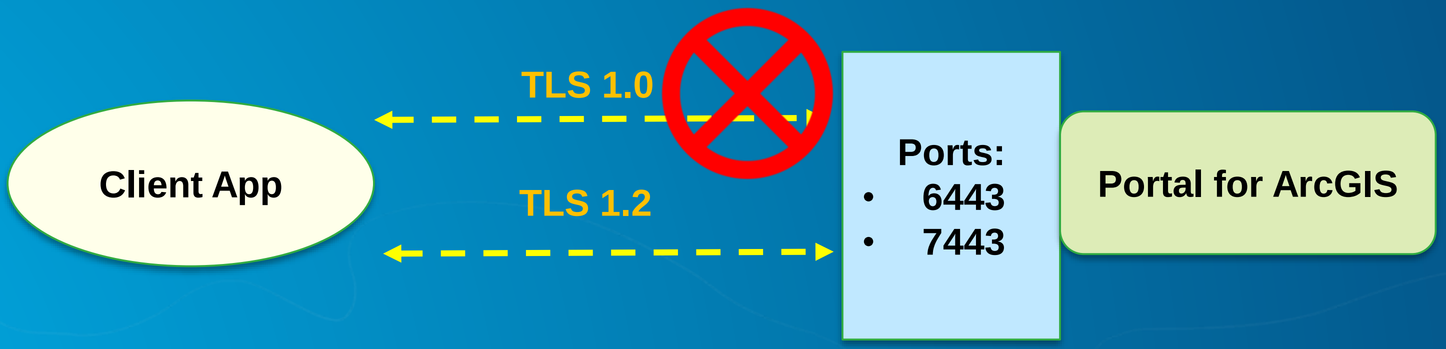
☑ Password will expire after 60 days

☑ Members may not reuse their last 24 passwords

SSL Property Configurations

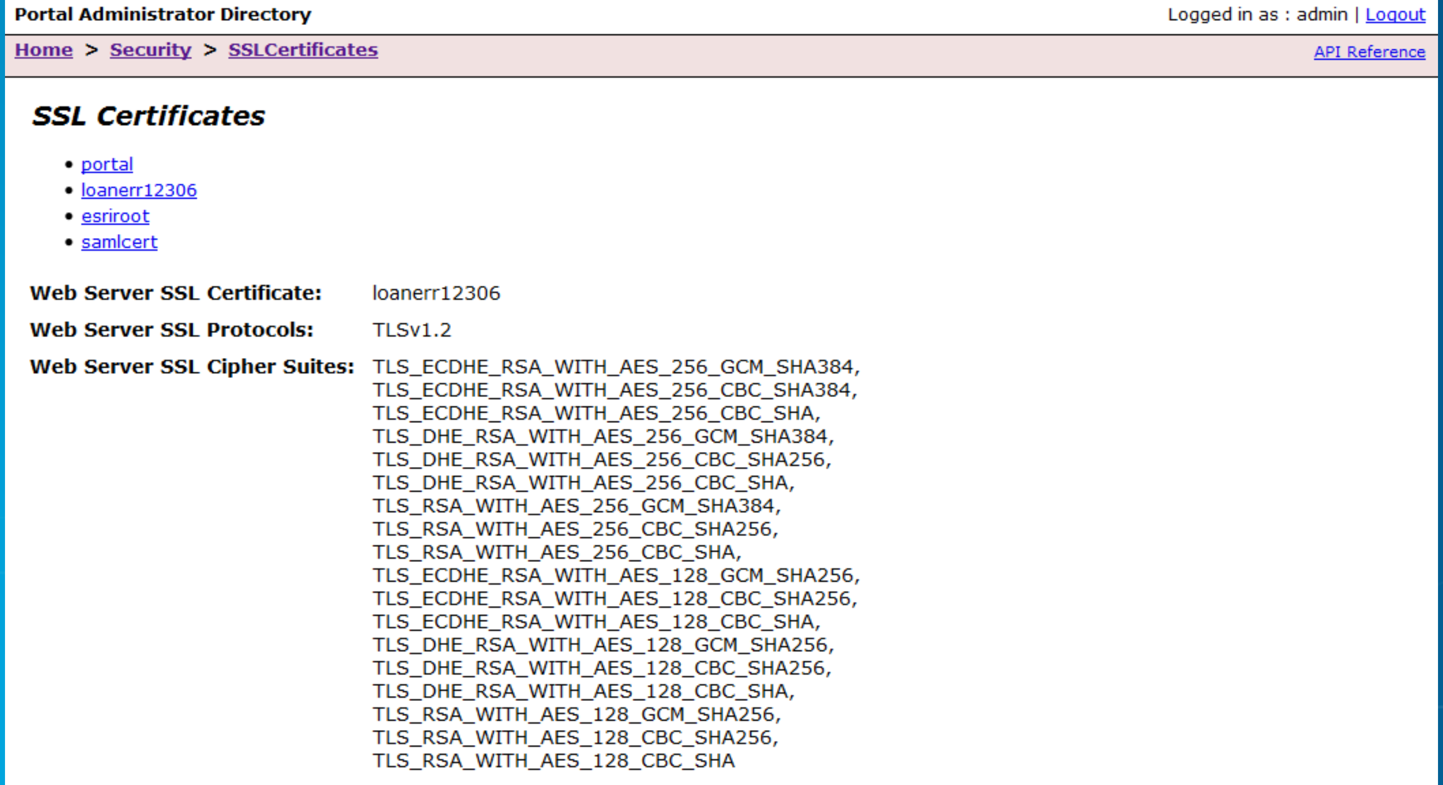
https://www.ssllabs.com/ssltest/clients.html

- In 10.4, both Server and Portal can be configured to limit which SSL protocol is accepted and used
- For organizations that are very security-aware, restricting Server and Portal to TLS 1.2 is highly recommended
- TLS (and it predecessor SSL) are cryptographic protocols designed to provide secure network communication between a client and a server



How to Specify Cipher Suites

- Access the Portal Administrator Directory
  - `Security > SSLCertificates > Update`
  - For the `SSL Protocols` text box, specify the protocols to be used



Portal Administrator Directory

Logged in as : admin | Logout

Home > Security > SSLCertificates

API Reference

SSL Certificates

- portal
- loanerr12306
- esriroot
- samlcert

Web Server SSL Certificate: loanerr12306

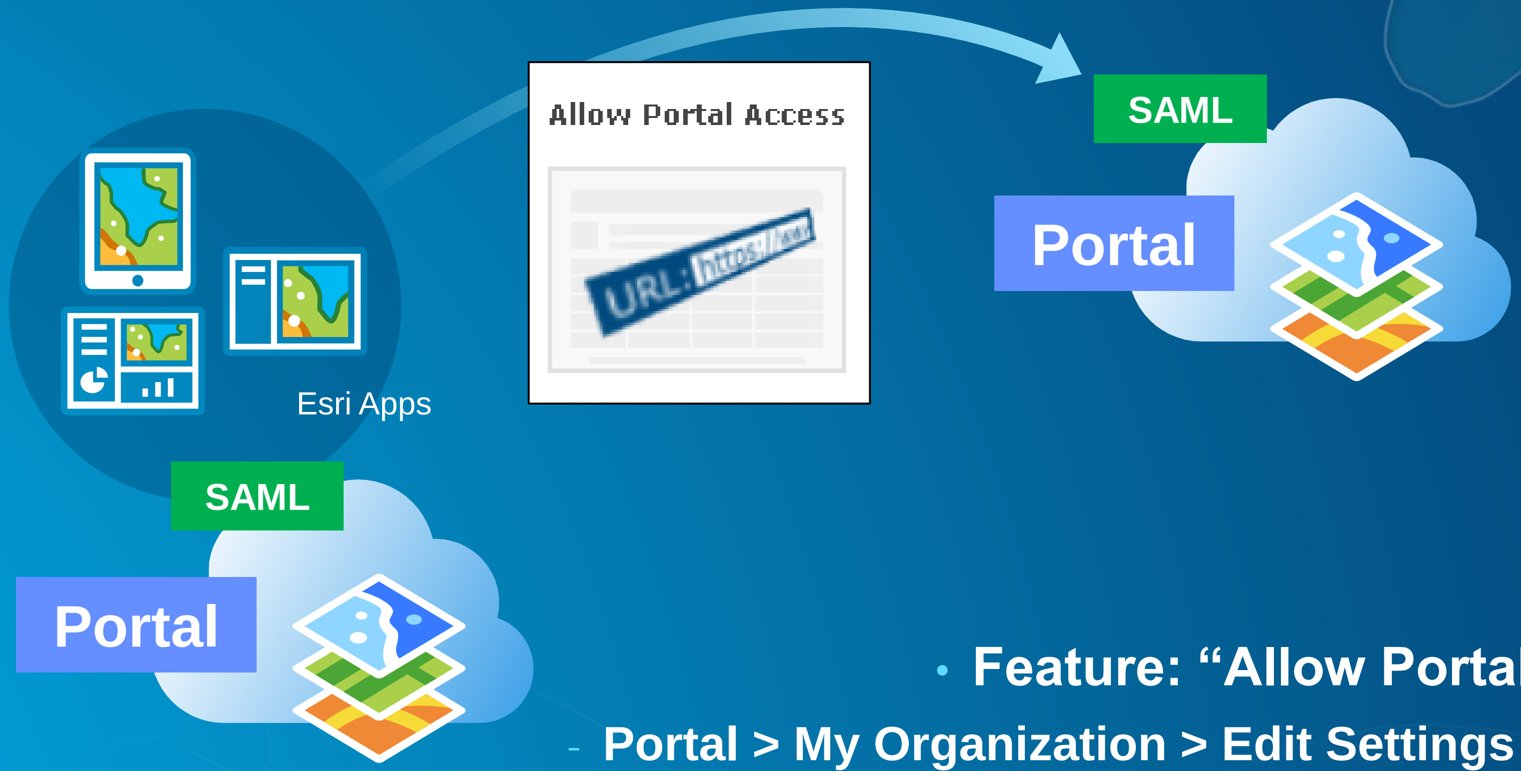
Web Server SSL Protocols: TLSv1.2

Web Server SSL Cipher Suites:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA
```

SAML Access to any ArcGIS Enterprise

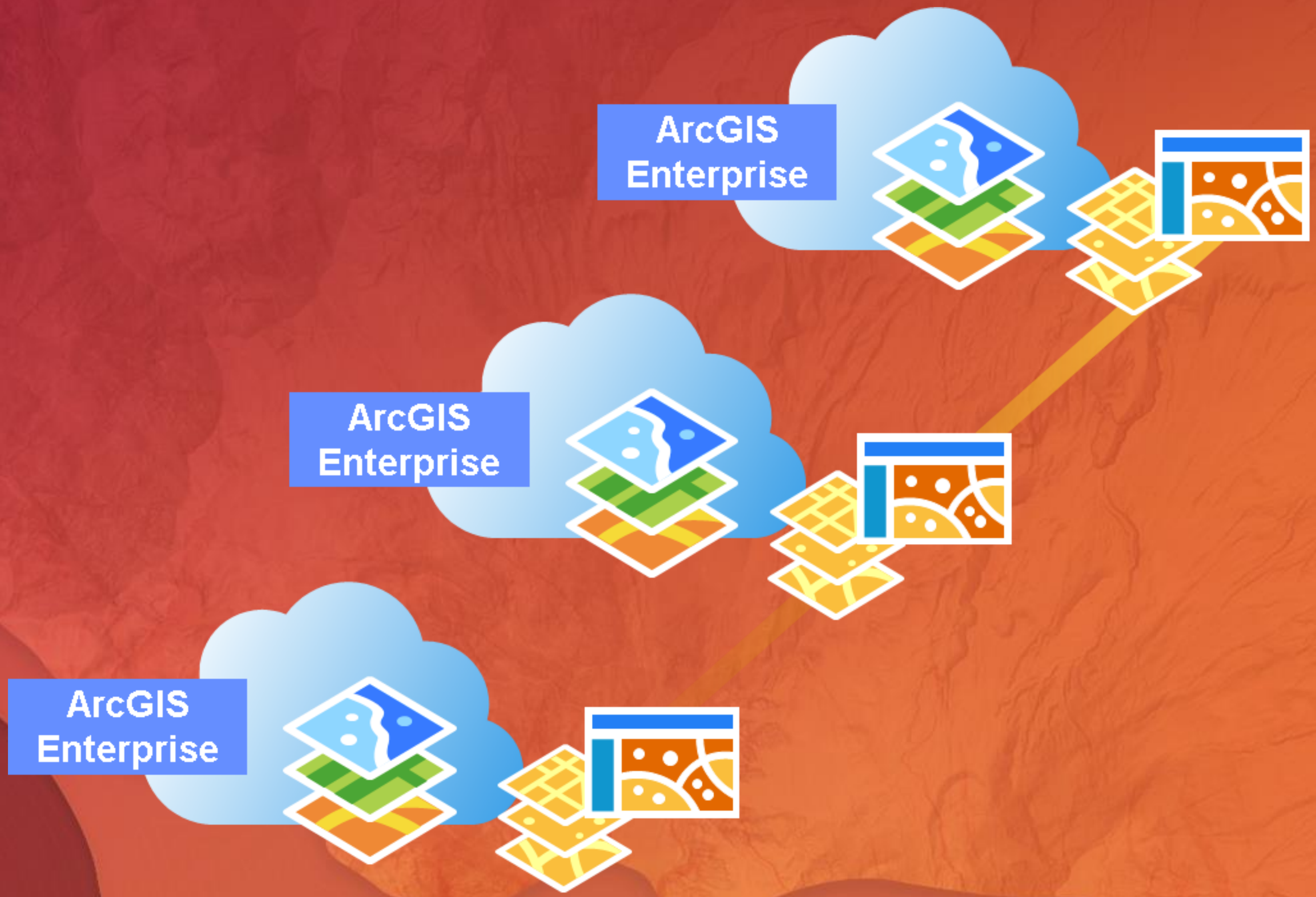
Bring secured services together from anywhere!



- Feature: “Allow Portal Access”
  - Portal > My Organization > Edit Settings > Security

Demo

Allow Portal Access



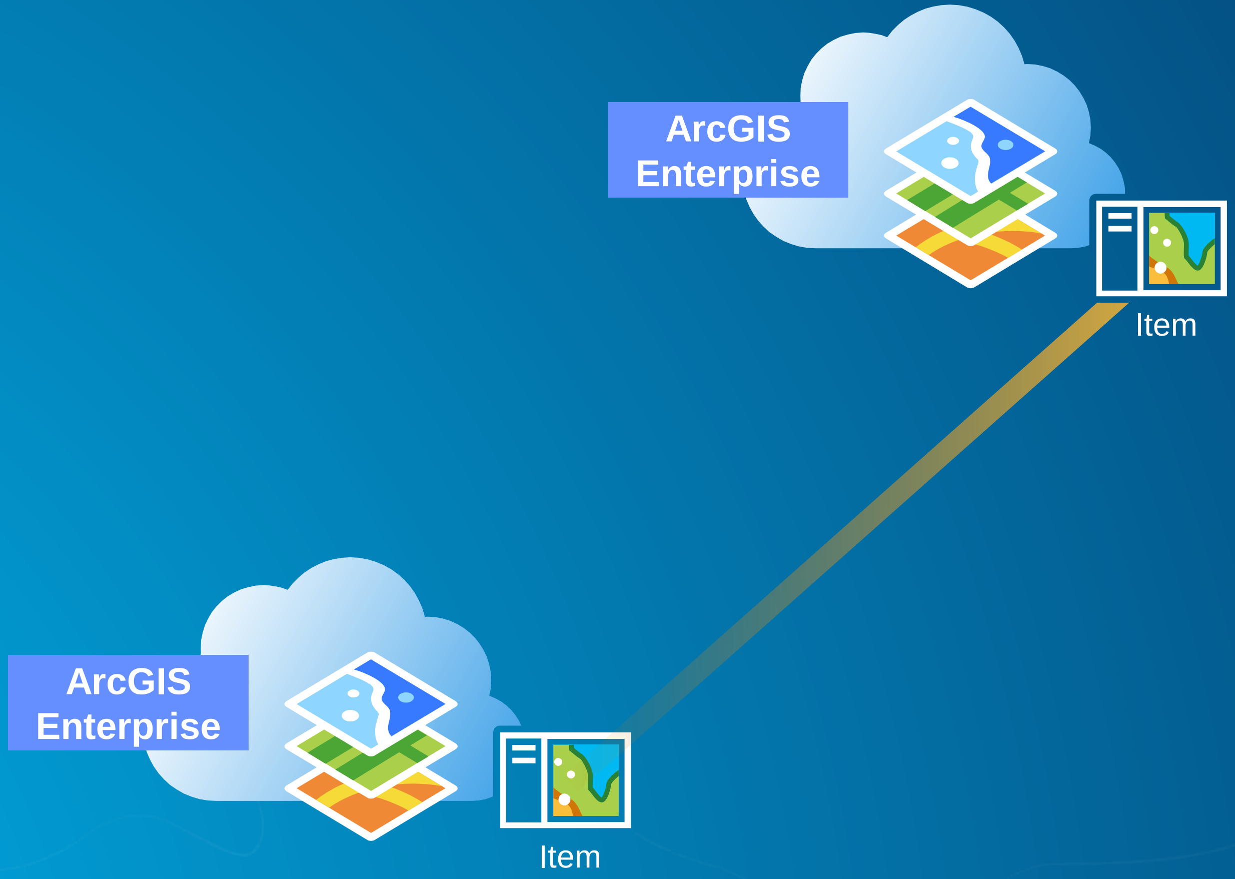
Collaboration

Security Considerations

Collaboration

What is it?

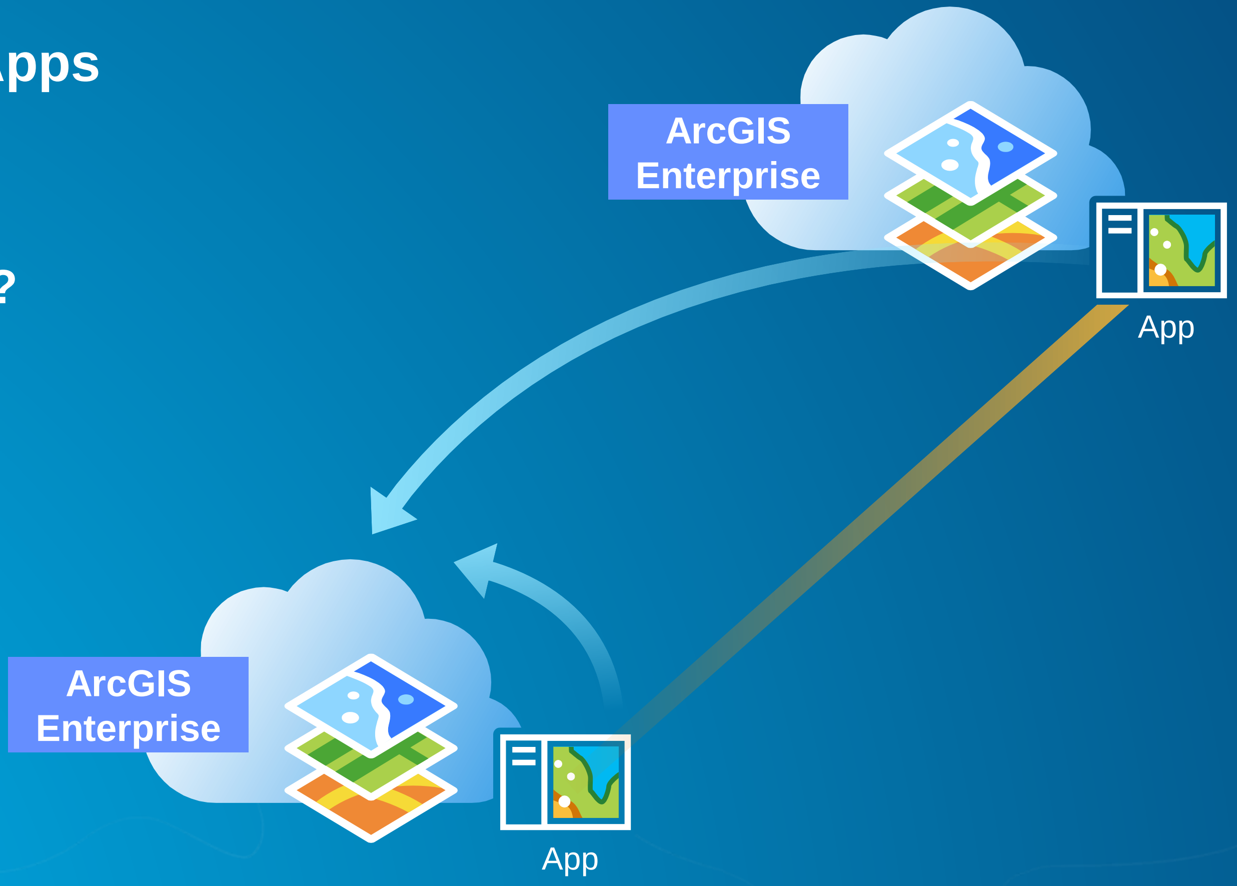
Collaboration



Collaboration

As a Developer what do I need to know?

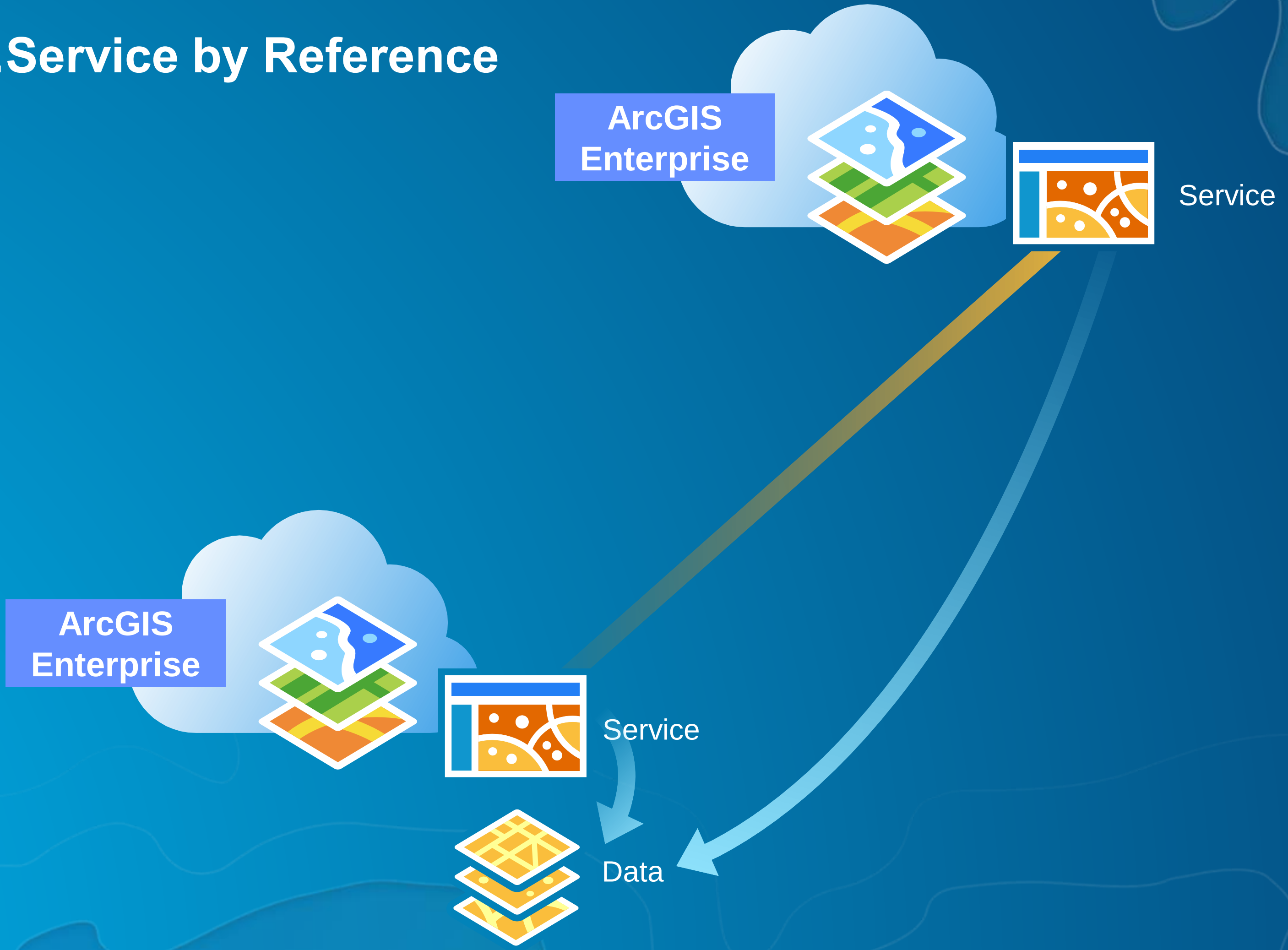
- Collaborating Apps
  - Oauth?
  - App ID?
  - Access Token?



Collaboration

As an Administrator what do I need to know?

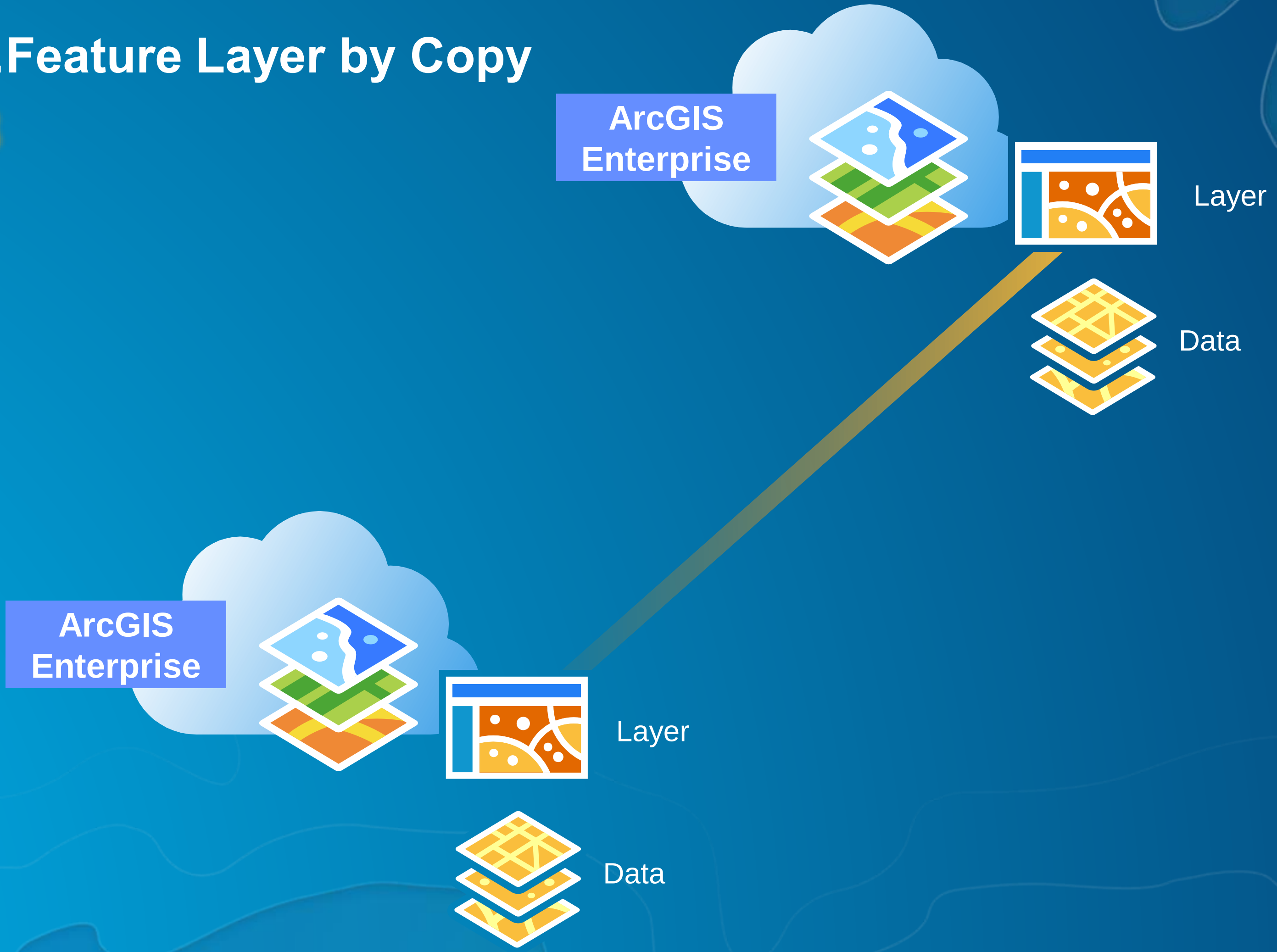
- Collaborating…Service by Reference
  - Low Risk



Collaboration

As an Administrator what do I need to know?

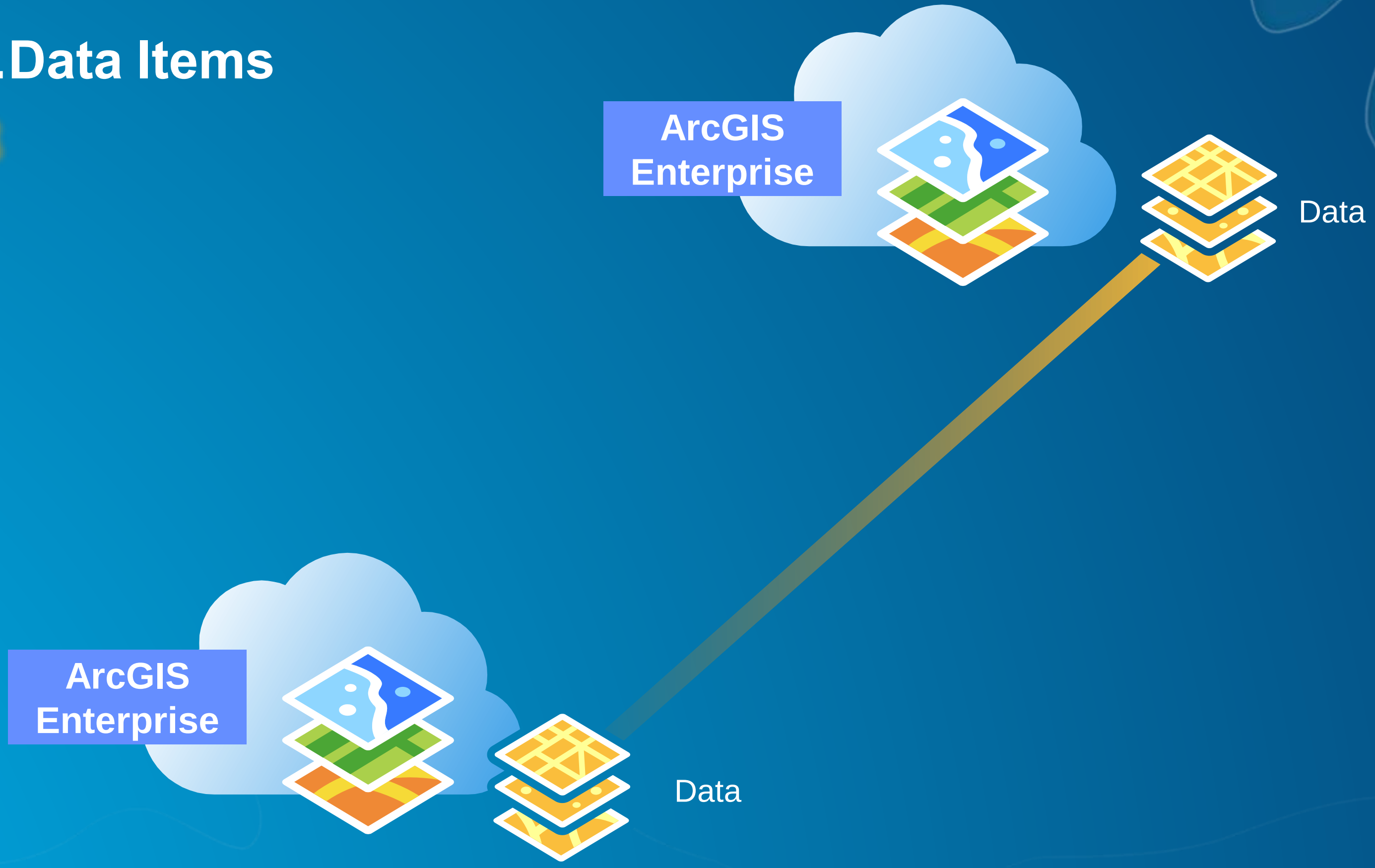
- Collaborating…Feature Layer by Copy
  - Moderate Risk



Collaboration

As an Administrator what do I need to know?

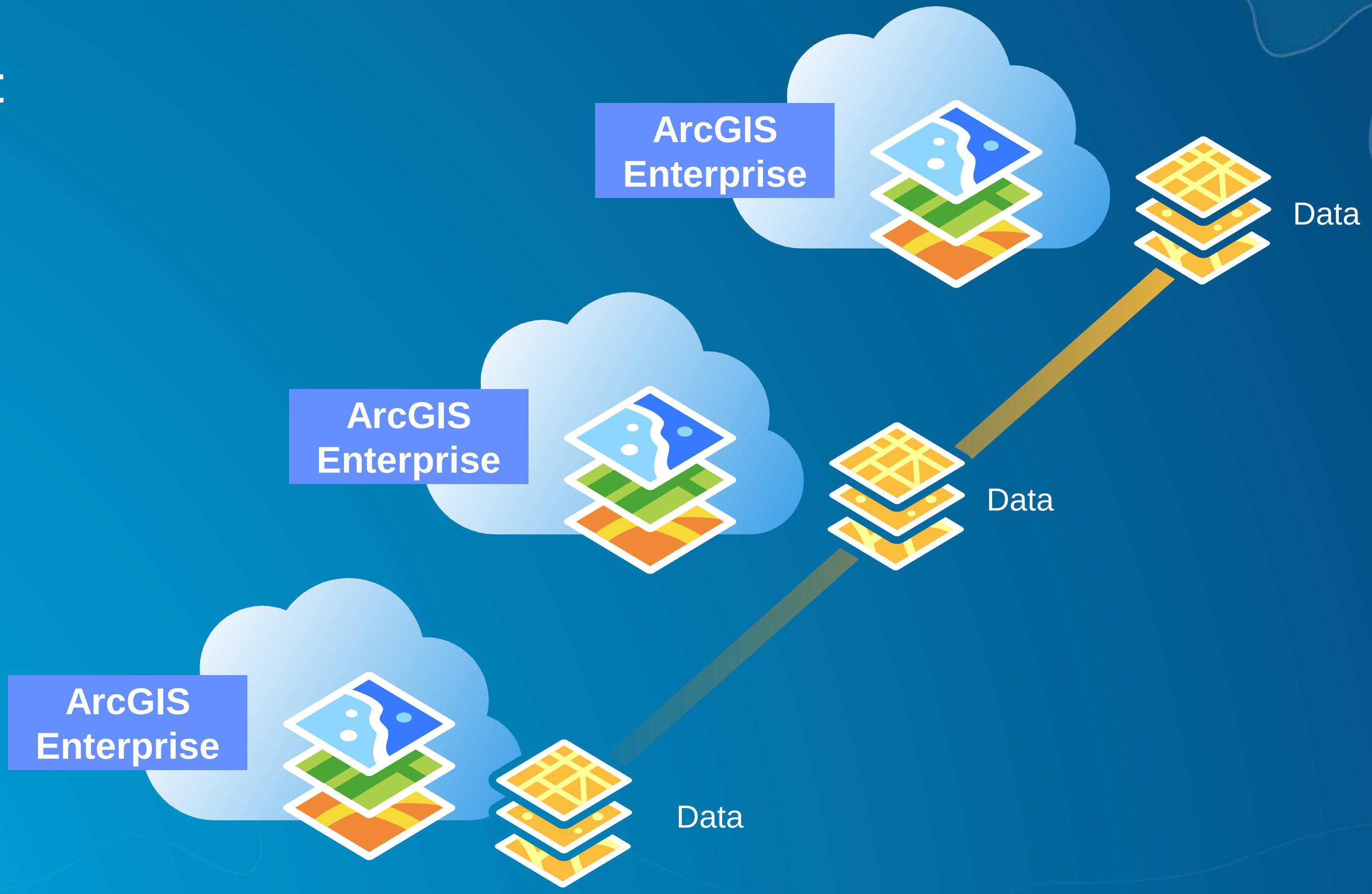
- Collaborating…Data Items
  - Moderate Risk



Collaboration

As an Administrator what do I need to know?

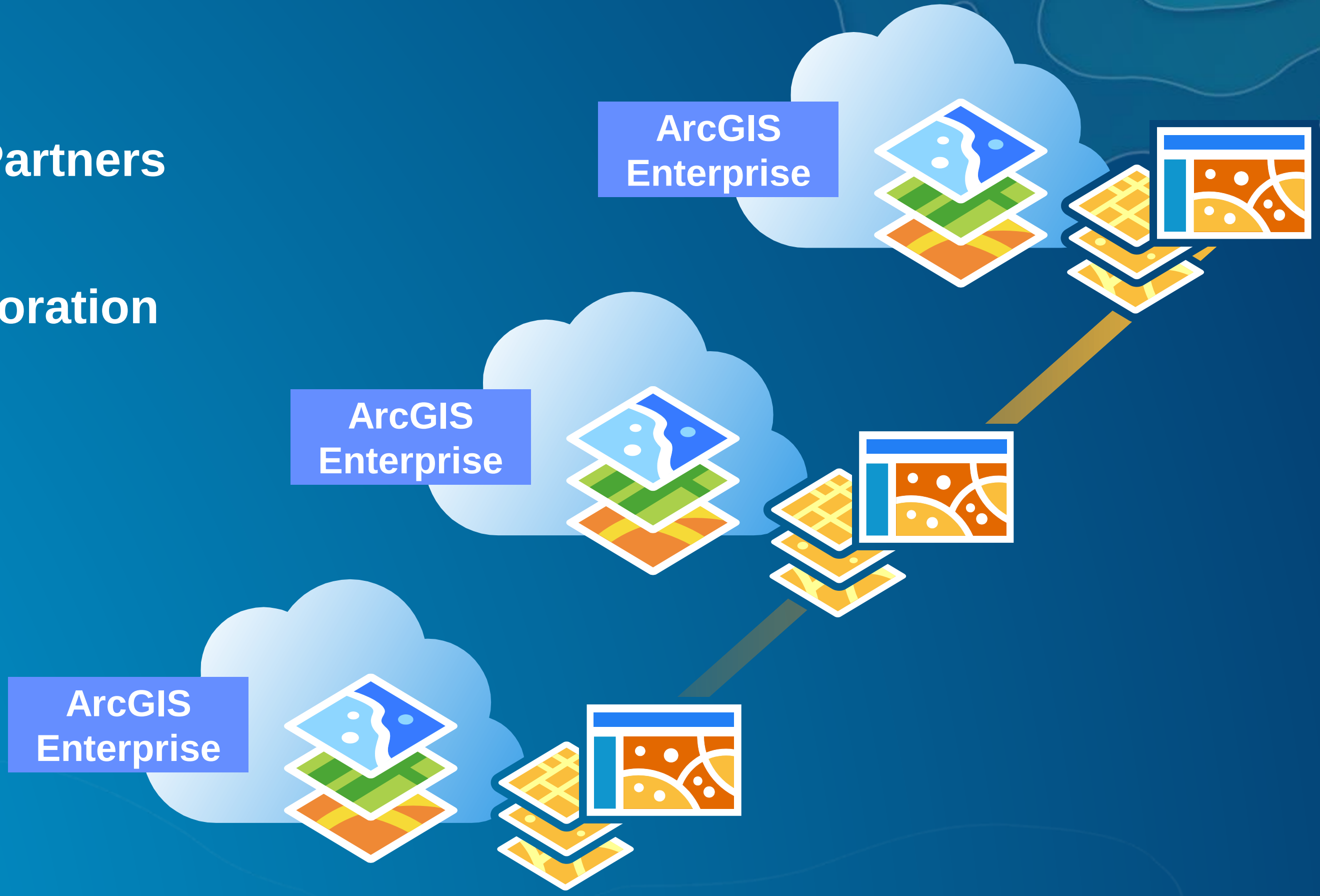
- Transitive Trust
  - High Risk



Collaboration

As an Administrator what do I need to know?

- Recommended Practices
  - Limit Collaborations to Trusted Partners
  - Collaborate Layers by Reference
  - Establish New Groups for Collaboration



Other Related Sessions

ArcGIS Enterprise Security: An Introduction	Tuesday, July 11, 10:15 AM	SDCC - Room 16 B
ArcGIS Enterprise Security: Advanced Topics	Tuesday, July 11, 1:30 PM	SDCC - Room 16 B
Designing a Web GIS Security Strategy	Tuesday, July 11, 3:15 PM	SDCC - Room 31 B
Building Security into Your System	Tuesday, July 11, 4:30 PM	SDCC - Esri Services (Showcase)
ArcGIS Enterprise: Introducing Portal for ArcGIS	Wednesday, July 12, 10:15 AM	SDCC - Room 09
ArcGIS Enterprise Security: An Introduction	Thursday, July 13, 8:30 AM	SDCC - Room 14 A
ArcGIS Enterprise Security: Advanced Topics	Thursday, July 13, 10:15 AM	SDCC - Room 14 A
Best Practices for Configuring Secured Services	Thursday, July 13, 12:30 PM	SDCC - Demo Theater 09
Designing a Web GIS Security Strategy	Thursday, July 13, 3:15 PM	SDCC - Room 32 A
ArcGIS Enterprise: Introducing Portal for ArcGIS	Friday, July 14, 9:00 AM	SDCC - Room 04

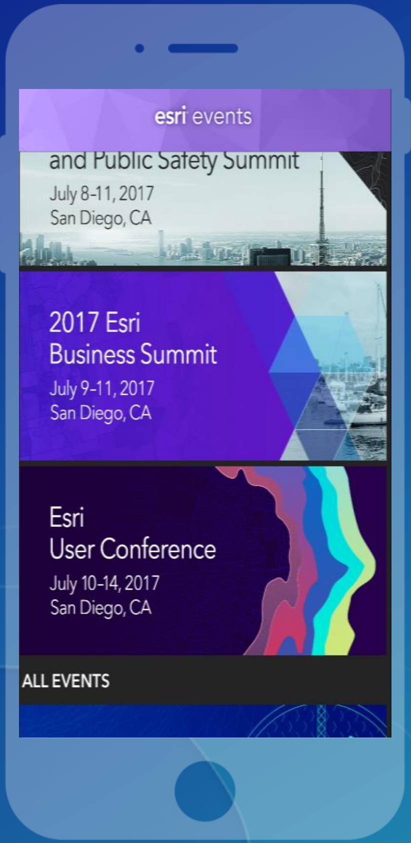
Key Takeaways

Summary

- **Use Server Scan Script to Validate ArcGIS Server Security**
- **Use Portal Scan Script to Validate Portal for ArcGIS Security**
- **Developers: Collaborating Apps = No code changes required**
- **Admins: Collaborate Carefully, *particularly when sharing Data Items***

Please Take Our Survey on the **Esri Events App!**

Download the Esri Events app and find your event



esri events

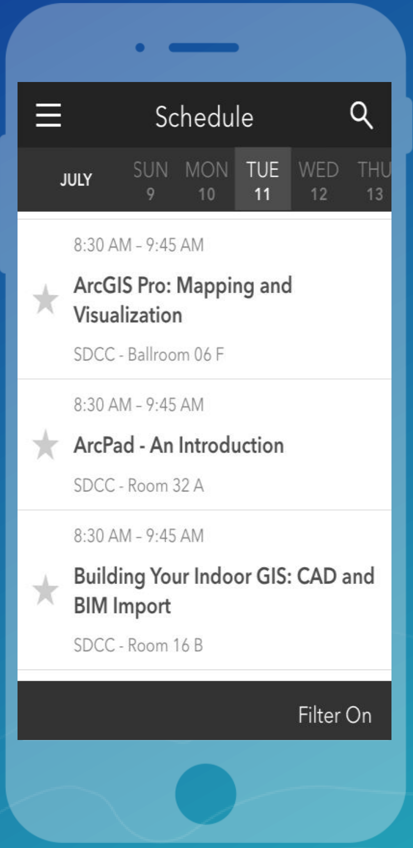
and Public Safety Summit
July 8-11, 2017
San Diego, CA

2017 Esri
Business Summit
July 9-11, 2017
San Diego, CA

Esri
User Conference
July 10-14, 2017
San Diego, CA

ALL EVENTS

Select the session you attended



Schedule

JULY	SUN	MON	TUE	WED	THU
	9	10	11	12	13

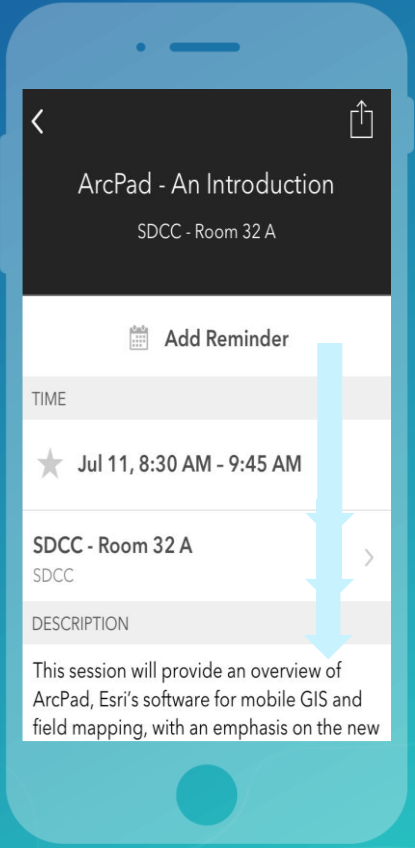
8:30 AM - 9:45 AM
ArcGIS Pro: Mapping and Visualization
SDCC - Ballroom 06 F

8:30 AM - 9:45 AM
ArcPad - An Introduction
SDCC - Room 32 A

8:30 AM - 9:45 AM
Building Your Indoor GIS: CAD and BIM Import
SDCC - Room 16 B

Filter On

Scroll down to find the survey



ArcPad - An Introduction
SDCC - Room 32 A

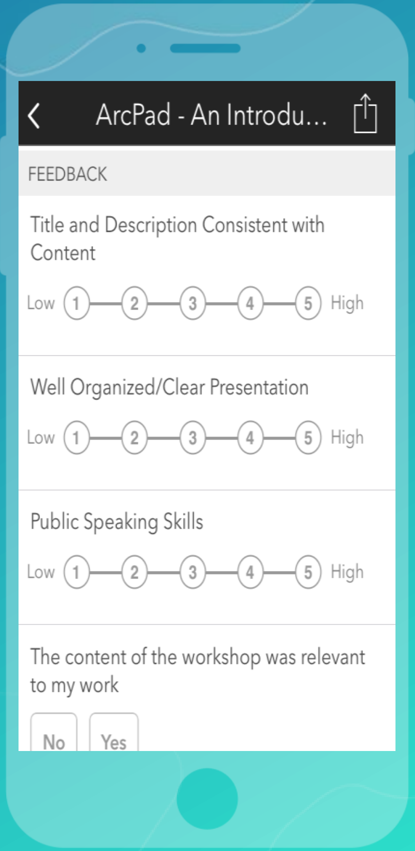
Add Reminder

TIME
Jul 11, 8:30 AM - 9:45 AM

SDCC - Room 32 A
SDCC

DESCRIPTION
This session will provide an overview of ArcPad, Esri's software for mobile GIS and field mapping, with an emphasis on the new

Complete Answers and Select "Submit"



ArcPad - An Introdu...

FEEDBACK

Title and Description Consistent with Content
Low ① ② ③ ④ ⑤ High

Well Organized/Clear Presentation
Low ① ② ③ ④ ⑤ High

Public Speaking Skills
Low ① ② ③ ④ ⑤ High

The content of the workshop was relevant to my work
No Yes