ArcGIS for Server Security: Advanced

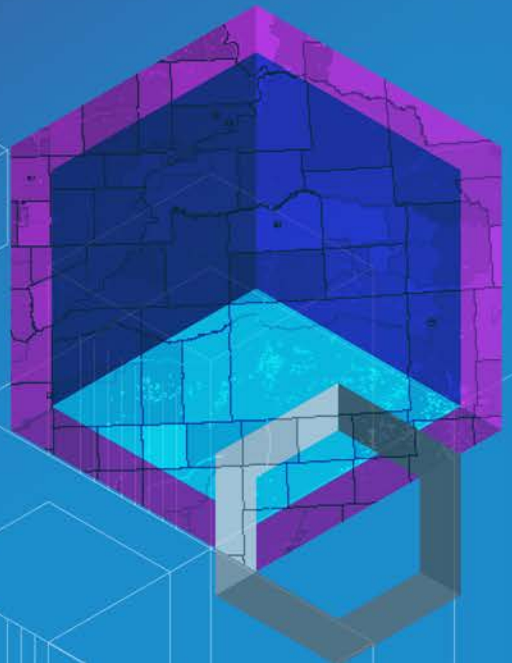
Gregory Ponto & Jeff Smith

June 29, 2016

Agenda

- Focus: Security best practices for Web GIS on-premises

- GIS Server
- Portal for ArcGIS
- Advanced options

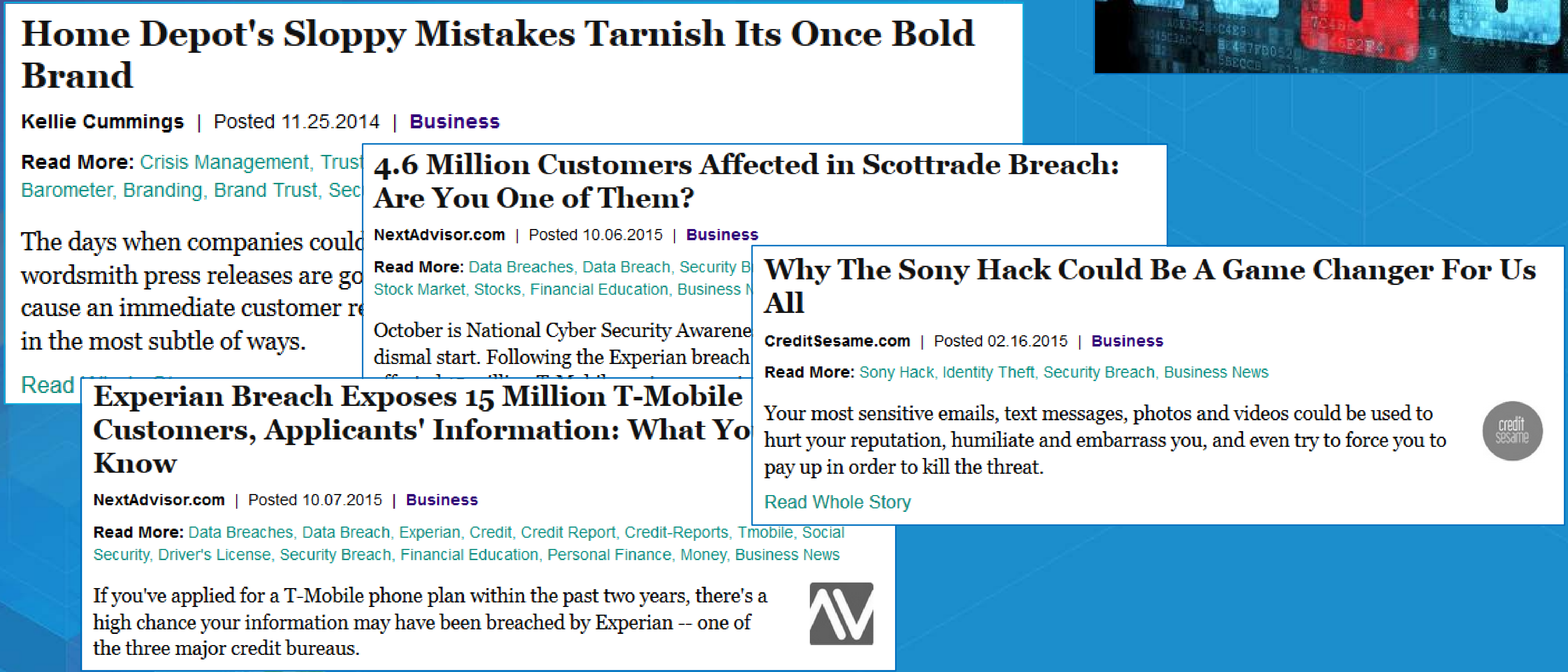


⚠ Strongly Recommend:

Knowledge of ArcGIS for Server and Portal for ArcGIS

Security is Important

http://www.huffingtonpost.com/news/security-breach/



Home Depot's Sloppy Mistakes Tarnish Its Once Bold Brand

Kellie Cummings | Posted 11.25.2014 | **Business**

Read More: Crisis Management, Trust
Barometer, Branding, Brand Trust, Sec

The days when companies could
wordsmith press releases are go
cause an immediate customer re
in the most subtle of ways.

Read

4.6 Million Customers Affected in Scottrade Breach: Are You One of Them?

NextAdvisor.com | Posted 10.06.2015 | **Business**

Read More: Data Breaches, Data Breach, Security B
Stock Market, Stocks, Financial Education, Business N

October is National Cyber Security Awarene
dismal start. Following the Experian breach

Why The Sony Hack Could Be A Game Changer For Us All

CreditSesame.com | Posted 02.16.2015 | **Business**

Read More: Sony Hack, Identity Theft, Security Breach, Business News

Your most sensitive emails, text messages, photos and videos could be used to hurt your reputation, humiliate and embarrass you, and even try to force you to pay up in order to kill the threat.

Read Whole Story

Experian Breach Exposes 15 Million T-Mobile Customers, Applicants' Information: What Yo Know

NextAdvisor.com | Posted 10.07.2015 | **Business**

Read More: Data Breaches, Data Breach, Experian, Credit, Credit Report, Credit-Reports, Tmobile, Social Security, Driver's License, Security Breach, Financial Education, Personal Finance, Money, Business News

If you've applied for a T-Mobile phone plan within the past two years, there's a high chance your information may have been breached by Experian -- one of the three major credit bureaus.

Defense In Depth Paradigm

- Security plans have many “layers” – multiple levels of security
- Layered security mechanisms increase the security of the system as a whole
- Each feature discussed is considered a “layer”

ArcGIS 10.4 for Server Release

- Major focus: improve and extend security in the software stack
- Provide more options and capabilities to make Web GIS infrastructure more secure

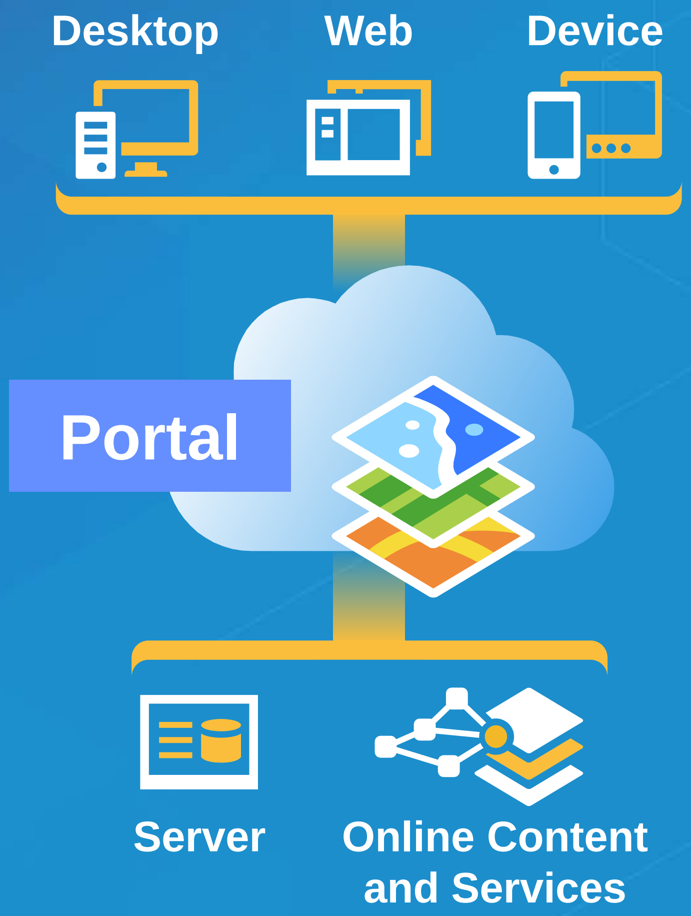
Review: ArcGIS for Server enables Web GIS On-Premises

Enabling GIS Everywhere

Simple

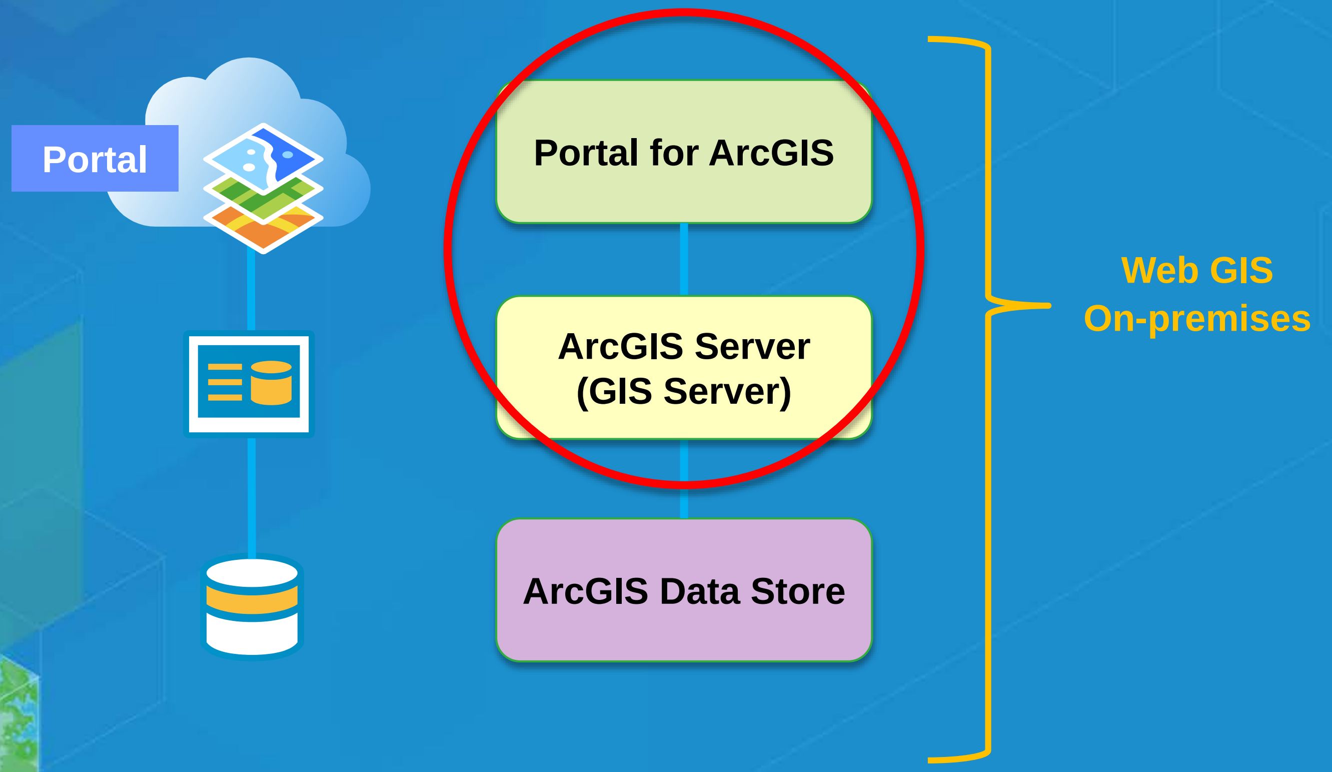
Integrated

Open



Web GIS Portal On-Premises: Behind the scenes

- Includes 3 components: Portal – GIS Server – ArcGIS Data Store



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

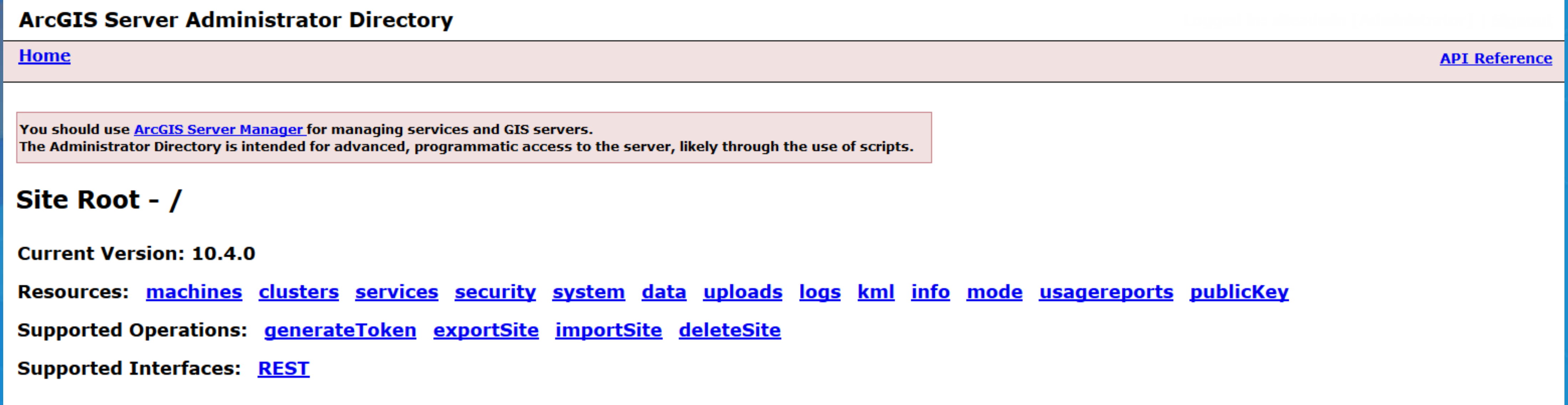
Portal for ArcGIS

ArcGIS Server
(GIS Server)

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

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: 10.4.0

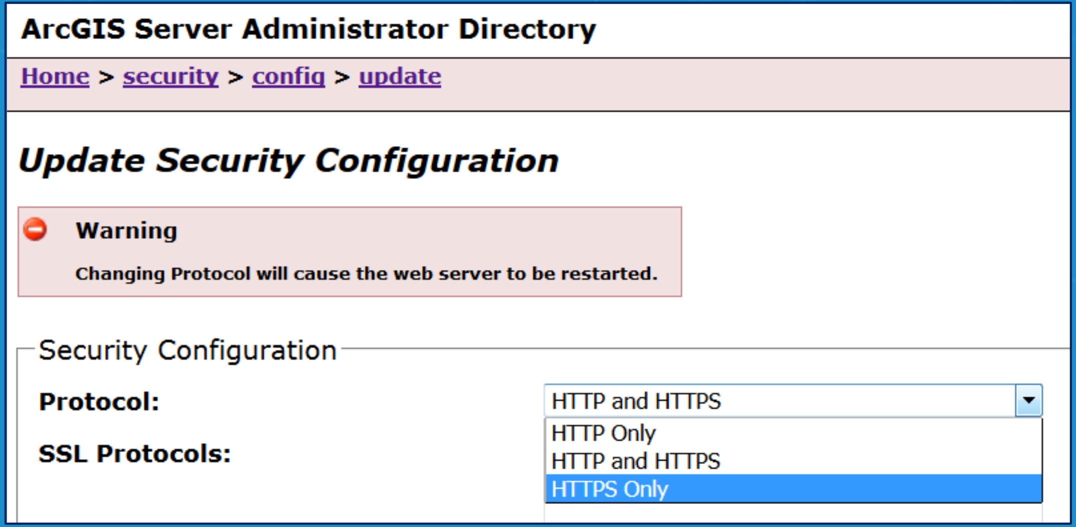
Resources: machines clusters services security system data uploads logs kml info mode usagereports publicKey

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

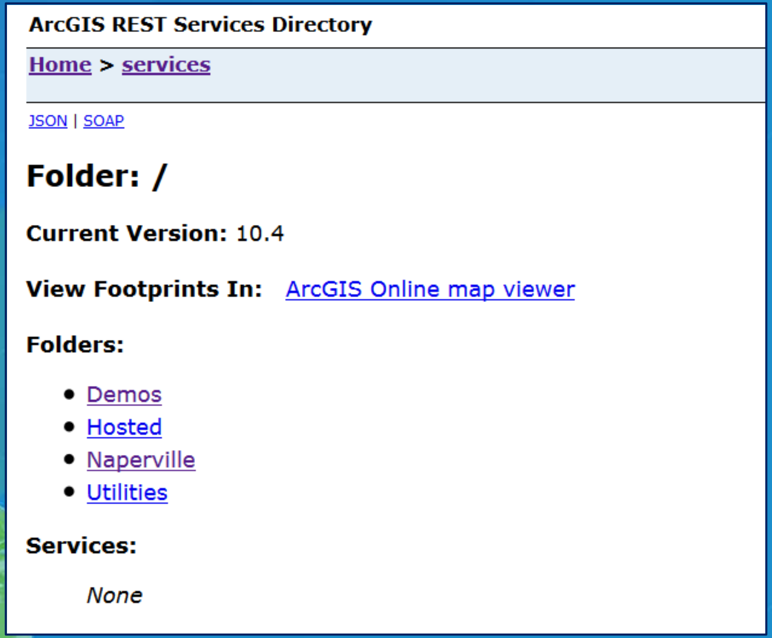
SSL Protocols:

Disable the Services Directory

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

REST

Before



ArcGIS REST Services Directory

Home > services

JSON | SOAP

Folder: /

Current Version: 10.4

View Footprints In: ArcGIS Online map viewer

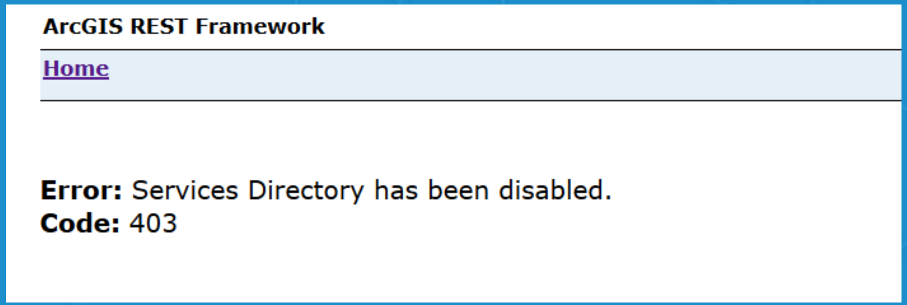
Folders:

- Demos
- Hosted
- Naperville
- Utilities

Services:

None

After



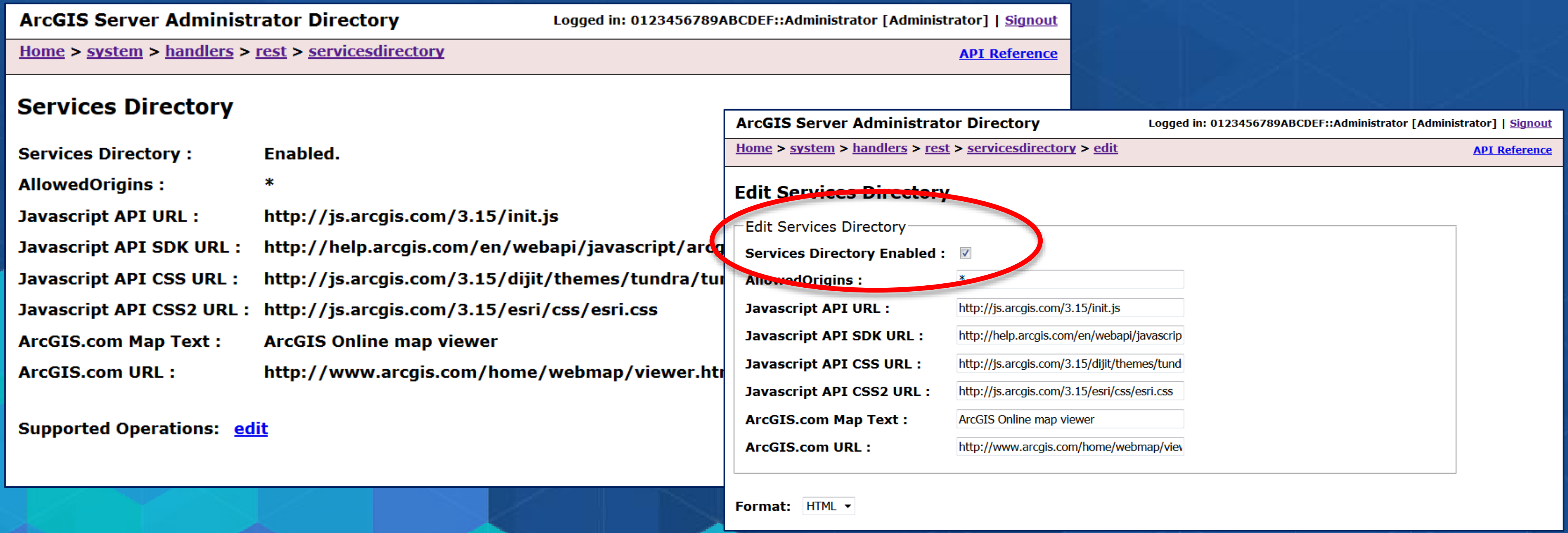
ArcGIS REST Framework

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 Logged in: 0123456789ABCDEF::Administrator [Administrator] | Signout

Home > system > handlers > rest > servicesdirectory API Reference

Services Directory

Services Directory : Enabled.

AllowedOrigins : *

Javascript API URL : http://js.arcgis.com/3.15/init.js

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

Javascript API CSS URL : http://js.arcgis.com/3.15/dijit/themes/tundra/tu

Javascript API CSS2 URL : http://js.arcgis.com/3.15/esri/css/esri.css

ArcGIS.com Map Text : ArcGIS Online map viewer

ArcGIS.com URL : http://www.arcgis.com/home/webmap/viewer.htı

Supported Operations: edit

ArcGIS Server Administrator Directory Logged in: 0123456789ABCDEF::Administrator [Administrator] | Signout

Home > system > handlers > rest > servicesdirectory > edit API Reference

Edit Services Directory

Edit Services Directory

Services Directory Enabled : ☑

AllowedOrigins : *

Javascript API URL : http://js.arcgis.com/3.15/init.js

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

Javascript API CSS URL : http://js.arcgis.com/3.15/dijit/themes/tund

Javascript API CSS2 URL : http://js.arcgis.com/3.15/esri/css/esri.css

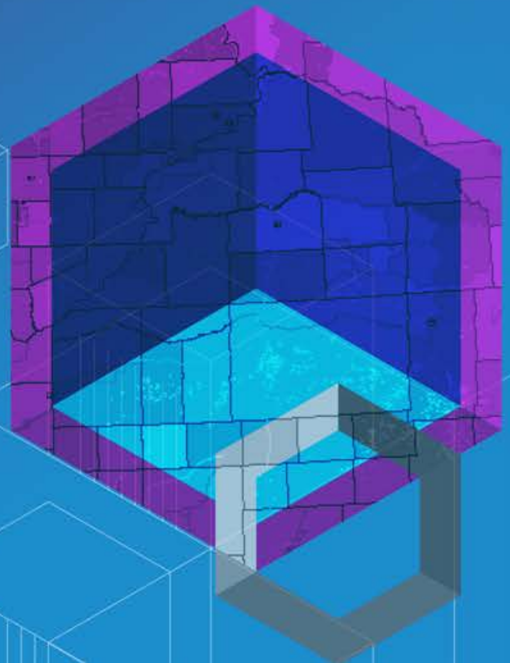
ArcGIS.com Map Text : ArcGIS Online map viewer

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

Format: HTML

Demo

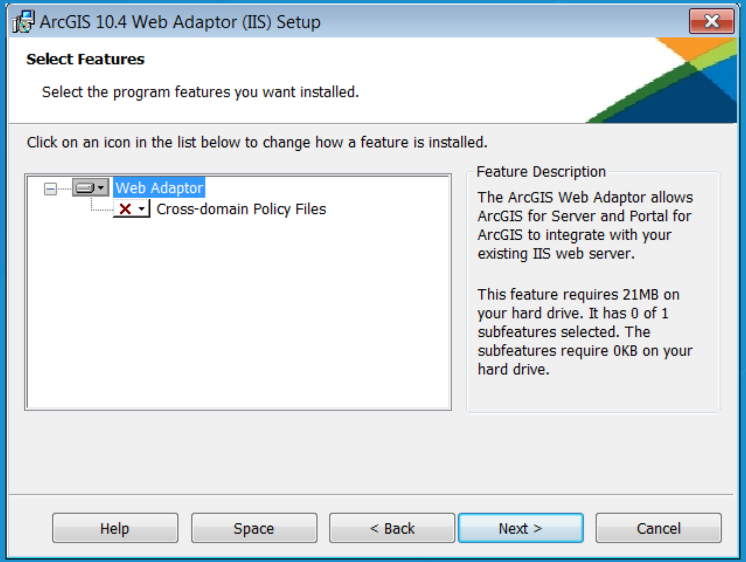
Disable Services Directory



Restrict Cross-Domain Requests

- By default, ArcGIS Server allows cross-domain requests so that client apps can invoke its services from any domain
  - E.g., Adobe Flash Player, Microsoft Silverlight, and JavaScript apps
- Cross-domain files installed with ArcGIS Web Adaptor
- Help topic: [Restricting cross-domain requests to ArcGIS Server]()

ArcGIS Web Adaptor



ArcGIS 10.4 Web Adaptor (IIS) Setup

Select Features

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Web Adaptor
  - ✗ Cross-domain Policy Files

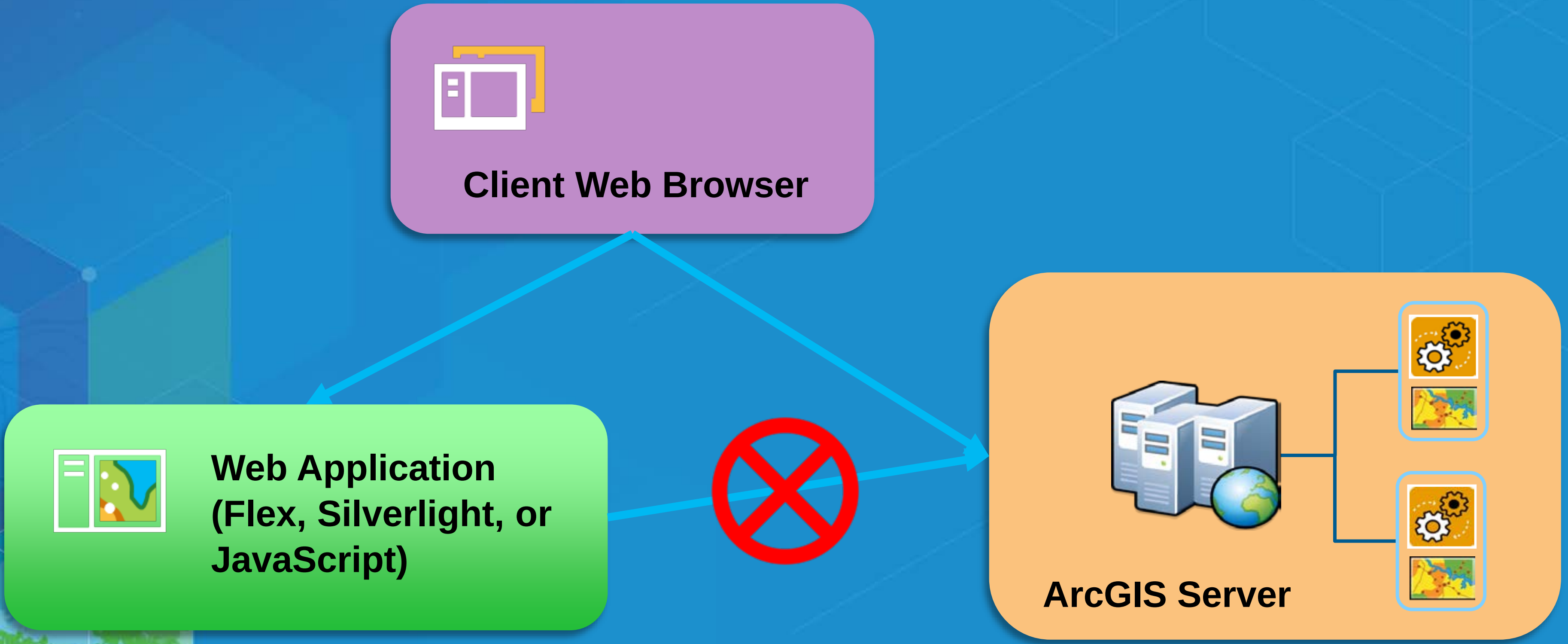
Feature Description

The ArcGIS Web Adaptor allows ArcGIS for Server and Portal for ArcGIS to integrate with your existing IIS web server.

This feature requires 21MB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.

What is a Cross-Domain Request?

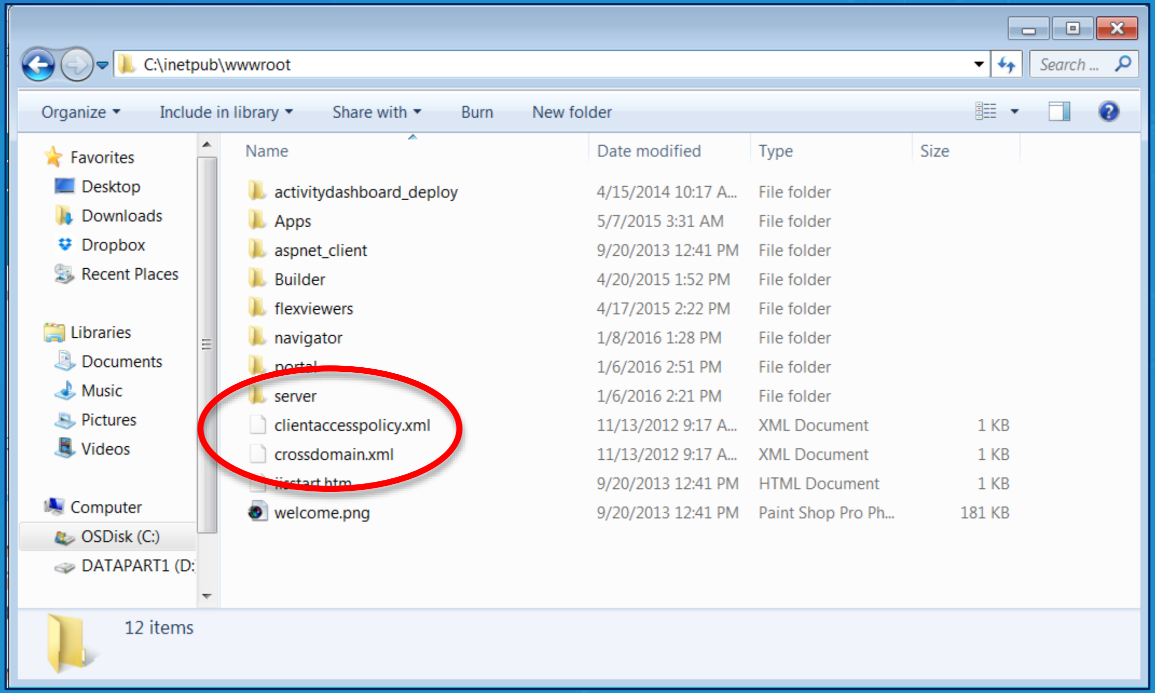
- A web application running on one server accessing resources that resides on another server
- Cross-domain security is enforced by the web browser



How to Restrict Cross-Domain Requests

- **For Adobe Flash Player** > edit *crossdomain.xml* file
- **For Microsoft Silverlight** > edit *clientaccesspolicy.xml* file

Web Server
E.g., IIS

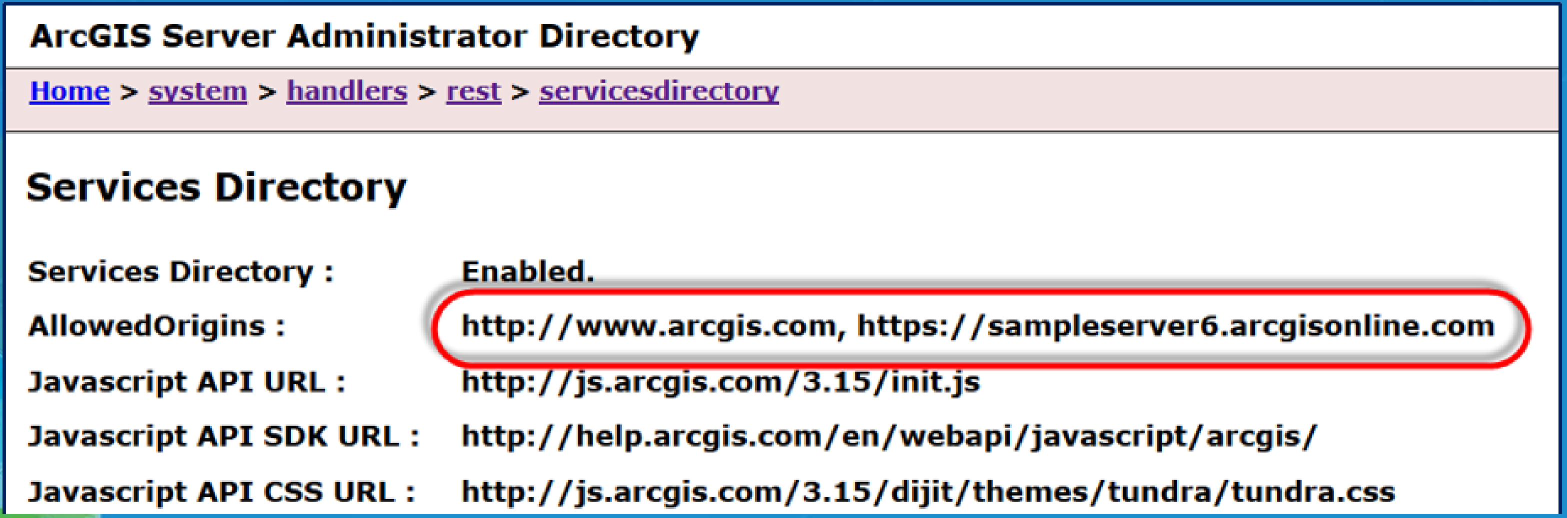


Name	Date modified	Type	Size
activitydashboard_deploy	4/15/2014 10:17 A...	File folder	
Apps	5/7/2015 3:31 AM	File folder	
aspnet_client	9/20/2013 12:41 PM	File folder	
Builder	4/20/2015 1:52 PM	File folder	
flexviewers	4/17/2015 2:22 PM	File folder	
navigator	1/8/2016 1:28 PM	File folder	
portal	1/6/2016 2:51 PM	File folder	
server	1/6/2016 2:21 PM	File folder	
clientaccesspolicy.xml	11/13/2012 9:17 A...	XML Document	1 KB
crossdomain.xml	11/13/2012 9:17 A...	XML Document	1 KB
iisstart.htm	9/20/2013 12:41 PM	HTML Document	1 KB
welcome.png	9/20/2013 12:41 PM	Paint Shop Pro Ph...	181 KB

12 items

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 :	Enabled.
AllowedOrigins :	http://www.arcgis.com, https://sampleserver6.arcgisonline.com
Javascript API URL :	http://js.arcgis.com/3.15/init.js
Javascript API SDK URL :	http://help.arcgis.com/en/webapi/javascript/arcgis/
Javascript API CSS URL :	http://js.arcgis.com/3.15/dijit/themes/tundra/tundra.css

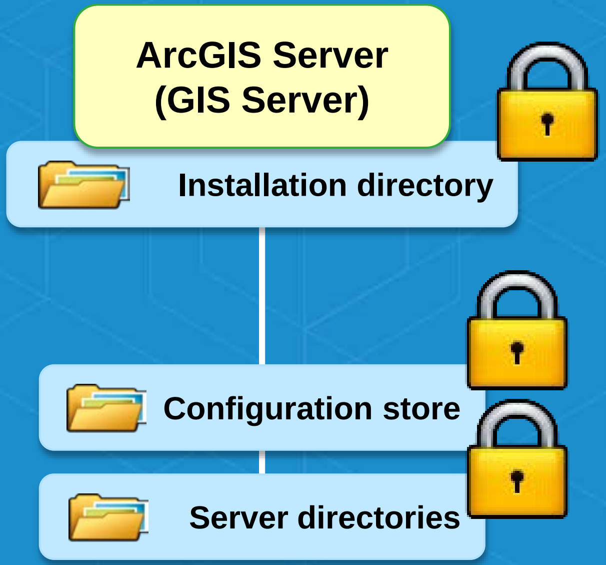
Demo

Restrict Cross-Domain Requests

Restrict File Permissions

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

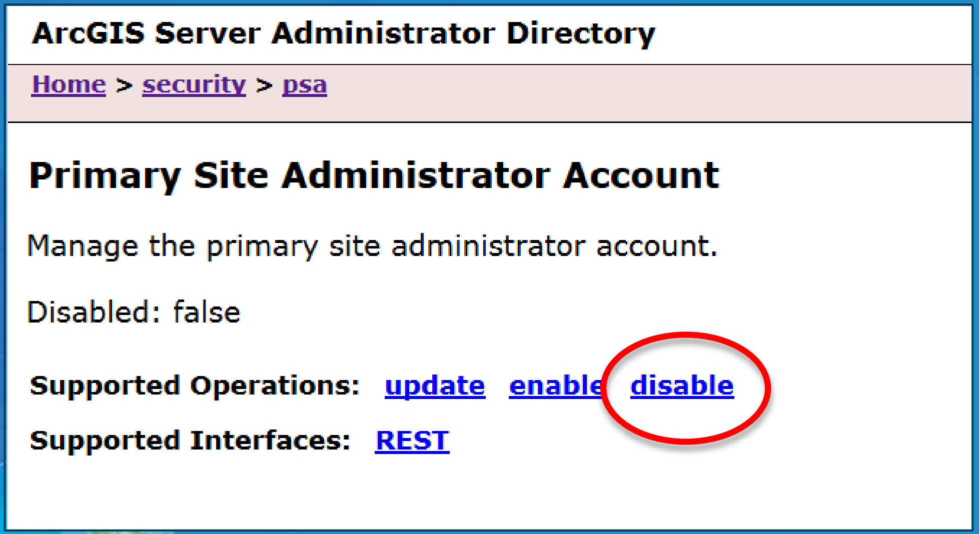
  to the ArcGIS Server account



- 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

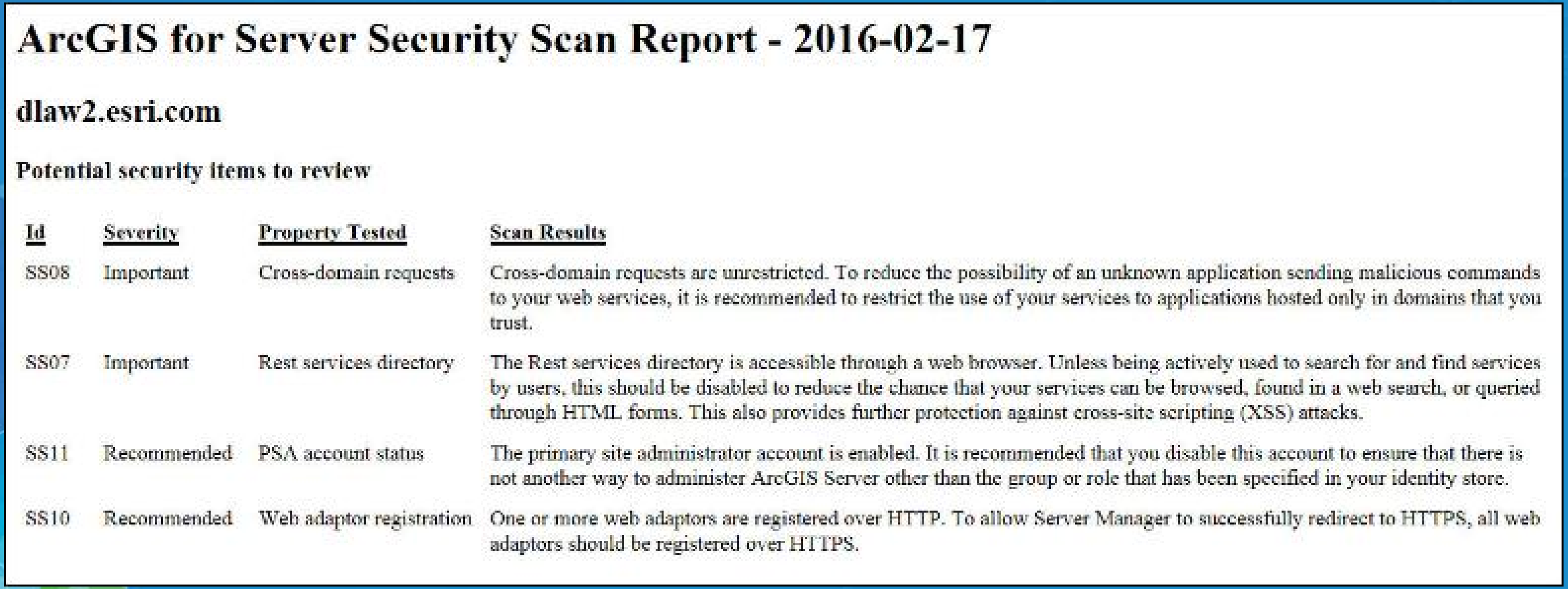
Supported Operations: update enable disable

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

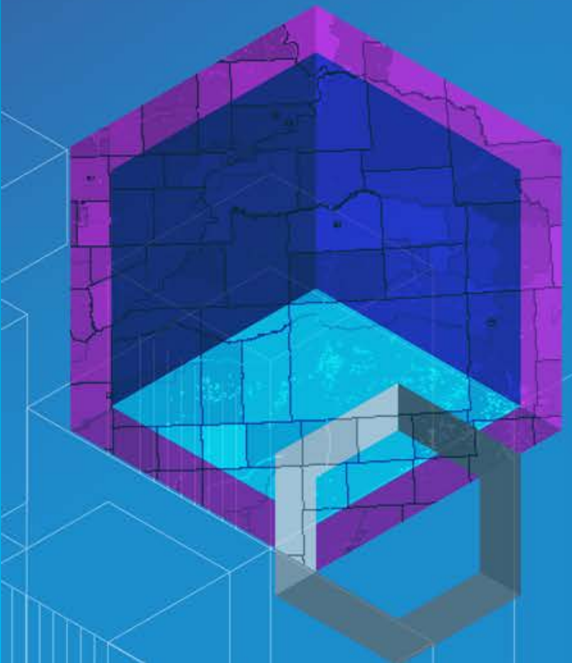


ArcGIS for Server Security Scan Report - 2016-02-17

dlaw2.esri.com

Potential security items to review

Id	Severity	Property Tested	Scan Results
SS08	Important	Cross-domain requests	Cross-domain requests are unrestricted. To reduce the possibility of an unknown application sending malicious commands to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust.
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.
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.
SS10	Recommended	Web adaptor registration	One or more web adaptors are registered over HTTP. To allow Server Manager to successfully redirect to HTTPS, all web adaptors should be registered over HTTPS.



Demo

Run *serverScan.py* Security Check

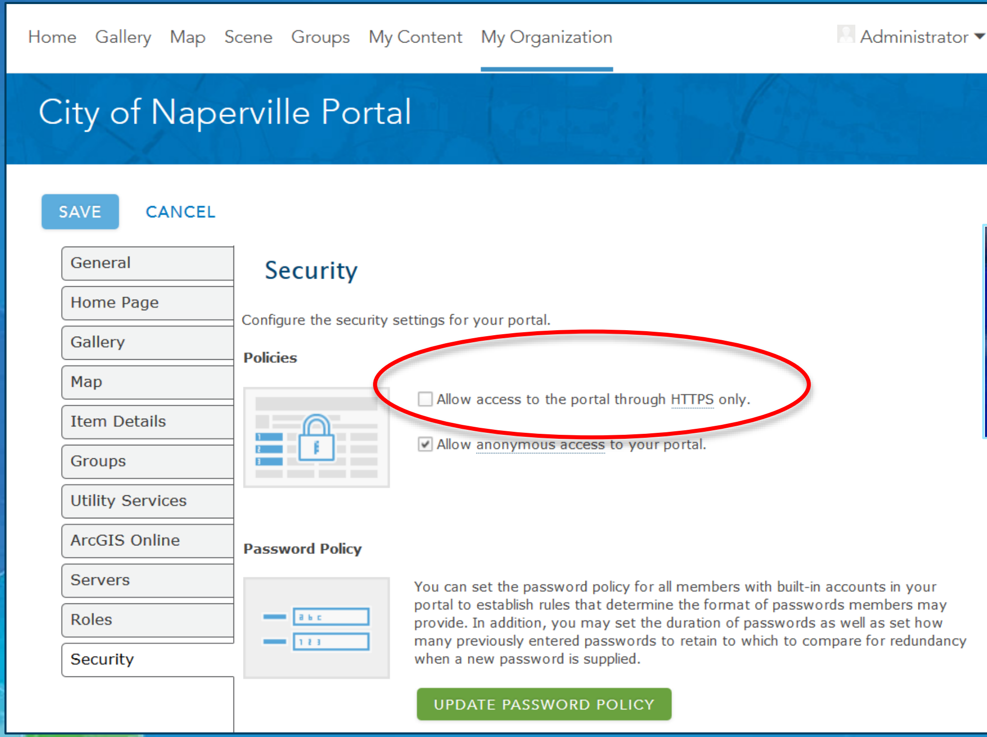
Agenda

- GIS Server
- Portal for ArcGIS
  - Enforce HTTPS Communication only
  - Disable ArcGIS Portal Directory (aka Sharing API)
  - Restrict proxies
  - Disable the ‘Create Account’ button on the sign-in page
  - Trusted servers list
  - Scan Portal script
- Advanced options

Portal for ArcGIS
ArcGIS Server (GIS Server)

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.

Password Policy

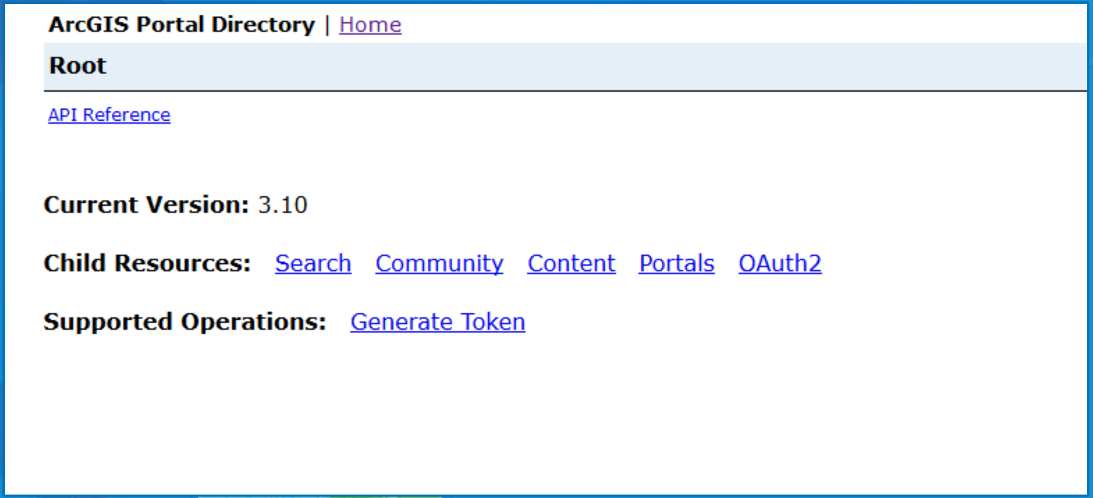
You can set the password policy for all members with built-in accounts in your portal to establish rules that determine the format of passwords members may provide. In addition, you may set the duration of passwords as well as set how many previously entered passwords to retain to which to compare for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

Disable ArcGIS Portal Directory

`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

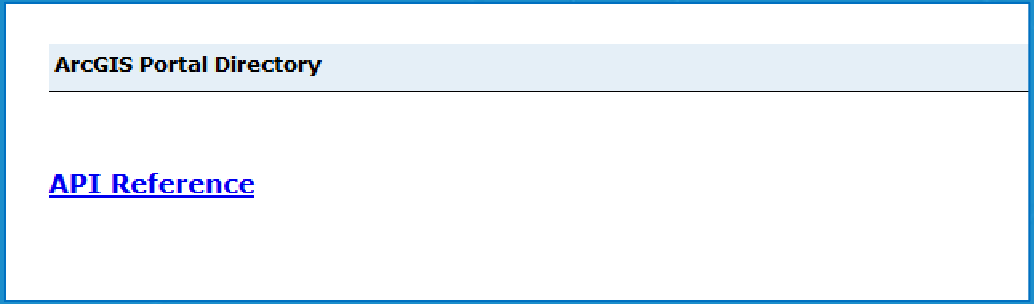
API Reference

Current Version: 3.10

Child Resources: Search Community Content Portals OAuth2

Supported Operations: Generate Token

After

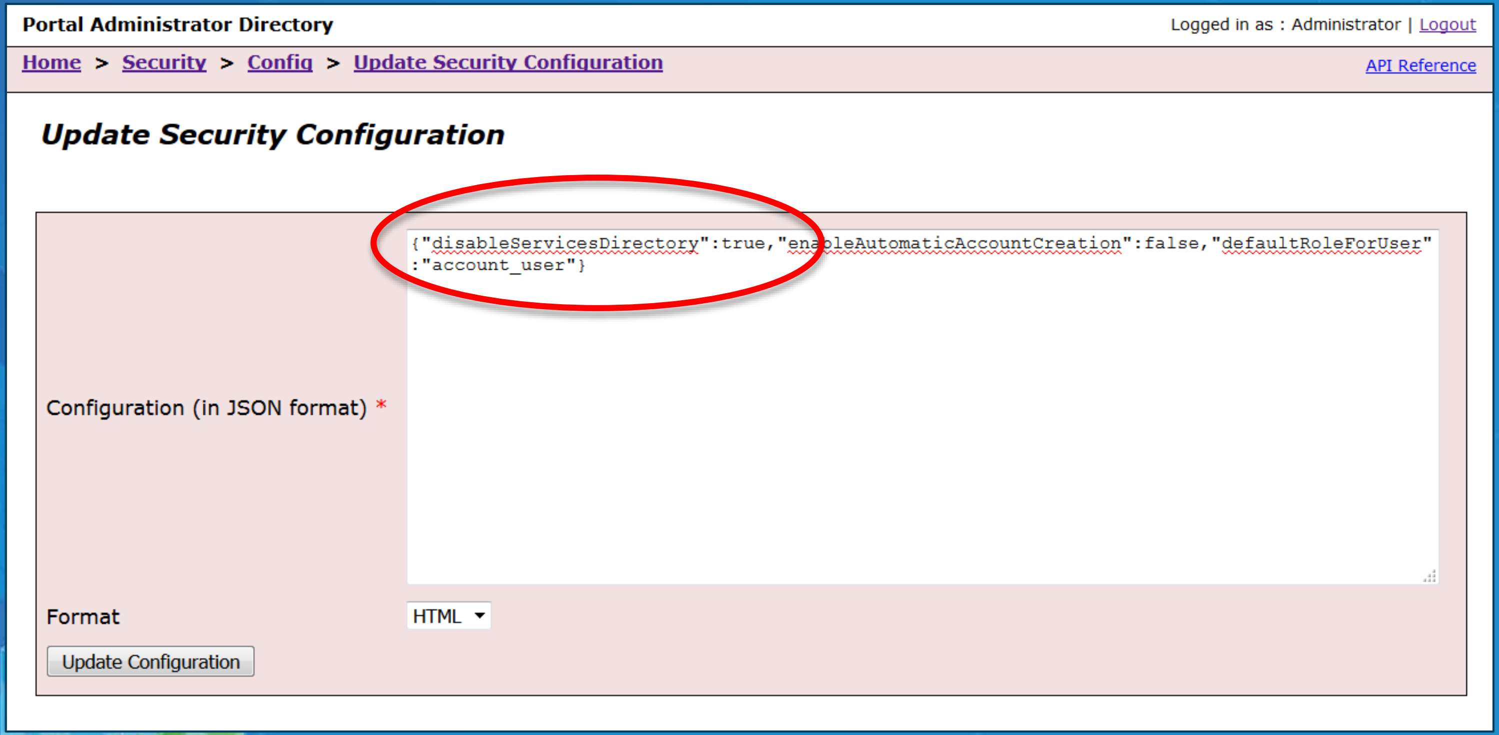


ArcGIS Portal Directory

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

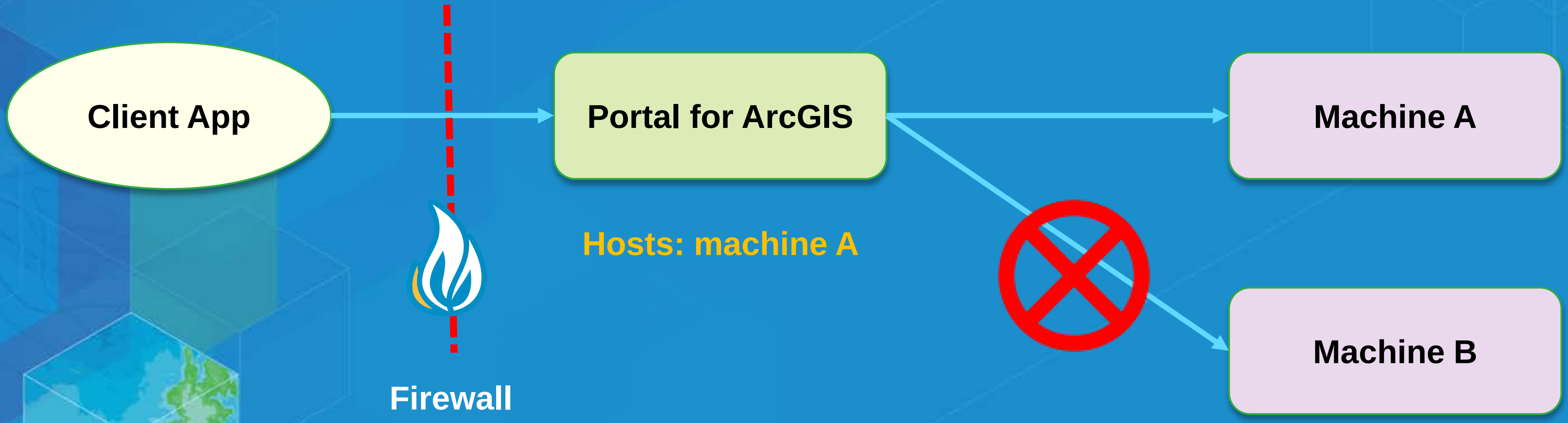
Configuration (in JSON format) *

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

Format: HTML

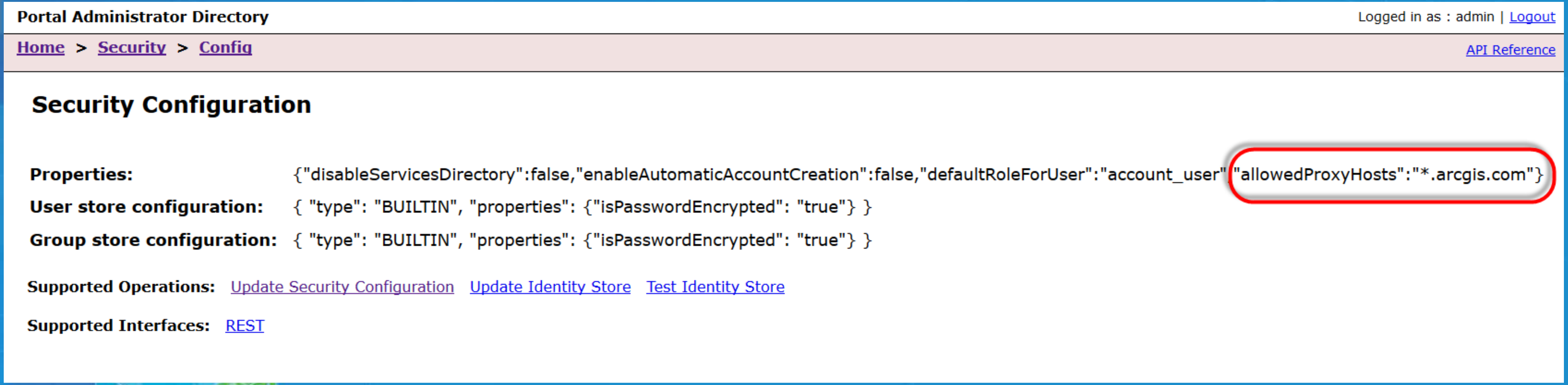
Restrict Proxies

- 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 not “locked down”
  - Could provide access to an internal resource that would normally be blocked by a firewall
- To mitigate this, it is strongly recommended to restrict the portal's proxy to a list of approved machines.



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

Logged in as : admin | Logout

Home > Security > Config

API Reference

Security Configuration

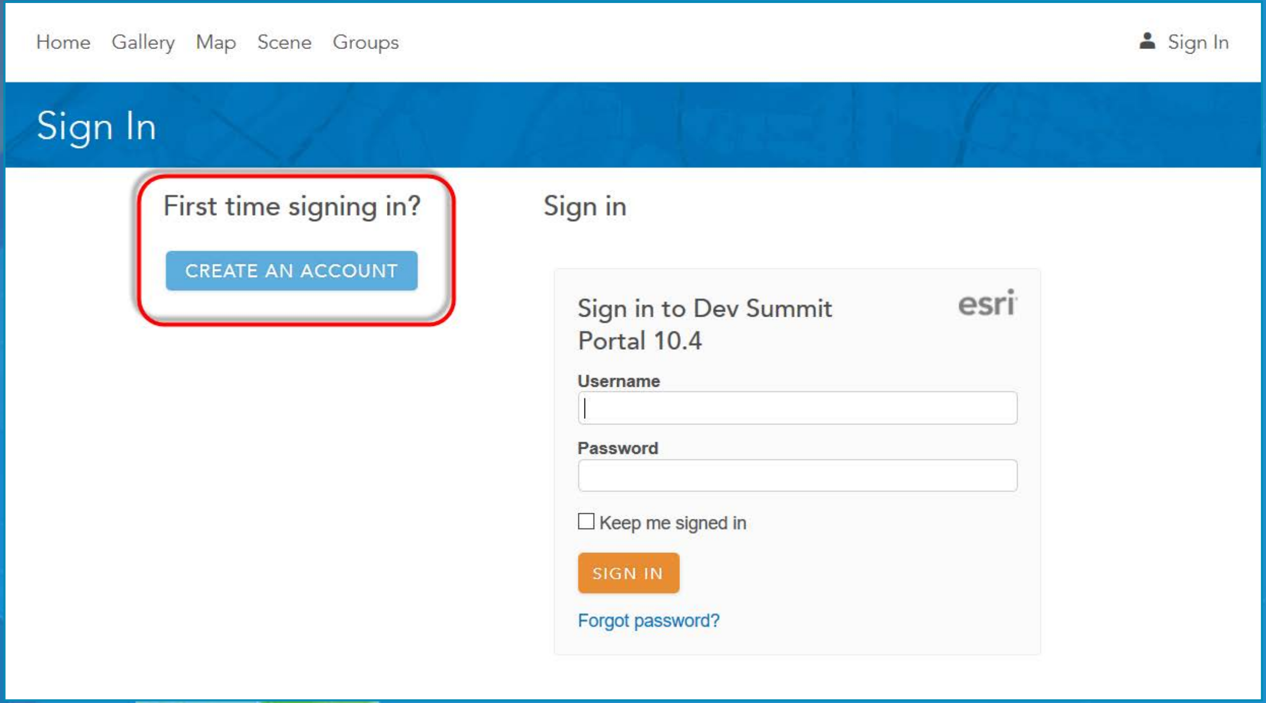
Properties:	{"disableServicesDirectory":false,"enableAutomaticAccountCreation":false,"defaultRoleForUser":"account_user","allowedProxyHosts":"*.arcgis.com"}
User store configuration:	{ "type": "BUILTIN", "properties": {"isPasswordEncrypted": "true"} }
Group store configuration:	{ "type": "BUILTIN", "properties":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

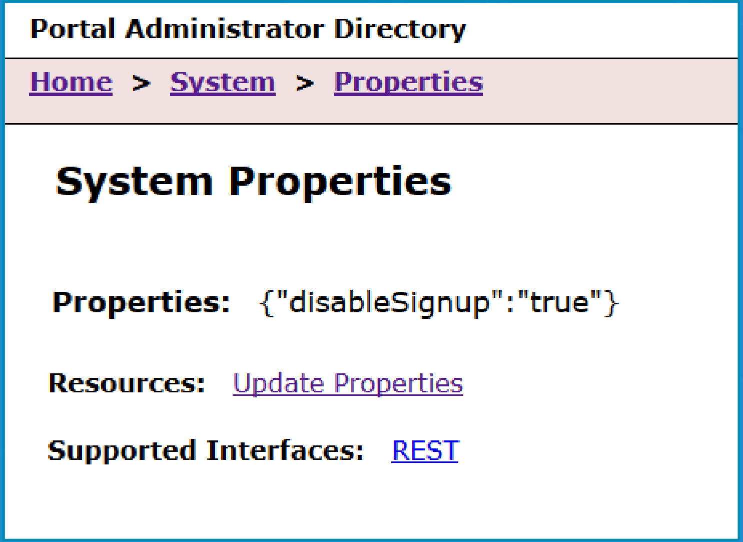
Supported Operations: Update Security Configuration Update Identity Store Test Identity Store

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

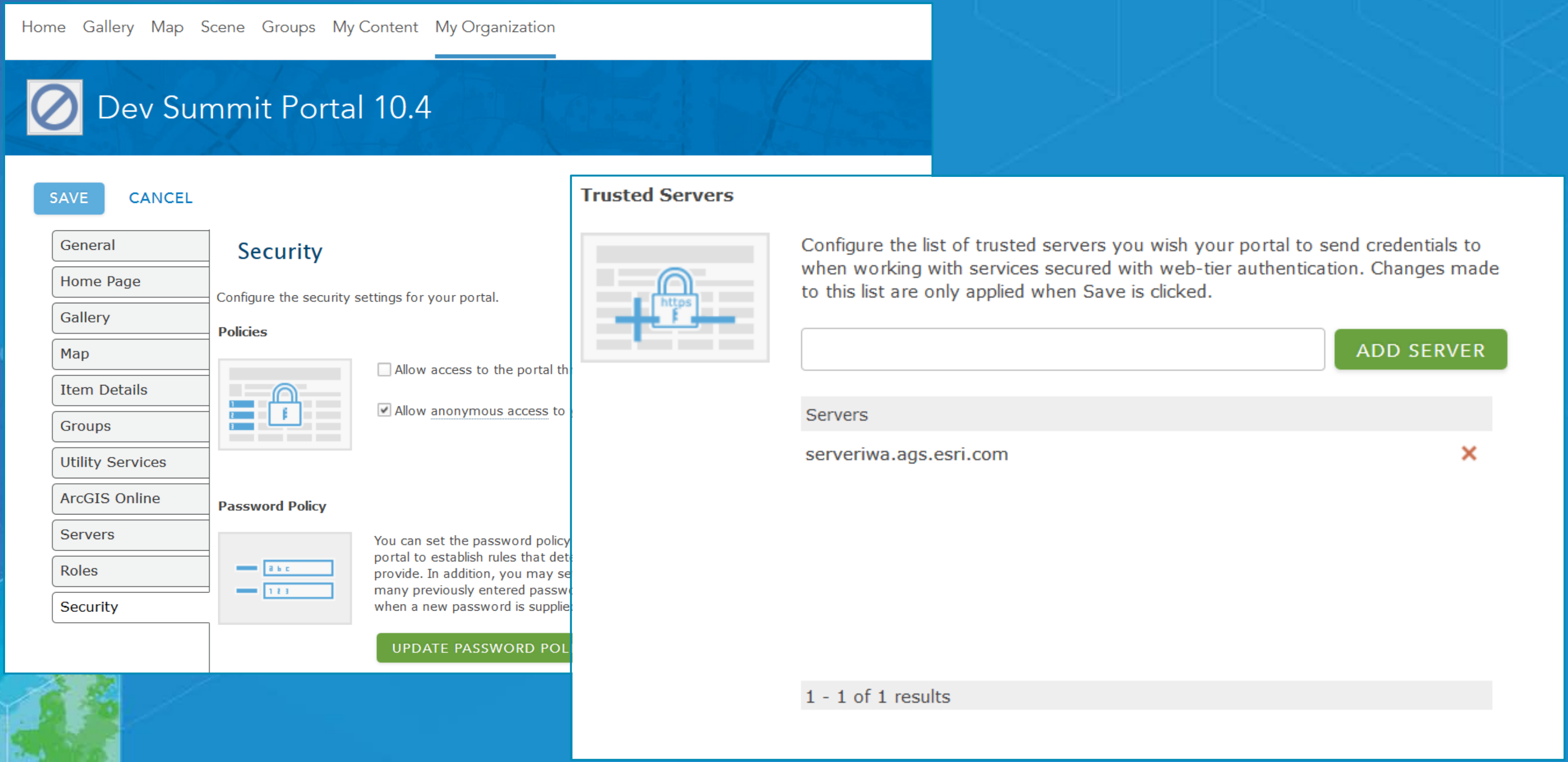
Properties: {"disableSignup":"true"}

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 th

☑ Allow anonymous access to

Password Policy

You can set the password policy portal to establish rules that det provide. In addition, you may se many previously entered passw when a new password is supplie

Trusted Servers

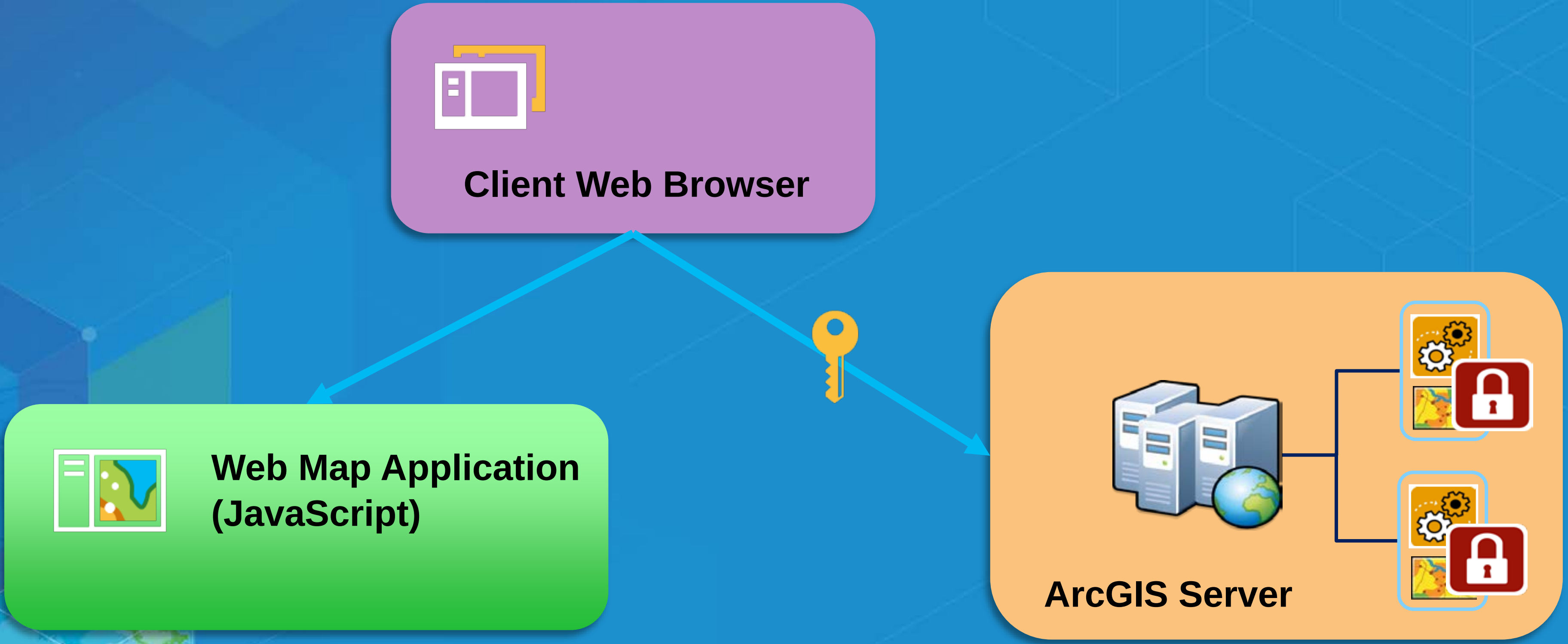
Configure the list of trusted servers you wish your portal to send credentials to when working with services secured with web-tier authentication. Changes made to this list are only applied when Save is clicked.

Servers	
serveriwa.ags.esri.com	✕

1 - 1 of 1 results

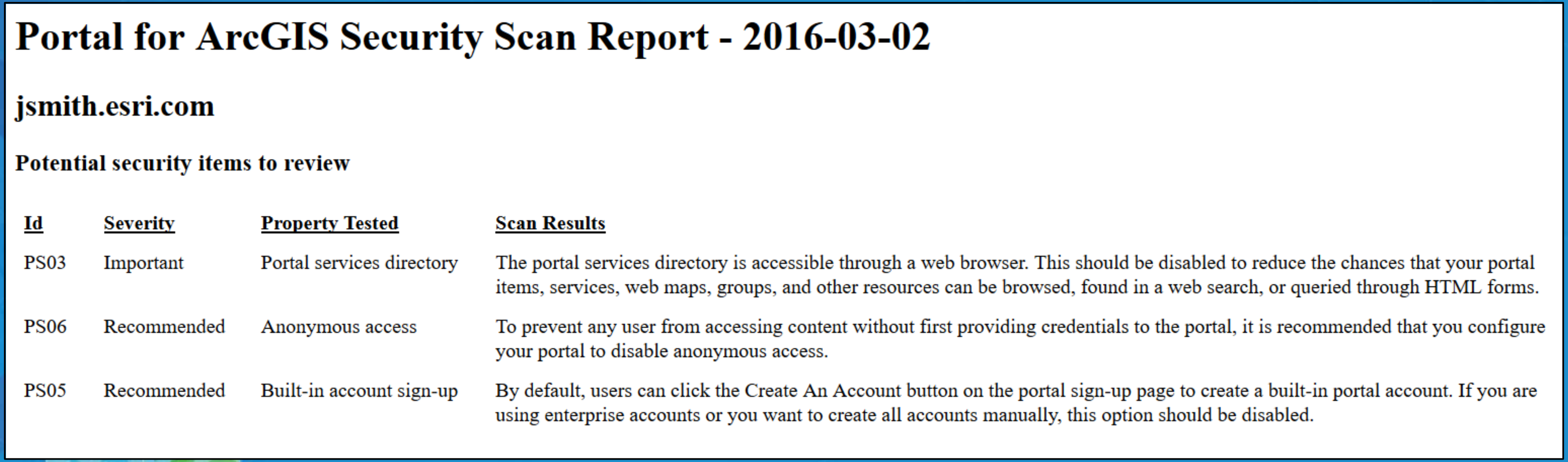
Trusted Servers in Portal

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



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 - 2016-03-02

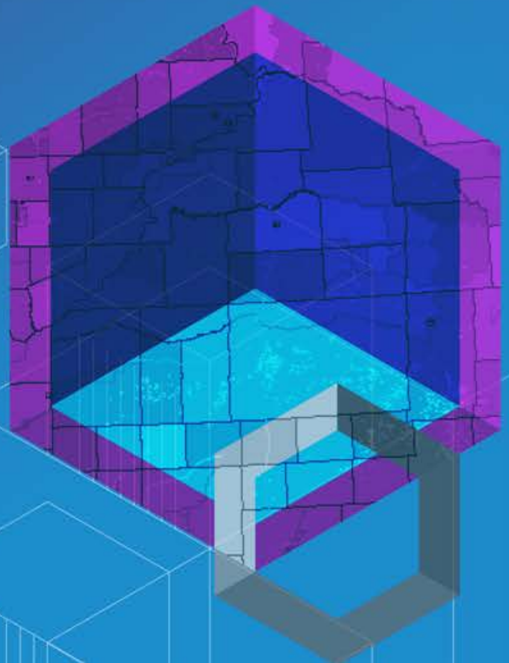
jsmith.esri.com

Potential security items to review

Id	Severity	Property Tested	Scan Results
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.
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.
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.

Demo

Run *portalScan.py* Security Check



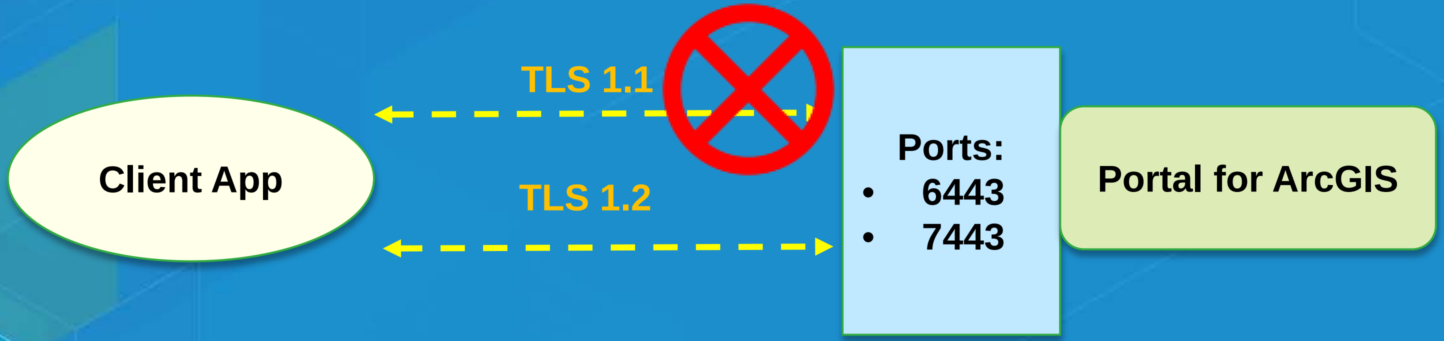
Agenda

- GIS Server
- Portal for ArcGIS
- Advanced options
  - SSL property configurations for Server and Portal
  - Define cipher suites to encrypt communications

Portal for ArcGIS
ArcGIS Server (GIS Server)

SSL Property Configurations

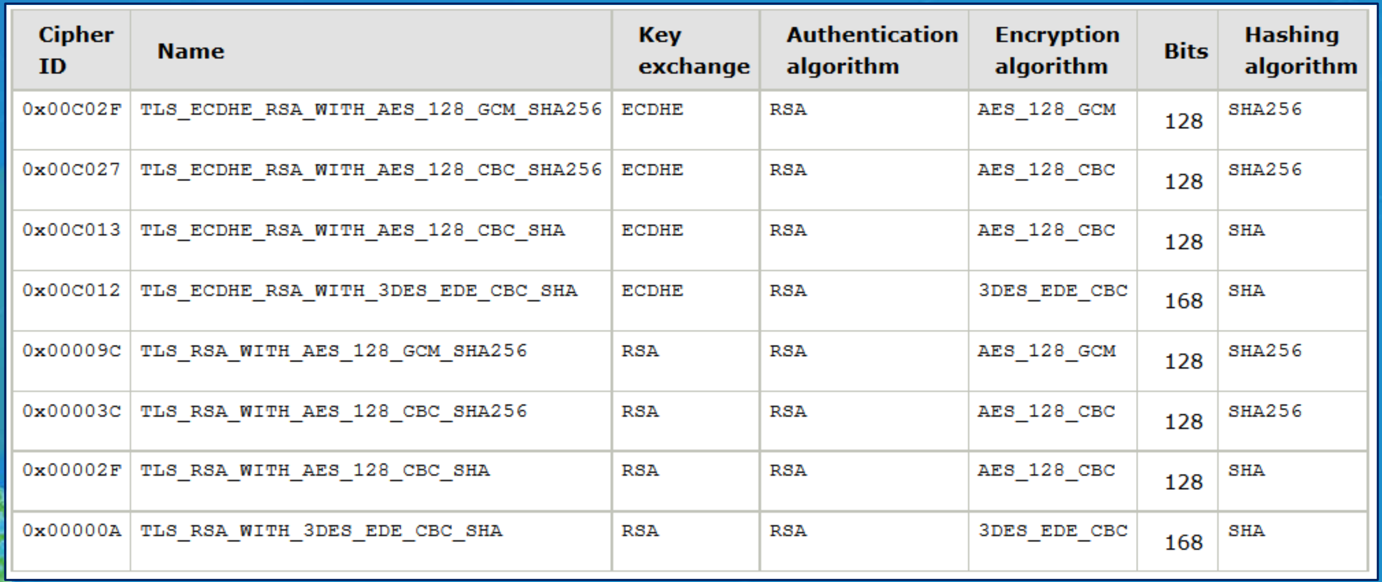
- In 10.4, both Server and Portal can be configured to limit which SSL protocol is accepted and used
- For organizations that are very security-aware, restricting Server and Portal to TLS 1.2 is highly recommended
- TLS (and it predecessor SSL) are cryptographic protocols designed to provide secure network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



Define Cipher Suites to Encrypt Communication

Advanced Settings

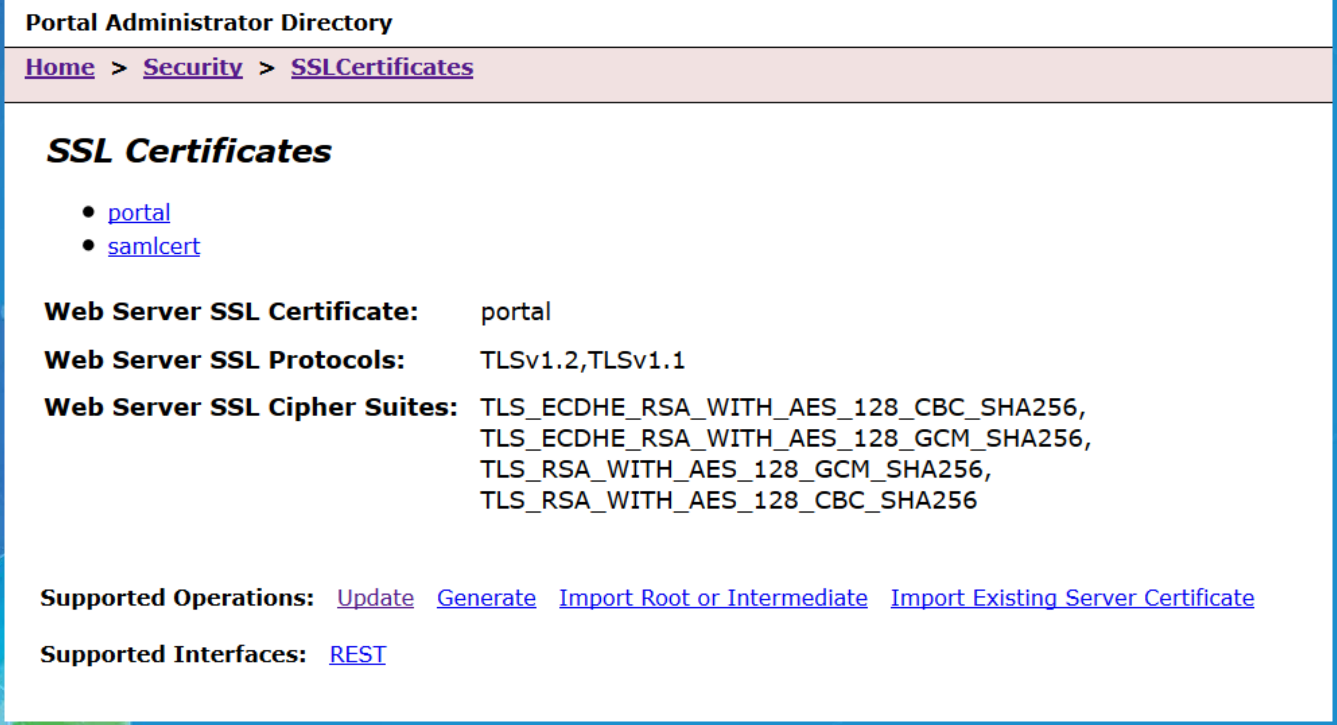
- With the ability to select which set of SSL protocols are used, both Portal and Server now allow users to define which cipher suites are used for encryption.
- A list of encryption algorithms that can be used is provided in the help documentation
- Help topic: Restrict SSL protocols and cipher suites



Cipher ID	Name	Key exchange	Authentication algorithm	Encryption algorithm	Bits	Hashing algorithm
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES_128_GCM	128	SHA256
0x00C027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES_128_CBC	128	SHA256
0x00C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE	RSA	AES_128_CBC	128	SHA
0x00C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE	RSA	3DES_EDE_CBC	168	SHA
0x00009C	TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AES_128_GCM	128	SHA256
0x00003C	TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	RSA	AES_128_CBC	128	SHA256
0x00002F	TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES_128_CBC	128	SHA
0x00000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES_EDE_CBC	168	SHA

How to Define 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

Home > Security > SSLCertificates

SSL Certificates

- portal
- samlcert

Web Server SSL Certificate:	portal
Web Server SSL Protocols:	TLSv1.2,TLSv1.1
Web Server SSL Cipher Suites:	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256

Supported Operations: Update Generate Import Root or Intermediate Import Existing Server Certificate

Supported Interfaces: REST

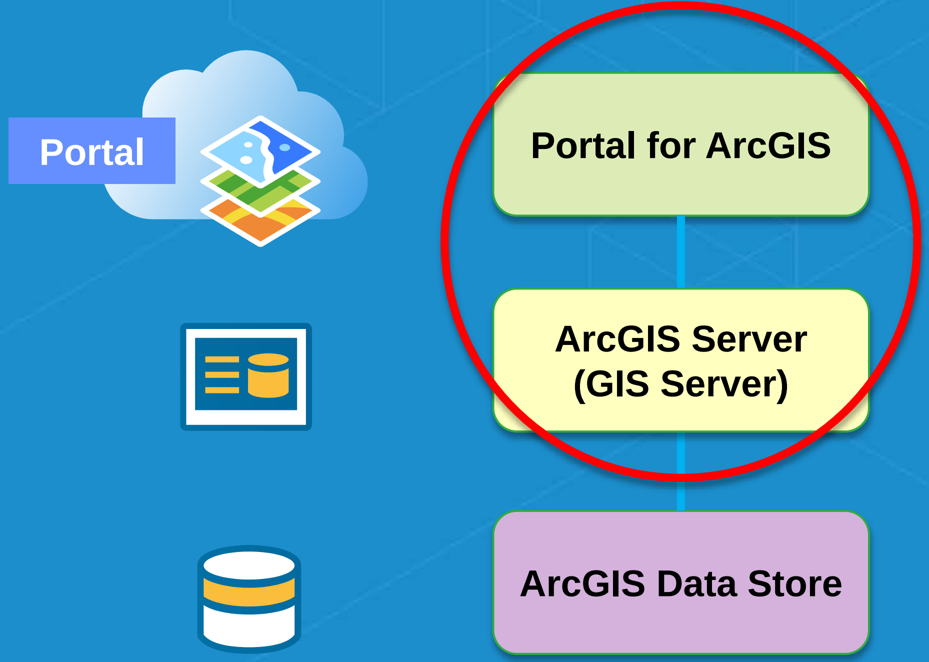
Demo

Define Cipher Suites in Web GIS Security

Summary

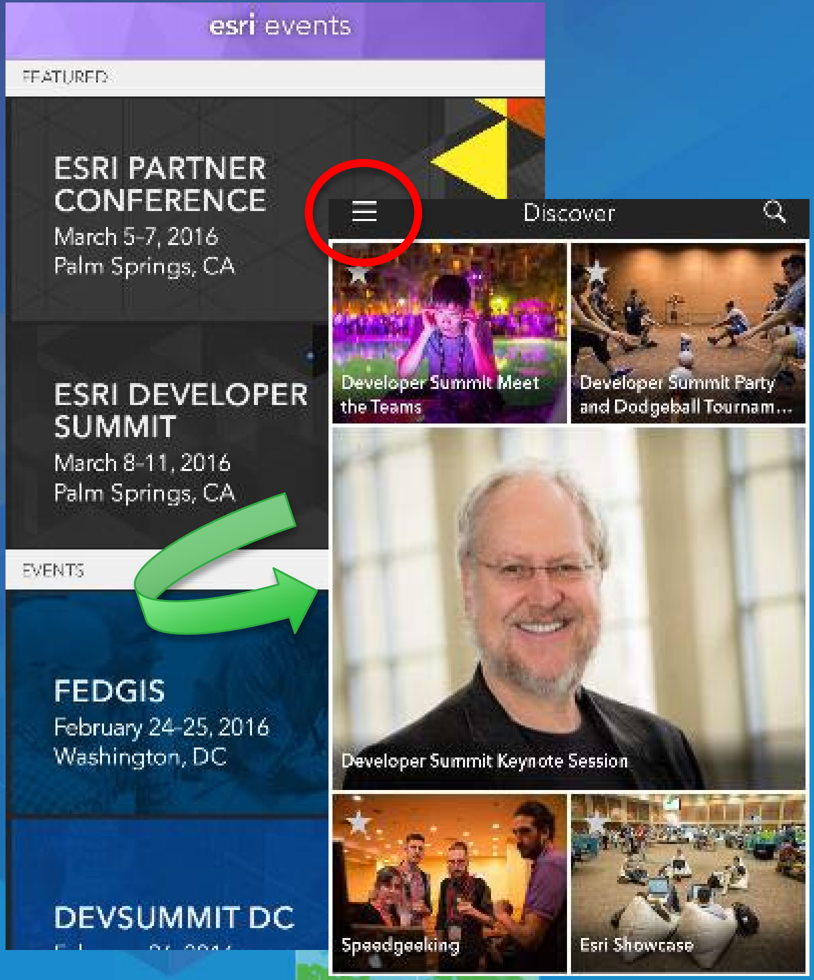
- Discussed and reviewed security best practices for Web GIS on-premises

- GIS Server
- Portal for ArcGIS
- What’s new in 10.4 release

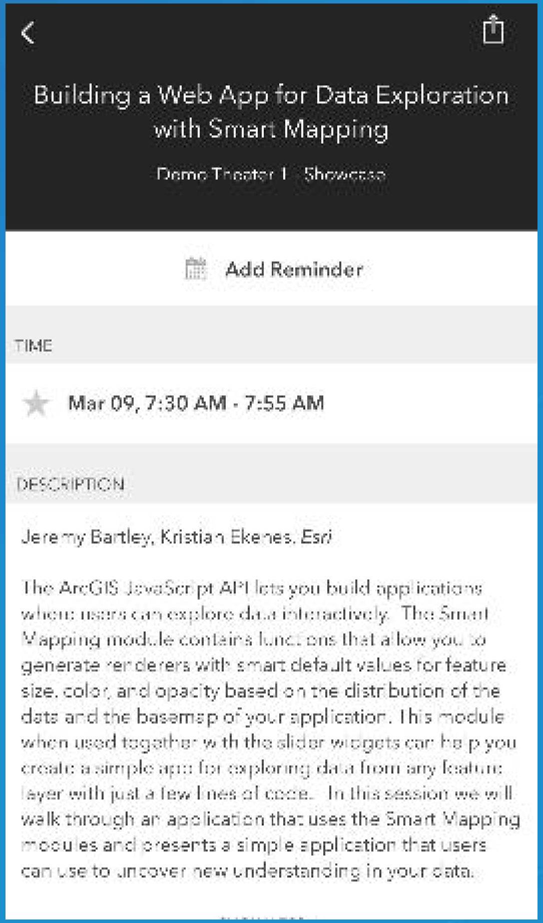


Please Take Our Survey! – No more memorizing Session ID numbers!! ☺

Download the Esri Events app and find your event



Select the session you attended



Building a Web App for Data Exploration with Smart Mapping

Demo Theater 1 - Showcase

TIME

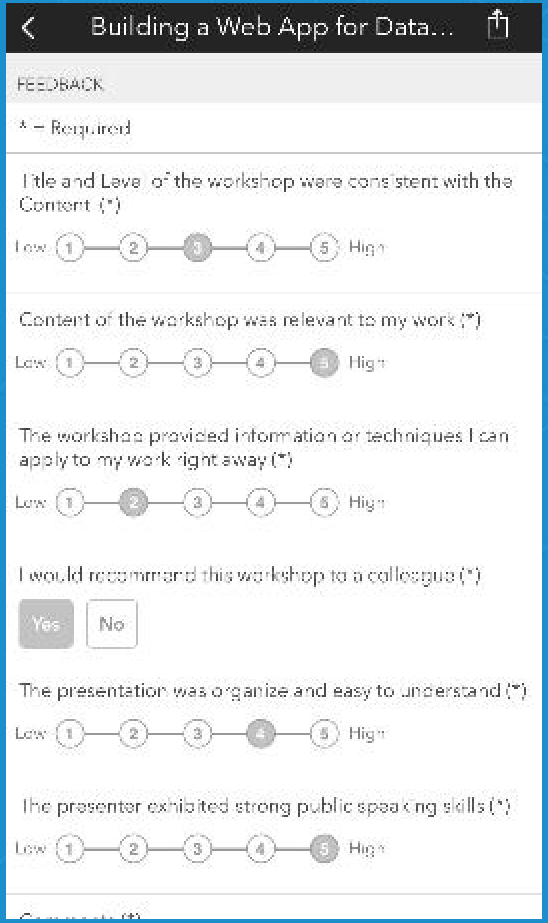
Mar 09, 7:30 AM - 7:55 AM

DESCRIPTION

Jeremy Bartley, Kristian Ekenes, Esri

The ArcGIS JavaScript API lets you build applications where users can explore data interactively. The Smart Mapping module contains functions that allow you to generate renderers with smart default values for feature size, color, and opacity based on the distribution of the data and the basemap of your application. This module when used together with the slider widgets can help you create a simple app for exploring data from any feature layer with just a few lines of code. In this session we will walk through an application that uses the Smart Mapping modules and presents a simple application that users can use to uncover new understanding in your data.

Scroll down to the “Feedback” section



Building a Web App for Data...

FEEDBACK

* = Required

Title and Level of the workshop were consistent with the Content (*)

Low 1 2 [✓ 3] 4 5 High

Content of the workshop was relevant to my work (*)

Low 1 2 3 4 [✓ 5] High

The workshop provided information or techniques I can apply to my work right away (*)

Low 1 [✓ 2] 3 4 5 High

I would recommend this workshop to a colleague (*)

[✓ Yes] No

The presentation was organize and easy to understand (*)

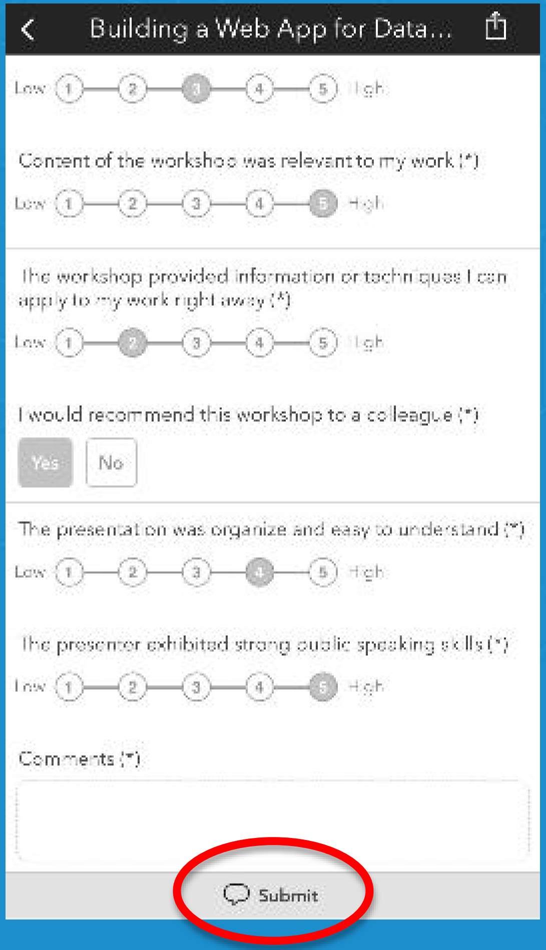
Low 1 2 3 [✓ 4] 5 High

The presenter exhibited strong public speaking skills (*)

Low 1 2 3 4 [✓ 5] High

Comments (*)

Complete Answers, add a Comment, and Select “Submit”



Building a Web App for Data...

Low 1 2 [✓ 3] 4 5 High

Content of the workshop was relevant to my work (*)

Low 1 2 3 4 [✓ 5] High

The workshop provided information or techniques I can apply to my work right away (*)

Low 1 [✓ 2] 3 4 5 High

I would recommend this workshop to a colleague (*)

[✓ Yes] No

The presentation was organize and easy to understand (*)

Low 1 2 3 [✓ 4] 5 High

The presenter exhibited strong public speaking skills (*)

Low 1 2 3 4 [✓ 5] High

Comments (*)

Security Topic Resources

- Securing your ArcGIS Server site
- Best practices for configuring a secure environment
- Disable the Services Directory
- Restricting cross-domain requests to ArcGIS Server
- Restrict SSL protocols and cipher suites

YOUR TITLE HERE

Your Name