



ArcGIS Enterprise: Security Best Practices

Jeff Smith, Randall Williams

2021 ESRI
DEVELOPER SUMMIT

Agenda

- **Focus: Security best practices for ArcGIS Enterprise**
- **ArcGIS Server**
- **Portal for ArcGIS**
- **Advanced Options**



Strongly Recommend:

**Knowledge of ArcGIS Server
and Portal for ArcGIS**

Defense In Depth Paradigm

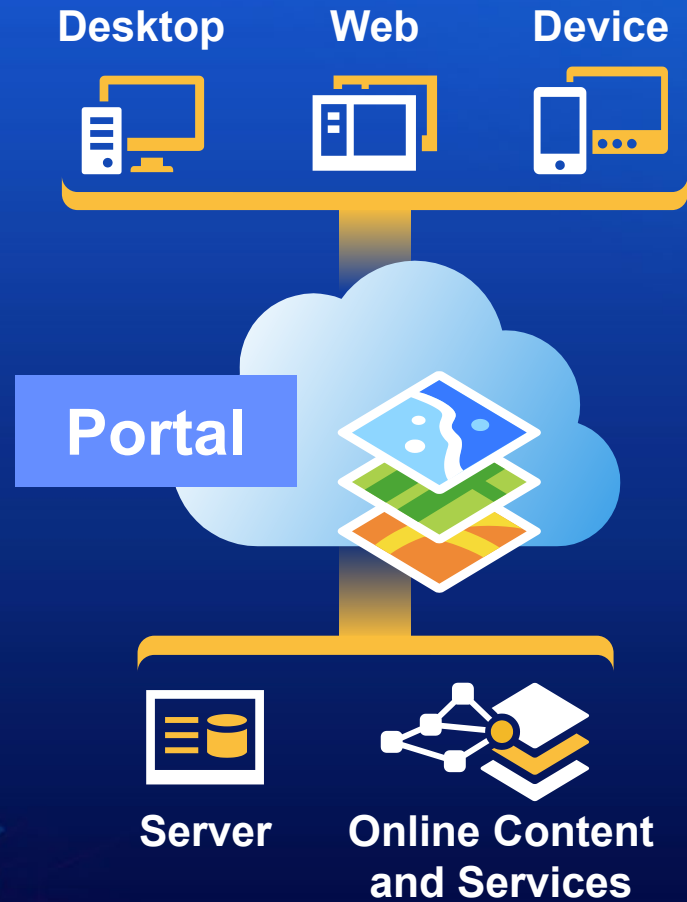
- Security plans have many **“layers”** – multiple levels of security
- Layered security mechanisms increase the security of the system as a whole
- Each feature discussed is considered a “layer”



Review: ArcGIS Enterprise On-Premises

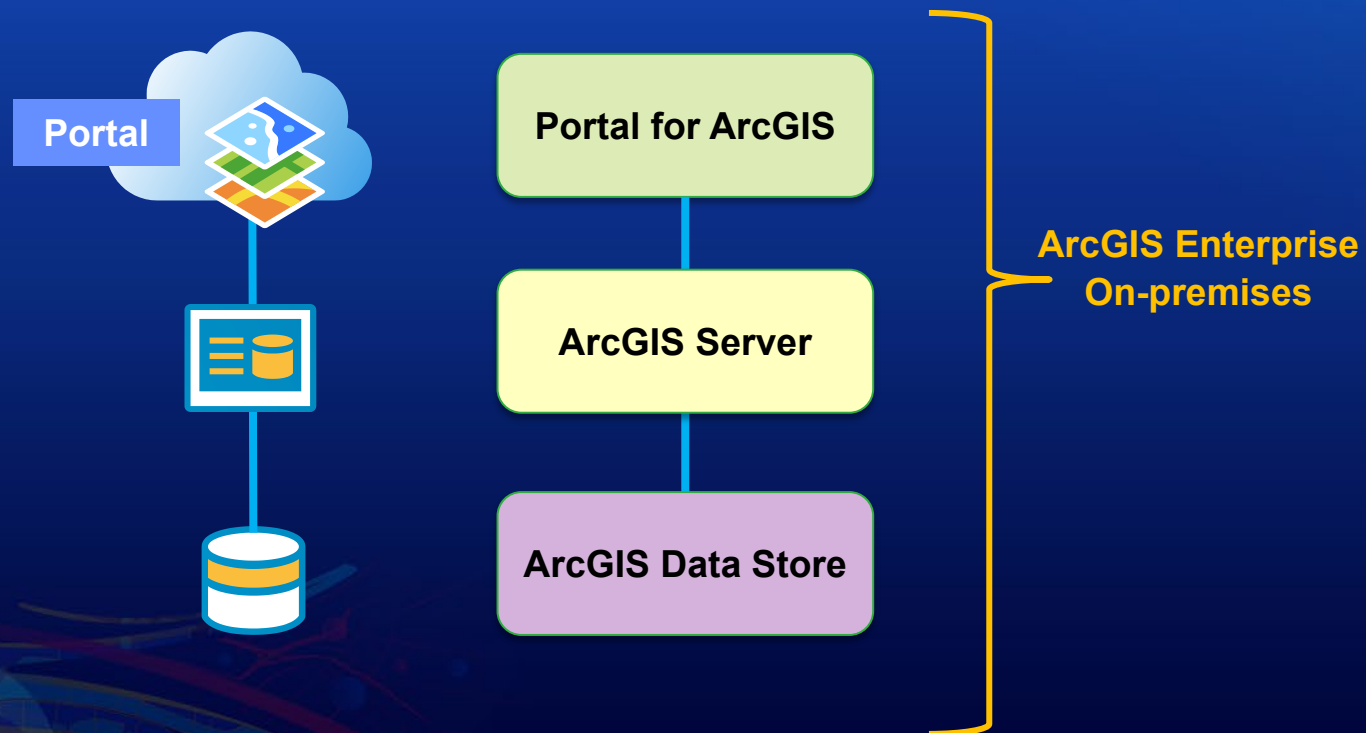
Enabling GIS Everywhere

Simple
Integrated
Open



ArcGIS Enterprise On-Premises: Behind the scenes

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



Check for Updates / Patch Notification

ArcGIS Enterprise Patch Notification

Installed Components

ArcGIS Data Store	10.7.1
ArcGIS Server	10.7.1
Portal for ArcGIS	10.7.1

Available Updates

ArcGIS Data Store

[ArcGIS License Manager 2019.0 License Availability Display Patch](#)
Products: Portal for ArcGIS, ArcMap, ArcGIS Server, ArcGIS Data Store
Release Date: 9/26/19

ArcGIS Server

[ArcGIS License Manager 2019.0 License Availability Display Patch](#)
Products: Portal for ArcGIS, ArcMap, ArcGIS Server, ArcGIS Data Store
Release Date: 9/26/19

[ArcGIS \(Desktop, Engine, Server\) Microsoft \(R \) Windows \(R \) June 2019 Security Update Compatibility Patch](#) ⬇️
Products: ArcGIS Engine, ArcMap, ArcGIS Server
Release Date: 7/23/19

[ArcGIS \(Desktop, Engine, Server\) Support for Oracle 19c Patch](#) ⬇️
Products: ArcGIS Server, ArcMap, ArcGIS Engine
Release Date: 8/29/19

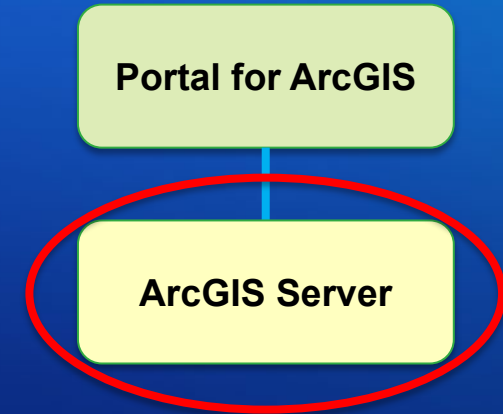
[ArcGIS \(Desktop, Engine, Server\) 10.7.1 Spatial Analyst Patch](#) ⬇️
Products: ArcMap, ArcGIS Server, ArcGIS Engine
Release Date: 1/27/20

[ArcGIS \(Desktop, Engine, Server\) Oracle Data Type Patch](#) ⬇️
Products: ArcGIS Server, ArcMap, ArcGIS Engine
Release Date: 6/4/20

⚙️

Agenda

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



Review: ArcGIS Server Administrator Directory

<https://localhost:6443/arcgis/admin>

- Provides interface into the 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: 10.9.0

Resources: [machines](#) [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
- HTTPS only by default in 10.7
- HSTS can also be used to strictly enforce HTTPS
- ArcGIS Server Admin Directory

Home > security > config > update

ArcGIS Server Administrator Directory

[Home](#) > [security](#) > [config](#) > [update](#)

Update Security Configuration

Warning
Once this operation completes, ArcGIS Server may be restarted. During this time, your ArcGIS Server resources will be temporarily unavailable.

Security Configuration

Protocol:

SSL Protocols:

SSL Cipher Suites:

HTTP Strict Transport Security (HSTS) enabled:

Disable the Services Directory

- ArcGIS REST Services Directory exposes web services api in HTML format
 - <https://server.mydomain.com/arcgis/rest>
- Recommended NOT to expose REST services directory on Production Servers



Before

ArcGIS REST Services Directory

[Home](#) > [services](#)

[JSON](#) | [SOAP](#)

Folder: /

Current Version: 10.9

View Footprints In: [ArcGIS Online Map Viewer](#)

Folders:

- [System](#)
- [Utilities](#)

Services:

- [Colorado](#) (FeatureServer)
- [Colorado](#) (MapServer)
- [SampleWorldCities](#) (MapServer)

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**

- Home > system > handlers > rest > servicesdirectory > edit
- Uncheck *Services Directory Enabled* option

ArcGIS Server Administrator Directory

[Home](#) > [system](#) > [handlers](#) > [rest](#) > [servicesdirectory](#)

Services Directory

Services Directory : Enabled.

AllowedOrigins : *

Javascript API URL : <https://js.arcgis.com/4.14/>

Javascript API SDK URL : <https://developers.arcgis.com/javascript/>

Javascript API CSS URL : <https://js.arcgis.com/4.14/esri/css/main.css>

ArcGIS.com Map Text : ArcGIS Online Map Viewer

ArcGIS.com URL : <https://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 : <https://js.arcgis.com/4.14/>

Javascript API SDK URL : <https://developers.arcgis.com/javascript/>

Javascript API CSS URL : <https://js.arcgis.com/4.14/esri/css/main.css>

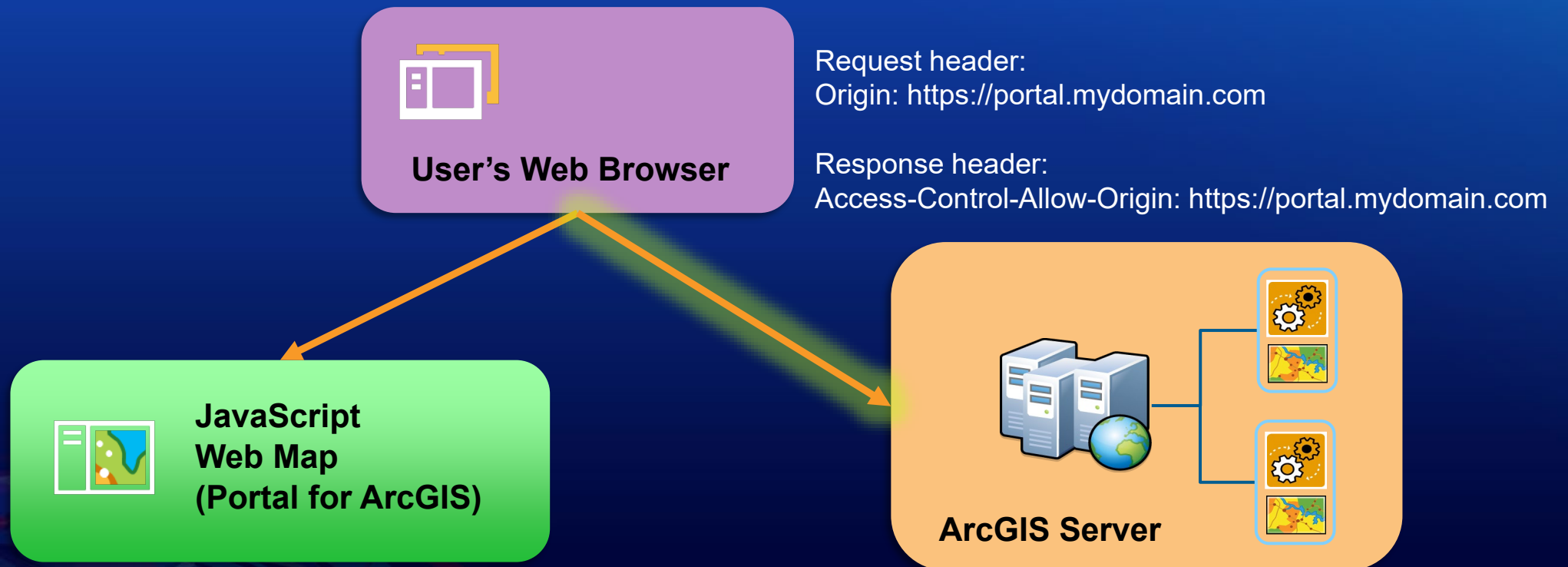
ArcGIS.com Map Text : ArcGIS Online Map Viewer

ArcGIS.com URL : <https://www.arcgis.com/home/webmap/view>

Restrict Cross-Domain (CORS) Requests

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

- **For JavaScript** applications, a common method used to make cross domain requests is called a CORS request (cross origin resource sharing)
- Used by default when retrieving JSON strings from external resources



How to Restrict Cross-Domain Requests

- By default, ArcGIS Server allows all cross-domain requests
- These can be restricted in the Server Administrator Directory
 - Home > system > handlers > rest > servicesdirectory > edit
 - AllowedOrigins - specify a comma-separated list of domain names that are allowed to make CORS requests to access your web services
- Does NOT restrict overall access to the web services

ArcGIS Server Administrator Directory

[Home](#) > [system](#) > [handlers](#) > [rest](#) > [servicesdirectory](#)

Services Directory

Services Directory : Enabled.

AllowedOrigins : **https://www.arcgis.com, https://portal.mydomain.com**

Javascript API URL : https://js.arcgis.com/4.14/

Javascript API SDK URL : https://developers.arcgis.com/javascript/

Javascript API CSS URL : https://js.arcgis.com/4.14/esri/css/main.css

The background features a vibrant, abstract digital graphic. It consists of various overlapping shapes and lines in shades of blue, red, and yellow. Some elements resemble stylized data points or network connections, while others are more fluid, organic forms. The overall aesthetic is modern and tech-oriented, set against a gradient background that transitions from a deep blue on the left to a lighter cyan on the right.

Restrict Cross-Domain Requests

Demo

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
 - Home > Security > PSA > disable

ArcGIS Server Administrator Directory

[Home](#) > [security](#) > [psa](#)

Primary Site Administrator Account

Manage the primary site administrator account.

Disabled: false

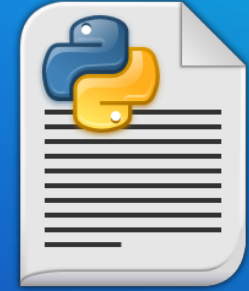
Supported Operations: [update](#) [enable](#) [disable](#)

Supported Interfaces: [REST](#)



PSA account

Scan GIS Server for Security Checks



- **serverScan.py** is a Python script in the Server installation directory
 - Located: `<install directory>\ArcGIS\Server\tools\admin`
- Checks for security configuration settings
 - 10.9 – 15 different settings are checked
- Generates an HTML report that makes recommendations to improve security
- Categorizes findings based on severity
 - Critical
 - Important
 - Recommended
- Help links provided for each finding
- Compatible with both Python 2.7 and 3.x

Sample ArcGIS Server Security Scan Report

ArcGIS Server Security Scan Report - 02/05/21

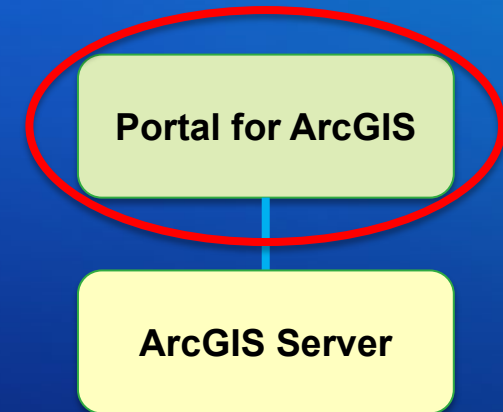
devsummit.webgtesting.net (10.9)

Potential security items to review

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
SS01	Critical	Web communication	HTTPS is not enabled for ArcGIS Server. To prevent the interception of any communication, it is recommended that you configure ArcGIS Server and ArcGIS Web Adaptor (if installed) to enforce SSL encryption.
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. 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.
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 configuration. More information

Agenda

- ArcGIS Server
- **Portal for ArcGIS**
 - **Feature Layer Security**
 - **Enforce HTTPS Communication only**
 - **Multifactor Authentication**
 - **Disable ArcGIS Portal Directory (aka Sharing API)**
 - **Restrict proxies**
 - **Restrict cross-domain (CORS) requests**
 - **Trusted Servers**
 - **Scan Portal script**
- **Advanced options**



Feature Layer Security and Editing

- Users who can always edit
 - Owner
 - Admins
 - Members of Groups w/ Update capability
- Enable Editing
 - Anyone who can access the service
 - Options
 - Add, update and delete features
 - Only update feature attributes
 - Only add new features
 - ...

General Feature Layer (hosted)

Editing

- Enable editing.
This layer is shared with everyone. Enabling editing means everyone can edit it. If that isn't your intent, create a view of this layer that allows editing. [Learn more.](#)
- Keep track of who created and last updated features.
- Enable Sync (disconnected editing with synchronization).

- Who can edit features?
Share the layer to specific groups of people, the organization or publicly via the Share button on the Overview tab. This layer is currently shared with: Everyone (public)
- What kind of editing is allowed?
 - Add, update, and delete features
 - Add and update features
 - Add features
 - Update features
 - Update attributes only
- What features can editors see?
 - Editors can see all features
 - Editors can only see their own features (requires tracking)
 - Editors can't see any features, even those they add
- What features can editors edit?
 - Editors can edit all features
 - Editors can only edit their own features (requires tracking)
- Who can manage edits?
 - You
 - Administrators
 - Data curators with the appropriate privileges

Enable HTTPS Communication

- Enforce HTTPS so that all communication in your portal is encrypted
 - Set by default in 10.7



The screenshot shows the 'Security' settings page in ArcGIS Online. On the left is a navigation menu with options: General, Home page, Gallery, Map, Items, Groups, Utility services, ArcGIS Online, Servers, Member roles, New member defaults, Collaborations, Security (highlighted), and Organization extensions. The main content area is titled 'Security' and contains several sections:

- Policies**
 - HTTPS**: A red oval highlights this section, which contains the toggle 'Allow access to the portal through HTTPS only.' which is currently turned on (blue).
- Access and permissions**
 - 'Allow anonymous access to your portal.' (turned on)
 - 'Allow members to edit biographical information and who can see their profile.' (turned on)
 - 'Allow users to create new built-in accounts.' (turned off)
- Sharing and searching**
 - 'Members can share content publicly.' (turned on)
 - 'Show social media links on item and group pages.' (turned off)

Multifactor Authentication

- New in 10.9, administrators can enable the option to allow members to choose whether to set up multifactor authentication for their built-in portal accounts
- Requirements:
 - 2 administrator accounts
 - Email configuration

Multifactor authentication

Multifactor authentication provides all members with built-in portal accounts in your organization with an extra level of security by requesting an additional verification code at the time of login. Email settings must be configured to enable Multifactor authentication. [Learn more](#)

Allow members to choose whether to set up multifactor authentication for their individual accounts.



Designated administrators

Designate at least two administrators who will receive email requests to troubleshoot members' multifactor authentication issues.

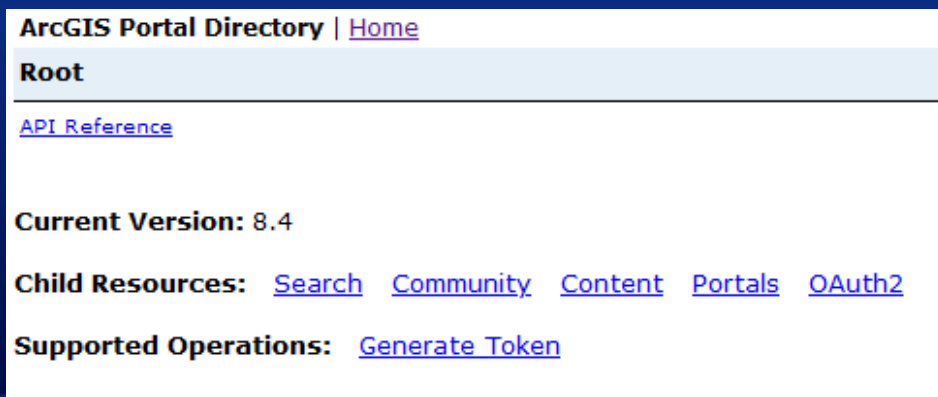
Add

Disable ArcGIS Portal Directory (Production Environment)

`https://portal.mydomain.com/arcgis/sharing/rest`

- Provides a browsable HTML-based representation of all of Portal items
 - services, web maps, and content
- Recommend disabling 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](#)

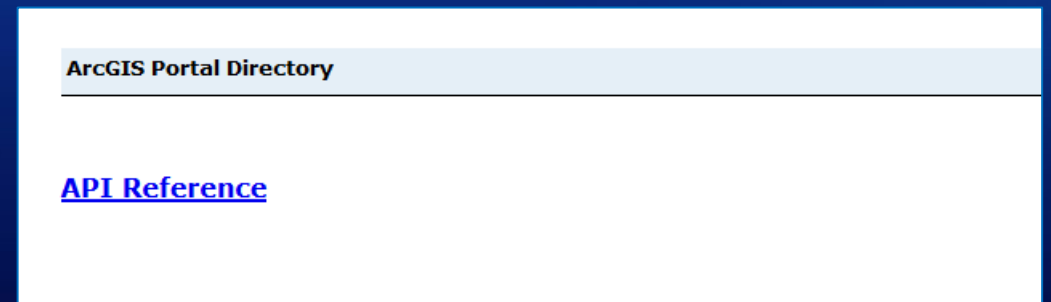
Current Version: 8.4

Child Resources: [Search](#) [Community](#) [Content](#) [Portals](#) [OAuth2](#)

Supported Operations: [Generate Token](#)



After

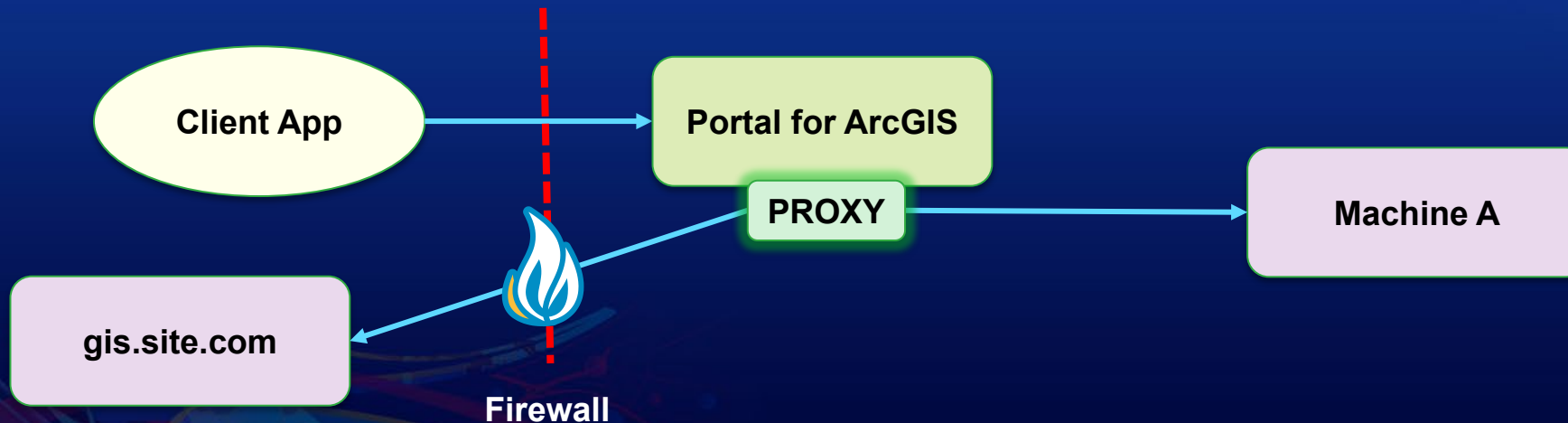


ArcGIS Portal Directory

[API Reference](#)

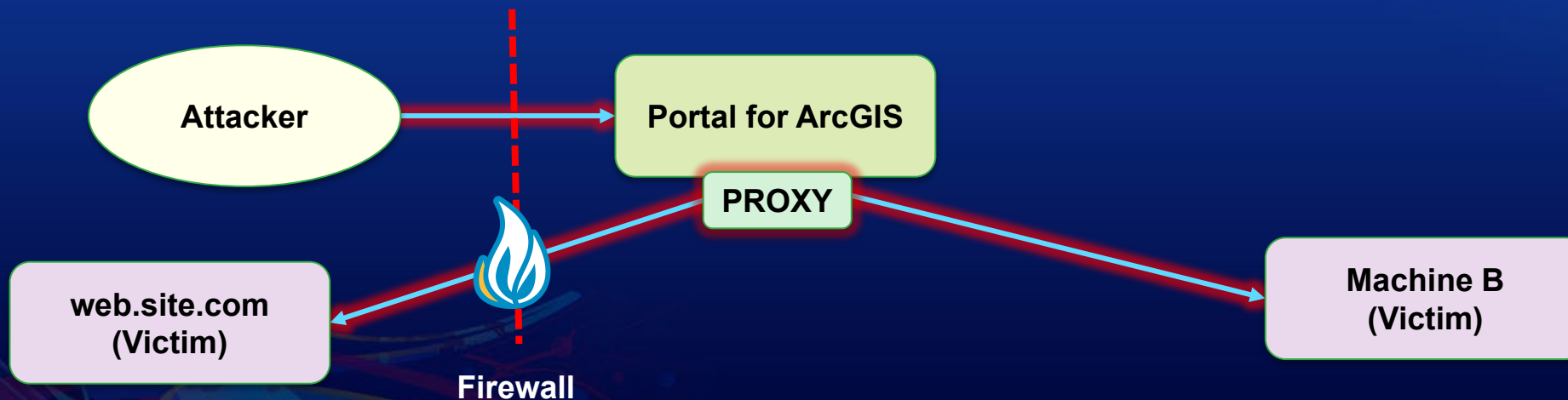
Restrict Machines Accessible by Portal Proxy

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on different machines
 - Storing credentials (ex. secured services, Online premium services)
 - Adding OGC services to Content
 - Accessing services from non-CORS systems



Restrict Machines Accessible by Portal Proxy

- By default the portal's proxy is open
 - No restrictions on what can be accessed through the proxy
- 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](#) > [Update Security Configuration](#)

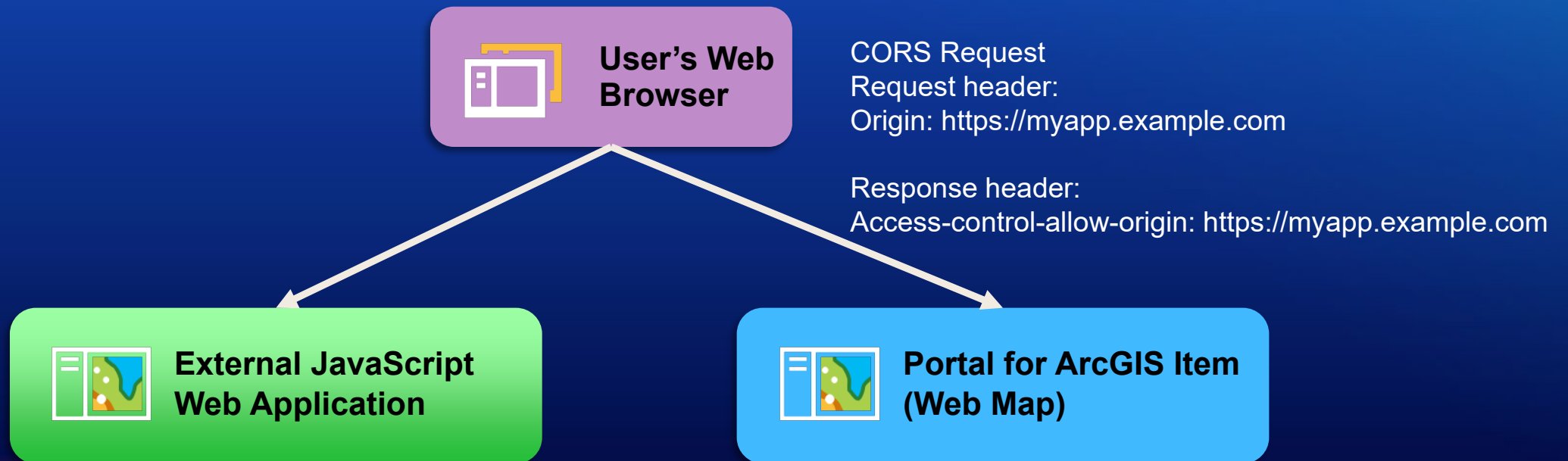
Update Security Configuration

```
Configuration (in JSON format) *  
{  
  "disableServicesDirectory":false,  
  "enableAutomaticAccountCreation":true,  
  "webgisServerTrustKey":"  
  "allowedProxyHosts": "(.*) .webgistesting.net"}  
}
```

Format

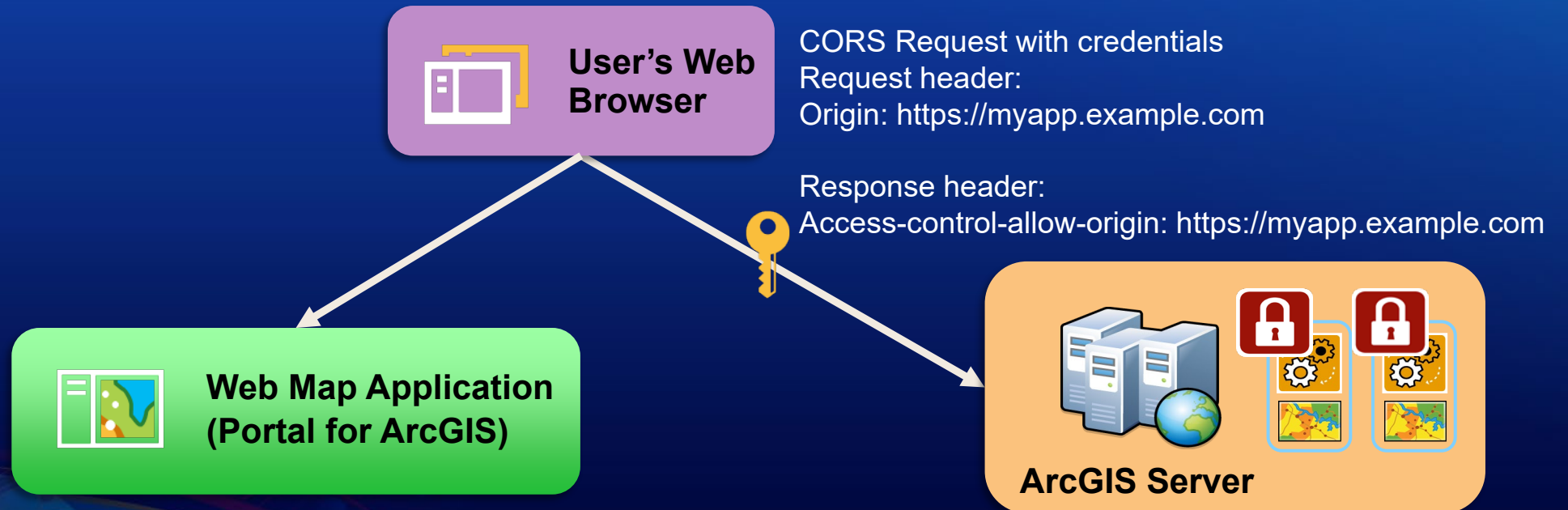
CORS Request From External JavaScript App to Portal Item

- Web applications hosted on a different server than Portal utilize CORS requests to access the Portal items



CORS Request From Portal App to a Secured Service

- CORS request to a service secured with web-tier authentication requires an authentication header be included in the request
- Since the request is asynchronous, the user would not be prompted to enter credentials
- Authentication headers are not included by default in CORS requests
- Managed with Trusted Servers



Trusted Servers and Allow Origins

The image shows a screenshot of the ArcGIS Online interface. The top navigation bar includes Home, Gallery, Map, Scene, Groups, Content, and Organization. The Organization page is active, showing a search bar for 'Search Settings' and a left sidebar with menu items: General, Home page, Gallery, Map, Items, Groups, Utility services, and ArcGIS Online. The main content area is titled 'Security' and contains two sections: 'Policies' and 'Access and permissions'. The 'Policies' section has a single policy: 'Allow access to the portal through HTTPS only.' The 'Access and permissions' section has a single permission: 'Allow anonymous access to your portal.' On the right side, there are two panels: 'Trusted servers' and 'Allow origins'. The 'Trusted servers' panel has an 'Add' button and a list with one entry: 'https://serveriwa.mydomain.com'. The 'Allow origins' panel has an 'Add' button and a list with two entries: 'https://www.arcgis.com' and 'https://portal.mydomain.com'.

Home Gallery Map Scene Groups Content Organization

Dev Summit 2021

Search Settings

General

Home page

Gallery

Map

Items

Groups

Utility services

ArcGIS Online

Security

Policies

HTTPS

Allow access to the portal through HTTPS only.

Access and permissions

Allow anonymous access to your portal.

Trusted servers

Configure the list of trusted servers you wish your organization to send credentials to when working with services secured with web-tier authentication.

Add

https://serveriwa.mydomain.com

Allow origins

Limit the web application domains that can connect via Cross-Origin Resource Sharing (CORS) to the ArcGIS REST API.

Add

https://www.arcgis.com

https://portal.mydomain.com

Sharing Content with Everyone

- Can restrict the ability for users to share items with everyone

Security

Policies

HTTPS

Allow access to the portal through HTTPS only.



Access and permissions

Allow anonymous access to your portal.



Allow members to edit biographical information and who can see their profile.



Allow users to create new built-in accounts.



Sharing and searching

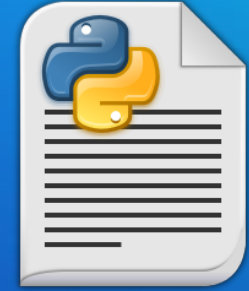
Members can share content publicly.



Show social media links on item and group pages.



Scan Portal for Security Checks



- `portalScan.py` is a script in the Portal installation directory
 - Location: `<install_directory>\ArcGIS\Portal\tools\security`
- Checks for security configuration settings
 - 10.9 – 12 different settings are checked
- Generates an HTML report that makes recommendations to improve security
- Categorizes findings based on severity
 - Critical
 - Important
 - Recommended
- Help links provided for each finding

Sample Portal for ArcGIS Security Scan Report

enterprise.arcgis.com > Search "portalScan.py"

Portal for ArcGIS Security Scan Report - 02/08/21

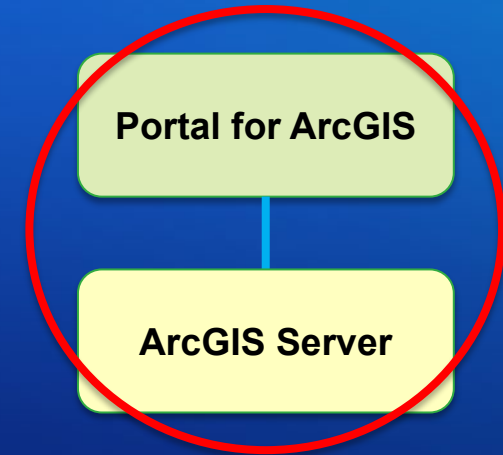
devsummit.webgtesting.net (10.9)

Potential security items to review

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
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 the Home application without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information
PS09	Recommended	Cross-domain requests	Cross-domain (CORS) requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. More information
PS08	Recommended	Portal SSL certificate	To help reduce web browser warnings or other unexpected behavior from clients communicating with your portal, it is recommended to import and use a CA-signed SSL certificate bound to port 7443. More information

Agenda

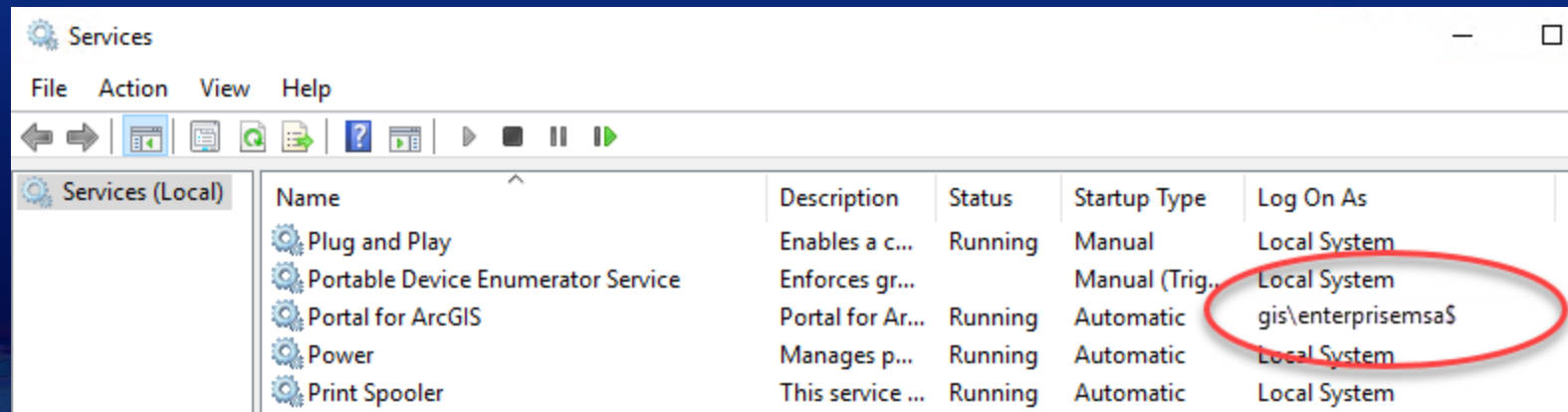
- ArcGIS Server
- Portal for ArcGIS
- **Advanced Topics**
 - **Group Managed Service Account (gMSA)**
 - **SSL protocols for Server and Portal**
 - **Define cipher suites to encrypt communications**



Group Managed Service Accounts (gMSA)

Windows only

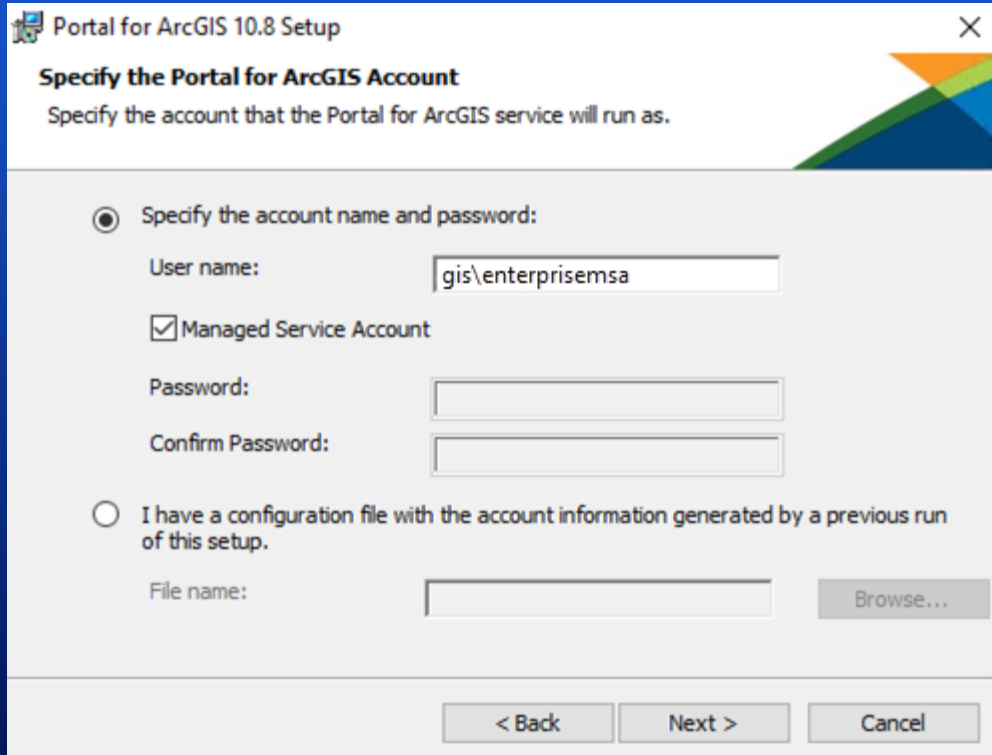
- Restricted Active Directory domain account
- Can only be used in a few places on Windows
 - “Log On As” account for Windows Services
 - IIS application pool identity
 - User account to run scheduled tasks
- “\$” is appended to the end of the account to indicate it is a gMSA



Security benefits of using a gMSA

- Password is managed internally by Active Directory
- Does not have a static password
 - Password is 128 UTF-16 characters
 - Automatically changed every 30 days (by default)
- No interactive logins
- Restricted to a pre-defined set of computers

How to use a gMSA in ArcGIS Enterprise



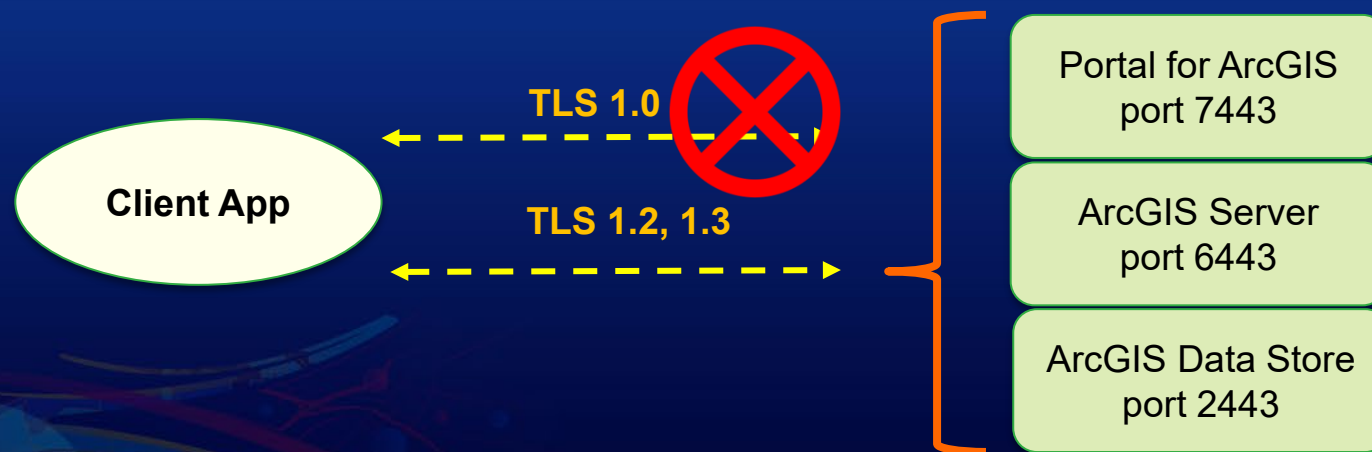
The screenshot shows the 'Portal for ArcGIS 10.8 Setup' window. The title bar reads 'Portal for ArcGIS 10.8 Setup'. The main heading is 'Specify the Portal for ArcGIS Account', with the instruction 'Specify the account that the Portal for ArcGIS service will run as.' below it. There are two radio button options. The first option, 'Specify the account name and password:', is selected. It includes a 'User name:' field containing 'gis\enterprisemsa', a checked 'Managed Service Account' checkbox, and 'Password:' and 'Confirm Password:' fields. The second option, 'I have a configuration file with the account information generated by a previous run of this setup.', is unselected and includes a 'File name:' field and a 'Browse...' button. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

- New installation
- Reconfigure service account tools
- **Note: Service account cannot be changed during an upgrade**

TLS Protocol Configurations

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

- Since 10.4, both Server and Portal can be configured to limit which SSL protocols are accepted
- In 10.9 support for TLS 1.3 was introduced so new installations of ArcGIS Enterprise enable TLS 1.2 and TLS 1.3 by default.
- Only impacts the communication with Portal, Server, and Data Store over ports 7443, 6443, and 2443 respectively
- Protocols used by the web adaptor or load balancer must be configured separately



SSL Protocols and Cipher Suites

- Portal Administrator Directory
 - Security > SSLCertificates

- Server Administrator Directory
 - Security > Config

Portal Administrator Directory

[Home](#) > [Machines](#) > [DEV0013899.ESRI.COM](#) > [SSLCertificates](#)

SSL Certificates

- [dev0013899](#)
- [domain-cert](#)
- [domain-root](#)
- [portal](#)
- [samlcert](#)

Web Server SSL Certificate:	domain-cert
Web Server SSL Protocols:	TLSv1.2, TLSv1.3
HTTP Strict Transport Security (HSTS) enabled:	false
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_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_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_AES_256_GCM_SHA384, TLS_AES_128_GCM_SHA256

ArcGIS Server Administrator Directory

[Home](#) > [security](#) > [config](#)

Security Configuration

Configuration Properties

Protocol:	HTTPS Only
SSL Protocols:	TLSv1.2,TLSv1.3
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_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_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_AES_256_GCM_SHA384, TLS_AES_128_GCM_SHA256
HTTP Strict Transport Security (HSTS) enabled	false

Security Findings?

Esri PSIRT!

- <https://trust.arcgis.com>

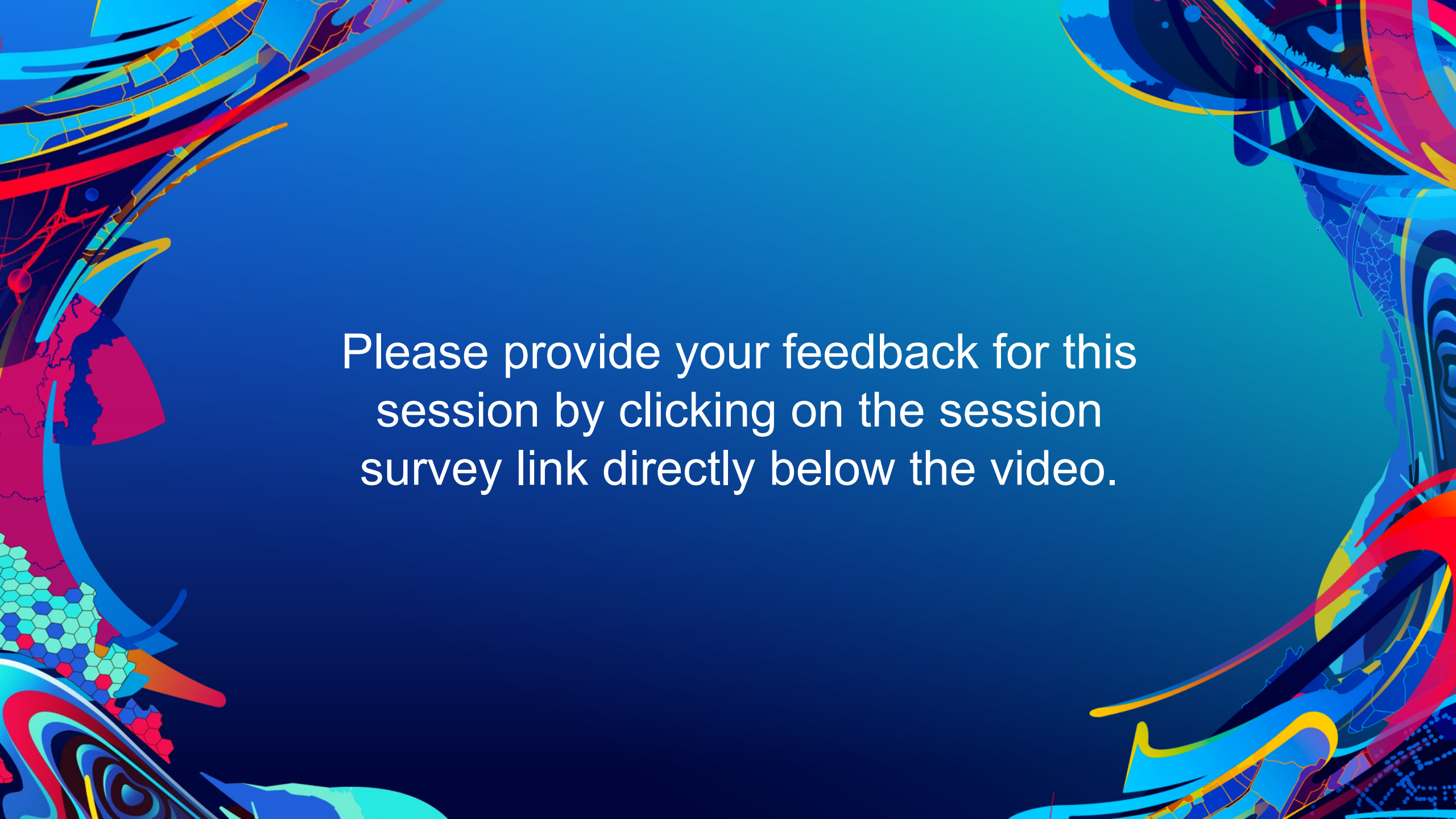


- Vulnerability - report a vulnerability found in our site or application.
- Suspicious E-mail from Esri - if you believe you were targeted by a possible phishing attack from an Esri e-mail address, or have received other suspicious e-mail correspondence from Esri.
- Privacy Issue - if you have a privacy concern related to our application or organization.
- Other - for all other security, privacy or compliance related concerns.



esri®

THE
SCIENCE
OF
WHERE®



Please provide your feedback for this session by clicking on the session survey link directly below the video.