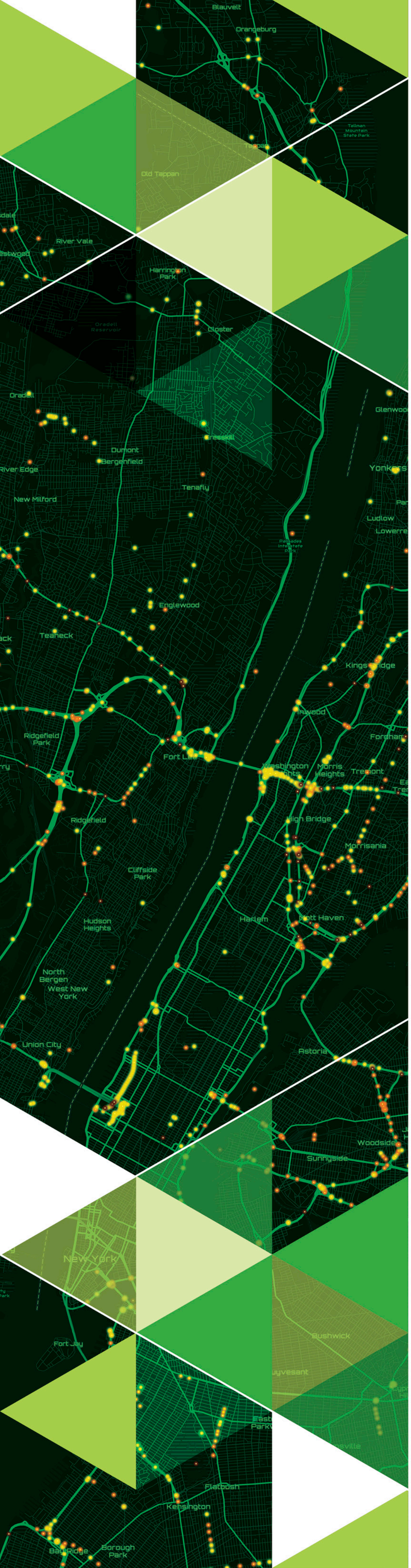


AN ESRI
TECHNICAL PAPER

July 2025

ArcGIS Enterprise Hardening Guide

[Click here to download latest guide from the ArcGIS Trust Center]

380 New York Street
Redlands, California 92373-8100 USA
909 793 2853
info@esri.com
esri.com

esri
THE SCIENCE OF WHERE®

Table of Contents

Introduction

This document describes strategies and associated settings that can be implemented to improve the security posture of ArcGIS® Enterprise deployments as recommended by Esri. It is designed for organizations planning a new deployment of ArcGIS Enterprise 11.5 and higher and existing deployments.

ArcGIS Enterprise is configured with a variety of default security settings such as the following:

- Enabling HTTPS by default
- Allowing users to share content publicly
- Allowing access to the REST Services Directory

The default settings are designed to facilitate ease of geospatial information sharing with everyone who has access to the system. Default settings are typically only sufficient for initial testing and development of your ArcGIS Enterprise deployment. In a production environment, you should configure the security of your implementation further. To navigate the large number of controls, organizations need guidance on configuring various security features.

Esri now provides security control guidance in the form of ***security profiles***, sometimes referred to as security baselines in the security industry. We recommend that you implement an industry-standard configuration that is broadly known and well tested, such as the ArcGIS Enterprise security profiles provided in this document and adjust it to your specific needs. Why? Creating a security profile from scratch or utilizing a generic hardening guide often leads to an insecure deployment that is more likely to break. Implementing the right ArcGIS Enterprise security profile level for your organization increases flexibility, availability, and security while minimizing costs.

This document addresses ArcGIS Enterprise security options through version 11.5. Please realize the criticality of regularly updating to the current release of ArcGIS Enterprise as cyberattacks on organizations continue to multiply. *If you are not utilizing the current ArcGIS Enterprise version, please refer to the Patch Management section of this document first.*

Audience

Administrators, systems architects, and security engineers can use this document to implement and validate that their ArcGIS Enterprise deployment is secured in alignment with best practices. If you are interested in diving deeper into the day to day management of ArcGIS Enterprise application security model to best configure the security of your content (such as layers and maps), please refer to our online documentation.

In addition to following this guide, you should monitor Esri’s ArcGIS Trust Center announcements at Trust.ArcGIS.com by using the RSS link on that page. You can find additional security guidance and late-breaking advisories for ArcGIS Enterprise there.

This guide will evolve, and Esri's Software Security & Privacy team welcomes feedback and suggestions at SoftwareSecurity@esri.com.

ArcGIS Enterprise Security Profiles

Every organization faces security threats; however, the types of security threats that are of most concern to one organization can be completely different from another organization. For example, an e-commerce company may focus on protecting its internet-facing web apps, while a hospital may focus on protecting confidential patient information. The one thing that all organizations have in common is a need to keep their apps and devices secure. These devices must be compliant with the security standards (or security profiles) defined by the organization.

A security profile is a group of Esri-recommended configuration settings that explains their security impact. These settings are based on feedback from Esri's Software Security & Privacy Team, product groups, partners, and customers. Because the system was developed and tested with availability, scalability, and other security concerns in mind, how you deploy ArcGIS Enterprise can have a significant impact on the security of the overall system.

No set of guidelines can cover all possible customer use cases. Each deployment of ArcGIS Enterprise can have its own IT environment, with differences in network topology, internal security systems and standards, customer requirements, and use cases. Some general guidelines are given to increase the overall security of the system. Where appropriate, more specific usage scenarios are also considered with guidance tailored to those particular cases. Nevertheless, the specific recommendations from this guide that you choose to follow ultimately depend on your unique deployment environment and the threats you determine to be a risk for your organization and want to mitigate.

This document contains two security profile levels:

Basic: Controls flagged as Basic are the recommended minimum security measures for production environments. The Basic profile is appropriate for over 95 percent of our customer base security needs. This profile aligns with industry security standards from the National Institute of Standards and Technology (NIST) as well as the International Organization for Standardization (ISO), which are applicable to a broad range of regulatory compliance frameworks commonly required by customer security policies.

Advanced: Controls flagged as Advanced are appropriate for deployments where ArcGIS Enterprise is categorized as critical software. Most customers should find the Basic profile appropriate for their operations; however, if your organization uses ArcGIS Enterprise for mission-critical operations or must prioritize stringent security compliance requirements over usability then the Advanced profile should be considered. The Advanced profile in this document supersedes the guidance found in the ArcGIS Server Security Technical Implementation Guide (STIG) as well as the generic DISA Application Security and Development STIG when using ArcGIS Enterprise. The Advanced profile addresses the security measures appropriate for software defined as critical by NIST, as well as appropriate STIGs, to meet the most rigorous customer security requirements around the world in a more standard, secure, and reliable manner. As stated under DISA rule APSC-DV-002970, "…products not covered by a STIG, should follow…vendors lock down guides and recommendations", which for ArcGIS Enterprise is this guide.

WARNING: Advanced controls may have an operational impact and limit functionality.

Note: Each security profile's controls begin with a standard **action** defined as follows:

- **Disable**—Enabled by default but should be disabled unless customer documents exception
- **Remove**—Not available via a configuration interface but should be removed
- **Consider**—Depends on the organization's requirements balanced against the risk of the activity
- **Verify**—Default configuration appropriate, but worth verifying not changed to less secure
- **Configure**—Typically a relatively easy change of settings to cover recommendations
- **Implement**—Typically requires more effort to enact, such as deploying supporting services
- **Manage**—Requires ongoing management activities
- **Avoid**—Implement controls to prevent and alert upon detection
- **WARNING —**Extra attention is necessary to ensure an issue is addressed appropriately

Security control structure:

- Template
  - {**Profile: Basic**, **Advanced**}: {**Action:** Disable, Remove, Consider, Verify, Configure, Implement, Manage, Avoid}: {**Security Control:** Free text description}

- Example
  - **Basic: Disable** ArcGIS Portal Directory

Software Components

ArcGIS Enterprise is your foundational system for data management, mapping and visualization, and location analytics. ArcGIS Enterprise enables you to connect to and share data with anyone, anywhere, on any device. Running on infrastructure you control, it is software that can be used in the cloud and on-premises. ArcGIS Enterprise is a collection of components that together provide a complete GIS solution. This guide references these components using the following terms:

ArcGIS Server
Primarily responsible for analytical workflows and web services. ArcGIS Server may be deployed as a *hosting* server that provides on-demand service delivery to GIS publishers and administrators or as a dedicated ArcGIS Server providing a system of record services such as mapping, image procressing, and geoprocessing. ArcGIS Server is a required component for all ArcGIS Enterprise deployments.

Portal for ArcGIS
A web portal and sharing platform of ArcGIS Enterprise through which you will primarily interact. Portal for ArcGIS aggregates services, files, apps, and capabilities provided by ArcGIS Server or other GIS web services providers as consumable items. Portal for ArcGIS is a required component of ArcGIS Enterprise.

ArcGIS Data Store
A spatial database managed by ArcGIS Enterprise that provides relational, NoSQL, and media databases to ArcGIS Server. ArcGIS Data Store is required to support hosting ArcGIS Server capabilities and is therefore a standard component of ArcGIS Enterprise.

ArcGIS Web Adaptor

A web proxy, deployed at the edge, through which all user requests go over HTTPS to Portal for ArcGIS or ArcGIS Server. *This can be an optional component* to ease deployment and can frequently be replaced with an industry-standard web application firewall (WAF)-enabled load balancer where groups such as Esri's professional services can assist.

Identity Providers (IDP)

Furnish you with identity management services. Azure Active Directory, now called Microsoft Entra ID, is the most common and widely deployed provider. These systems allow service providers such as ArcGIS Online and ArcGIS Enterprise to support centralized authentication with the identity provider through industry-standard protocols such as SAML (Security Assertion Markup Language) and OIDC (OpenID Connect).

ArcGIS Pro

Supports user and administrative workflows necessary to fully utilize all ArcGIS Enterprise capabilities. While many structural administrative tasks can be performed with ArcGIS Enterprise web interfaces, GIS data administration workflows such as publishing utility networks, geoprocessing, and geocoding services require ArcGIS Pro.

Web Application Firewall (WAF)

Provide layer 7 (application layer) protection for web services by intercepting, decrypting, and inspecting HTTP traffic and blocking suspicious activity. WAFs provide a basic layer of protection against SQL injection (SQLi), cross-site scripting (XSS), server-side request forgery (SSRF), remote file inclusion (RFI), and denial of service (DoS) attacks. Any service exposed to the public internet must employ the use of a WAF that implements a baseline rule set that covers these attack vectors. Esri recommends and documents a means of implementing the Open Worldwide Application Security Project (OWASP) Core Rule Set as a baseline web application firewall configuration within the ArcGIS Trust Center documents called ArcGIS Enterprise Web Application Filter Rules.

Security Information Event Management (SIEM)

Provide log/event collection, correlation, and analysis services. Splunk, Elastic LogStash, and Microsoft Sentinel are common examples of products that deliver SIEM services. As a baseline capability, a SIEM is necessary to ensure secure and efficient management of log events at scale across multiple systems and compute layers.

Web Scanner

A class of dynamic scanner that focuses on web application and service scanning, fuzzing, and vulnerability detection of systems at runtime. These tools are specialized in driving mobile code and web services such as JavaScript, WebAssembly, REST, SOAP, OAuth, HTTPS/TLS, etc. Such tools provide baseline detection and compliance alignment by continually monitoring the current runtime state of applications against a feed of new and emerging threat patterns.

Devices

ArcGIS Enterprise allows you to consume GIS services of all types (features, data, items, files, models, addresses, geoanalytics, applications, etc.) through a variety of client devices including web browsers, mobile devices/phones, thick clients such as ArcGIS Pro, and custom clients provided by third-party vendors.

Enterprise Geodatabase	Hosted within a traditional RDBMS (Microsoft SQL Server, PostgreSQL, Oracle, etc.) the ArcGIS Enterprise Geodatabase provides a system of record that delivers data services to data production users, GIS administrators, and dedicated services published to ArcGIS Enterprise.
ArcGIS Online	A cloud-based mapping software that many customers utilize to supplement their ArcGIS Enterprise capabilities, such as accessing basemaps or utility services.

Note: Many extensions and licensing roles can be added to the above base ArcGIS Enterprise software components that are compatible with this guide but may require additional component-specific hardening measures to be implemented as defined within an organization's corresponding documentation.

Secure Deployment Patterns

There are three operating environment options for ArcGIS Enterprise: Windows, Linux, and Kubernetes. For Windows and Linux, you can deploy ArcGIS Enterprise manually, installing and configuring each component in sequence, or you can automate the deployment process by using one of the ArcGIS Enterprise deployment automation tools. Deployment automation tools include Chef, PowerShell DSC, Amazon Web Services (AWS), Azure, and ArcGIS Enterprise Builder. Please be aware that these automation tool scripts do **not** configure systems to meet the Basic security profile described in this document. By default, Esri® automation tool scripts only provide sufficient security for initial testing and development of your ArcGIS Enterprise deployment. This guide provides controls that enhance these default configurations to bring ArcGIS Enterprise to a **Basic** production security posture that has minimal operational impact, as well as **Advanced** controls that further reduce attack surface but require additional management to maintain.

Customers interested in deploying ArcGIS Enterprise on Kubernetes should have a Kubernetes cluster available as well as appropriate expertise in managing a Kubernetes environment. Kubernetes customers can use the "ArcGIS Enterprise on Kubernetes Security FAQ" (ArcGIS login required) paper located in the ArcGIS Trust Center to supplement the security guidance found in this document.

This section summarizes the following secure deployment patterns with ArcGIS Enterprise and supporting security infrastructure components:

- Standard Secure Enterprise Pattern
- Standard Secure Enterprise Publishing Pattern
- System of Record Added Pattern
- System of Record + Data Production Added Pattern
- System of Record + System of Engagement Added Pattern

Note: These patterns are not physical deployment representations of individual systems but are architectural representations of key components deployed as part of a secure ArcGIS Enterprise. This discussion builds upon patterns described in the ArcGIS Architecture Center.

Standard Secure Enterprise Pattern

The standard production-ready ArcGIS Enterprise deployment pattern leverages security infrastructure components common to most application delivery solutions including SIEM systems for log management, centralized identity providers, web application vulnerability detection systems, and a web application firewall that bridges the network edge through which user workflows traverse.

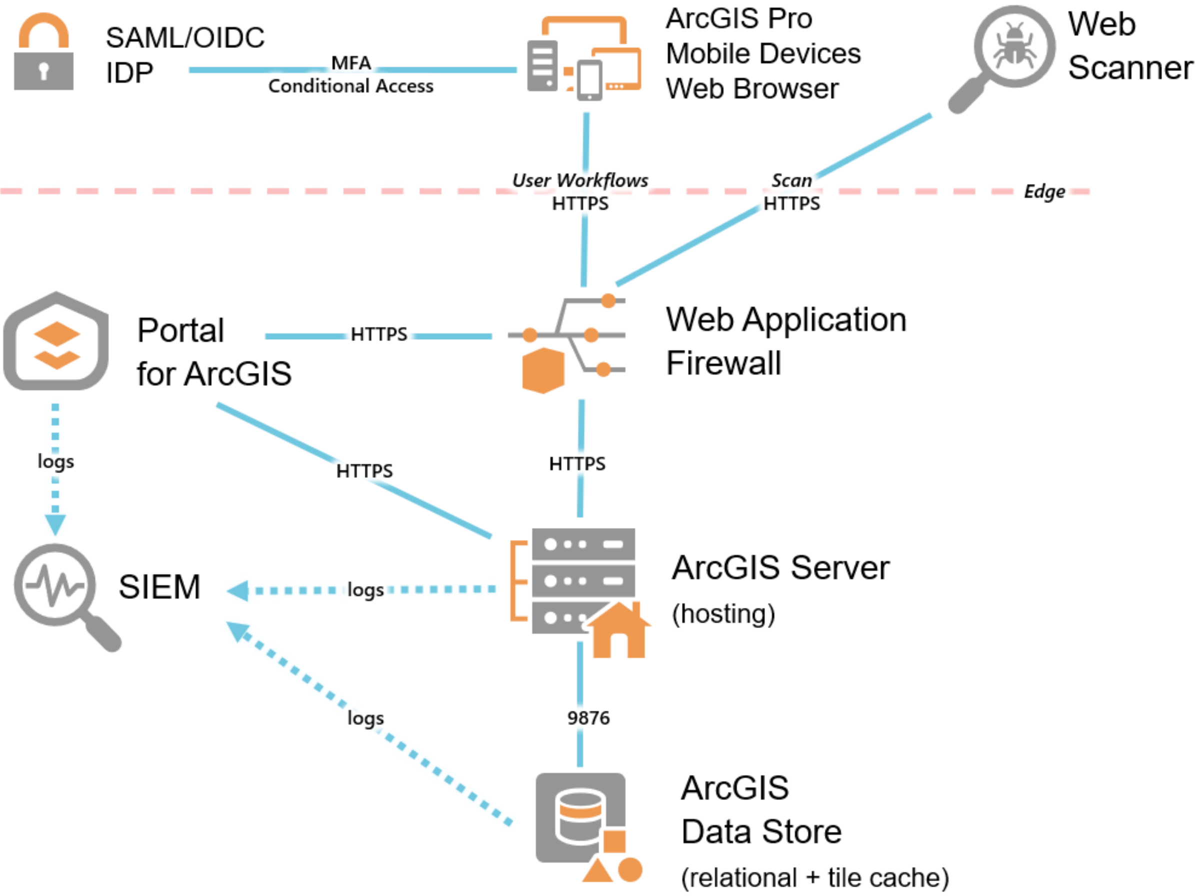


Figure 1—Standard Secure Enterprise pattern leveraging a centralized IDP, WAF, web scanner, and SIEM

Note: The focus of this paper is on ArcGIS Enterprise security; however, customers increasingly utilize a hybrid deployment of both ArcGIS Enterprise and ArcGIS Online to help address their geospatial service needs. Previously, some customers would utilize ArcGIS Enterprise more than ArcGIS Online due to the security of the software as a service (SaaS) offering not aligning with their organization's security and privacy requirements. Mid-2023, ArcGIS Online received an Agency FedRAMP Moderate authorization, which meets and exceeds the security assurance of other industry security standards such as ISO or SOC. This means the security of ArcGIS Online is in alignment with most organizational requirements around the world and opens new opportunities for balancing capabilities and datasets with appropriate segmentation across ArcGIS Enterprise and ArcGIS Online.

Secure Pattern + Admin Publishing

Publishing and administrating ArcGIS Enterprise services via ArcGIS Pro is not compatible with standard WAF rules. Therefore, instead of degrading the recommended ArcGIS Enterprise OWASP WAF rules for all external (edge/public) communications, ArcGIS Pro publication is allowed to occur directly to ArcGIS Enterprise systems as shown in Figure 2 below. Administrative and publishing workflows continue to function without being blocked as they either are in the *allow list* by the WAF or bypass the WAF entirely.

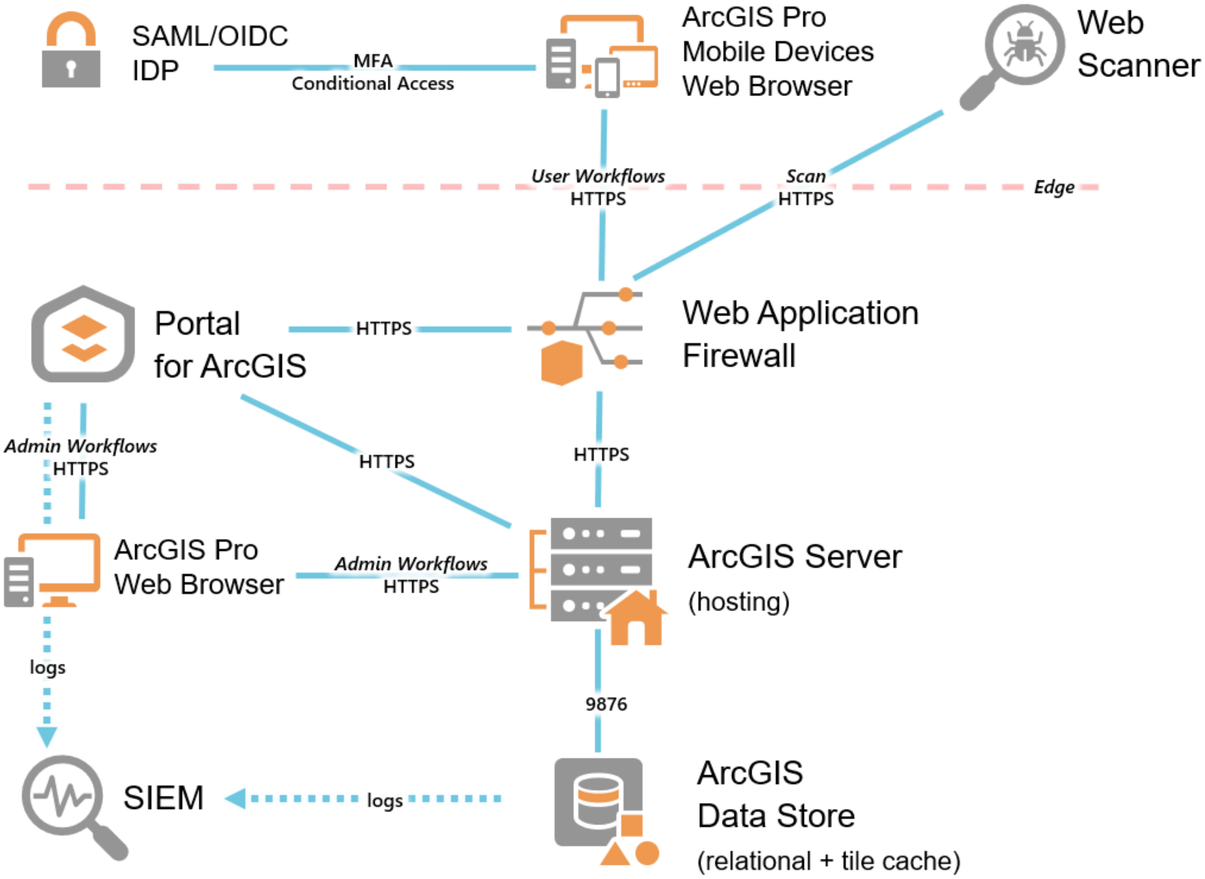


Figure 2—Secure Pattern + Admin Publishing incorporates direct ArcGIS Pro for service publishing

Secure Pattern + System of Record

The standard secure ArcGIS Enterprise pattern incorporates Portal for ArcGIS, a *hosting* ArcGIS Server implementation, and ArcGIS Data Store, which provides a solid *system of engagement* for dynamic service publishing and web data delivery and collection. Organizations that need to also deliver a *system of record* may expand this pattern further to incorporate ArcGIS Server tiers that deliver dedicated mapping, imaging, geoprocessing, and geocoding services that consume data from an enterprise geodatabase hosted within a supported RDBMS such as SQL Server, Oracle, PostgreSQL, etc.

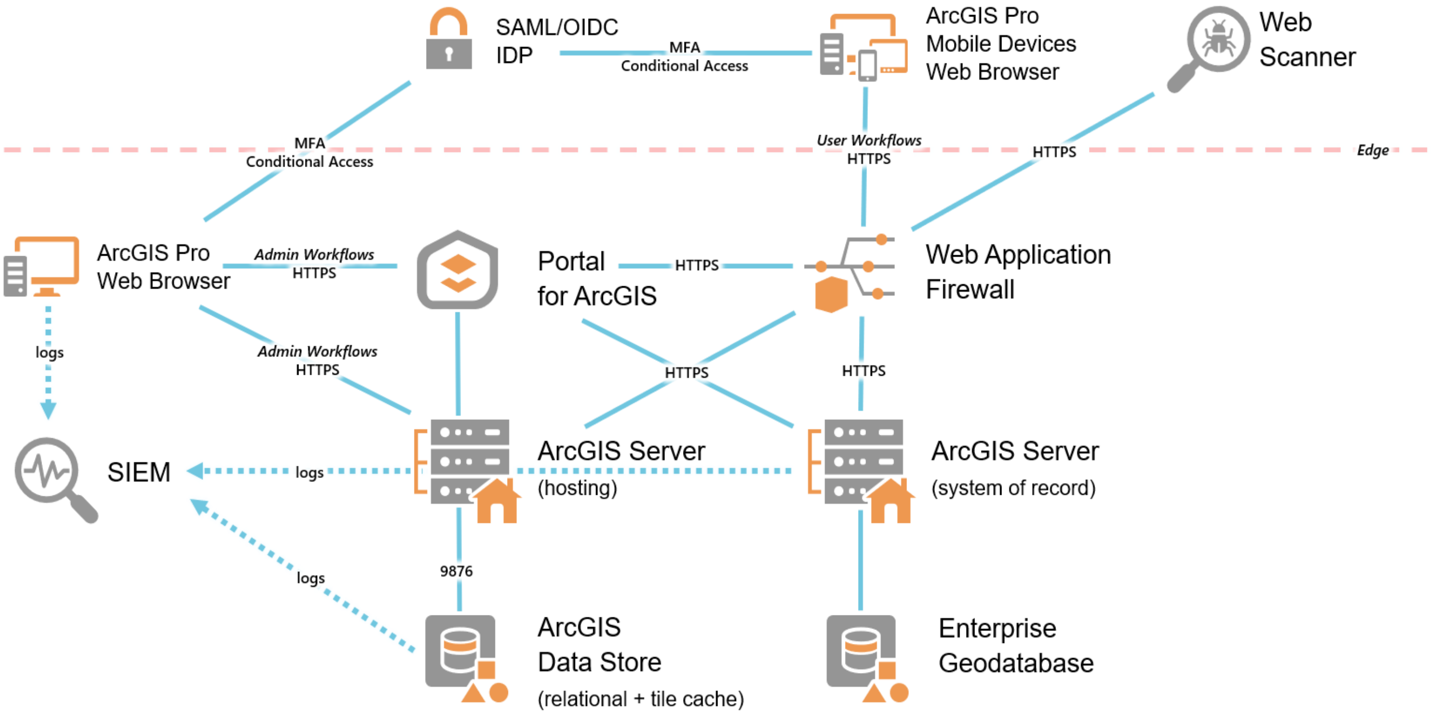


Figure 3—A system of record involves federating dedicated ArcGIS Server tiers to an existing ArcGIS Enterprise pattern

Secure Pattern + System of Record + Data Production

Expanding the ArcGIS Enterprise system of record concept incorporates ArcGIS Pro to support *data production* including geodatabase versioning and replication, which enable GIS data stewards to manage the integrity of data production workflows and replicate datasets to ArcGIS Enterprise for end-user delivery, shown in Figure 4 below.

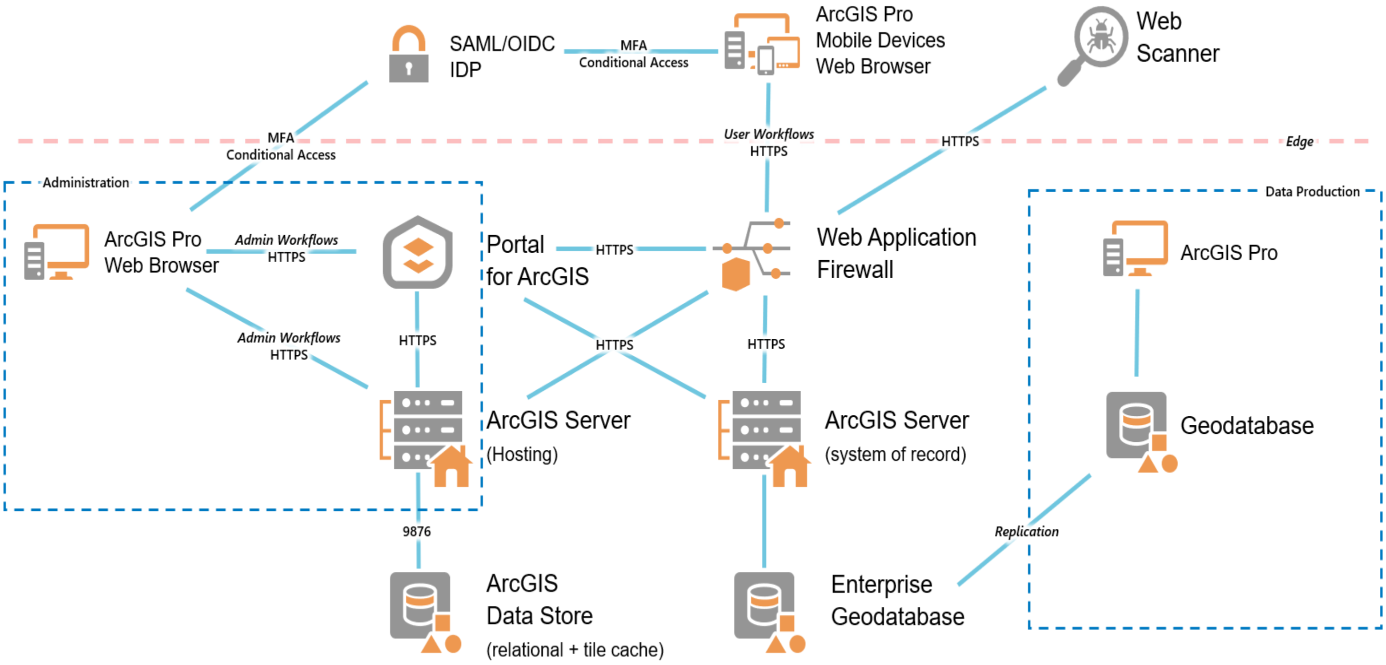


Figure 4—Secure Data Production Infrastructure

Scaling

While scaling an ArcGIS Enterprise deployment to meet the growing demands of customers and organizations is beyond the scope of this paper, the secure patterns described above can be used with any of the supported ArcGIS Enterprise scaling strategies. Table 1 summarizes ArcGIS Enterprise scaling deployment strategies and corresponding security considerations for each. Security details for each these strategies are available within Appendix B.

Table 1—Security Considerations for ArcGIS Enterprise Scaling Deployment Strategies

Scaling Strategy	How to Secure?	How to Deploy?
Single Machine	Appendix B - Figure 21	Online Documentation
Multimachine	Appendix B - Figure 22	Online Documentation
Highly Available	Appendix B - Figure 23	Online Documentation

Tip: Administrators seeking a general understanding of ArcGIS Enterprise architecture should review the ArcGIS Enterprise: Architecting Your Deployment overview and the ArcGIS Architecture Center.

Zero Trust Architecture

In the current threat environment, organizations can no longer depend on conventional perimeter-based defense to protect critical systems and data. A transition to a "zero trust" approach to security provides a defensible architecture for this new environment. The foundational tenet of Zero Trust Architecture (ZTA) is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, verification must occur for anything and everything attempting to establish access. It is a dramatic security paradigm shift from verify once at the perimeter, to continual verification of each user, device, application, and transaction.

Numerous governments and organizations require ZTA for operations moving forwards. However, the security capabilities to support ZTA have different levels of maturity/ standards supporting them. This hardening guide focuses on the foundational ZTA capabilities organizations should implement immediately as well as plan for in the short-term. New ZTA mandates provide clarity concerning deployment priorities, such as OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. There are 15 foundational ZTA capabilities identified that all organizations should either implement now, or plan for. The mandated capabilities were selected from the Zero Trust Maturity Model from CISA and span the five ZTA pillars of Identity, Devices, Networks, Apps/Workloads and Data. These capabilities are applicable to all customers for consideration to establish a strong ZTA foundation to build upon over time.

Table 2 – Foundational ZTA Capabilities

Requirement	**ArcGIS Enterprise Support**	**Priority****
Establish ZTA implementation plan	Hardening Guide	Immediate
Phishing resistant MFA – Organization Accounts	SAML/OIDC w/ FIDO2/WebAuthN MFA, or PIV cards	Immediate
Disable special character password policy*	Managed via IDP	Immediate
Disable password rotation password policy*	Managed via IDP	Immediate
Endpoint Detection & Response (EDR) across systems	AV/EDR exception listing available for Enterprise	Immediate
Accept external vulnerability reports	ArcGIS Trust Center Report a Security Issue	Immediate
Categorize sensitive datasets	Utilize categories or tags to identify data sensitivity	Immediate
Centralized IDP - No anonymous access	Available via SAML 2.0 / OIDC	Plan
IDP must incorporate at least 1 device-level signal	Managed via IDP	Plan
Ongoing complete asset inventory	Managed via Inventory system	Plan
Encrypted DNS (Enforce DoT and/or DoH)	Managed via clients	Plan
HSTS for HTTPS enforcement (internally & externally)	Enterprise supports HSTS enforcement	Plan
Preload HSTS for domains	Submit domain to HSTSPreload.org or Get.gov	Plan
Automated & manual expert security analysis	Security Adviser + Hardening Guide	Plan
Immutable workloads	Cloud-based deployments supported	Plan

* Despite Immediate priority, don't enforce these policies until IDP, MFA and device-level signal requirements in place.
** Priority based on M-22-09 capabilities that should be in place for 2024, and others which need to be planed for.

Capabilities such as Secure Web Gateways (SWG's) and Identity Aware Proxies (IAP's) are *NOT listed as mandated / foundational* as standards are still solidifying around these types of ZTA capabilities. We will continue to monitor industry ZTA mandates and recommendations while working on ensuring our products align with key additional ZTA capabilities and standards over time.

Security Profile Checklists

This document provides separate ArcGIS Enterprise security profile checklists for new deployments:

- **Basic** security profile implementation see **Tables 3,4,5**
- **Advanced** security profile implementation with all controls see **Appendix A**

The checklists are intended as a quick reference for implementing the security controls outlined in this document. While many security controls can be implemented in any order, **red** controls should only be completed after the preceding controls are completed.

Checklists cover the following stages of implementing ArcGIS Enterprise:

- Preinstallation (Table 3)
- Postinstallation (Table 4)
- Maintenance (Table 5)

NOTE: For existing ArcGIS Enterprise deployments, we have incremental control implementation guidance, get started with just the top 20 most severe impact controls! Check out Appendix I: Existing Deployment Control Prioritization

*Table 3-**Preinstallation Basic** Security Controls*

#	Control	Responsible	Prerequisites
1	**Basic: Implement** Vendor Security Baselines	SA, GA	-
2	**Basic: Implement** Endpoint Detection and Response	SA	-
3	**Basic: Consider** Not Using ArcGIS Web Adaptor	SA, GA	-
4	**Basic: Implement** Network Segmentation	SA	-
5	**Basic: Implement** Personal Secrets Management	SA, GA, GU	-
6	**Basic: Implement** Group Managed Service Account (gMSA)	SA	-
7	**Basic: Implement** Web Application Firewall	SA	-
8	**Basic: Verify** HTTPS Is Enforced	SA	-
9	**Basic: Configure** HTTP Strict Transport Security Enforcement	SA	-

SA: System Administrator
GA: GIS Administrator
GU: GIS User

*Table 4-**Postinstallation** **Basic** Security Controls*

#	Control	Responsible	Prerequisites
1	**Basic: Remove** Silverlight and FLEX Policy Files	SA	Pre 10.8.1
2	**Basic: Consider** Disabling Anonymous Access	GA	-
3	**Basic: Verify** Self-Creation Built-In User Accounts Disabled	GA	-
4	**Basic: Verify** Dynamic Workspaces/Layers Map Services Disabled	GA	-
5	**Basic: Verify** Token Acquisition via HTTP GET Disabled	GA	-
6	**Basic: Verify** Portal for ArcGIS Legend Servlet Disabled	GA	-
7	**Basic: Verify** Portal for ArcGIS Print Servlet Disabled	GA	-
8	**Basic: Verify** Portal for ArcGIS WFS Servlet Disabled	GA	-
9	**Basic: Configure** Access Notice / Information Banners	SA	-
10	**Basic: Configure** Built-In Accounts Password Policy	GA	Built-In Accounts
11	**Basic: Verify** Standardized Queries Enabled	GA	-
12	**Basic: Verify** Header Enabled	GA	-
13	**Basic: Configure** ArcGIS Logging Level	GA	-
14	**Basic: Implement** Centralized User Account Management	SA, GA	-
15	**Basic**: **Disable** Members Can Share Content Publicly	GA	-
16	**Basic: Disable** Public User Profile Sharing for Organization Users	GA	
17	**Basic: Implement** SAML Signed and Encrypted Assertions	SA, GA	SAML IDP
18	**Basic: Configure** New Member Default Role as Viewer	GA	-
19	**Basic: Implement** Password Reset Email Notification	SA, GA	SMTP Server
20	**Basic: Implement** Signed CA Certificates	SA, GA	Obtain CA Cert
21	**Basic: Configure** Portal for ArcGIS Proxy Allow List	SA, GA	-
22	**Basic: Disable** Primary Site Administrator Account (ArcGIS Server)	GA	New PAA
23	**Basic: Disable** ArcGIS Server Services Directory	GA	-
24	**Basic: Disable** ArcGIS Portal Directory	GA	-

*Table 5—**Maintenance Basic** Security Controls*

#	Control	Responsible	Prerequisites
1	Basic: **Verify** Filter Web Content Is Enabled for All Feature Services	GA, GU	-
2	Basic: **Verify** featureServiceXSSFilte Is Enabled for All Feature Services	GA	
3	Basic: **Configure** callbackFunctionsEnabled	GA	
4	Basic: **Verify** Server System Services Are Secured	GA	-
5	Basic: **Avoid** Embedding User Identities in Scripts	SA, GA, GU	-
6	Basic: **Avoid** Embedding Application Identities in Client Applications	SA, GA, GU	-
7	Basic: **Avoid** Storing Secrets in Source Code	SA. GU	-
8	Basic: **Configure** All Administrator Accounts with MFA	SA	-
9	Basic: **Implement** Group-Based Sharing	GA	-
10	Basic: **Configure** Least Privilege User Types and Roles	GA	-
11	Basic: **Configure** Decentralized Profile Visibility	GA	-
12	Basic: **Manage** Content via Role-Based Access Control	GA	-
13	Basic: **Configure** Default Group Membership Assignments	GA	-
14	Basic: **Disable** Public User Profile Sharing for Organization Users	GA	-
15	Basic: **Disable** Show Social Media Links	GA, GU	-
16	Basic: **Consider** Using Feature Layer Views	GA	-
17	Basic: **Consider** Publication Governance and Delivery Pipelines	SA, GA	-
18	Basic: **Consider** Defining Content Access Requirements	GA	-
19	Basic: **Verify** Content Ownership Rights	GA	-
20	Basic: **Implement** Permission Guardrails	GA	-
21	Basic: **Manage** Accounts and Reduce User Permissions	GA	-
22	Basic: **Manage** Access Based on Employee or Project Life Cycle	SA, GA	
23	Basic: **Implement** Backup Strategy and Test Regularly	SA, GA	-
24	Basic: **Consider** File Geodatabases	SA, GA	-
25	Basic: **Implement** Database Transparent Data Encryption	SA, GA	-
26	Basic: **Implement** Whole Disk Encryption	SA	-
27	Basic: **Implement** Software Inventory	SA, GA	-
28	Basic: **Manage** Only General Availability Product Versions	GA	-
29	Basic: **Configure** Vendor Patch Notification	SA, GA	-
30	Basic: **Implement** Security Patches within One Month	SA, GA	-
31	Basic: **Manage** Configuration Drift	GA	-
32	Basic: **Implement** Security Information and Event Management	SA	-
33	Basic: **Manage** Webhooks	SA, GA	-
34	Basic: **Implement** CSIRT Process	SA	-
35	Basic: **Consider** Data Anonymization	SA	-
36	Basic: **Implement** Role-based Training Plans	SA, GA, GU	-
37	Basic: **Manage** Ongoing Awareness Activities	SA, GA, GU	-
38	Basic: **Implement** Vulnerability Scanning Tools	SA	-
39	Basic: **Manage** Vulnerable Components with Patching	SA, GA	-

Application Security

Application security settings are customer-configurable ArcGIS security controls allowing customers to do the following:

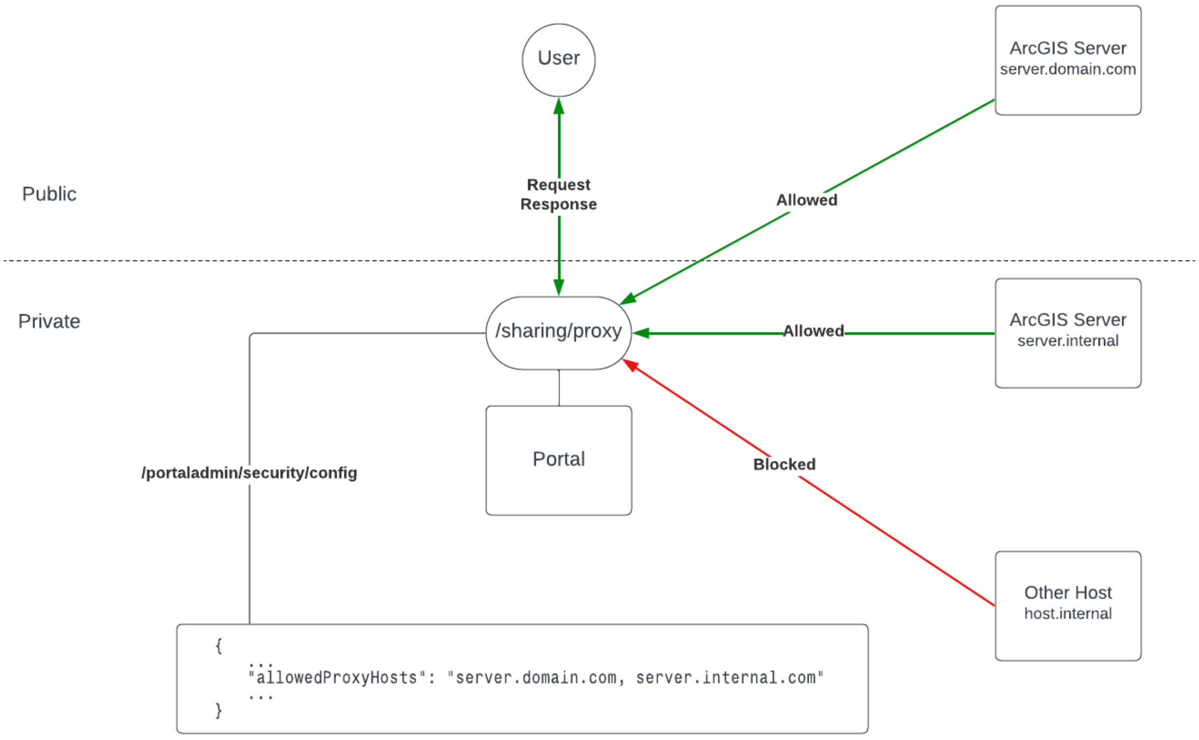
- Strengthen Application Security Capabilities
- Disable Infrequently Utilized Services/Capabilities
- Disable Setup Accounts

Strengthen Application Security Capabilities

ArcGIS Enterprise has numerous security settings that are critical for a secure production implementation, some of which require significant configuration while others just require validation that the default configuration has not been modified.

Basic: **Configure** Portal for ArcGIS Proxy Allow List (AllowProxyHosts)

Configuring this allow list is **critical** for minimizing the attack surface of your Portal for ArcGIS deployment as there is an unauthenticated reverse proxy that supports connectivity to internal and external ArcGIS Server services as described in the documentation here: Restrict the Portal's proxy capability.



```
{
    ...
    "allowedProxyHosts": "server.domain.com, server.internal.com"
    ...
}
```

Figure 5—Properly Securing the Sharing Proxy

There are three scenarios requiring entries to be added to the allow list:

- Admin URL domains
- External ArcGIS Enterprise service domains with embedded credentials (including GeoRSS/KML)
- Legacy CORS support domains

See **Appendix J:** Determining Domains to Include for Proxy Allow List for procedure to properly populate the `allowProxyHosts` allow list.

Basic: **Implement** Password Reset Email Notification

Frequently, scenarios emerge that require password resets of built-in user accounts regardless of your main user storage mechanism. These workflows should always use an associated SMTP server to ensure a basic security posture. Other credential reset workflows are cumbersome and unnecessarily expose credentials to administrators when transacting with users. This setting is not configured by default as the SMTP service must be supplied by the organization implementing ArcGIS Enterprise. Configure this setting by following the guide in Configure security settings—Portal for ArcGIS | Documentation for ArcGIS Enterprise.

WARNING: Not configuring ArcGIS Enterprise to utilize an SMTP service to validate password reset requests if using built-in accounts is a high-risk configuration. Password reset capability can be disabled for the graphical user interface but is NOT an effective mitigation.

Basic: **Configure** Access Notice / Information Banners

By default, an access notice banner is not enabled within ArcGIS Enterprise. Configure an access notice and information banner to be displayed to both ArcGIS Enterprise organization members and users who access ArcGIS Enterprise anonymously. Access notices are appropriate to establish rules of behavior; provide copyright, intellectual property, and fair use notifications; and explain privacy rights and any other public use limitation notices.

Informational banners can be used to describe terms and conditions and new app or feature announcements or notify users of maintenance windows.

Basic: **Verify** Filter Web Content Is Enabled for All Feature Services

By default, web content filtering is enabled for all feature services, which limits text input values to simple data (strings, numbers). This secure default must be preserved for a hardened ArcGIS Enterprise deployment as disabling this protection enables input of unstructured HTML that does not conform to the ArcGIS allowed HTML specification, which can lead to XSS exploits. Refer to Feature services and client applications—ArcGIS Server | Documentation for ArcGIS Enterprise to verify Filter Web Content is enabled for feature services.

Basic: **Verify** featureServiceXSSFilter to “input”

By default, when services are created, they are configured to scan edits for potential scripts and block them, but not to scan features retrieved from the feature service. An attacker may bypass this edit scanning by editing the features in ways that aren't scanned, such as directly editing the database through SQL. Refer to Scan for cross-site scripting attacks to verify that the featureServiceXSSFilter property is enabled via the ArcGiS Server Administrator Directory and clicking System > Properties.

Advanced: **Configure** featureServiceXSSFilter to “inputOutput”

Building on top of the default “input” setting discussed previously, the “inputOutput” value directs ArcGIS Server to configure new feature services to scan both edits (input) and returned features (output). Configuring ArcGIS Server to scan for cross site scripting is more secure but may introduce performance overhead. To set this system property to inputOutput, sign in to the ArcGIS Server Administrator Directory, click System > Properties, copy the existing JSON object and modify it by adding the featureServiceXSSFilter to “inputOutput” to that existing JSON object.

Note: The featureServiceXSSFilter property is set globally (Recommended) but may be overridden in individual feature service’s settings (Not recommended).

Basic: **Configure** callbackFunctionsEnabled set to false

By default, JSONP callback request functions are enabled. The callbackFunctionsEnabled option allows older clients a way to make CORS requests without being restricted by the same-origin policy. All modern browsers support CORS. Disable this feature to reduce XSS attacks.

Basic: **Configure** Built-In Accounts Password Policy

While the Basic profile uses centralized identity management (SAML/OIDC) third-party identity providers, there are use cases for some built-in accounts such as service accounts. Secure these accounts by requiring a strong password policy aligned with your information technology policy.

ArcGIS password complexity requirements allow you to configure the following:

- Minimum number of characters* (default is 8)
- Uppercase letters
- Lowercase letters
- Numbers
- Special characters

* Password length has been found to be a primary factor in characterizing password strength—the longer the password, the better. If your organization does not have a password policy, a useful reference is NIST 800-63 (referred to as memorized secrets).

Basic: **Verify** Standardized Queries Enabled

By default, standardized queries are enabled globally in ArcGIS Server. Standardized queries check SQL syntax passed to web services hosted by ArcGIS Server and ensure that functions and syntax are composed in a database-agnostic manner. Standardized queries make it easier for developers to create applications regardless of the back-end database, limit potential attackers from understanding those back-end database technologies, and help prevent attackers from passing database-specific injections. There is no option to disable standardized queries for hosted feature services.

Ensure this feature is enabled in ArcGIS Enterprise by following the guide in Enforce standardized SQL queries—ArcGIS Server | Documentation for ArcGIS Enterprise. Verify that the **System Properties** value for standardizedQueries is blank (default) or set to:

{"standardizedQueries": "true"}

Basic: **Verify** Server System Services Are Secured

Occasionally users update the security options for ArcGIS Server system services needlessly. ArcGIS Server system services include the following:

- CachingControllers, CachingTools, DistributedWorker, FeatureServiceTools, GeoAnalyticsTools, LocationReferencingSystemTools, OrthoMappingTools, ParcelFabricTools, PublishingTools, RasterAnalysisTools, RasterProcessing, RasterProcessingGPU, RasterRendering, ReportingTools, SceneCachingControllers, SceneCachingTools, SpatialAnalysisTools, SyncTools, TopographicProductionSystemTools, UtilityNetworkTools, ValidationTools, VersionManagementTools

In most use cases, there will never be a need to expose these system services beyond their default settings. Exposing these services beyond the default settings may result in resource consumption issues and potentially a denial of service if abused.

Validate on ArcGIS Server if nondefault permissions are applied to any service in the system folder in Server Manager (see ServerScan SS06). To ensure only administrators and publishers have access to the services in the system folder, no roles should be assigned.

Validate that none of the system services have been shared as a Portal for ArcGIS item (see ServerScan SS15). To ensure the proper permissions, these services are not intended to be shared through a portal. It is recommended to remove the associated portal item to restore the default service permissions.

Basic: **Verify** NoSniff Header Enabled

By default, beginning at version 10.7, ArcGIS Enterprise sends an X-Content-Type-Options nosniff header message with each HTTP response instructing the user's web browser to honor the content type advertised in the response.

This header blocks the browser from MIME sniffing, in which a browser attempts to determine the content type of a response and changes the content type for the user. MIME sniffing exposes the user to potential XSS attacks. The nosniff header is an effective defense against XSS.

Administrators can disable the no-sniff header. Because it is a security best practice to keep this header enabled, administrators should be cautious and understand the risks involved with disabling it.

WARNING: There is rarely a valid reason to disable this header and presents a significant security risk to your operations if disabled.

Basic: **Configure** ArcGIS Logging Level

By default, ArcGIS Enterprise only logs Warnings, which is not adequate to capture an appropriate level of security event information for production systems, therefore:

- Basic deployments should increase logging to “Info” level
- Advanced deployments should increase logging to “Fine” level

ArcGIS Server and Portal for ArcGIS log settings are configured separately as described in the corresponding documentation below:

- Use ArcGIS Server Manager to configure Log level at Logs > View Logs > Settings
- Use Portal Administrator Directory to Edit Log Settings at Logs > Settings > Edit

Note that at 11.4 Portal and 11.5 Server support audit logs in addition to standard logs, see: Understand audit logs—Portal for ArcGIS | Documentation for ArcGIS Enterprise

Advanced: **Configure** Token Expiration with Organization Policy

Depending on the organization's policy and regulatory compliance requirements, the default token expiration for short- and long-lived tokens may need to be changed (e.g., NIST 800-53: AC-12: Session Termination). If applicable, the maxTokenExpirationMinutes can be adjusted by following the guidance in Specify the maximum token expiration time—Portal for ArcGIS | Documentation for ArcGIS Enterprise. Note that setting this value to a value such as *20* affects all tokens issued by ArcGIS Enterprise. Modifying this value may impact the product usability of many web applications, which will require reauthentication once this token expires.

Disable Infrequently Utilized Services/Capabilities

There are a variety of ArcGIS Enterprise capabilities that are disabled by default or are infrequently utilized, which should be disabled unless there are specific business drivers for the capability and supplementary security measures are in place to mitigate any increased risk.

Basic: **Disable** ArcGIS Portal Directory

By default, the ArcGIS Portal Directory provides developers with an HTML interface to the REST API that supports Portal operations. Leaving the ArcGIS Portal Directory enabled presents a recon opportunity for attacks and should be disabled in production operations. See Disable the ArcGIS Portal Directory for steps to implement this control.

Basic: **Disable** ArcGIS Server Services Directory

By default, the ArcGIS Server Services Directory provides developers with an HTML interface to the REST API that supports ArcGIS Server operations. Leaving the ArcGIS Server Services Directory enabled presents a reconnaissance opportunity for attacks and should be disabled in production operations. See Disable the Services Directory for steps to implement this control.

Basic: **Remove** Silverlight and FLEX Policy Files

Versions of ArcGIS Enterprise (prior to 10.8.1) included Silverlight and FLEX policy (crossdomain.xml and client-access-policy.xml) files by default. These files helped limit cross-domain requests to ArcGIS services. Both Adobe Flash and Microsoft Silverlight technologies are retired and therefore extraordinarily insecure, as are ArcGIS API for Flex and ArcGIS API for Silverlight. Web applications using ArcGIS API for Flex or ArcGIS API for Silverlight should be migrated to ArcGIS API for JavaScript or other modern frameworks, and supporting policy files should be deleted.

Warning: Using a mature or retired version of ArcGIS Enterprise is insecure; therefore, we highly recommend upgrading as soon as possible to a general availability release.

Basic: **Consider** Disabling Anonymous Access

The portal's anonymous access option controls access to the portal website. Customers who do not need to share content anonymously (to everyone) should disable anonymous access to the Portal for ArcGIS website to reduce reconnaissance opportunities for attackers. Specifically, configure the following setting to Disabled:

- Allow anonymous access to your Portal for ArcGIS: Disabled

To reduce data spillage, some customers disable ArcGIS Enterprise anonymous access and utilize ArcGIS Online for sharing content anonymously. Note that Portal for ArcGIS administrators can still publish content for anonymous consumption even when the above settings are disabled. Lastly, disabling anonymous access to your ArcGIS Enterprise services is the first step toward establishing a Zero Trust Architecture (ZTA) implementation.

Basic: **Verify** Self-Creation Built-In User Accounts Disabled

By default, ArcGIS Enterprise does not allow self-creation of new accounts. This is the required setting for a hardened implementation. Validate this feature is disabled in Configure security settings—Portal for ArcGIS | Documentation for ArcGIS Enterprise > Allow users to create built-in accounts

Basic: **Verify** Dynamic Workspaces/Layers Map Services Disabled

Dynamic workspaces expose database/workspace details over REST. This is not enabled by default and should be disabled as a hardening step to reduce the attack surface of ArcGIS Server services *if* there is no scenario where your organization needs this capability. See Enable dynamic layers on a map service in Manager—ArcGIS Server | Documentation for ArcGIS Enterprise.

Basic: **Verify** Token Acquisition via HTTP GET Disabled

The ArcGIS *token* is the authentication unit that a user exchanges for credentials that grant them access to services and items and ascribes privileges to their actions against ArcGIS Enterprise. By default, this sensitive exchange is handled through the POST method, ensuring that credentials exchanged for a token are not logged. Verify GET is not configured as described in this guide Enable token acquisition through an HTTP GET request—ArcGIS Server | Documentation for ArcGIS Enterprise, ensuring that the following parameters are configured for the **Token Manager Configuration** within ArcGIS Server:

```
        "allowHttpGet": "false",
        "allowHttpPostQueryParams": "true",
```

Basic: **Verify** Portal for ArcGIS Legend Servlet Disabled

Portal for ArcGIS provides a service to assist with creating map legends. To limit exposure to SSRF-style vulnerabilities, Esri recommends disabling the legend servlet. This servlet is disabled by default because ArcGIS Server, federated with the portal and designated as the portal's hosting server, provides this functionality. Introduced at 10.9, verify System Property *enableLegendsService* is set to false to ensure it is disabled.

Note: When updating System Properties such as *enableLegendsService*, you **must** pass in all of the previously modified system properties by first requesting the properties following the format:
https://machine.domain.com/webadaptor/portaladmin/system/properties?f=json
Then you add the property to be modified and update the System Properties.

Basic: **Verify** Portal for ArcGIS Print Servlet Disabled

Portal for ArcGIS provides a service to assist with printing web services when it is not federated with an ArcGIS Server. To limit exposure to SSRF-style vulnerabilities, Esri recommends disabling the print servlet.

Introduced at 10.9, verify System Property *enablePrintService* is set to false to ensure it is disabled.

Basic: **Verify** Portal for ArcGIS WFS Servlet Disabled

Disabled by default, Portal for ArcGIS provides a service to assist with rendering the Open Geospatial Consortium (OGC) Web Feature Services (WFS). To limit exposure to SSRF-style vulnerabilities, Esri recommends keeping the WFS servlet disabled.

Introduced at 10.9.1, verify System Property *enableWfsService* is set to false to ensure it is disabled.

Basic: **Implement** Group Managed Service Account (gMSA)

This control is applicable only for Windows deployments and provides strong security value with reduced ongoing security maintenance but requires significant effort to initially implement. As ArcGIS Enterprise does its work, it needs to start and stop processes, read and write data to locations on the file system, and communicate between machines. Instead of using a local or standard domain account for this work, it is recommended to use a Group managed service account.

A gMSA is a special Active Directory domain account that provides automatic password management. The account cannot be used for interactive logins and is restricted for use on only a predefined group of servers. Using a gMSA is especially advantageous when a service account governs software on multiple machines, such as a multiple-machine ArcGIS Server site. Because the gMSA works at the domain level, it can regularly change the service account password on each machine with no manual steps required.

When you use a gMSA as the ArcGIS Account, Pass the Hash style attacks are mitigated because the password for the group Managed Service Account is randomized, unknown, has a 240-byte length, the keys are frequently rotated by the Key Distribution Service (KDS), and the autogenerated passwords are automatically cycled every 30 days. Esri further suggests that domain administrators enable Server Message Block (SMB) signing, Disable LLMNR (Link-Local Multicast Name Resolution), and disable NBT-NS [attack.mitre.org], as these options are effective in preventing attacks against NTLM hashes.

When establishing a gMSA account, the following principles of least privilege applies:

- Determine rights required to use ArcGIS Enterprise and connect to data stores ensuring only limited rights are applied to the gMSA.
- Don't add gMSA to Active Directory (AD) privileged groups as ArcGIS Enterprise should *never* be installed on a domain controller.
- Limit gMSA access and location.

The ServerConfigurationUtility command line tool, which is described below, can be used to configure the ArcGIS Server service to run under a gMSA. For the username parameter, the gMSA can be specified

either with or without the $ symbol at the end. The password parameter is not needed.
The readconfig and writeconfig parameters both function the same with a gMSA. Following is a sample command to configure a gMSA as the ArcGIS Server account:

```
ServerConfigurationUtility.exe /username mydomain\enterprise-gmsa$
```

Note: The ServerConfigurationUtility can output a server configuration to disk using the /writeconfig option, which is useful for configuring multiple machines in an ArcGIS Enterprise site to guarantee identical configuration. The configuration file contains sensitive information and should only be utilized for configuring the systems and then immediately destroyed across **all** systems in which it was stored.

Additional guidance covering the implementation of gMSA's across Portal for ArcGIS and ArcGIS Data Store is available as a Support How To article.

When using gMSA, forward proxies that require passing an identity are not supported. There is no way to configure a gMSA account profile to use gMSA.

Advanced: **Consider** Disabling KML and GeoRSS Servlets

By default, ArcGIS Enterprise provides servlets to support displaying GeoRSS and KML layers in both the Map Viewer and Map Viewer Classic. To limit exposure to SSRF-style vulnerabilities, Esri recommends evaluating the need to support KML and GeoRSS layers. If GeoRSS and KML layers are not used in your operations, disable these servlets.

Introduced at 10.9.1, change System Property *enableRssService* and *enableKmlService* are set to false to ensure they are disabled.

Advanced: **Verify** Utility Service External System Dependencies Approved

During setup, some utility services such as Geocoding default to processing a request via ArcGIS Online instead of the local system. The administrator can also choose to have other utility services such as Symbols, Routing, Elevation, Orthomapping Elevation, Hydrology, and Geoenrichment. Sometimes, end users or even subsequent administrators are surprised that datasets are set to ArcGIS Online when these services are configured in this capacity. Therefore, it is important to periodically verify that these services are processing data via services and in locations your organization has approved. User education concerning how utility services work is also important as sometimes users send batch information containing extensive personally identifiable information (PII) to a utility service thinking it remains within their company's ArcGIS Enterprise instance but instead is sent to a cloud-based service for processing.

Disable Setup Accounts

Both ArcGIS Server and Portal for ArcGIS have specialized administrative accounts useful for initial setup but are rarely needed afterwards and should be disabled for production operations after setup is completed.

Basic: **Disable** Primary Site Administrator Account (ArcGIS Server)

ArcGIS Server enables a PSA account by default but should be disabled for production operations once your ArcGIS Enterprise systems are federated. Disabling the PSA ensures that the only way to manage ArcGIS Server is through the group or role you've specified in your enterprise identity store.

Disabling the PSA is equivalent to disabling the Linux root operating system or the default Windows administrator account. This concept is an industry-standard best practice.

Before proceeding, ensure that the identity store you are planning to use to maintain the administrator accounts is in working order and available. If your identity store becomes corrupted or unavailable, you won't be able to log in to your site or use ArcGIS Server.

NOTE: Some use cases require that the ArcGIS PSA remain enabled such as for ArcGIS Monitor accessing a stand-alone ArcGIS Server (non-federated)

Advanced: **Remove** Initial Admin Account (Portal for ArcGIS)

After you've installed Portal for ArcGIS, an initial administrator account (IAA) is created and is therefore enabled by default. After the initial setup of ArcGIS Enterprise, including the configuration of ArcGIS Web Adaptor and/or configuring IWA, LDAP, or PKI, another account should be promoted to administrator and the IAA removed or deleted. Remember to change the ownership of items created using the IAA to the new account.

Disabling the IAA is equivalent to disabling a headless administrator account. This concept is an industry-standard best practice.

Identity and Access Management

To use ArcGIS Enterprise services, you must grant your users and applications access to resources. Production operations require robust identity management and permissions to ensure that the right people have access to the right resources under the right conditions. ArcGIS Enterprise offers a large selection of capabilities to help you manage your user and application identities and their permissions. The best practices for these capabilities fall into the following areas:

- User and Application Identities
- Centralized Identity Management
- User Groups and Attributes
- Permissions Management

User and Application Identities

ArcGIS Enterprise identities grant access to items and services and come in two forms:

- User Identities—also known as members, named users, or ArcGIS identity
- Application/Developer Identities—also known as developer credentials or service account

User Identities

User identities are expressed as actors that perform interactive sign-in against ArcGIS Enterprise; that is, a human supplies a username, password, and a multifactor authenticator (recommended). These identities are described as *members* throughout the documentation (see Add members to your portal — Portal for ArcGIS Help).

Application/Developer Identities

Application identities or developer credentials provide a means for developers to author non-interactive workflows against items they own and produce applications that consume credit-based services (e.g., batch geocoding) without requiring users to interactively sign in. In effect, application identities are *headless* identities that can access developer-owned items. Application identities authenticate by exchanging Client ID and Client Secret values for authentication tokens that are then used to assert their identity (authenticate) to access items and services in alignment with the OAuth 2.0 specification (see Add and register an app—Portal for ArcGIS Help).

Basic: **Avoid** Embedding User Identities in Scripts

If you find yourself setting up built-in user identities, see if you can make use of an application identity instead. User identities are for humans; therefore, avoid making use of them for authenticating machine-to-machine interactions. Following this principle will help with the enforcement of multifactor authentication (MFA) across your user identities instead of making exceptions that can lead to unnecessary risk for your operations.

Basic: **Avoid** Embedding Application Identities in Client Applications

Most applications that users interact with are client applications, that is, they deliver the functional code to a client such as a browser, mobile device, or installation. These applications run their code locally, exposing any embedded credentials associated with application identities to end users, creating opportunities for misuse/abuse. Client applications such as JavaScript, TypeScript, iOS, Android, and even thick-client applications installed on desktop machines should make use of user identities and support interactive logins as well as MFA.

Basic: **Implement** Personal Secrets Management

Small organizations can achieve effective password management by simply requiring employees to use personal credential management. Employees who utilize personal password managers will find they can use stronger passwords, store passwords securely, and improve their operational efficiency by leveraging browser and mobile-integrated apps and plug-ins to deliver credentials to websites and apps on demand.

Human-interactive secrets such as usernames and passwords remain a common source of compromise. Factors including weak credentials, credential reuse, and poor credential handling practices, such as using unencrypted files such as spreadsheets to store secrets, all contribute to the problem. Personal password management is a readily available, low-cost solution to credential sprawl/handling. Products such as LastPass, Bitwarden, 1Password, and Keeper provide a host of products that range from basic/individual storage to organization-auditable solutions that can validate compliance and detect exposed credentials as well as support secure credential sharing.

Advanced: **Implement** Organization Secrets Management

The same tools that deliver basic personal secrets management such as Keeper also offer organization- and team-oriented secrets management. The premium nature of these products includes support for organization auditing and awareness of at-risk and compromised credentials, validation of insecure credentials, and secure credential sharing and distribution. These advantages deliver strong value when compared to the effort involved in resolving loss of confidentiality, integrity, or availability as is the case when secrets are unexpectedly exposed.

Basic: **Avoid** Storing Secrets in Source Code

When developing applications, developers will make use of credentials to perform testing. These credentials may be supplied as runtime secrets including usernames, passwords, client IDs, client secrets, auth tokens, refresh tokens, etc. A common error when handling such secrets is to store them directly in code supplied to variables. This practice leads to compromise as these secrets will then be embedded in source control systems and exposed. Because source control systems are designed to be extremely durable historical code records, secrets exposed this way must be assumed as compromised and rotated.

A basic practice to mitigate this risk is to store secrets in .env files with accompanying entries in *.ignore files and programmatically read secrets into runtime applications. Delivered this way, development secrets are available to the local developer host but will not find their way into source control systems. A variety of free, open-source, and premium products are available to facilitate this practice including Dotenv.

Advanced: **Implement** Developer IDE-Integrated Secrets Management

An ArcGIS Enterprise workload requires an automated capability to prove its identity to databases, resources, and third-party services. This is accomplished using secret access credentials, such as API access keys, passwords, and OAuth tokens. Using a purpose-built service to store, manage, and rotate these credentials helps reduce the likelihood that those credentials become compromised.

Organizations seeking a higher level of secrets management assurance should use IDE-integrated vaults that can securely store, check in/check out, and rotate secrets according to organization or regulatory compliance requirements. Products including Password & Secrets Management | Keeper Security and HashiCorp Vault—Manage Secrets and Protect Sensitive Data deliver such capabilities.

Basic: **Configure** All Administrator Accounts with MFA

Using **any** administrator account without MFA is a high-risk configuration, whether for ArcGIS Enterprise or supporting infrastructure components such as a database system. All ArcGIS Enterprise accounts granted the role of Administrator must require MFA. ArcGIS Enterprise supports the following MFA patterns:

- Built-in accounts with multifactor authentication using Google or Microsoft authenticator apps
    - Note: The use of built-in accounts should be minimized (see Implement Centralized User Account Management for recommended strategy).
- SAML- or OpenID-based third-party MFA such as Azure AD Enterprise allowing the following:
    - Passwordless authentication (e.g., Azure Passwordless authentication)
    - FIDO2 (e.g., Yubikey) hardware key authentication
- Certificate authentication secured by smart cards such as PKI or CAC

It is highly recommended that phishing-resistant MFA options be utilized or efforts started to migrate to such a solution. The table below describes where these authentication options map to organization security requirements, as well as the level of effort to adopt and manage each authentication option:

Table 6—MFA Authentication Options

MFA Authentication Type	Basic	Advanced	Effort
Built-In (Multifactor) for Admins	X		Low
Built-In (Multifactor) for All		X	Low
SAML/OpenID Connect	X		Moderate*
Passwordless		X	Moderate
FIDO2 Key		X	High
Certificate/CAC/Smart card		X	High

*Low for organizations with an IDP already in place

Advanced: **Configure** All User Accounts with MFA

If your organization would be willing to consider one Advanced control, this is the one to implement with the strongest security value for your implementation. Don't be surprised to see this become a Basic control in the next year to two because of the value and criticality of the control. To be clear, this is another prerequisite to support ZTA with ArcGIS Enterprise. This control covers all authentication types covered in Table 6. For SAML or OIDC IDP accounts, ensure you deploy phishing-resistant MFA solutions such as FIDO2 and WebAuthN.

Centralized Identity Management

A production ArcGIS Enterprise implementation should not establish a separate silo of user accounts but instead utilize centralized identify management systems. Built-in ArcGIS Enterprise accounts should be documented as exceptions for specific use cases. Establishing a strong foundation for identities utilized to access systems is a key pillar to advancing the ZTA initiative that subsequently requires authentication and authorization at all exposed system interfaces, eliminating anonymous access to your implementation.

Basic: **Implement** Centralized User Account Management

Organizations with SAML or OIDC identity provider capabilities should configure their use with ArcGIS Enterprise. This reduces the administrative burden on the GIS Administrator by delegating the creation and management of ArcGIS Enterprise credentials to the identity administrator of the organization (e.g., Active Directory Administrator).

SAML: See Configure a SAML-compliant identity provider with Portal for ArcGIS for step-by-step tutorials on configuring a variety of common SAML identity providers with ArcGIS Enterprise.

OIDC: See Configure OpenID Connect logins for guidance on setting up OpenID Connect with ArcGIS Enterprise logins. If you utilize OIDC logins, you should utilize Proof Key for Code Exchange (PKCE) to eliminate transmitting the client secret over the network – see guidance here.

Refer to Organization-specific Logins FAQ for troubleshooting and answers to common questions on configuring either SAML or OIDC with ArcGIS Enterprise.

Note: The use of Integrated Windows Authentication (IWA) is only acceptable for ArcGIS Enterprise implementations not exposed to the internet and is therefore not detailed here.

Basic: **Implement** SAML Signed and Encrypted Assertions

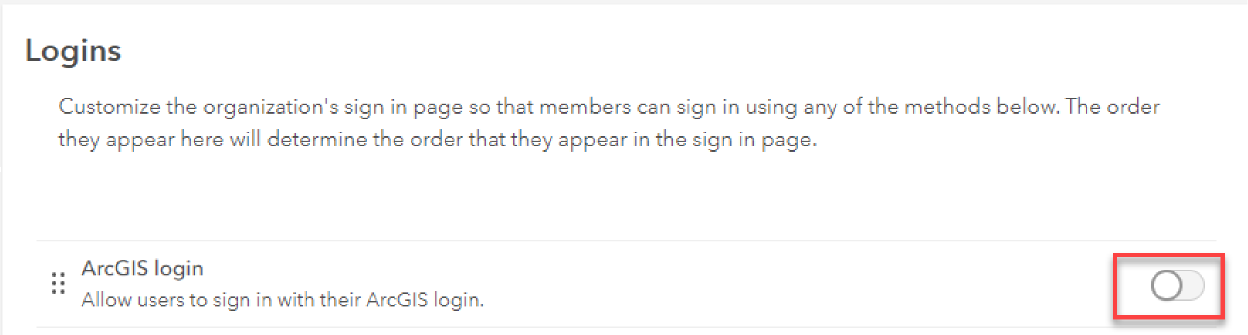
SAML is a powerful and convenient web SSO (Single Sign On) technology that when configured securely is safe and effective. However, SAML authentication is based on trust between an identity provider (such as MS Entra ID) and a service provider (ArcGIS Online or ArcGIS Enterprise) facilitated by a mutual certificate exchange and assertion signing that, if overlooked, creates opportunities for attackers to exploit gaps in this trust arrangement. To mitigate this risk, any SAML implementation must enforce signed and encrypted assertions. Implementing signed and encrypted assertions is a two-part process:

1. On the Service Provider (ArcGIS Enterprise/ArcGIS Online):
   a. Enable/Require Signed and Encrypted Assertions.
2. On the Identity Provider (e.g. MS Entra ID):
   a. Configure SAML Signed Tokens—See Microsoft Entra example.
   b. Configure SAML Token Encryption—See Microsoft Entra example.

WARNING: Failing to enforce signed assertions is a high-risk SAML configuration pattern that should not be employed in production operations. Always ensure SAML assertions are, at minimum, signed and preferably encrypted.

Advanced: **Disable** ArcGIS Logins

After configuring an SAML or OIDC login (see: Implement SAML or OpenID Connect), organizations with advanced security requirements should disable the ArcGIS login:



Logins

Customize the organization's sign in page so that members can sign in using any of the methods below. The order they appear here will determine the order that they appear in the sign in page.

ArcGIS login
Allow users to sign in with their ArcGIS login. ○

Figure 6—ArcGIS Enterprise Security Login Configuration showing ArcGIS Login disabled as recommended.

This will force all logins to flow through the organization's defined SAML or OIDC identity provider automatically, thereby shifting identity governance onto the identity provider, ensuring alignment with the organization's policies. Refer to Configure Security Settings >Logins for more details on configuring this feature with ArcGIS Enterprise.

Advanced: **Configure** SAML/OIDC Identity Provider Lockouts

Although SAML/OIDC identity providers vary, each includes a mechanism to mitigate brute-force authentication attacks. Azure AD, for example, provides a smart lockout feature that can respond to and automatically lock and unlock accounts in the face of a brute force attack (see Prevent attacks using smart lockout—Azure Active Directory—Microsoft Entra | Microsoft Learn). Okta IDPs deliver a similar feature through password policies (see Configure a password policy | Okta). Whichever IDP your organization uses for SAML/OIDC authentication, ensure the account lockout feature is enabled.

Advanced: **Implement** Identity Provider Strong Credential Flow

Organizations with security requirements that cannot be met with standard multi-factor authentication alone should consider advanced providers that support strong credential flows such as Azure AD Passwordless authentication delivered through SAML IDP integration with ArcGIS Enterprise. Organizations that can use MS Entra ID benefit from these advanced authentication options that provide stronger security assurance while reducing end-user login effort. To meet this requirement, implement the following:

1. Configure ArcGIS Enterprise to use a SAML IDP following the guide described in Configure a SAML-compliant identity provider with a portal—Portal for ArcGIS | Documentation for ArcGIS Enterprise; specifically, see the latest guide for configuring the most common SAML identity providers in https://github.com/Esri/idp/tree/main/Documentation/SAML.
2. Configure the implemented IDP to use the desired strong credential flow. For example, see Passwordless authentication options for Azure Active Directory Azure AD for help setting up Passwordless or FIDO2 security key-based authentication.

Upon completing these steps, you will be redirected from ArcGIS Enterprise to your IDP (e.g., Azure AD) where the required credentials including Passwordless authentication, FIDO2 Security Keys, CAC/PIV, Smart card, MFA, or Biometric auth can be supplied. Once authenticated, you will be redirected back to ArcGIS Enterprise as an authenticated user.

Advanced: **Implement** Certificate-Based Authentication (PKI/PIV/CAC)

Certificate-based authentication (PKI) secured by a personal identity verification (PIV)/common access card (CAC) smart card remains the most secure user authentication option available. In this model, the user is issued a private key from their identity provider's trusted certificate authority, which is then stored on a physical smart card, that requires a PIN or biometric authentication to unlock. The result is a convenient authentication option for users that is effectively impossible to forge. ArcGIS Enterprise has been validated to function with smart card authentication when implemented in the web server or in the identity provider.

To configure certificate-based authentication with ArcGIS Enterprise using Microsoft Entra ID as a SAML identity provider, consider the following resources:

1. Get started with certificate-based authentication in Microsoft Entra ID with federation.
2. Store user certificates on a smart card (e.g., SafeNet IDPrime Smart cards).
3. MS Entra ID (SSO) Integration with ArcGIS Enterprise Tutorial.

Alternatively, organizations that prefer to use fully integrated on-premises Active Directory or LDAP may also use this legacy pattern to deliver PKI authentication with ArcGIS Enterprise.

User Groups and Attributes

As the number of users you manage grows, you will need to determine ways to organize them so that you can manage them at scale. Place users with common security requirements in groups defined by your identity provider. Put mechanisms in place to ensure that user attributes that may be used for access control (e.g., department or location) are correct and updated. Use these groups and attributes to control access, rather than controlling access of individual users. This allows you to manage access centrally by changing a user's group membership or attributes once with a permission set rather than updating many individual policies when a user's access needs change.

Basic: Implement Group-Based Sharing

ArcGIS Enterprise uses a group-based sharing model that allows the assignment of ArcGIS Items (data) and ArcGIS Enterprise Users to one or more groups. Users can access Items that have been shared with a common Group.

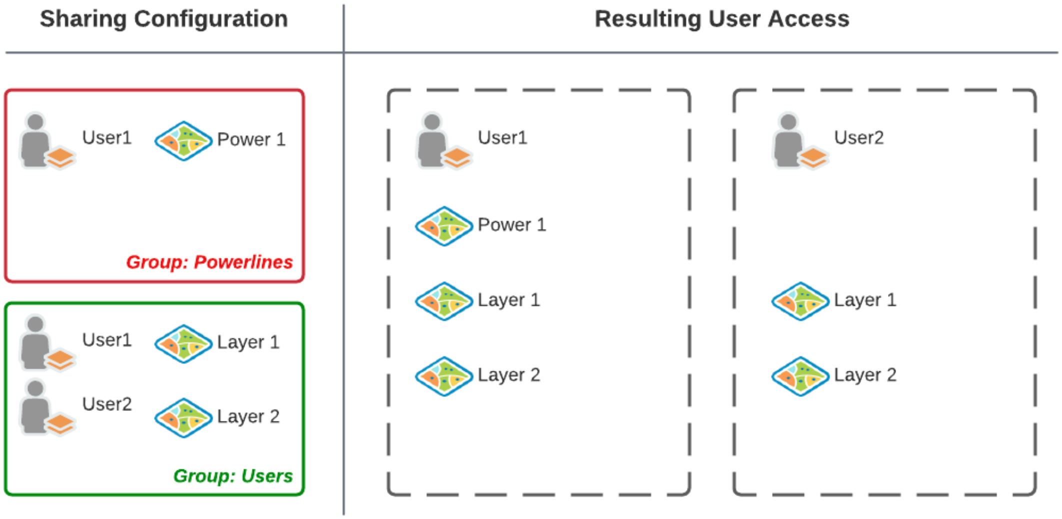
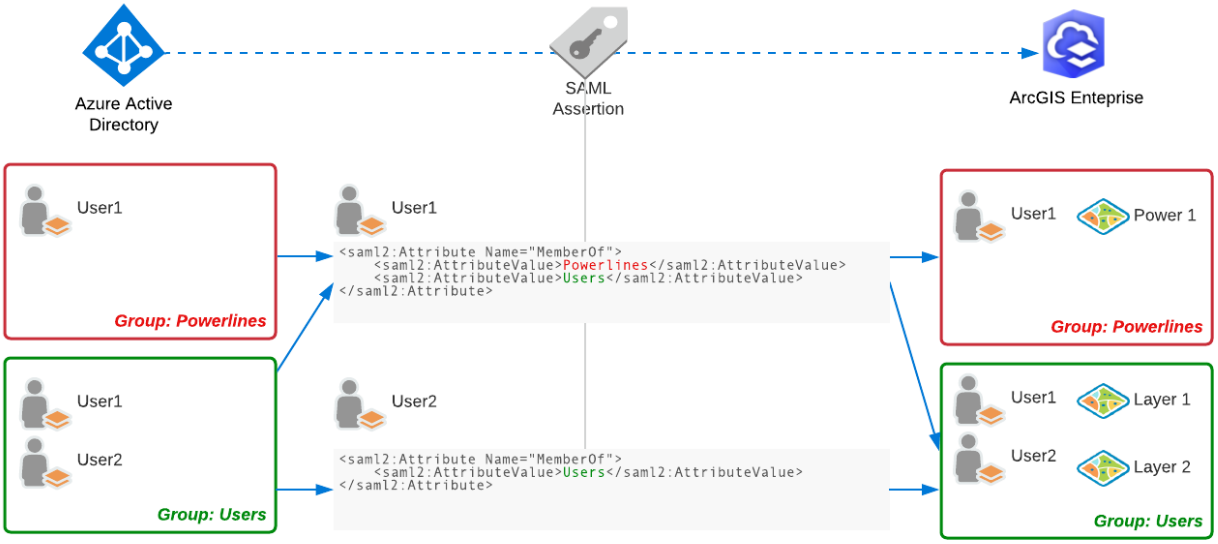


Figure 7—Group-Based Sharing Model

See Managing Groups for additional details on configuring Users, Groups, and Items to support group-based sharing.

Advanced: Configure SAML Group Membership

Esri recommends organizations with Advanced security requirements implement SAML identity provider-based authentication with ArcGIS Enterprise. As a part of that configuration, organizations should consider enabling SAML-based group membership that allows group memberships in an organization's identity store to propagate to ArcGIS Enterprise via SAML Assertion passed by users as they sign in. This concept is illustrated below:



```
<saml2:Attribute Name="MemberOf">
    <saml2:AttributeValue>Powerlines</saml2:AttributeValue>
    <saml2:AttributeValue>Users</saml2:AttributeValue>
</saml2:Attribute>
```

```
<saml2:Attribute Name="MemberOf">
    <saml2:AttributeValue>Users</saml2:AttributeValue>
</saml2:Attribute>
```

Figure 8—SAML-Based Group Membership

In Figure 7 above, with SAML-based group membership enabled, once User1 completes a login flow, User1 gains access to the Power1 secured layer automatically because they are a member of the Powerlines Active Directory (AD) group. As a member of the AD Group: Users, User1 also gains access to Layer 1 and Layer 2. In this same example, User2's SAML Assertion only includes Users, so they will only have access to content shared with the Users group in ArcGIS Enterprise but will be denied access to content shared with the group Powerlines.

See Link Active Directory, LDAP, or SAML groups from an IDP for more details on this feature.

Privilege Management

Privileges determine who can, and under what conditions, access, configure, or otherwise use a resource.

Advanced: **Consider** Disabling Item Comments

ArcGIS Enterprise is a social sharing tool for geospatial content. If desired, Portal for ArcGIS can be configured to allow users to create comments and display those comments on item details pages. Consider your ArcGIS Enterprise use case, and, if possible, disable the collection and display of item comments as the unmanaged content can become a source of personally identifiable information to manage, and/or source of accidental over-disclosure, or source of misinformation.

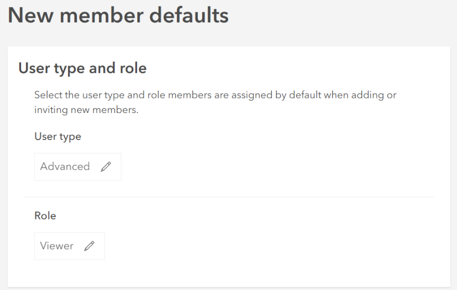
Advanced: **Implement** Custom Roles

ArcGIS Enterprise provides a series of default roles defined in Member roles—Portal for ArcGIS | Documentation for ArcGIS Enterprise, which group privileges along a spectrum from least privileged (Viewer) to most privileged (Administrator). However, organizations with Advanced security requirements will need to define custom roles that scope privileges tailored to roles defined by their organization. See Configure roles and privileges—ArcGIS Enterprise Sites | Documentation for ArcGIS Enterprise for guidance on this process.

Basic: **Configure** New Member Default Role as Viewer

New members in ArcGIS Enterprise will inherit the default role of User with privileges to create and share content and edit features they have access to. While this inheritance ensures ease of use in nonproduction operations, it can quickly lead to unexpected information sets being shared more broadly than expected. To protect against scenarios where users may accidentally share content to a wider audience than intended or edit service data unexpectedly, **it is recommended that new users be assigned the Viewer role**. The Viewer role is the least privileged role delivered with ArcGIS Enterprise and serves as an ideal default role for new accounts.

For additional details, see Configure new member defaults—Portal for ArcGIS | Documentation for ArcGIS Enterprise.



New member defaults

User type and role

Select the user type and role members are assigned by default when adding or inviting new members.

User type: Advanced

Role: Viewer

Figure 9—Set New Member Defaults

Basic: **Configure** Least Privilege User Types and Roles

ArcGIS Enterprise supports role-based access control, allowing administrators to use built-in roles or define custom roles with granular privileges. Users may then be assigned membership to these roles. A role defines the set of privileges granted to users who are members of the role. All ArcGIS Enterprise users are assigned membership in a role. Only users with privileges to update User roles may change a user's role membership. Only an administrator can add or remove users from the Administrator role. Use custom roles to delegate administrative tasks and for separation of duties. Limit use of designated administrative accounts. Do not use an administrative account for day-to-day, nonadministrative tasks. Assign roles to users using least privilege principles.

When elevating users' roles beyond those assigned by default, start with providing new members with a minimal set of privileges (recommend Viewer role) and elevate privileges as required by your use case. Use custom role membership as a means of delegating permissions and establishing separation of duties. It is not advised to preset a member's role attribute in a list to be imported from a file as an administrator. Instead, use a custom role or promote a user to the Administrator role as business needs require. If an imported user list does not specify default roles or user types, the defaults selected here are used.

Default Roles

ArcGIS Enterprise predefines a set of privileges for the following default roles:

- Viewer
- Data Editor
- User
- Publisher
- Administrator

Details regarding the definitions for these default roles are found in the ArcGIS Enterprise documentation.

Custom Roles

Esri recommends refining default roles to create custom roles that provide a more fine-grained set of privileges.

You have the ability to create custom roles that include administrative privileges to manage the Portal for ArcGIS settings. This allows administrators to delegate a specific set of administrative tasks to users without giving them the full set of privileges in the default Administrator role. For example, a user with a custom role that includes the **Organization website** privilege will have the ability to manage Portal for ArcGIS website settings without the ability to perform other administrative tasks, such as managing security or server settings.

The privileges that can be granted to a member through a custom role cannot exceed those associated with the member's assigned user type. For example, a member with a Viewer user type cannot be assigned a role with editing privileges.

User Types

User types assigned to ArcGIS Enterprise organization members are based on user workflows, needs, and licensing requirements. The user type determines the privileges that can be granted to the member through a default or custom role. Each user type also includes access to specific apps.

Provided user types include the following:

- Viewer
- Contributor
- Mobile Worker
- Creator
- Professional
- Professional Plus

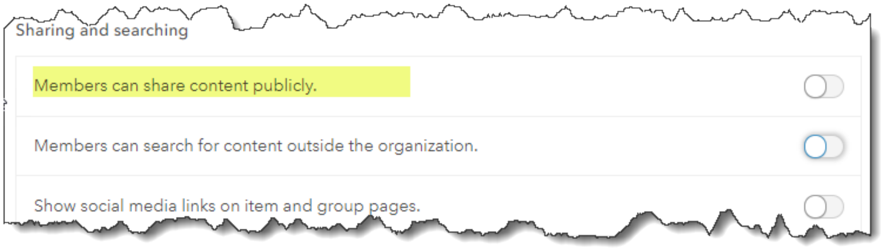
Details regarding the definitions of and privileges assigned to ArcGIS user types are found in the ArcGIS Enterprise documentation.

For full details regarding ArcGIS Enterprise user types, roles, and privileges, review the ArcGIS Enterprise documentation.

Basic: **Disable** Members Can Share Content Publicly

Users can share their geospatial content (such as maps, layers, and apps) with others in the organization, as well as with external users or the public, depending on their permissions. Access to shared content can be controlled at various levels, including individual items, groups, or the entire organization. By limiting a user's ability to share content publicly without elevated privileges, you provide an opportunity for editorial content review. A robust content review policy and procedure prevents unintended public sharing of PII, protected health information (PHI), and other confidential information.

When this setting is disabled, only administrators can share content publicly. This allows administrators to setup a workflow where members can share content to a group, the administrator reviews it and can then share it publicly (see GIS Data Publication Management for more workflow guidance).



Sharing and searching

Members can share content publicly. ○

Members can search for content outside the organization. ○

Show social media links on item and group pages. ○

Figure 10—Public Sharing Settings

Basic: **Disable** Public User Profile Sharing for Organization Users

Disabling public user profile sharing mitigates the risk that organization members may leak PII as part of their biographical user profile information. If profile information is not needed for members, we recommend disabling the option called Allow members to edit biographical information and who can see their profile found under Settings/Security/Policies/Access and permissions.

Basic: **Disable** Show Social Media Links

Disabling social media links on items and group pages reduces the risk of viral information leaks and rapid sharing mistakes.

Basic: **Configure** Decentralized Profile Visibility

By default, members can modify the biographical information in their profile and specify who can see their profile if Public User Profile Sharing has not been disabled. Ensure you develop a set of guidelines or policies for your organization that outlines the type of biographical information users should enter, if any, and the desired profile visibility settings. Communicate these guidelines to all users and encourage them to follow them when setting up or updating their profiles. Esri recommends that users without a clear need to publicly identify themselves by name limit what profile details others can see and set profile visibility to Private.

Advanced: **Implement** Central Profile Policy

ArcGIS Enterprise provides a global policy to allow or disallow members to edit biographical information and who can see their profile. Disable this option to prevent the oversharing of biographical information and to prevent members from marking profiles as public.

Basic: **Manage** Content via Role-Based Access Control

It is the responsibility of the organization administrator of ArcGIS Enterprise to organize roles, privileges, groups, and group membership to secure content and capabilities in line with the organization's goals. To meet this need, ArcGIS Enterprise organization administrators should familiarize themselves with the concepts outlined in the following:

- Manage content—Portal for ArcGIS | Documentation
- Manage groups—Portal for ArcGIS | Documentation
- Manage members—Portal for ArcGIS | Documentation

Esri encourages ArcGIS Enterprise administrators to leverage custom roles to delegate tasks reserved for traditional administrators to nonadministrative roles. Use of full administrator accounts should be limited. Never use an account with full administrative privileges for daily use activities.

Administrators can create user accounts, assign built-in or create custom roles, and manage permissions for individuals or groups within the organization. Users can be authenticated using the built-in user store or integrated with external identity providers, such as Active Directory, LDAP, or organization-specific identity providers like SAML 2.0 or OIDC-based identity providers. ArcGIS Enterprise supports linking AD, LDAP, or SAML groups from an enterprise identity provider.

Basic: **Configure** Default Group Membership Assignments

Select the groups that members are added to by default when adding or inviting new members. Use the principle of least privilege when selecting default groups. Avoid adding members to groups with shared update capabilities by default. Setting information can be found at Settings\New member defaults\Groups.

Advanced: **Manage** Distributed Collaboration Securely

Distributed collaboration allows organizations to share and sync content via ArcGIS Enterprise deployments or an ArcGIS Enterprise deployment and ArcGIS Online.

Fundamentally, distributed collaboration (or simply collaboration) is based on a foundation of trust between participating organizations and is motivated by common goals and initiatives that support data access and sharing.

Collaboration can be useful for many workflows, including exposing ArcGIS Enterprise content to the public through ArcGIS Online, making data visible across different departments in an organization, or managing field data collections.

When your organization participates in a distributed collaboration, Portal for ArcGIS initiating the collaboration assumes the host role. As the host, you may invite one or more ArcGIS Enterprise guests to share layers, maps, and files via groups. When collaborating with ArcGIS Online, the ArcGIS Online organization is always the host in a distributed collaboration with an ArcGIS Enterprise deployment.

Distributed collaboration is a trusted relationship where the terms and conditions set by all organizations apply. For additional collaboration information see the following resources:

- Presentation covering distributed concepts
- Documentation describing ArcGIS collaboration

Collaboration Security FAQ

- A collaboration uses asymmetric cryptography to authenticate communication between the participants.
  - An exchange of public keys happens when the invitation/response files are shared. When a host creates an invitation file, the JSON file contains a public key, which is shared with their guest(s).
  - Likewise, when the guest creates a response file, a public key is created, which is then shared with the host. Each participant has a unique key per collaboration. If these

invitation and response files are tampered with, they will be rendered invalid and will be rejected by the receiving system.

- Collaborations only allow communication over HTTPS and trusted certificates. This provides a secure channel in which to transfer data.
- Collaboration never shares/transfers named user identities or credentials.
- Should an environment be compromised, the attacker would not be able to access any resources in another participant's' environment that were not already explicitly shared at the collaboration.
- Collaboration participants can choose from the following how they want to share data:
    - They may perform a full copy of the web service where the copy result is hosted in the recipient's collaboration workspace.
    - They may share the content as a reference, where the data doesn't move, and the original web service is referenced in place (requiring a login if secured).
- To allow communication in an ArcGIS Enterprise-to-ArcGIS Enterprise collaboration, the guest's network firewall rules must support outbound communication over port 443.
- When collaborating between ArcGIS Enterprise and ArcGIS Online, all communication is initiated by Portal for ArcGIS, and network firewall rules must support outbound communication over port 443.

Collaboration Security Considerations

When working with collaboration groups, there are two options:

- Sharing feature layer and viewing data as copies
    - This option copies content from the host portal to the guest portal for editing by both host and guest portal members simultaneously. Edits are synced on demand or in an interval defined by the collaboration manager.
- Sharing feature layers as a reference
    - This option references live feature layers provided by the collaboration host. Data is not copied to the guest portal, and updates made by the members of the host organization are reflected immediately in the hosted feature layer.

The best security practice for collaborations is to share feature layers and views by reference. Sharing by reference prevents data from being copied to guest portals. Collaboration via reference ensures that data products your organization has created and owned cannot be rehosted elsewhere without your explicit knowledge and consent.

Depending on the use case and sensitivity level of the content in the collaboration groups, some customers choose to harden their implementation further by implementing technologies like VPN or IPSec. Frequently, these technologies are combined in a site-to-site VPN connection.

Collaboration Security Considerations—IPSec and VPN

Site-to-site VPN offers the following advantages:

- Provides a secure connection between two or more networks
- Enables users to access resources in another location or office
- Encrypts traffic between networks to enhance security

- Offers a cost-effective solution for interconnecting networks
- Provides a high level of network performance and reliability

The following are opportunity costs to configuring a site-to-site VPN:

- Site-to-site VPN is more technically complex and requires an additional level of management over remote access VPN, which is typically used by individual client machines to authenticate and access a work network.
- Site-to-site VPN requires network peripherals (typically routers) that can be configured to support these configurations.

Basic: **Implement** GIS Data Publication Management Process

When customers share GIS datasets, they assume the responsibility of protecting the privacy of data subjects, confidential records, and proprietary business-critical information from being accessed by unauthorized actors. The best way to prevent unauthorized actors from accessing private data is to not publish it at all, especially when aspects of the dataset are intended to be publicly consumed.

When sensitive data must be collected and/or published, ArcGIS Enterprise provides tools to assist with managing access to fields, datasets, and web services, such as the following:

- Hosted feature service views
- Group and role-based access controls
- ArcGIS distributed collaboration tools

While these tools are helpful, a robust GIS data publication and review process is highly recommended to prevent publication and sharing of sensitive content, which results in data spills that may have costly and embarrassing consequences.

Lessons Learned: How can ArcGIS Enterprise information leaks be prevented?

Information leaks can be minimized by implementing many of the best practices discussed in this document. The topics below summarize common pitfalls that, if best practices are effectively implemented, can be proactively limited or entirely prevented. Real-life case studies that resulted in this collection of lessons learned are found in this document's appendixes.

Basic: **Consider** Using Feature Layer Views

Hosted feature service views (described at Create hosted feature layer views—Portal for ArcGIS Help | Documentation) allow publishers to scope the capabilities available to a feature layer such as disabling editing and applying a data filter. The security value of feature layer views is further clarified within the technical paper “Limiting Access to Public Survey123 Reponses” found within the ArcGIS Trust Center documents.

Basic: **Consider** Publication Governance and Delivery Pipelines

- Validate the content before publication is available for public discovery.
    - Create a process for content review.
    - Nominate a committee of subject matter experts to review content.
    - Validate if the resource contains PII, PHI, or other proprietary or sensitive Information.
        - If so, the content does not pass the gateway. Disallow publication until content issues are remediated.
- Do not allow publication of content until the review is complete.
- Disable user ability to share content with the public. Users designated as publishers can share once the publication gateway is satisfied.

Basic: **Consider** Defining Content Access Requirements

- Determine the audience: Is the information intended for a public or private audience?
- Define the requirements: Is editing enabled or required? By whom?
    - Limit public editing ability.
    - Use feature service views to limit the discovery of new public feature edits prior to review.

Basic: **Verify** Content Ownership Rights

At a minimum, prepare answers to the following questions for an officially published service:

- Is the content proprietary or a trade secret?
    - If so, do you have authorization to share the content?
- Is the content authoritative?

Basic: **Manage** Accounts and Reduce User Permissions

- Regularly review the roles and permissions assigned to users.
- Remove unnecessary permissions from users. Use least privilege principles as a guide.
- Elevate user privileges as required per use case.
    - Document privilege escalations.
    - Revoke privileges when tasks requiring elevated privileges are complete.
    - Leverage custom roles to delegate tasks.
    - Severely limit access to the administrator role.

Basic: **Implement** Permission Guardrails

- Never perform day-to-day tasks as an administrator.
- Reserve the use of the Administrator role for administration tasks only.
- Use the Administrator role to govern and deploy security guardrails that enhance member accounts, like creating custom roles to delegate tasks to users.

Basic: **Manage** Access Based on Employee or Project Life Cycle

- Use centralized user administration tools like organization-specific logins (SAML). Revoke privileges when a user leaves the organization or changes roles.
- Regularly review built-in accounts (e.g., contractors or other stakeholders who are not employees) and remove or disable privileges from inactive users.

Supporting Infrastructure

Infrastructure security incorporates all controls that apply to the network, operating system, database, and web server tiers supporting the application. Security at this layer reduces the attack surface and provides defense-in-depth protections that serve to reduce the impact of a compromise at the application tier. Be aware that keeping supporting infrastructure components up-to-date is just as important as using the latest version of ArcGIS Enterprise application software. We highly recommend staying with at least the General Availability-supported versions of software for production operations; extended support and end-of-life versions are less secure than current versions and have fewer protection mechanisms available.

Items addressed within the Supporting Infrastructure section include the following:

- Security Baselines—Zero Trust Alignment
- Boundary Protections
- Privileged Access Network-Based Administration

Security Baselines

All supporting information technology components such as operating systems, databases, and more should be security hardened to a standard/recommended benchmark/baseline such as vendor security baselines (e.g., Microsoft Security Baseline, CIS benchmarks, or the Defense Information Systems Agency's [DISA] Security Technical Implementation Guide [STIG]) as described below. Operating system (OS) hardening is a requirement common to most security control frameworks (e.g., NIST 800-53, ISO 27001) and is a foundational step in supporting a Zero Trust Architecture (ZTA) strategy.

Basic: **Implement** Vendor Security Baselines

Any ArcGIS Enterprise component (Portal for ArcGIS, ArcGIS Server, ArcGIS Data Store, etc.) running on an OS, exposed either directly or indirectly to a network of lesser trust (e.g., corporate extranet, public internet) should be hardened at a minimum to the recommendations provided by the OS 'vendor's security baseline. OS hardening should be performed before ArcGIS Enterprise is installed.

ArcGIS Enterprise 10.9.1+ has been tested to function with no operational impacts on systems hardened to the Microsoft Security Baseline for Windows Server 2019. Note that you will not be able to utilize Internet Explorer (retired in 2022) to create a new site on a hardened OS, instead, you will need to use a current browser. Do *not* utilize retired software as part of your implementation as it presents extraordinary high risk to your operations.

Linux has many variations, and those that should be considered for production operations have associated baselines.

Similar hardening baselines should be applied to all other significant components utilized to support your ArcGIS Enterprise implementation. This includes any optional enterprise database products (Oracle, Microsoft SQL), web servers (Apache), or even underlying cloud infrastructure providers (Azure, AWS).

For example, if you are utilizing MS SQL Server with ArcGIS Enterprise, Esri recommends applying best practices for SQL security provided by Microsoft, which helps to address controls required by CIS benchmarks and FedRAMP regulatory compliance frameworks. To apply SQL security, run the Vulnerability assessment for SQL Server against all ArcGIS Enterprise geodatabases hosted on SQL Server and address all **Medium** (or higher) **Risk** findings.

Advanced: **Implement** Advanced Benchmarks

Unless your organization is required to provide DISA STIG's or Center for Internet Security (CIS) Level 2 benchmarks, you should likely utilize vendor security baselines instead. For example, Microsoft uses its security baseline instead of STIG and CIS benchmarks for its public cloud services as it has found its baseline to provide the right balance of security, stability, and performance for enterprise demands, similar to our Basic security profile.

If you are a customer who has DISA STIG security hardening requirements, our Advanced security profile can be utilized to satisfy your application STIG requirements for ArcGIS Enterprise. See the checklist of Basic and Advanced controls in Appendix H to align with STIG requirements, including severity, and automated check mechanisms.

Advanced: **Consider** Secure Web Gateways (SWG)

One mechanism some organizations are using to help meet the ZTA principle of ensuring all traffic is authenticated while avoiding the use of VPN is through Secure Web Gateways (SWG) and Identity Aware Proxies (IAP's). IAP's are designed to make HTTPS-based services publicly available to authorized individuals; however, the market is still immature with two main offerings from Google and F5. Other vendors are releasing more extensive SWG's such as Microsoft's Entra, with capabilities rapidly evolving.

ArcGIS Enterprise web clients can be used successfully with IAP's today; however, thick clients and mobile offerings commonly have issues at this time and are actively being reviewed by Esri for compatibility improvements.

Note: It is highly recommended that you only consider such services as part of your deployment if you have dedicated resources to specifically manage these rapidly evolving security services. Otherwise, postpone consideration until associated capabilities solidify more and more robust operating and security practices established.

Advanced: **Verify** Log Folder Security Permissions

Logs always contain sensitive information, therefore it is important to verify the folder security permissions on the OS for the ArcGIS Enterprise log folders to ensure inappropriate accounts do not have access to manipulate or view its contents. It is important to periodically audit folder security permissions due change or drift over time for various factors such as troubleshooting. There are several Windows assigned built-in groups such as “SYSTEM” and “Administrators” which have Full Access. The System Administrator’s account should be in the “Administrators” group to inherit the necessary administrative permissions. The ArcGIS Service account should have Full Control of the log folders. If utilizing a SIEM to ingest logs the SIEM agent should only have read permissions to only the log's audit directory. Non-System Administrator accounts with access to the log folders should removed.

Boundary Protections

Boundary protection techniques include any of the following measures that reduce the network attack surface and alert administrators of potential network compromise. These protections ascribe a network boundary that provides a *first line of defense* that narrows application attack surface to ports and protocols that are minimally required for the proper operation of ArcGIS Enterprise. These controls can take the form of the following:

- Monitors at external boundaries and key internal boundaries within the system including network firewalls and network-based intrusion detection systems (NIDS)
- Network segmentation of publicly accessible system components from internal organizational networks
- Managed network interfaces that include boundary protection devices

Basic: **Implement** Network Segmentation

Deploy ArcGIS Enterprise on a network that is logically or physically segmented (e.g., DMZ) from internal networks to reduce the risk that a compromise of ArcGIS Enterprise will lead to lateral compromise of organization systems and vice versa. Refer to the Secure Deployment Patterns section of this document for details on how to segment networks to suit various ArcGIS Enterprise deployments.

Basic: **Consider** Not Using ArcGIS Web Adaptor

ArcGIS Web Adaptor is an optional component of an ArcGIS Enterprise deployment that serves the specific purpose of delivering third-party web server-managed security such as IWA or PKI Authentication. It is recommended that the Web Adaptor is NOT utilized for Internet-facing ArcGIS Enterprise deployments unless necessary for your use case. The recommended pattern is to use a production-grade WAF-enabled load balancer as a front end for ArcGIS Enterprise; however, for ease of setup, customers might use ArcGIS Web Adaptor in a Basic deployment. Please see Appendix J: Load-balancer Rules When NOT Utilizing Web Adaptor.

Basic: **Implement** Web Application Firewall

Access to ArcGIS Enterprise should be gated by a Layer 7 firewall such as a WAF-enabled load balancer, proxy, or network access gateway. WAFs allow fine-grained inspection and filtering of HTTP sessions. Though a WAF requires ongoing management, it is now considered a basic component of a secure deployment involving web-based applications and services.

ArcGIS Enterprise has been operationally validated with specific OWASP Core Rules for use with WAFs (see ArcGIS Enterprise Web Application Filter Rules).

Important: Improper deployment of WAF rules including the OWASP Core Rule Set will create operational problems with ArcGIS Enterprise. To avoid an operational outage, Esri recommends testing any WAF configuration in Detect mode before switching any web application firewall to Protect mode.

Note: There is no capability to disable SOAP through the ArcGIS Enterprise user interface or API. A WAF can block SOAP requests, however it can disrupt ArcGIS Pro's ability to consume some ArcGIS Enterprise services (see Secure Pattern + Admin Publishing solution). For guidance on blocking SOAP, refer to the ArcGIS Enterprise WAF filter rule set.

WARNING: Exposing ArcGIS Enterprise directly to the public internet/Edge without a WAF is a high-risk deployment pattern. Organizations considering this pattern should instead explore publishing internet-accessible services to ArcGIS Online.

Advanced: **Consider** Allow Listing File Extensions

You can restrict file extensions to a known set (an Allow List) that is compatible with ArcGIS Enterprise that the web server is allowed to serve or intercept using a WAF. See additional information on OWASP's guidance concerning minimizing unrestructured file uploads where Allow Listing file extensions are addressed. If your organization regularly incorporates new file types into your ArcGIS Enterprise deployment, this control might be more disruptive than the security value it provides.

To help populate a file extension allow list within a WAF or Web Server setting, the full list of file extensions required by ArcGIS Enterprise 11.1 and later to function is available in Appendix C: Web Server Extensions to Allow. Test this extension list thoroughly in your DEV/QA environments before making these changes in production as they can have operational impact.

Troubleshooting tip: If organization-specific logins are implemented, include the top level domain (TLD), for instance, .com, .net, .org. If your domain is example.com, add .com to the list of extensions so that patterns in web responses are not inadvertently blocked.

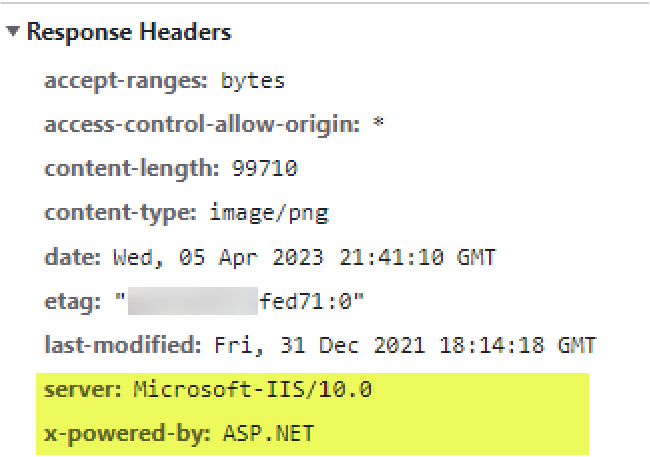
Advanced: **Disable** Web Tier Technology Identifiers and Banners

By default, most web servers set headers that identify the server type and version. They frequently also identify the underlying technologies used to support the websites the web servers host.

As best practice, Esri recommends disabling these headers:

a. Server
b. X-Powered-By
c. X-ASPNet-Version
d. X-ASPNetMvc-Version

This list is non-exhaustive, and your front-end web server, load balancer, or other gateway technology may reveal other details that may be useful to an adversary for constructing exploits. Review your specific front-end technologies vendor documentation for details regarding the provided headers and pivot as required.



```
▼ Response Headers
    accept-ranges: bytes
    access-control-allow-origin: *
    content-length: 99710
    content-type: image/png
    date: Wed, 05 Apr 2023 21:41:10 GMT
    etag: "[redacted]fed71:0"
    last-modified: Fri, 31 Dec 2021 18:14:18 GMT
    server: Microsoft-IIS/10.0
    x-powered-by: ASP.NET
```

Figure 11—Web Tier Header Before Mitigation

Advanced: **Implement** Intermachine Network Restrictions

ArcGIS Enterprise is a distributed computing platform that is designed to scale horizontally across multiple physical or virtual machines as described in Appendix B. In these patterns, organizations with Advanced security requirements must construct network firewall rules to permit intermachine communication port connections between ArcGIS Enterprise components without setting overly broad network rules. Table 7 shows recommended intermachine network rules by ArcGIS components.

Table 7—Recommended Intermachine Network Rules by ArcGIS Components

Source	Destination	Required Inbound Ports
Portal for ArcGIS	Self (Local Traffic)	*
Portal for ArcGIS	Portal (HA Configuration)	5701-5703, 7120, 7443, 7654
Portal for ArcGIS	Server	443, 6443
Portal for ArcGIS	Data Store	None
ArcGIS Server	Self (Local Traffic)	*
ArcGIS Server	Server (Multimachine Site)	443, 6443
ArcGIS Server	Portal	443, 7443
ArcGIS Server	Data Store	2443, 9829, 9876, 9220, 9320, 29080, 29081
ArcGIS Data Store	Self (Local Traffic)	*
ArcGIS Data Store	Data Store (Standby)	2443, 9876
ArcGIS Data Store	Server	None
ArcGIS Data Store	Portal	None

**ArcGIS Enterprise components open a variety of local ports for intermachine communication, including random ports in wide ranges. Esri does not recommend restricting system-local network ports with ArcGIS Enterprise.*

See Appendix J: ArcGIS Enterprise Ports Utilized Diagram and the ArcGIS Enterprise System Requirements: Firewall Settings documentation.

Advanced: Implement Network Intrusion Detection System

NIDS have no operational impact on ArcGIS Enterprise provided they are configured to permit minimally required ports and protocols to communicate (refer to Portal used by Portal for ArcGIS for required ports and protocols) or make use of TAP/SPAN ports to deploy intrusion detection systems out-of-band where they monitor but do not interfere with network traffic. Examples of products that offer these features include the following:

- Palo Alto Networks
- Cisco ZTA security platform
- Snort

None of the above NIDS solutions require specific ArcGIS Enterprise or NIDS configuration; organizations with Critical infrastructure requirements may use any NIDS solution with ArcGIS Enterprise.

Privileged Access Network-Based Administration

Follow privileged access management principles for network-based administration of critical software. Examples of possible implementations include using hardened platforms dedicated to administration and verifying before each use, requiring unique identification of each administrator and proxying and logging all administrative sessions to critical software platforms.

Basic: Avoid Forward Proxy Authentication

Some organizations require that outbound access from the organizational domain to the public internet be governed through a single egress point which may be a forward proxy. A forward proxy may be used to assist with ensuring user anonymity, content filtering and outbound traffic monitoring.

Some organizations configure their forward proxy to require the connecting client to provide authentication before allowing traffic to reach the public internet. ArcGIS Enterprise supports forward proxies that require authentication. However, Esri does not recommend this configuration. Forward proxies can be easily misconfigured, allowing authentication headers to leak to the outside world.

Like many software solutions, ArcGIS Enterprise uses basic authentication to authenticate with forward proxies. Basic authentication is not encrypted, instead Basic authentication is base64 encoded. Should an attacker gain access to authentication headers that use base64 encoding, the credentials are trivially decoded. For this reason, it is more secure to NOT use Basic Authentication between a customer’s forward proxy and ArcGIS Enterprise servers.

Advanced: **Implement** Administrative Network Segments

Limit administrative access to ArcGIS Enterprise to administrative network segments. Two options for employing this control are outlined below; organizations may choose the pattern (or both patterns) that best suits their operational capabilities and resources:

Option 1 (Recommended): Block administrative endpoints to ArcGIS Enterprise by deploying a web application firewall that employs the Application-Specific Endpoint Filtering (Block Admin API) rules outlined in ArcGIS Web Application Filter Rules. Note that this option imparts operational impact to administrative functions that are not necessary for the day-to-day operations of Portal for ArcGIS. This option improves the security of your deployment by limiting the attack surface of end-user access to administrator capabilities of both ArcGIS Server and Portal for ArcGIS.

Option 2: Deploy ArcGIS Web Adaptor, disabling administrative access for ArcGIS Server. There is not a similar Web Adaptor option for Portal for ArcGIS.

While optional, the ArcGIS Web Adaptor component is commonly deployed on Internet Information Services (IIS), or Java application server, to serve as a proxy to support third-party authentication services to ArcGIS Enterprise and limited filtering of administrative endpoints. Disable access to administrative endpoints through ArcGIS Web Adaptor by referring to the documentation Configuring the Web Adaptor from the configuration web page.

WARNING: Implementing these controls has an operational impact and will block administrative functions including administrative workflows with ArcGIS Pro.

Advanced: **Configure** Cross-Origin Resource Sharing Allow List

The CORS allow list only allows specified domains to consume your web services for applications that honor CORS. Starting at version 10.7, ArcGIS Enterprise (ArcGIS Server and Portal for ArcGIS) allows ArcGIS administrators to define a list of application origins (domains where web applications are hosted) that ArcGIS Enterprise is allowed to respond to. Application servers that allow CORS requests from all domains may be open to exploit. Domains allowed to make CORS requests to ArcGIS Enterprise should be defined in the CORS allow list.

See Restrict cross-domain requests to ArcGIS Server and Restrict cross-domain requests to your portal for full details on this security feature in ArcGIS Enterprise.

Important: When configuring CORS-allowed origins, you cannot use the * wildcard character in the domain name as a substitute for machine names or subdomains, such as https://*.example.com. You must specify the fully qualified domain name of each machine or subnet in the list.

Note: Some applications do not honor CORS such as Map Viewer Classic. Accordingly, organizations should migrate to using modern applications including the currently available default Map Viewer within ArcGIS Enterprise.

Advanced: **Implement** Content Security Policy

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including XSS cross-site scripting and data injection attacks. The CSP header consists of one or more *directives* that tell the browser how to behave and which resources it can access when interacting with a given website.

Introduced at 11.4, the contentSecurityPolicy property defines the Content-Security-Policy (CSP) response headers that are included when accessing the organization's portal website or any of its associated applications. The CSP for the portal website, and the CSP for its applications, are defined separately. The values for each CSP can be one or more of the CSP directives based on the CSP specifications. For more information on CSP syntax and directives, reference the Content-Security-Policy documentation maintained by MDN Web Docs.

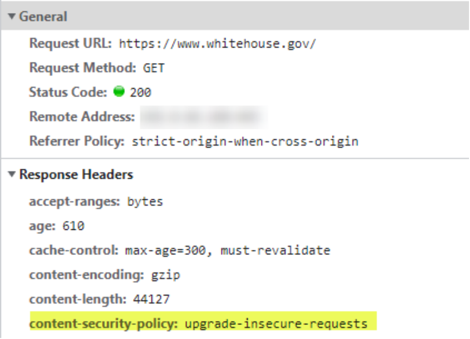
By default, Portal for ArcGIS Sets a CSP to prevent the Portal website from being framed in external domains. The default CSP is:

```
"contentSecurityPolicy": {
"home": "frame-ancestors 'self';",
"apps": "
}
```

Apps hosted on Portal for ArcGIS can also set a CSP to determine where they may be framed. There are many additional CSP directives that the ArcGIS Enterprise administrator can apply. Defining an appropriate CSP can be as easy or as complicated as the mission requirement. CSPs can determine the origins of where content, web services, images, and other files may be consumed on a website. Administrators who consume content from remote hosts may find that maintaining an effective CSP is burdensome, as a complete inventory of hosts that consume services provided *and* an inventory of hosts that consume your content and services may be required.

A basic CSP may include setting the upgrade insecure requests directive. This policy ensures that all content is provided over HTTPS—even in the case where some files (images, documents, etc.) are not explicitly referenced via HTTPS. This directive is intended for websites with large numbers of insecure legacy URLs that need to be rewritten.

```
Content-Security-Policy: upgrade-insecure-requests
```

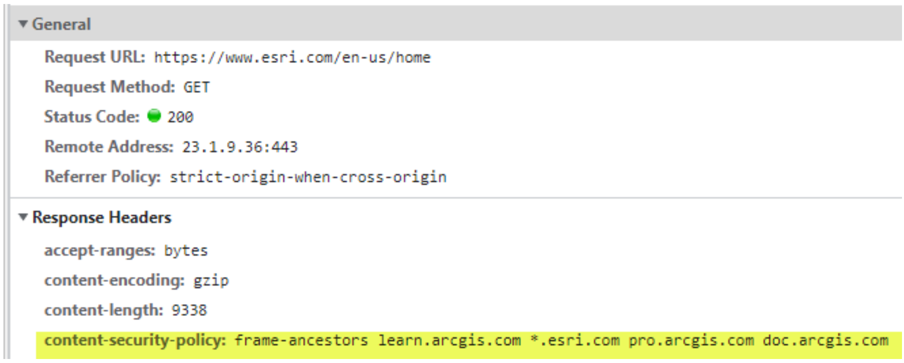


```
▾ General
    Request URL: https://www.whitehouse.gov/
    Request Method: GET
    Status Code: ● 200
    Remote Address: [redacted]
    Referrer Policy: strict-origin-when-cross-origin
▾ Response Headers
    accept-ranges: bytes
    age: 610
    cache-control: max-age=300, must-revalidate
    content-encoding: gzip
    content-length: 44127
    content-security-policy: upgrade-insecure-requests
```

Figure 12—Content Security Policy Upgrade Insecure Requests Header

The Esri.com home page sets a CSP to explicitly define origins that can be included in a frame.

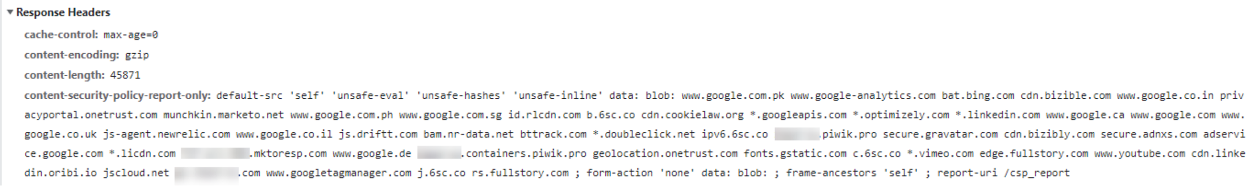
Content-Security-Policy: Frame Ancestors



```
▼ General
    Request URL: https://www.esri.com/en-us/home
    Request Method: GET
    Status Code: ● 200
    Remote Address: 23.1.9.36:443
    Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers
    accept-ranges: bytes
    content-encoding: gzip
    content-length: 9338
    content-security-policy: frame-ancestors learn.arcgis.com *.esri.com pro.arcgis.com doc.arcgis.com
```

Figure 13—Content Security Policy Frame Ancestors Header

More complicated CSPs may define domains where scripts, cascading style scripts (CSS), and frames can be loaded; which websites are able to frame your content; and where images and other media can be consumed; etc. In this example, CSP sets many directives.



```
▼ Response Headers
    cache-control: max-age=0
    content-encoding: gzip
    content-length: 45871
    content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: www.google.com.pk www.google-analytics.com bat.bing.com cdn.bizible.com www.google.co.in priv
    acyportal.onetrust.com munchkin.marketo.net www.google.com.ph www.google.com.sg id.rlcdn.com b.6sc.co cdn.cookielaw.org *.googleapis.com *.optimizely.com *.linkedin.com www.google.ca www.google.com www.
    google.co.uk js-agent.newrelic.com www.google.co.il js.driftt.com bam.nr-data.net bttrack.com *.doubleclick.net ipv6.6sc.co [redacted].piwik.pro secure.gravatar.com cdn.bizibly.com secure.adnxs.com adservi
    ce.google.com *.licdn.com [redacted].mktoresp.com www.google.de [redacted].containers.piwik.pro geolocation.onetrust.com fonts.gstatic.com c.6sc.co *.vimeo.com edge.fullstory.com www.youtube.com cdn.linke
    din.oribi.io jscloud.net [redacted].com www.googletagmanager.com j.6sc.co rs.fullstory.com ; form-action 'none' data: blob: ; frame-ancestors 'self' ; report-uri /csp_report
```

Known Limit:

A CSP used for ArcGIS Enterprise versions that support apps written with the ArcGIS API for JavaScript v3.x and apps written in the ArcGIS Maps SDK for JavaScript 4.x that support 3D functions may need to set unsafe-eval, unsafe-inline or wasm-unsafe-eval in any script-src directive.

Any CSP will need to be well-tested, but writing an effective CSP can be complicated and error prone. To apply a CSP to an existing website, first determine the directives you need to support and leave the allow lists for each directive blank. Run the CSP in report-only mode for a month or so. In this manner, you can monitor the violations sent via POST in JSON format to a resource you specify. You can then determine which resources should be set on an allow list based on your use case.

Data Protection

Under Executive Order 10428, NIST describes data protection in part as establishing fine-grained access control for data resources, protecting data at rest, protecting data in transit, and proper backup management. The guidance below is aimed at the following:

- Data Management and Backups
- Protect Data at Rest
- Protect Data in Transit
- Fine-Grained Access Control

Data Management and Backups

Store sensitive information, such as passwords and secret keys, securely using encrypted storage mechanisms provided by your operating system or third-party tools. When using ArcGIS Data Store for storing hosted feature layers and other content, you can enable encryption for data at rest. Configure your relational or tile cache data stores to use encrypted connections by obtaining and installing SSL certificates for your data store machines.

Basic: **Implement** Backup Strategy and Test Regularly

Ensure the durability of ArcGIS Enterprise and its data by establishing and automating a backup strategy that takes into account Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

RTO is an organizations' downtime tolerance to restore ArcGIS Enterprise operations. If this window is measured in minutes or seconds, the best practice is to maintain a replicated deployment of ArcGIS Enterprise (warm) or a High Availability ArcGIS Enterprise (hot) deployment to ensure near-zero downtime in the event of a disaster:

- Automate replication to a standby deployment—Portal for ArcGIS | Documentation
- High Availability in ArcGIS Enterprise—Portal for ArcGIS | Documentation

The Recovery Point Objective defines an organization's tolerance for data loss in the event of a disaster. This value governs the frequency by which backups must be performed. For example, if an organization can tolerate no less than 1 hour of data loss, the appropriate backup strategy would be the following:

- Daily Full Backup: ArcGIS Enterprise backups—Portal for ArcGIS | Documentation
- Hourly Incremental Backup: ArcGIS Enterprise backups—Portal for ArcGIS | Documentation

Equally important is the need to test/validate the backup/restore process at least annually or when making any change to the process to ensure backups can be restored when needed. To test (and execute) a restore from the backups taken above, review the guidance at Restore ArcGIS Enterprise—Portal for ArcGIS | Documentation.

Basic: **Consider** File Geodatabases

There are different ways to expose information to the public. However, when it comes to exposing content from a geodatabase to the public, the security best practice is to publish content from a referenced data source such as a file geodatabase.

A file geodatabase is a collection of files in a folder on disk that can store, query, and manage spatial and nonspatial data. A security benefit of using a file geodatabase is that it can be a useful intermediary and help mitigate potential SQL injection attacks.

It is recommended practice for an organization to classify its data or content and assign tags or labels that define the following:

- **Public:** Business data that is freely available and approved for public consumption
- **Confidential:** Business data that can cause harm to the organization if shared publicly

With a public share use case, using a file geodatabase is ideal because the content is deemed to be of low or no risk to the organization. Content classified as confidential can be stored or hosted in an enterprise geodatabase behind the corporate firewall where it is safe, and then the other datasets with a lower risk classification can be hosted in a file geodatabase with a server in the DMZ where publicly accessible services are hosted.

Protect Data at Rest

Protecting data at rest is defined as the process of encrypting sensitive data in a manner consistent with NIST's cryptographic standards. In terms of ArcGIS Enterprise, this means that both file-based and data-based geospatial data must be encrypted either at the file level, disk level, or both. ArcGIS Enterprise supports data encryption and has several best practices for ensuring data security.

Ensure you encrypt sensitive data stored on disk, such as user credentials, feature attachments, and other content. You can use file system-level encryption or database-level encryption, depending on your infrastructure and requirements. For file system-level encryption, consider using solutions like Windows Encrypting File System (EFS) or other third-party encryption tools. For database-level encryption, utilize your database management system's built-in encryption capabilities, such as Transparent Data Encryption (TDE) in SQL Server and Oracle.

Basic: Implement Whole Disk Encryption

Encryption at REST is a supplemental deployment to ArcGIS Enterprise. ArcGIS Enterprise has been validated to function on systems that use BitLocker whole disk encryption to encrypt the disks that ArcGIS Enterprise uses for storing content and configurations. In this configuration, the data disks that support the following functions should be encrypted using BitLocker or other whole disk encryption technology that uses FIPS 140-2 validated cryptographic modules.

To encrypt the volume on Windows-hosted ArcGIS Enterprise volumes, enable BitLocker to drive encryption and auto-unlock against drives where ArcGIS Enterprise components read/write data. By default, these locations are the following:

- Portal: \arcgisportal\
- Server: \arcgisserver\
- Data Store: \arcgisData Store\

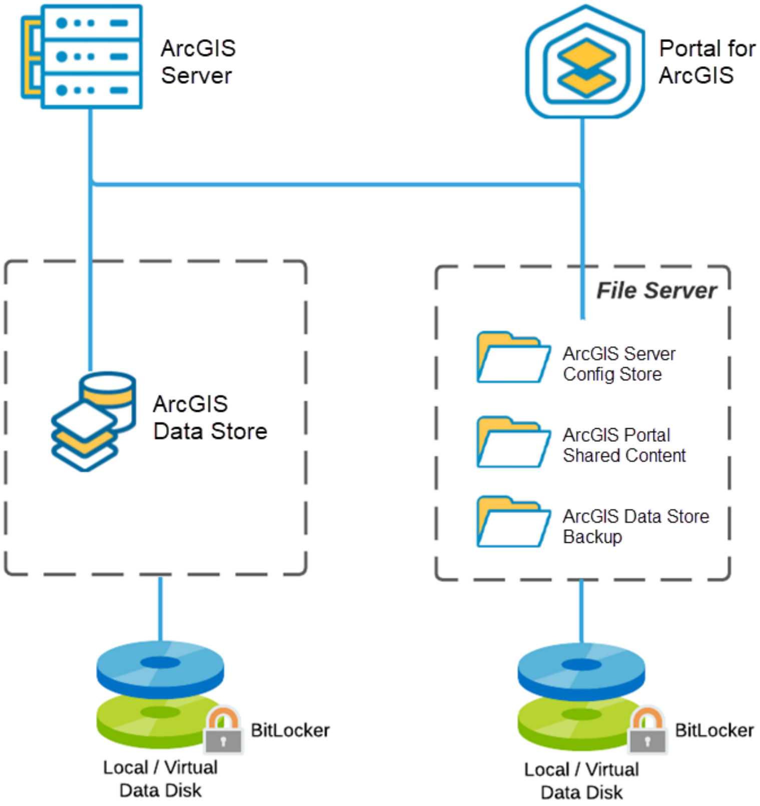

ArcGIS Server
Portal for ArcGIS
ArcGIS Data Store
File Server
ArcGIS Server Config Store
ArcGIS Portal Shared Content
ArcGIS Data Store Backup
BitLocker
Local / Virtual Data Disk
BitLocker
Local / Virtual Data Disk

Figure 14—BitLocker Encryption

To enable BitLocker whole disk encryption, execute the guidance below:

1. Enable-BitLocker (BitLocker) | Microsoft Learn
2. Enable-BitLockerAutoUnlock (BitLocker) | Microsoft Learn

Note: BitLockerAutoUnlock is only available on non-OS volumes; if the data locations defined above reside on the OS volume, migrate to non-OS volumes using guidance in the following:

- **Portal for ArcGIS:** Changing the portal content directory—Portal for ArcGIS | Documentation
- **ArcGIS Server:** Add a server directory in Server Manager—ArcGIS Server | Documentation
- **ArcGIS Data Store:** Create a data store—Portal for ArcGIS | Documentation

Basic: **Implement** Database Transparent Data Encryption

Organizations with enterprise geodatabase data hosted on a relational database management system (RDBMS) should consider encrypting database files, logs, and backups as a component of a security baseline for ArcGIS Enterprise. This is best addressed with TDE. The ArcGIS Enterprise geodatabase component has been validated with SQL Server TDE and Oracle TDE systems.

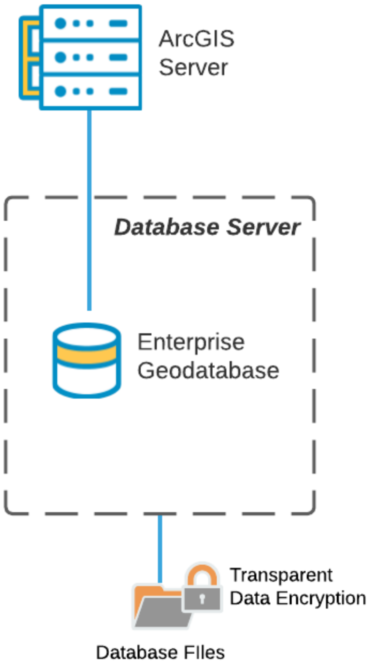


Figure 15—Transparent Data Encryption with Enterprise Geodatabase

To enable TDE with ArcGIS Enterprise, encrypt the database on which the ArcGIS Enterprise Geodatabase is hosted using the guidance from the respective vendor:

- SQL Server: Enable TDE
- Oracle: Configuring TDE

Reference:

- Does ArcGIS Support TDE with enterprise geodatabases stored in SQL Server?

Protect Data in Transit

ArcGIS Enterprise provides encrypted communications with external systems via HTTPS and current mechanisms such as TLS 1.2 and TLS 1.3 by default. Customers with more advanced security needs may want to supplement this mechanism.

Basic: **Verify** HTTPS Is Enforced

Clients to your ArcGIS Enterprise deployment should communicate through an enterprise-grade Web Application Firewall and load balancer, also referred to as a security gateway device. Customers utilizing this configuration allow your Information System Management team to control/update ciphers used between the gateway and clients without the need to configure individual application server end points.

Using such a security gateway is significantly more agile and flexible for meeting customer transport communication requirements with client applications and devices. Ensuring the communication between your ArcGIS Enterprise systems and the security gateway is as secure as possible is part of a security-in-depth strategy. To ensure secure HTTPS communication, all edge-exposed ArcGIS Enterprise components, web servers, gateways and other peripherals should be configured to support TLS 1.2+ using 256-bit (or stronger) encryption algorithms and must enable HSTS (Strict Transport Security).

See the following guidance on how to validate that the default parameters are in place:

- Documentation for Restricting Portal for ArcGIS TLS protocols and ciphers suites
- Documentation for Restricting ArcGIS Server TLS protocols and ciphers suites

Basic: **Configure** HTTP Strict Transport Security Enforcement

The HTTP Strict Transport Security enforcement (HSTS) header, when set by the web server, requires web clients to connect over HTTPS and to refuse to connect over HTTP. This security control protects clients from inadvertently sending data over HTTP.

See the following documentation for guidance on how to configure this setting within Portal for ArcGIS and ArcGIS Server respectively:

- Enforce strict HTTPS communication—Portal for ArcGIS | Documentation
- Enforce strict HTTPS communication—ArcGIS Server | Documentation

Advanced: **Configure** Hardened TLS Algorithms

Ideally, CBC and TLS_RSA ciphers should not be utilized, however, this configuration reduces the number of backwards compatible clients that can connect to your implementation. The Advanced cipher configuration recommendations below provide broad current client connectivity while eliminating weaker ciphers. Current client compatibility with these ciphers can be validated by Qualys SSL Labs' free analysis service.

See the following guidance on how to configure hardening the TLS algorithms specified below:

- Documentation for Restricting Portal for ArcGIS ciphers suites
- Documentation for Restricting ArcGIS Server ciphers suites

A suggested set of secure ciphers for Advanced customers to consider are as follows:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_AES_256_GCM_SHA384 (TLSv1.3 only)
- TLS_AES_128_GCM_SHA256 (TLSv1.3 only)

Basic: **Implement** Signed CA Certificates

Initial deployments of ArcGIS Enterprise edge components (Portal for ArcGIS and ArcGIS Server) are configured to use HTTPS through self-signed certificates generated at installation time. Self-signed certificates are sufficient for development and basic testing, but production deployments must use certificates signed by a certificate authority (CA).

For internal use-only deployments, use Active Directory Certificate Services (AD CS), a Windows server role that provides customizable services for issuing and managing public key infrastructure (PKI) certificates. AD CS allows administrators to create and deploy digital certificates to users, computers, and other network resources within their organization.

For public use case deployments, obtain certificates from a trusted CA. A trusted CA is a third-party entity that issues digital certificates such as DigiCert, VeriSign, etc. These certificates are signed by the CA and can be verified by anyone with access to the CA's root certificate. Obtaining certificates from a trusted CA ensures that your certificates are recognized by all major web browsers and operating systems.

Free certificate authorities such as Let's Encrypt can be leveraged. Let's Encrypt is a nonprofit certificate authority that provides free, automated SSL/TLS certificates to enable secure HTTPS connections for websites.

The benefit of a trusted CA certificate is that it allows you to implement certificate pinning, a technique that allows you to ensure that your clients only accept certificates issued by trusted CAs. This is done by comparing the public key of the certificate presented by the server with a preconfigured value. If the values match, the certificate is considered trusted, and this can protect against man-in-the-middle attacks.

The documentation below describes how to deploy CA-signed certificates onto ArcGIS Enterprise edge components:

- Portal for ArcGIS: Import a certificate into the portal—Portal for ArcGIS
- ArcGIS Server: Configure ArcGIS Server with a new CA-signed certificate—ArcGIS Server

Ensure that your SSL/TLS certificates are up-to-date and replace them before they expire. Using expired certificates can lead to security vulnerabilities and affect the availability of your ArcGIS Enterprise services.

Advanced: **Consider** FIPS 140-2 Encryption

While ArcGIS Enterprise utilizes secure encryption algorithms by default, some customers (such as federal and Defense agencies) may be required to use FIPS-validated encryption at rest and transport. If your organization is not mandated to use FIPS encryption as part of a compliance requirement, then you will likely **not** want to enforce it as its security value is debatable for most deployments.

For Windows deployments, Esri products are compatible with the operating system *Use FIPS compliant algorithms* security setting. For Linux deployments, ArcGIS Enterprise can be configured to use FIPS-approved algorithms for encryption in transport and supplemented with third-party mechanisms to enforce FIPS-compliant encryption of data at rest (such as self-encrypting hard drives).

One mechanism to provide FIPS-compliant endpoints for client systems is to utilize a security gateway or WAF in front of your ArcGIS Enterprise deployment that includes a *FIPS mode* capability as discussed earlier in the Protect Data in Transit section of this document.

Limiting Data Access

Implement data protection mechanisms relative to resources used by critical software enforcing the principle of least privilege to the extent possible.

Advanced: **Implement** Data Segmentation

ArcGIS Enterprise supports data segregation and provides best practices to help organizations manage and protect their geospatial data effectively. Data segregation in ArcGIS Enterprise can be achieved through various means, ensuring that sensitive data is isolated from less sensitive or public data.

Here are data segregation best practices for ArcGIS Enterprise:

1. Separate storage for sensitive data: Store sensitive geospatial data in separate databases or data stores from nonsensitive data. This can help minimize the risk of unauthorized access or data breaches.
2. Use of ArcGIS Data Store types: Leverage different types of ArcGIS Data Store, such as the relational data store, tile cache data store, and spatiotemporal big data store, to segregate data based on their purpose, sensitivity, or performance requirements.
3. Separate Instances: In large organizations or multidepartment deployments, consider using separate ArcGIS Enterprise instances or portals for each department or business unit. This can help segregate data and applications based on their intended audience and access requirements.

4. Network segmentation: Implement network segmentation to isolate sensitive data and services in separate network zones, protected by firewalls, intrusion detection systems, and other security controls.
5. Access control: Use role-based access control (RBAC) to manage user access to sensitive data and services. Create roles with specific permissions and assign them to users or groups to ensure that only authorized users can access the segregated data.
6. Item-level access control: Set fine-grained access control on individual geospatial items, such as feature layers or map services, to control who can view, edit, or manage the data.
7. Secure GIS services: Secure your GIS services using various security mechanisms, such as token-based authentication or federated identity providers, to ensure that only authorized users and applications can access the data.
8. Data encryption: Encrypt sensitive data at rest and in transit, and store encryption keys separately from the encrypted data to further protect against unauthorized access.

Advanced: **Consider** Server Object Interceptors for Unique Requirements

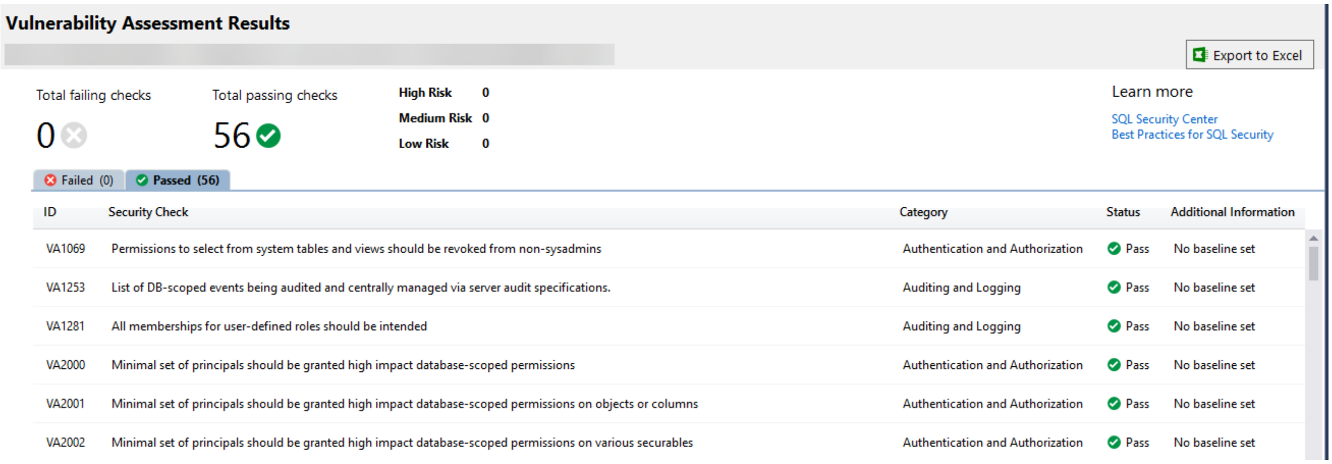
Esri highly recommends using standard security systems and practices before creating custom security mechanisms. ArcGIS Enterprise server object interceptors (SOI's) should only be considered if all other avenues to address your security concerns have been validated as deficient and must be addressed through custom mechanisms. Custom security mechanisms can easily become a source of security compromise in your organization; therefore, incorporating custom SOI's to address a security concern should only be considered if your organization has extensive resources available including threat modeling experts, static code analysis tools, and a rigorous maintenance and update program for the code. SOIs require knowledge of web development, ArcGIS developer tools, and programming languages.

SOIs can add new business logic or behavior on top of the existing ArcGIS Server operations in a way that is transparent to existing client applications. You can develop SOIs to implement custom business logic, such as security or auditing requirements that are not met by the default map or image service as examples. SOI's should only be used as a last resort to address unusual security concerns and even then, it's probably better to start with an enhancement request from Esri before pursuing this path.

WARNING: Implementing an SOI to address a specific security concern can easily become a high security risk configuration if extensive resources are not incorporated into the initial design as well as ongoing updates.

Advanced: **Remove** PUBLIC Access to Enterprise Geodatabase

Organizations deploying critical infrastructure may need to address all (e.g., Low Risk) findings when using the Vulnerability assessment for SQL Server to apply the Best Practices for SQL Security.



Vulnerability Assessment Results

[redacted]

Total failing checks 0

Total passing checks 56

High Risk	0
Medium Risk	0
Low Risk	0

Learn more
SQL Security Center
Best Practices for SQL Security

ID	Security Check	Category	Status	Additional Information
VA1069	Permissions to select from system tables and views should be revoked from non-sysadmins	Authentication and Authorization	✓ Pass	No baseline set
VA1253	List of DB-scoped events being audited and centrally managed via server audit specifications.	Auditing and Logging	✓ Pass	No baseline set
VA1281	All memberships for user-defined roles should be intended	Auditing and Logging	✓ Pass	No baseline set
VA2000	Minimal set of principals should be granted high impact database-scoped permissions	Authentication and Authorization	✓ Pass	No baseline set
VA2001	Minimal set of principals should be granted high impact database-scoped permissions on objects or columns	Authentication and Authorization	✓ Pass	No baseline set
VA2002	Minimal set of principals should be granted high impact database-scoped permissions on various securables	Authentication and Authorization	✓ Pass	No baseline set

Figure 16—Vulnerability Assessment Results

In these cases, revoking PUBLIC access to the enterprise geodatabase becomes a common requirement. Before taking this hardening step, consider the following caveats:

1. Esri has validated that *runtime operations* of ArcGIS Enterprise are *not impacted* by this hardening step provided the service account associated with ArcGIS Enterprise has the minimum necessary privileges required (see *https://enterprise.arcgis.com/en/server/latest/manage-data/windows/database-privileges.htm).*
2. Esri has found that *major maintenance operations* such as upgrades of the enterprise geodatabase are *impacted* by this hardening step. See the workaround described below:

During the maintenance window under which the enterprise geodatabase is planned for an upgrade, restore PUBLIC access to all objects within the enterprise geodatabase. Upon completing the upgrade, revoke PUBLIC access to all objects within the enterprise geodatabase. For additional details please discuss this further with our support team.

Advanced: **Disable** Mixed Mode SQL Server Authentication

Organizations with advanced security requirements should disable Mixed Mode/SQL Server Authentication on their database instance, supporting Windows authentication only for a significantly more secure implementation. Refer to https://docs.microsoft.com/en-us/sql/relational-databases/security/choose-an-authentication-mode?view=sql-server-ver15 for more details on SQL Server Authentication modes and Microsoft's recommendations.

Advanced: Migrate ArcGIS Data Store Object Store to cloud object storage service

Beginning with ArcGIS Enterprise 11.4, organizations running ArcGIS Enterprise in the Amazon Web Services (AWS) or Microsoft Azure cloud can use a cloud object storage service in place of the ArcGIS Data Store object store.

The following diagram represents these two options:

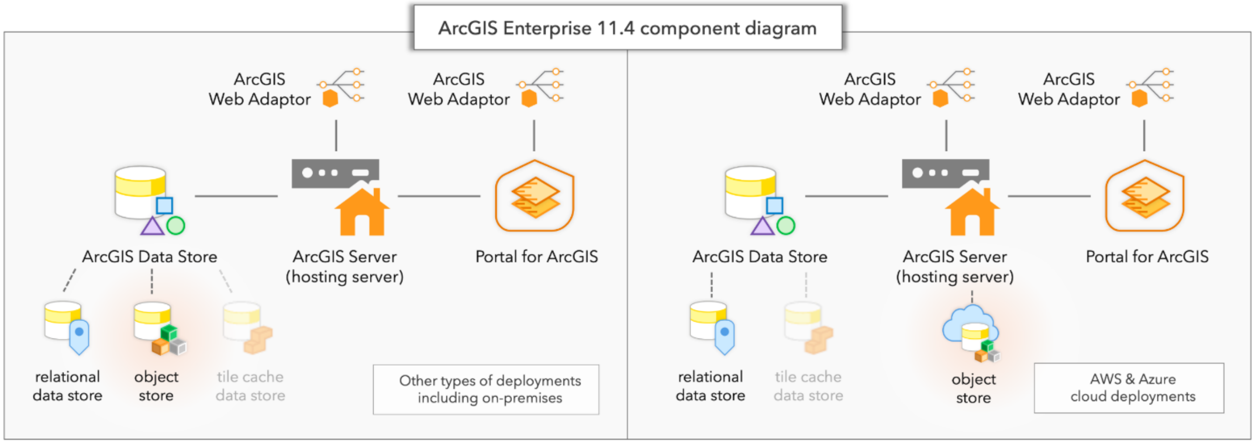


Figure 17—Object Store deployment options.

The ArcGIS Enterprise portal's hosting server only supports having one object store registered. It can be provided by the ArcGIS Data Store object store or a cloud object storage service.

Cloud services are optimized for performance, scalability, resiliency, and reliability and security across multiple regions. In ArcGIS Enterprise 11.4, two cloud object storage services are supported: Amazon S3 and Azure Blob Storage. Organizations running ArcGIS Enterprise 11.4 on AWS or Azure can register a cloud object store with their hosting server, as an alternative to the ArcGIS Data Store object store. This option serves the same purpose but leverages a cloud service instead of local disk storage.

Cloud object storage services deliver superior scalability, cost efficiency, high availability, and robust security features, making them a smart choice for data storage. ArcGIS Enterprise is cloud native. Take advantage of cloud data stores whenever possible. If cloud native data stores are not feasible for your use case, review the help documentation for the ArcGIS Enterprise provided ArcGIS Data Store object store.

Inventory and Maintenance

The goal of system inventory and maintenance is to protect the integrity of critical software platforms in the face of new vulnerability disclosures and exploits. With respect to ArcGIS Enterprise, this means customers must do the following:

- Identify and maintain an inventory for ArcGIS Enterprise systems[1] and integrations.
- Utilize General Availability (GA)-supported product versions.
- Implement patch management and verification.
- Ensure strong configuration management and regular validation.

Inventory Software

Establish and maintain a software inventory for all platforms running critical software and ALL software deployed to each platform.

Basic: **Implement** Software Inventory

Creating an inventory can lead to the discovery of systems or applications that are outdated, vulnerable, unnecessary, or unknown entirely. It also allows administrators and relevant outside groups to know the overall solution's composition at a glance; routinely updating the inventory is necessary to preserve its usefulness and discover changes to the platform that result in the problems mentioned above.

What Does the Inventory Look Like?

The component inventory is a descriptive record of the components within an organization. The components include Esri products as well as any external systems or services with which they interact. The inventory can take different forms, contain different amounts of detail, and have varying levels of granularity, depending on your level of hardening. Each component is associated with only one system and system owner; every item in the component inventory falls within the authorization boundary of a single system. Whenever inventorying Esri products, components should be listed at the level of granularity so that each can be updated by the end user.

Baseline inventories may be in human or machine-oriented formats, such as a spreadsheet or .csv/.json/.spdx files respectively. The choice of format should be based on whether the inventory will be created, updated, and/or reviewed manually or in an automated fashion, as well as how complicated the system is overall. For example, an organization running a single ArcGIS Enterprise instance in Kubernetes on a cloud platform will have a much simpler inventory to create, maintain, and review than an organization running multiple ArcGIS instances with no containerization on in-house infrastructure; the latter example will likely necessitate an automated approach regardless of other factors. The inventory should be updated at least monthly.

[1] Items specific to non-Windows installations will be covered separately.

The level of detail in a baseline inventory should at least include a component's name, version, location, and anything else that may be required to identify the component in a manual or automated review. The level of granularity for components should be at least to the level where each component listed can be updated by the organization's administrators if a newer version is available that works with the rest of the system.

Establishing the inventory can be broken down into three general phases, with some number of steps in each:

Research and Prototyping

Similar to developing a product, the inventory will begin its life as a prototype. This prototype inventory could draw on existing knowledge and materials surrounding system and software requirements for the relevant infrastructure, as well as research into the infrastructure's current state to discover previously unknown items. This research may take the form of a manual examination of systems and components or using tools/applications to collect this information in a more streamlined fashion. The goal for this initial prototype is to capture the current state of existing infrastructure as well as what is expected for any new infrastructure that will be part of this inventory.

Refinement

Once the inventory has been prototyped, the process of moving the inventory into its final state is a cycle of finding and removing superfluous components, updating existing components or possibly replacing problematic components without clear or realistic remedial options, and testing the new iteration of the inventory to ensure the relevant infrastructure can still function. This will likely require creating a sandbox/testing environment to avoid direct experimentation on production infrastructure.

Deploy and Enforce

Now that the inventory has been created, tested to ensure that operational performance is maintained, and minimized to reduce complexity and ongoing maintenance burdens, a method to deploy and enforce the inventory across all relevant pieces of infrastructure should be created and used. Some or all elements of this method may have been devised already as part of the earlier phases.

To limit which components can be installed on a system, the system's permissions framework will likely need to be utilized to control who can modify the components on the system. On Windows, Group Policies can be a useful tool for accomplishing this; other options may also be considered depending on the needs and setup of an organization.

To help ensure that packages installed on a system are trustworthy, package management systems can be used to control and centralize where installable components originate. While UNIX-like systems have long had native package management tools, Microsoft recently launched one for Windows as well. All these operating systems can also make use of non-native package managers with availability depending on the specific system. These systems can be configured to pull packages from specified locations that are trusted by the organization.

Basic: **Manage** Only General Availability Product Versions

As cyberattacks continue to increase, the importance of regularly updating products to stay with current released versions falling under a classification called General Availability support has increased. Each new release of products not only updates underlying frameworks but also provides new security capabilities, as can be seen in the Appendix G: Security Features by Release section of this document.

Esri's Product Life Cycle Support Policy outlines support phases that have been summarized below from a security risk perspective.

- **Latest Release**—ArcGIS Enterprise typically has two releases per year. Ideally, organizations should schedule resources to update to these new versions within months of their release.
- **General Availability**—Production enterprise systems exposed to the internet should *only* utilize general availability release versions.
- **Extended—**Only utilize on an exception basis, and additional mitigations should be considered to offset the significant additional risk this version presents to operations.
- **Mature—**No production enterprise systems should utilize mature product versions. This is a high-risk configuration with likely publicly documented vulnerabilities that could be exploited.
- **Retired—**No systems should use these versions and present a critical risk to customer operations.
- **Deprecation—**If a deprecation announcement is made for a product or capability, customers should immediately implement a plan to ensure they are shifting away from the product or capability as typically there will be no further patches to address security issues. ArcMap™ software is an example of a deprecated product and as such fails to meet even the Basic security profile requirements. Any customer with ArcMap and any security requirements should immediately transition to ArcGIS Pro (it's replacement).

We understand that there are a variety of historical reasons customers may have for not staying with GA releases, some of which Esri has addressed and others may require a joint effort:

- **Update difficulty**—Esri has taken significant steps to ease the update process for ArcGIS Enterprise, reducing the time to update, and increasing reliability over the last several years.
- **Interdependent products**—If your challenge with regular updates to GA versions is with a partner or other interdependent products taking too long to provide compatible versions, please escalate this issue with the corresponding organization and re-evaluate other options.
- **Resource availability—**If adequate resources are not available to ensure at least the Basic security profile is maintained for production operations, then see the warning below.

WARNING: If your organization is regularly unable to keep your production systems updated with GA release product versions (resulting in a high-risk configuration), different deployment/management strategies should be highly considered to reduce risk as soon as possible:

- Utilize Managed Cloud Service offerings of ArcGIS Enterprise.
- Utilize software as a service, such as ArcGIS Online.
- Engage professional services resources to facilitate streamlined update processes.

Patch Management

Use patch management practices to maintain all software deployed in your ArcGIS Enterprise deployment.

Esri regularly releases patches, updates, and new versions to address security vulnerabilities, fix bugs, and introduce new features. It's crucial for administrators to keep ArcGIS Enterprise up-to-date to maintain a secure and stable environment. Regularly apply security patches and updates to the software to ensure that known vulnerabilities are addressed in a timely manner. This will help prevent attackers from exploiting known vulnerabilities to gain unauthorized access to the system.

Some best practices for security patch management in ArcGIS Enterprise include the following:

1. Monitor Esri's security advisories: Stay informed about the latest security vulnerabilities, patches, and updates by regularly checking Esri's ArcGIS Trust Center (Trust.ArcGIS.com). Subscribe to the RSS feed to be made aware of new security advisories and patches.
2. Test patches and updates: Before applying patches or updates to your production environment, test them in a staging or test environment that mirrors your production setup. This helps identify any potential issues or conflicts that may arise and allows you to address them before they impact your production environment.
3. Backup before updating: Before applying patches or updates, create backups of your data and configuration settings. This ensures that you can recover your system in case of any issues during the update process.
4. Document the patch management process: Maintain clear documentation of your organization's patch management process, including the steps to apply patches and updates, the testing process, and any known issues or conflicts.
5. Monitor system performance: After applying patches or updates, monitor your system's performance to ensure that there are no unexpected issues or performance impacts. If issues are identified, work to resolve them promptly.

Basic: Manage Vulnerable Components with Patching

It is likely that this inventorial process will reveal systems or components that are outdated; ensure that these outdated components are addressed. It is also possible that the inventory will reveal components with known issues. Upon discovery of a vulnerable component, each vulnerability must be triaged and a resolution path outlined by asking the following questions:

1. Can the vulnerability be remediated through a patch or software change? If so, this is the ideal path to resolution.
2. If no patch is available, can the vulnerability be mitigated through security control? Mitigation is the process of applying a security control that prevents a vulnerable component from being exploited.
3. Is neither remediation nor mitigation available? The organization must evaluate and determine whether to accept the risk of the component.

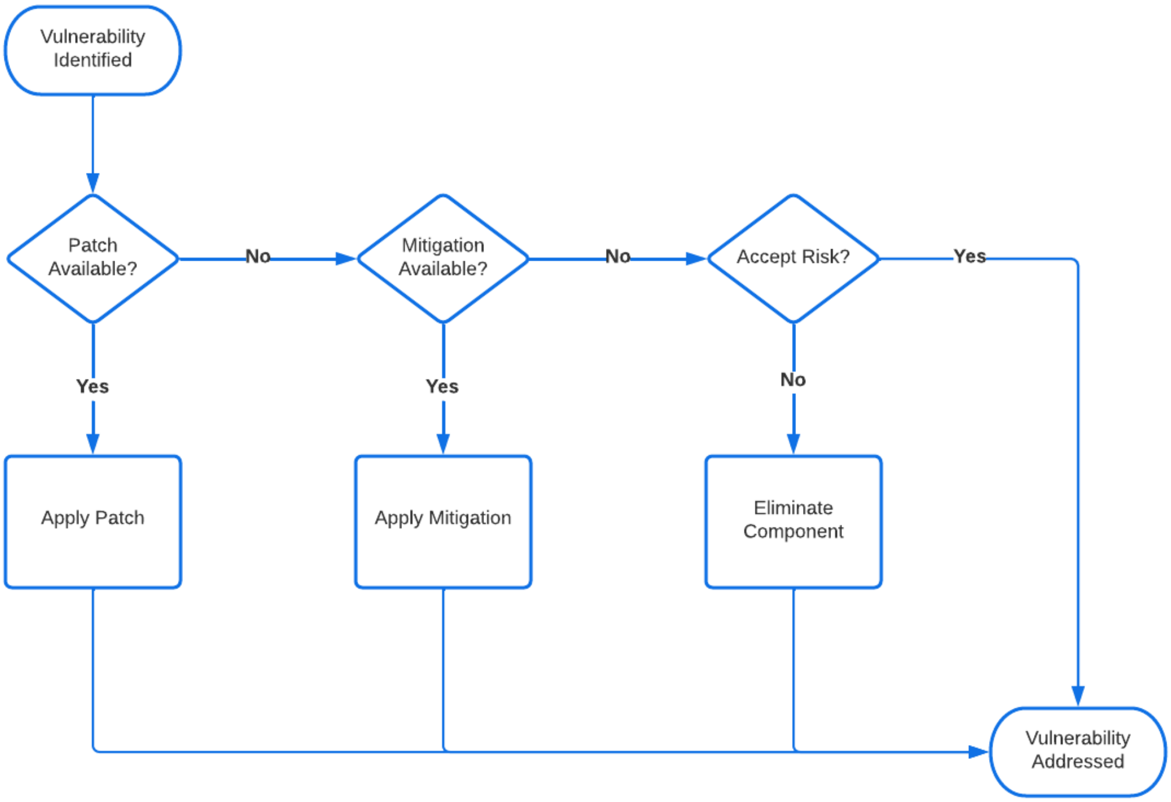


Figure 18—Sample Vulnerability Resolution Workflow

These components will need to be mitigated in some way to address these issues, particularly if they are related to security or privacy. If no remedial solution can be found, then the component may need to be replaced with a suitable alternative.

Basic: **Configure** Vendor Patch Notification Subscription

Esri provides patch notifications through a variety of feeds. Trust Center RSS feed is useful for security resources who what instant awareness of Esri's answers for media hyped industry-wide security issues as well as what security patches have been released for our products along with criticality. Subscribe to one or more of the notification feeds (see Table 8) to avoid missing a critical software update or security patch:

Table 8—Esri Patch Notification Sources

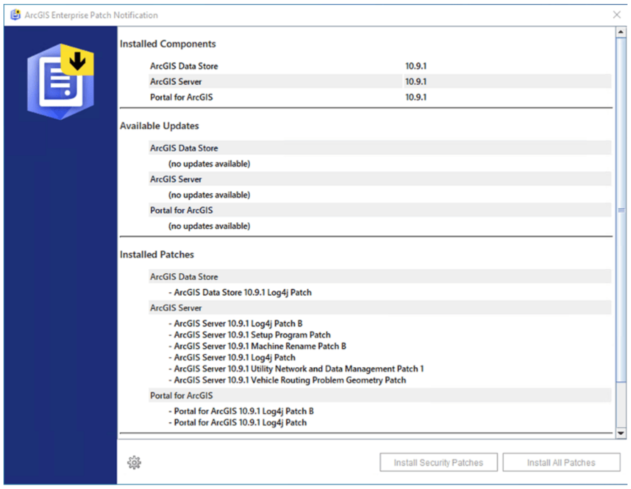
Website	Context	Subscription Link
ArcGIS Trust Center RSS	Security Patches & Alerts	esri.com/arcgis-blog/feed/atom/?post_type=blog&product=trust-arcgis
Esri Support Downloads	All Patches & Releases	support.esri.com/en/downloads
Esri Downloads	Machine-readable patch info	downloads.esri.com/patch_notification/patches.json

Basic: Implement Security Patches within One Month

Industry standards typically require high-severity vulnerabilities to be patched within 30 days of a patch release. Esri typically releases several security patches separately per year for each ArcGIS Enterprise component, so your organization should plan accordingly.

Esri provides a Temporal Common Vulnerability Scoring System (CVSS) score and qualitative rating, typically medium, high, or critical for security patches. This information is designed to help customers understand the severity of the vulnerability as well as the criticality of applying it to systems. By default, your organization should ensure that ArcGIS Enterprise security patches are deployed to your production systems within 30 days of release.

Once you receive an alert via your subscription that a new security patch is available, you should first deploy the patch to your nonproduction system for validation before patching your production environment. To ease obtaining the correct security patch for your system and validate that other patches are in place, we recommend utilizing the Patch Notification utility that is deployed during the installation of each component of ArcGIS Enterprise on Windows and Linux. If you have a highly available ArcGIS Enterprise environment, please follow the specific workflow listed in the documentation.



Installed Components

ArcGIS Data Store	10.9.1
ArcGIS Server	10.9.1
Portal for ArcGIS	10.9.1

Available Updates

ArcGIS Data Store
(no updates available)
ArcGIS Server
(no updates available)
Portal for ArcGIS
(no updates available)

Installed Patches

ArcGIS Data Store
- ArcGIS Data Store 10.9.1 Log4j Patch

ArcGIS Server
- ArcGIS Server 10.9.1 Log4j Patch B
- ArcGIS Server 10.9.1 Setup Program Patch
- ArcGIS Server 10.9.1 Machine Rename Patch B
- ArcGIS Server 10.9.1 Log4j Patch
- ArcGIS Server 10.9.1 Utility Network and Data Management Patch 1
- ArcGIS Server 10.9.1 Vehicle Routing Problem Geometry Patch

Portal for ArcGIS
- Portal for ArcGIS 10.9.1 Log4j Patch B
- Portal for ArcGIS 10.9.1 Log4j Patch

Figure 19—ArcGIS Enterprise Patch Notification Utility

Note: Most ArcGIS Enterprise security patches are cumulative, so they address older as well as current security fixes for your product version. Noncumulative security patches happen periodically (maybe every other year if that) and are noted as noncumulative in the patch documentation and are typically for more urgent concerns or targeted capabilities.

WARNING: All Esri product versions in mature status do not receive patches and therefore should *never* be used for production operations.

Configuration Management

Use configuration management practices to maintain critical software platforms and all software deployed to those platforms.

Basic: Manage Configuration Drift

Esri provides tools to assist with identifying security best practice items, configuration drift issues, or potential oversharing of content. Use these tools at least monthly to validate the current state of your ArcGIS Enterprise site and correct issues accordingly.

ArcGIS Security and Privacy Adviser

The ArcGIS Security and Privacy Adviser is a freely available application provided by the Esri Software Security & Privacy Team. It checks if your ArcGIS Enterprise is configured in alignment with a number of the recommendations in this document providing you with an easy-to-understand red, yellow, and green dashboards. In addition to best practice alignment checks, it allows you to see user actions over time and changes to your Portal for ArcGIS security settings, and it will continue to expand coverage over time.

We have recently introduced a new beta version of the tool, which allows exporting the results via CSV, JSON, and PDF for ease of reporting over time. Until the beta version is ready for general availability, you may be more comfortable with the classic version. Both versions are available to you by simply browsing the ArcGIS Trust Center home page (Trust.ArcGIS.com) where you will see the Launch Security Adviser blue button at the top right of the page.

To log in to ArcGIS Enterprise, you first need to register ArcGIS Security & Privacy Adviser as an application in your Portal for ArcGIS. This will generate an AppID that can identify this app as an approved client of Portal for ArcGIS. To register this app, follow the instructions here, using Web Mapping as the Type of App and the URL of the current page https://goto.arcgis.com/security-privacy-adviser as the redirect URI.

Enterprise Security Validation Python Scripts

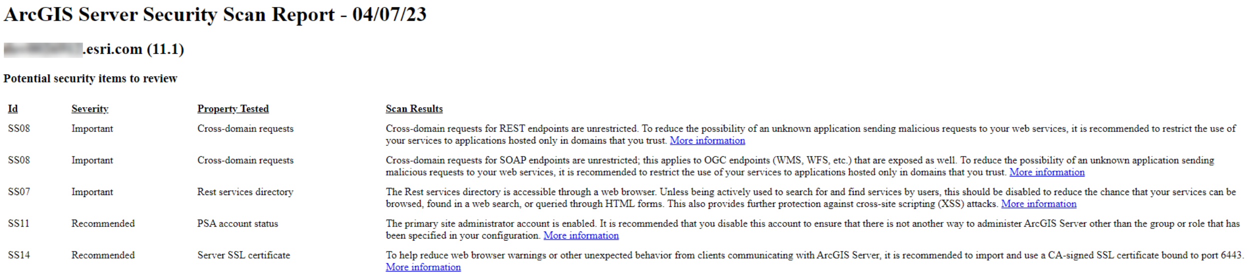
For more advanced users, both ArcGIS Server and Portal for ArcGIS have separate scripts that can be run against the corresponding systems to check for alignment with various best practices. For a person new to Python scripts, it may be tempting to use hard-coded credentials in scripts for regular validation.

WARNING: *Don't include hard-coded credentials in scripts.*
Hard-coded credentials create a significant security hole that allows an attacker to bypass the authentication that has been configured by the product administrator as the scripts require elevated permissions. This hole might be difficult for the system administrator to detect and may potentially lead to a compromise of ArcGIS Enterprise.

serverScan.py

ArcGIS Server comes with a Python script tool, serverScan.py, that scans for some common security issues. The tool checks for problems based on some of the best practices for configuring a secure environment for ArcGIS Server. It analyzes many criteria or configuration properties and divides them into three severity levels: Critical, Important, and Recommended.

The scan generates a report in HTML format that lists any best practices configuration items described in the serverScan.py documentation that may have been found in the specified ArcGIS Server site.



ArcGIS Server Security Scan Report - 04/07/23

[redacted].esri.com (11.1)

Potential security items to review

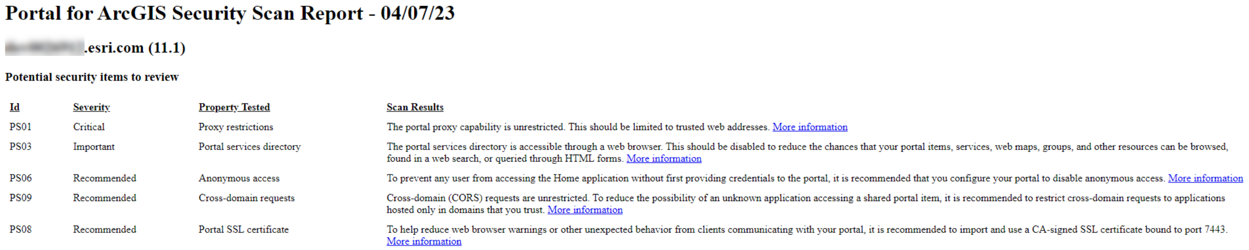
Id	Severity	Property Tested	Scan Results
SS08	Important	Cross-domain requests	Cross-domain requests for REST endpoints are unrestricted. To reduce the possibility of an unknown application sending malicious requests to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. More information
SS08	Important	Cross-domain requests	Cross-domain requests for SOAP endpoints are unrestricted; this applies to OGC endpoints (WMS, WFS, etc.) that are exposed as well. To reduce the possibility of an unknown application sending malicious requests 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
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
SS14	Recommended	Server SSL certificate	To help reduce web browser warnings or other unexpected behavior from clients communicating with ArcGIS Server, it is recommended to import and use a CA-signed SSL certificate bound to port 6443. More information

Figure 20-ServerScan.py Security Report

portalScan.py

Portal for ArcGIS comes with a Python script tool, portalScan.py, that scans for common security issues. The tool checks for problems based on some of the best practices for configuring a secure environment for your portal. It analyzes many criteria or configuration properties and divides them into three severity levels: Critical, Important, and Recommended.

The scan generates a report in HTML format that lists any best practices configuration items described in the portalScan.py documentation that may have been found in the specified Portal for ArcGIS instance.



Portal for ArcGIS Security Scan Report - 04/07/23

[redacted].esri.com (11.1)

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 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

Figure 21-PortalScan.py Security Report

Advanced: **Manage** Software Inventory through Automation

Advanced inventories and alert triggers for unexpected changes should be updated at least every five minutes. Accordingly, the entire process must be automated, and the reports must be in whatever format the automated monitoring program requires in addition to any formats required for compliance purposes such as Software Package Data Exchange (SPDX). Esri is actively working on creating Software Bill of Materials (SBOM's) for ArcGIS Enterprise and expects them to be available on demand to customers in 2024.

The level of detail in an advanced inventory should include any and all the information about a component that could help determine if it is outdated, misconfigured, unnecessary, or should otherwise be revised, along with information necessary for compliance with applicable regulations. The level of granularity for components should be to a level where Common Vulnerabilities and Exposures (CVE's) or other notations of vulnerabilities/defects can be assigned to them individually. The purpose of this is to create awareness of the vulnerabilities present at the surface level of components as well as vulnerabilities in any deeper components that are utilized by top-level components (referred to hereafter as dependencies). Even if a top-level component has no known vulnerabilities, the vulnerabilities of a dependency can be a concern if the top-level component utilizes problematic portions of the dependency. This means that an advanced software inventory will likely reveal vulnerabilities that an end user can only address by updating the top-level component, asking the component vendor to update their dependencies, avoiding the use of component functions that utilize vulnerable pieces of code (including in dependencies), or replacing the component entirely. It is not generally recommended for an end user to update the dependencies of components themselves, and any such exercise should only be done after a thorough investigation of the consequences and the other options already listed.

Advanced: **Remove** Superfluous Components

All components and systems within the affected infrastructure will need to be inventoried, analyzed, maintained, and accounted for on a regular basis. Issues of substantive concern for a component/system may need to be mitigated manually until a vendor solution is released to avoid potential exploitation and compromise of the infrastructure. In the case of components that are present on the relevant infrastructure but unnecessary to its function, this perpetual burden can be avoided by simply removing them. This also acts as a preventive measure against future threats by reducing the overall attack surface of your infrastructure where malicious actors could discover weaknesses.

A simple example would be as follows: If an organization is running ArcGIS Enterprise Server on an instance of Windows, what other inventoried applications, tools, components, etc. are not necessary for the server or Windows itself to run? Each item that can be removed simplifies the inventory, lowers the perpetual burden described earlier, and reduces possible future avenues of attack for malicious actors.

Advanced: **Implement** Separation of Monolithic Systems

While the infrastructure being hardened likely performs multiple functions to accomplish its overall purpose, the components that are not directly dependent on each other, and therefore do not need to be on the same system, should be put onto separate systems and communicate using remote API's, client-server setups, or some other interface that facilitates cross-system communication. Doing this is essentially an exercise in removing components that are superfluous *from the perspective of an individual component*.

Returning to the simple example from earlier, if an organization utilizes an email server to send mail based on events occurring within its ArcGIS Enterprise server, does that mean that the two components need to share the same Windows instance? From the perspective of the ArcGIS server, all that is necessary is a component that it can utilize to send mail to a server located locally or otherwise. From the perspective of the email server, the ArcGIS server doesn't need to exist at all. By moving each server to a separate Windows instance, unnecessary components are removed from the perspective of each individual component, and each instance of Windows can now be stripped down to only resources necessary for the component on that system as well as Windows itself to run.

Breaking up monolithic systems allows for the establishment of multiple smaller/simpler systems. This reduces the maintenance burden/downtime and attack surface of individual systems, improves overall infrastructure resilience, and creates an inner layer of defense against infrastructure compromise as organizations take steps to control and regulate intersystem communication. It can also reduce the conceptual complexity of evaluating individual systems for security and privacy issues.

Detection and Response

This section provides ArcGIS Enterprise administrators and managers with guidance for quickly detecting, responding to, and recovering from threats and incidents that impact confidentiality, data integrity, and system availability offered by ArcGIS Enterprise. The guidance below covers:

- Detection & Monitoring Logs
- Incident Response

Detection and Monitoring Logs

Frequent review of ArcGIS Enterprise logs is critical in the practice of continuous monitoring and incident response. Use the guidance provided in the tables below to configure ArcGIS Enterprise and supporting systems to meet the product security baseline.

Logging involves recording events of interest from a system. Auditing is the practice of inspecting those logs to ensure your system is functioning desirably or to answer a specific question about a particular transaction that occurred.

- Log events of interest such as who is publishing services.
- Ensure logging is used across the system at the application, operating system, and network layers.
- Ensure logs are reviewed at an organization-defined interval for potential privacy risks.
- Collect application server logs from Portal for ArcGIS, ArcGIS Data Store, and ArcGIS Server.
- Collect web server access logs from any intermediate tiers including API gateways, load balancers, WAFs, web servers, and web adaptors.
- The use of SIEM is beneficial to aid in automatic correlation.

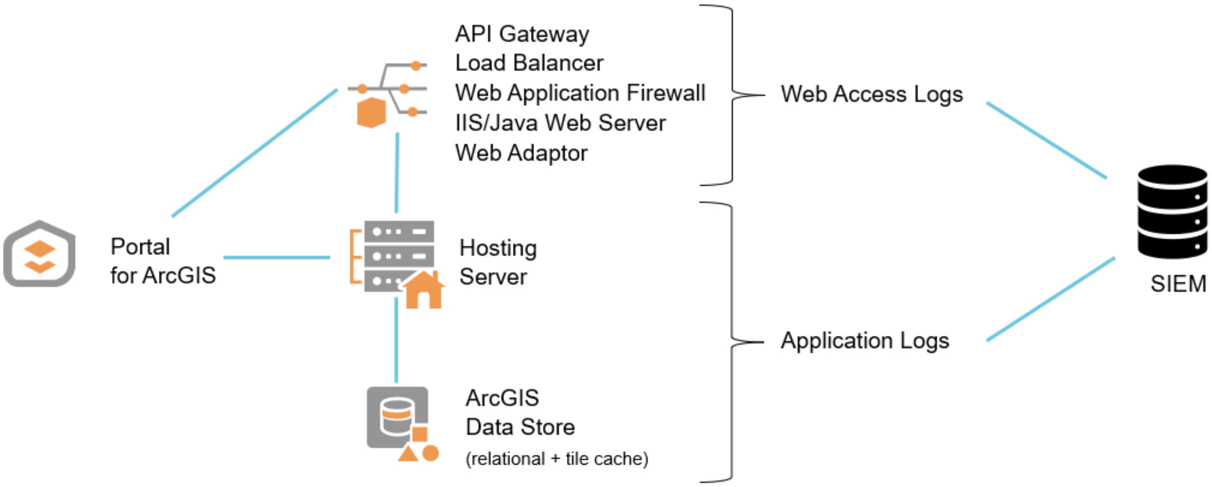


Figure 22—Utilizing a SIEM to Facilitate Correlation Across Logs

Basic: **Implement** Security Information and Event Management

SIEM technology supports threat detection, compliance, and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.

Core capabilities of a SIEM include log and event collection, correlation analysis, and monitoring across disparate sources. SIEM solutions are typically integrated with operational capabilities such as incident management, dashboards, and reporting.[2]

A SIEM enables teams to rapidly obtain a clear threat picture supported by analytics by filtering potentially massive amounts of security data and prioritizing the security alerts the software generates. SIEM software enables organizations to detect incidents that may otherwise go undetected.[3]

Common log management systems include Azure Monitor, Splunk, and Elastic Logstash. The Splunk Universal Forwarder and Microsoft Sentinel have been verified as capable of consuming ArcGIS Enterprise logs. Refer to our documentation for more information concerning working with ArcGIS Enterprise logs.

See Appendix E: SIEM Log Shipping Guidance for example implementation details.

Basic: **Implement** Endpoint Detection and Response

Anti-virus tools are no longer adequate to address today's security demands, instead Endpoint Detection and Response (EDR) tools should be deployed widely across systems. Such tools allow proactive detection of cybersecurity incidents as well as "hunt" capabilities during incident response. Issues detected with such tools are fed to the SIEM for prioritization and awareness. Depending on how the EDR operates, your organization may want to consider implementing scan exclusions similar to what is available for Anti-virus tools and ArcGIS products, available within the ArcGIS Trust Center.

Note: Anti-Virus (AV) tool aggregators like VirusTotal are good general heuristic tools. However, the engines these aggregators ingest cannot usually distinguish between operating systems or OS specific code and may produce false positives as a result. It is not uncommon for some AV tools designed for Windows to falsely identify Linux code as infected, or for AV tools designed for Linux to falsely identify Windows code as infected. It is recommended to use an EDR or AV tool designed to validate software running on the operating system you've installed ArcGIS Enterprise on, or at least consider the threat margins (the number of AV Tools identifying a threat) and filter the results to reflect your environment. Remember that "generic" labels like gen", "susgen", "W32.Trojan.Gen", or detections labeled "malicious" are not known malware detections – the generic label means some code "looks" suspicious.

[2] Citation: https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

[3] Citation: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

If in doubt, we encourage security teams to contact AV tool providers to validate a suspected false positive.

Basic: **Manage** Webhooks

Webhooks define event criteria under which ArcGIS Enterprise will execute an outbound request to a service URL. These outbound HTTP requests represent a vector for regular (intentional) data exfiltration and should therefore be carefully monitored and managed. Verify if ArcGIS Enterprise has been configured to use webhooks by interrogating the API as shown below:

Request:

```
https://{portal}/{context}/sharing/rest/portals/0123456789ABCDEF/webhooks?f=json&token={access_token}
```

(Example)

```
https://server.domain.com/arcgis/sharing/rest/portals/0123456789ABCDEF/webhooks?f=json&token=j123kj1...9u1jk..
```

Response:

```
{"webhooks":[]}
```

An empty JSON response as shown above reveals no webhooks are configured. If any other value is returned, inspect the URL of the service and event criteria under which the webhook is configured and ensure the target is expected, trusted, and secured to the same standard as ArcGIS Enterprise. For more details on managing webhooks with ArcGIS Enterprise, refer to Webhooks in ArcGIS Enterprise—Portal for ArcGIS | Documentation.

Basic: **Implement** Vulnerability Scanning Tools

Automated vulnerability scanning tooling can provide insight into vulnerabilities in software products. However, software scanning tools that only compare CVE IDs against third-party components often raise false positives due to lack of context. Automated security scanning tools that only compare a third-party component's self-described version number against a table of CVEs (vulnerabilities) typically create needless noise whose results must be manually reviewed and validated by a qualified security professional to provide actionable value.

Esri's automated vulnerability scanning guidance (requires Esri login) provides step-by-step instructions for preparing for and validating the results of scans to create a well-formatted document describing exploitable findings generated by automated tooling. Esri encourages submitting the document to Esri's product security incident response team (PSIRT) using the Report a Security or Privacy Concern form available on Trust.ArcGIS.com. If a well-formatted report that provides a proof of concept of a demonstrable exploit relative to Esri software is responsibly submitted to Esri's PSIRT, Esri will, after due diligence and evaluation, provide an update or patch to address it.

Advanced: **Consider** ArcGIS Monitor

Organizations with critical infrastructure requirements should consider deploying ArcGIS Monitor. ArcGIS Monitor is designed to help analyze and optimize the health of ArcGIS Enterprise by providing timely and insightful system metrics on the status, availability, usage, system performance, and resource usage of your enterprise GIS. Alerts and analysis tools provide system administrators with real-time notifications to facilitate rapid resolution when measurements are outside defined system thresholds. Reports with statistics can be used to visualize historical data and enhance communications among GIS, IT, business owners, and senior management.

ArcGIS Monitor utilizes proprietary, noninvasive methods of monitoring enterprise GIS and IT infrastructure including databases, networks, and GIS software. This includes the detection of existing system infrastructure and operational problems to facilitate rapid resolution. It also provides actionable reports and quantifiable metrics to improve communications among GIS and IT staff, business owners, and senior management.

WARNING: ArcGIS Monitor falls under the definition of Critical Software due to it having direct or privileged access to networking or computing resources across an ArcGIS Enterprise deployment. This means that federal customers utilizing ArcGIS Monitor must be able to demonstrate compliance with the Security Measures for Critical Software; however, nonfederal organizations should also highly consider alignment with the specified security measures to minimize operational risk.

Because Esri has announced that there is “no active development as it uses legacy technology” *and* it is no longer covered by GA support, customers should no longer utilize ArcGIS Monitor 10.8.1 as part of production operations, and if currently in use, should immediately migrate to the current ArcGIS Monitor 2024 release.

Alerts

When a system is functioning less than optimally, there may be multiple alerts in the dashboard for review. For analysis, ArcGIS Monitor divides the alerts into three categories: critical, warning, and info.

Ensuring that all critical alerts are addressed should be a priority for all administrators as they impact your enterprise GIS's availability. Warning alerts show that your resources are running low—memory, disk, CPU, or network bandwidth. Info alerts show informational logs to the administrator.

Several options are available to investigate errors—you can view the time each error occurs, search log entries for the time indicated, or click on the reported log errors links and admin URLs to check site details.

Root Cause Analysis

While the *when* is important, the *how* is equally if not more important to understand the root cause of a problem. For example, if ArcGIS Data Store experiences an outage, the outage impacts all the tiers above it. The source, in this case ArcGIS Data Store, causes a chain reaction that impacts ArcGIS Server and Portal for ArcGIS sites.

System overload is a common cause of outages. If the system exceeds its intended capacity, the result is excessive resource utilization, low free memory, or zero idle disk. This lowers the performance of the machine and cause time outs and may impact the overall stability of the enterprise implementation.

Other common issues are system bottlenecks. These impact performance and stability. Bottlenecks manifest during increased user load such as the above example.

Lastly, unstable infrastructure can manifest in issues for the deployment. Some examples of processes and workflows that can impact system stability are restarting services, changing permissions, expired or expiring passwords, or virtualization overallocation. Examples may include unexpected processes consuming memory, CPU usage spikes, stopped ArcGIS Server services, reboot conditions, and databases not running.

ArcGIS Monitor provides an accurate reporting mechanism that administrators can use to better manage their deployments. Monitor can show you where the issues are occurring through quantifiable key performance indicators and metrics.

Incident Response

The flow of detected potential information security incidents must be triaged and each one qualified as an information security incident (true positive) or as a false alarm (false positive) using manual and/or automated analysis. This may require manual or automated gathering of additional information, depending on the detection use case. Priority should be given to the analysis of potentially more critical information security incidents to ensure a timely reaction to what is most important. Structured qualification of detected potential information security incidents enables effective continuous improvement in a directed way by identifying detection use cases, data sources, or processes with quality issues.

Basic: Implement CSIRT Process

A CSIRT (Computer Security Incident Response Team) is a team or process, either dedicated or ad hoc, that should be formed to manage computer-related threats. The mission of a CSIRT is to help the organization prevent, identify, document, and respond to security incidents like breaches, viruses, and other potentially catastrophic incidents in enterprises that face significant security risks. A CSIRT is composed of organization employees and other technical subject matter experts who can quickly respond to and guide executives on appropriate messaging during and after the incident response process.

CSIRT processes include the following:

- **Isolate compromised systems:** The CSIRT or process must be capable of isolating systems suspected of being compromised.
- **Preserve evidence:** To prevent the destruction of evidence and maximize the chances of identifying the attacker, no interaction with the machine will occur until the incident handling team is in place.

- **Set up an incident handling team:** The CSIRT contact and the reporting system administrator will set up an incident handling team composed of system SMEs. Under the guidance of the CSIRT contact, the team will perform the following:
    1. Investigate the extent and type of occurrence and determine, possibly with disk imaging and analysis, if it is a security incident. If it is, the team will contact law enforcement and other stakeholders as required.
    2. Work with the system administrator and law enforcement to collect proper evidence, in keeping with the organization's security and privacy policies and determine the impact of the incident.
    3. Generate official reports for stakeholders and management. The report will outline the type and extent of the incident and list actions required and recommended to mitigate future incidents.
- **Clean up and Restoration:** Unless additional evidence is required, sanitize and bring the system back online.
- **Postmortem Documentation:** The CSIRT and incident handling teams evaluate the response and notification process and incorporate changes to address weaknesses.

For additional details and guidance regarding CSIRT concepts, see FIRST CSIRT Services Framework.

Training Guidance

The goal of training is to strengthen the understanding and performance role-based actions that foster the security of software platforms. Key roles that exist in ArcGIS Enterprise are GIS Administrator, System Administrator, Publisher, GIS User, Data Editor, and Viewer. Each role has an impact on organizational security and should be considered based on deployment.

Training is essential in preparing new users within your workforce and keeping current users up-to-date on organizational security requirements and threats. This section is a high-level overview for organizations to consider adopting in the use of ArcGIS Enterprise in a role-based approach. Recommendations of frequent and ongoing training to adopt into your existing organizational training are also included.

Common Roles

GIS Administrator: Full administrative access to the ArcGIS Enterprise deployment including, but not limited to, setting up enterprise logins, viewing the location tracks of other users, changing member roles to or from an administrator, and much more. An organization must have at least one administrator, but two are recommended and should be limited to only those who require the additional privileges associated with this role. This role has significant security implications for the organizational data and requires detailed training to ensure the individual understands these risks and implications.

System Administrator: For a Basic profile deployment, it is not unusual for the GIS Administrator to be the same resource as the System Administrator. However, when an organization wants to take on the Advanced profile, it will need to ensure that separate, dedicated resources are available. A System Administrator's focus is not on the mastery of the application security control but more on the supporting infrastructure components.

Database Administrator: If your organization utilizes an enterprise geodatabase which is created and maintained outside of ArcGIS Enterprise a database administrator is strongly recommended. Most database maintenance tasks are done outside of ArcGIS with except for tools such as the Create Role, or Create Database User tools and functions. Geodatabase administrators do not require as many privileges as the database administrators and their privileges vary by database management system.

Publisher: GIS User privileges plus the ability to publish hosted web layers and ArcGIS Server layers, register data stores, publish from data store items, and perform feature and raster analyses. The Publisher role is compatible with the Creator, GIS Professional, and Insights Analyst (retired in February 2023) user types. This role has security implications for the organizational data and requires detailed training to ensure the individual understands these risks and implications.

GIS User: Data Editor role privileges plus the ability to view content shared by other ArcGIS users; use the organization's maps, apps, layers, and tools; and join groups that allow members to update all items in the group. Members who are assigned the User role can also create maps and apps, edit features, add items to Portal for ArcGIS, share content, and create groups. The User role is compatible with the Creator, GIS Professional, and Insights Analyst (retired in February 2023) user types. This role has some security implications for the organizational data and requires detailed training to ensure the individual understands these risks and implications.

Data Editor: Viewer role privileges plus the ability to edit features shared by other ArcGIS users. The Data Editor role is compatible with all user types except the Viewer role. This role has some security implications for the organizational data and requires detailed training to ensure the individual understands these risks and implications.

Viewer: Allows items to be viewed such as maps, apps, scenes, and layers that have been shared with the public, the organization, or a group to which the member belongs. Join groups owned by the organization. Members assigned the Viewer role cannot create or share content or perform analysis. The Viewer role is compatible with all user types. This role has minimal security implications for the organizational data and requires detailed training to ensure the individual understands these risks and implications.

Basic: **Implement** Role-based Training Plans

Build a training plan for each GIS role in your organization to develop appropriate expertise and security awareness. Suggest each team member complete the training offerings based on the organization job assignment and ArcGIS Enterprise role assignment. Take advantage of Esri's training resources (See Table 9) to improve workforce security awareness within your organization:

Table 9—Train Users by Role and Responsibility

Role	Learning Plan
All	Stopping Data Leakage
Administrator	ArcGIS Enterprise: Administration Workflows
Administrator	Content Management Techniques for Your ArcGIS Enterprise Portal
Publisher	Publishing Content and Services

Basic: **Manage** Ongoing Awareness Activities

Reinforce training for all roles (at least annually) and measure the training's effectiveness for continuous improvement purposes. Suggest each team member complete the training offerings based on the organization job assignment and ArcGIS Enterprise role assignment. Take advantage of Esri's training resources to improve workforce security awareness within your organization as recommended in Table 10 below.

Table 10—Conduct Frequent Awareness Activities

Role	Continuing Education
All roles	Subscribe to ArcGIS Trust Center announcements
	Attend Esri User Conferences
	Review latest ArcGIS Trust Center content

Privacy

The aspect of data privacy requires careful consideration when dealing with geospatial infrastructure, especially that which utilizes ArcGIS Enterprise technology. This ArcGIS Enterprise Hardening Guide provides key insights on critical approaches customers should adopt when protecting private information. A successful privacy assurance process requires strict adherence to established privacy protocols and ensuring adequate measures are in place to work toward minimizing risks associated with inadvertent disclosure or malicious breaches of sensitive data stored within your ArcGIS Data Store. By following the recommendations presented in this section, you will establish a trusted system both for yourself as well as external entities who have vested interests in protected data.

See Esri's ArcGIS Trust Center privacy pages for details on our privacy best practices and compliance.

Completing a Privacy Impact Assessment

A thorough understanding of Privacy Impact Assessment (PIA) fundamentals is paramount to implementing an effective information privacy program. PIAs provide vital insights into how customers can manage risks posed by personal data gathering, storage, and use. Complying with established PIA best practices ensures adherence to regulatory requirements while establishing robust strategies for shielding sensitive information from unauthorized access. This section is useful for customers who are sensitive to privacy considerations for ArcGIS Enterprise and to complete a PIA for their deployment.

Ensuring Alignment with Privacy and Data Protection Regulations

ArcGIS Enterprise provides features and tools that help customers maintain compliance with various privacy and data protection laws and regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other privacy regulations. While the platform itself does not guarantee compliance, it does enable customers to implement necessary security measures, processes, and practices to meet regulatory requirements. These measures and practices include access control, authentication, data encryption, and monitoring.

Ultimately, compliance with privacy and data protection laws and regulations is the responsibility of the customer. By leveraging ArcGIS Enterprise features and implementing privacy best practices, customers can create an environment that adheres to relevant laws and regulations.

Minimizing Personal Datasets

Data minimization is a critical aspect of our security and privacy strategies. We recommend that customers only collect and process the minimum amount of personal data necessary to accomplish their intended purposes. This includes regularly reviewing and deleting any personal data that is no longer required. By implementing data minimization practices, customers can reduce their risk of data breaches and protect the privacy of customers and employees. Key objectives for implementing data minimization practices are as follows:

- Identify the purpose: Before collecting any personal data, clearly identify the purpose for which the data is needed. This will help to ensure that only the necessary data is collected and processed.

- Limit the scope: Once the purpose is identified, limit the data collection's scope to only the information necessary to accomplish the intended purpose. For example, if you need to verify a user's identity, you may only need to collect the user's name and email address rather than their full address and phone number.
- Use privacy-enhancing technologies: Use privacy-enhancing technologies such as data masking, data encryption, and data pseudonymization to reduce the amount of personal data that is visible or accessible.
- Regularly review and delete data: Once the intended purpose has been achieved, delete the personal data unless it is required for legal or regulatory purposes. Regularly reviewing and deleting personal data that is no longer necessary can help reduce the risk of data breaches and unauthorized access.
- Train employees: Provide training to employees on data minimization practices, including how to identify the purpose of data collection, how to limit the scope of data collection, and how to delete personal data that is no longer necessary. This will help to ensure that data minimization practices are followed consistently across the organization.

Implementing a Data Retention and Destruction Schedule

As part of our commitment to providing secure software solutions, we recommend that our customers follow best practices for data retention and destruction to protect the privacy and security of their data. The following guidelines will help you establish effective data retention and destruction practices for your software implementation:

- Establish a data retention policy: Develop a policy that defines the types of data you will collect, the purposes for which it will be used, and how long it will be retained. Your policy should also specify how you will securely store and protect the data during the retention period.
- Determine retention periods: Determine how long each type of data should be retained based on its sensitivity, legal requirements, and business needs. Ensure that you are only retaining data necessary for the intended purposes and avoid retaining data longer than necessary.
- Securely store data: Ensure that you are securely storing data during the retention period. This includes using appropriate physical and technical security measures such as access controls, encryption, and regular backups.
- Securely destroy data: When data is no longer needed, it should be securely destroyed using industry-standard methods such as shredding, degaussing, or overwriting with random data. Ensure that all copies of the data are destroyed, including backups and archives.
- Document retention and destruction practices: Keep detailed records of your data retention and destruction practices, including the types of data collected, retention periods, and destruction methods used. These records can help demonstrate compliance with applicable laws and regulations.
- Manage third-party service providers: Ensure that any third-party service providers who handle or process data on your behalf follow appropriate data retention and destruction practices. Review and document their practices regularly to ensure they meet your standards.
- Regularly review and update practices: Regularly review and update your data retention and destruction practices to ensure they remain effective and compliant with applicable laws and regulations.

Access and Analyze Data Being Collected, Stored, and Processed

Understanding the types of data collected (e.g., personal information, sensitive information, user access, timestamps or location data) and the methods of data collection is essential to ensure compliance with applicable privacy regulations as well as help customers adhere to privacy principles such as minimization, purpose limitation, and transparency.

Data Collection and Processing

Evaluate what types of data are collected, processed, and stored within ArcGIS Enterprise. Assess how the data is collected (e.g., user inputs, third-party integrations) and ensure data collection complies with applicable privacy regulations. Key practices include the following:

- Conduct a data flow analysis: Map the data flow within the ArcGIS Enterprise system, identifying how data is collected, processed, stored, and shared among different components, such as Portal for ArcGIS, ArcGIS Server, and ArcGIS Data Store.
- Review the data model: Examine the data model of the ArcGIS Enterprise implementation, including the databases, layers, and feature services. Identify the types of data being collected, such as personal information, sensitive information, or location data.
- Analyze data collection methods: Investigate the methods through which data is collected in ArcGIS Enterprise. This may include user inputs, application-generated data, data imported from external sources, or data gathered through third-party integrations.

Data Access and Sharing

Data access and sharing are critical in ArcGIS Enterprise because they allow customers to manage and regulate the flow of information while protecting sensitive data. Adequate access controls and sharing configurations ensure that only authorized users may access and interact with specified resources, lowering the risk of data breaches and privacy violations. Proper data access and sharing management improves cooperation; ensures compliance with privacy standards; and develops confidence among users, stakeholders, and regulators.

Determine who has access to the data stored within ArcGIS Enterprise, including employees, contractors, and other users. Evaluate data sharing configurations, such as public sharing, organization-level sharing, and group-level sharing. Review access controls and permissions to ensure proper data access limitations are in place.

Risk Mitigation Measures

The following risk mitigation measures for ArcGIS Enterprise can help customers minimize privacy risks related to data collection, storage, sharing, and processing:

- Access controls: Implement role-based access controls (RBAC) to restrict user access to data and system components based on their roles and responsibilities.
- Authentication: Enforce strong authentication mechanisms such as MFA to ensure the identity of users accessing ArcGIS Enterprise.
- Secure communication: Use encryption protocols such as HTTPS via TLS 1.2 or later versions to secure communication between ArcGIS Enterprise components and client applications.

- Data encryption: Encrypt sensitive data at rest (e.g., using database encryption) and in transit (e.g., using SSL/TLS) to protect against unauthorized access and data breaches.
- Monitoring and logging: Enable auditing and monitoring features within ArcGIS Enterprise to track user activities, system events, and potential security incidents.
- Network security: Deploy firewalls, network segmentation, and intrusion detection/prevention systems (IDS/IPS) to protect ArcGIS Enterprise from external and internal threats.
- Regular security updates: Ensure that your ArcGIS Enterprise deployment is up-to-date with the latest security patches and updates released by Esri.

Third-Party Integrations

Evaluate any third-party integrations with ArcGIS Enterprise, such as extensions, widgets, or custom applications. Assess the privacy and security practices of these third parties and ensure that they comply with applicable privacy regulations.

Implement Cookie Management

Proper cookie management is an essential aspect of securing information. Cookies are small pieces of data that a website or application stores on a user's device to remember their preferences or login information. However, if not managed correctly, cookies can be used to track user activity and steal sensitive information. ArcGIS Enterprise utilizes cookies in various aspects of its operation and Esri incorporates best practices for cookies to ensure security, privacy, and compliance with applicable regulations. However, as your organization extends your ArcGIS Enterprise deployment with custom applications or solutions, you will want to ensure the following aspects are addressed.

Purpose of Cookies

ArcGIS Enterprise uses cookies primarily for authorization session management, user authentication, and maintaining user preferences. Cookies are essential for providing a seamless and secure user experience within the application. ArcGIS Enterprise does not provide third-party cookies that track or collect data based on your online behavior.

Secure Attribute

To protect the confidentiality of user data, ArcGIS Enterprise uses the secure attribute in authorization cookies, which are transmitted over HTTPS only. This prevents unauthorized interception or manipulation of cookie data.

HttpOnly Attribute

ArcGIS Enterprise sets the HttpOnly attribute on authorization cookies, which prevents client-side scripts (e.g., JavaScript) from accessing the cookies. This helps mitigate the risk of XSS attacks.

SameSite Attribute

ArcGIS Enterprise supports the SameSite attribute on cookies, which helps prevent cross-site request forgery (CSRF) attacks. By setting the SameSite attribute to Strict or Lax, you can control the behavior of cookies when cross-site requests are made.

Cookie Lifespan

Administrators can configure the lifespan of authorization tokens used in authorization cookies in ArcGIS Enterprise to balance security and user convenience. Shorter token lifespans can help minimize potential security risks, while longer lifespans can improve user experience by reducing the need for frequent reauthentication.

Privacy Compliance

Customers deploying ArcGIS Enterprise should be aware of applicable privacy regulations, such as the GDPR or CCPA, which may have specific requirements for cookie management, including obtaining user consent before setting cookies. Make sure to consult with your legal and compliance teams to ensure that your cookie management practices align with these regulations.

Recommended Privacy Settings

Advanced: **Disable** or Location Lock Clients with EUEI Analytics

The Esri User Experience Improvement (EUEI) program is not utilized within ArcGIS Enterprise as no user analytics are collected from this product. However, customers frequently utilize ArcGIS Online and/or ArcGIS Pro in combination with ArcGIS Enterprise, and both of these other offerings provide EUEI analytics. The primary goal of EUEI is to identify areas for improvement, enhance product functionality, and provide a better user experience.

Customers can opt out of analytics collection within ArcGIS Pro and/or ArcGIS Online; however, doing so may limit Esri's ability to improve its products based on your organization's usage patterns.

- Esri takes privacy and security seriously, and the data collected through EUEI is anonymized, aggregated, and stripped of any PII or sensitive data. Esri uses this data solely for the purpose of improving its products and services.

Many customers want Esri to improve the ArcGIS Pro capabilities they use most first, so they want to keep EUEI enabled but want to ensure that the information is locked to being stored in the United States or European Union. This can be accomplished by setting a Windows registry setting and specifying the location. Deploying this setting via a Windows group policy can ensure that all ArcGIS Pro systems have the setting enforced with the customer's preference.

Basic: **Consider** Data Anonymization

Data anonymization is the process of protecting private or sensitive information by erasing or encrypting identifiers that link an individual to stored data. In the context of ArcGIS Enterprise, this often pertains to geographic data and attributes that can be linked to specific individuals or entities. Before you can anonymize data, you need to understand what data you have. Identify which datasets contain PII or other sensitive information. Not all data needs the same level of anonymization. Decide on the level of anonymization based on the sensitivity of the data and its intended use. ArcGIS Enterprise processes various types of personal data. To manage privacy risks, users need to employ techniques like redaction, pseudonymization, de-identification, masking, hashing, and anonymization. These techniques modify personal data elements based on their identifiability:

- **Direct identifiers:** Unique identifiers like Social Security numbers, full names, or addresses
- **Indirect identifiers:** Data that, when combined, can identify an individual (e.g., ZIP code, birth date)
- **Anonymized data:** Data that can no longer be linked to any individual

Techniques

Geohashing

Geohashing is a method of encoding geographic coordinates (latitude and longitude) into a short string of characters. This method can be used to anonymize the exact location while still providing a general idea of the area.

For example: GPS coordinates are 47.6062° N, 122.3321° W, corresponds to Seattle, however, for a California citizen under CCPA regulations to not be considered precise geolocation, the location must be less precise then 1,850ft, which a geohash length of six or less provides. Different regions around the world have different precision requirements, so please refer to your applicable regulations for location precision requirements.

Field Masking

Field masking is a data protection technique used to obscure specific data fields to prevent the direct identification or exposure of sensitive information. By replacing or hiding certain parts of a data field, field masking ensures that the sensitive or personally identifiable portions of the data are not readily visible while still allowing the nonsensitive parts to be displayed or processed. This technique is commonly used in scenarios where partial data visibility is required. This can be done using the Field Calculator in ArcGIS. For example: Instead of John Doe, 1234 Elm Street, the map's pop-up might display John D., 123* Elm Street.

Deletion, Redaction, or Obfuscation

Direct identifiers are covered, eliminated, removed, or hidden. These techniques are difficult to accomplish well, particularly on unstructured data, and the use of unsophisticated techniques may enable easy re-identification.

Example:
Jane Doe—DOB 8/15/1970—Los Angeles
[redacted]—DOB 8/15/1970—Los Angeles

Pseudonymization

Information from which direct identifiers have been eliminated, transformed, or replaced by pseudonyms, but indirect identifiers remain intact. Reidentification may occur where there is a failure to secure the pseudonymization method or key used and/or when reverse engineering is successful. For example: Jane Doe—DOB 8/15/1970—Los Angeles → ID:TRXD 8/15/1970 Los Angeles

Deidentification

Direct and known indirect identifiers (perhaps contextually identified by a particular law or regulation such as that of the Health Insurance Portability and Accountability Act [HIPAA]) have been removed or mathematically manipulated to break the linkage to identities. For example: Jane Doe—DOB 8/15/1970—Los Angeles → Female 1970 Los Angeles

Anonymization

Direct and indirect identifiers are removed or manipulated together with mathematical and technical guarantees, often through aggregation, to prevent reidentification. Anonymization is intended to be irreversible. For example: Jane Doe—DOB 8/15/1970—Los Angeles → Female Adult LA

Security and Privacy Alignment

It should be recognized that security and privacy practices and requirements are interrelated and mutually reinforced. Security focuses on protecting systems, networks, and data from unauthorized access and malicious activity, while privacy is about ensuring that personal information is collected, used, stored, and shared in accordance with the rights, persons, and applicable regulations.

Both areas aim to protect sensitive information and maintain trust in the digital ecosystem. By implementing strong security measures such as encryption, access controls, and regular monitoring, organizations can prevent unauthorized access and data leakage, helping to ensure the privacy of personal information.

Table 11—Alignment of Security and Privacy Principles

Issue/Control	Description	Recommendations
Data Encryption	Data at rest and in transit should be encrypted to protect sensitive information and ensure privacy compliance.	Implement encryption for data at rest using ArcGIS Data Store and use SSL/TLS for securing data in transit.
Authentication and Authorization	Proper authentication and authorization mechanisms are crucial to ensure that only authorized users have access to sensitive data.	Configure and enforce strong authentication mechanisms, such as SAML, OAuth 2.0, or integrated Windows authentication. Set up appropriate user roles and permissions.
Access Logging and Monitoring	Monitoring user activities and logging access to sensitive data are essential to detect potential privacy breaches.	Enable and configure logging within ArcGIS Enterprise components. Implement monitoring and auditing tools for user activities.
Data Minimization	Collecting and processing the minimum amount of personal data necessary reduces privacy risks.	Review data collection practices and ensure that only the necessary personal data is collected and processed.
Privacy Settings for Shared Content	Inadvertent sharing of sensitive data with unauthorized users can lead to privacy breaches.	Configure default sharing settings and provide guidance to users on sharing content securely and responsibly.
Anonymization and Pseudonymization	Anonymizing or pseudonymizing personal data can help reduce privacy risks by limiting the identification of individuals.	Implement anonymization or pseudonymization techniques where appropriate, especially when sharing or analyzing personal data.
Retention and Deletion Policies	Proper data retention and deletion policies should be in place to ensure compliance with privacy regulations.	Define and implement data retention and deletion policies in line with legal and regulatory requirements.
Privacy Notice and Consent Management	Users should be informed about data collection practices and provided with the ability to exercise their privacy rights.	Implement mechanisms for providing notice, obtaining informed consent, and allowing users to exercise their privacy rights.

Appendixes

Appendix A: Advanced Profile Implementation Checklist

This checklist is intended as a quick reference tool for implementing the Advanced profile security controls (consisting of relevant Basic and Advanced controls) outlined in this document. Please be aware that the Basic profile is appropriate for most customers. The Advanced profile is for a much smaller set of customers who have a large security team at their disposal and are willing to limit application capabilities to meet compliance requirements. While many security controls can be implemented in any order, **red** controls should only be completed after the preceding controls are completed. The following deployment stages are addressed in the Advanced profile checklist below:

- Preinstallation
- Postinstallation
- Maintenance

*Table 12—Preinstallation **Advanced** Profile Controls*

Order	Task	Basic/Advanced	Responsible Role	Prerequisites
1	Implement Advanced Benchmarks	**Advanced**	System Admin GIS Admin	Have DISA STIG hardening requirements
2	Separate Monolithic Systems	**Advanced**	System Admin	-
3	Implement Network Segmentation	**Basic**	System Admin	-
4	Consider Not Utilizing ArcGIS Web Adaptor	**Basic**	System Admin GIS Admin	-
5	Implement Vendor Security Baselines	**Basic**	System Admin	-
6	Disable Web Tier Technology Identifiers and Banners	**Advanced**	System Admin	-
7	Implement Network Intrusion Detection System	**Advanced**	System Admin	-
8	Implement Intermachine Network Communication Restrictions	**Advanced**	System Admin	-
9	Implement Personal Secrets Management	**Basic**	GIS Admin GIS Users System Admin	-
10	Make Use of Organization Personal Secrets Management	**Advanced**	System Admin	-
11	Make Use of IDE-Integrated Secrets Management/Vaults	**Advanced**	System Admin	-
12	Implement ArcGIS Enterprise Group Managed Service Account	**Basic**	System Admin	-

Order	Task	Basic/Advanced	Responsible Role	Prerequisites
13	Verify HTTPS Is Enforced	Basic	System Admin	-
14	Configure HTTP Strict Transport Security Enforcement	Basic	System Admin	-
15	Implement Web Application Firewall	Basic	System Admin	-

Table 13—Postinstallation Advanced Profile Controls

Order	Task	Basic/Advanced	Responsible Role	Prerequisites
1	Remove Silverlight and FLEX Policy Files	Basic	System Admin	Enterprise prior to 10.8.1 is installed
2	Consider Disabling Anonymous Access	Basic	GIS Admin	-
3	Verify Self-Creation of Built-In User Accounts Is Disabled	Basic	GIS Admin	-
4	Verify Dynamic Workspaces/Layers for Map Services Is Disabled	Basic	GIS Admin	-
5	Verify Token Acquisition via HTTP GET Is Disabled	Basic	GIS Admin	-
6	Verify Portal for ArcGIS Legend Servlet Is Disabled	Advanced	GIS Admin	-
7	Verify Portal for ArcGIS Print Servlet Is Disabled	Advanced	GIS Admin	-
8	Verify Portal for ArcGIS WFS Servlet Is Disabled	Advanced	GIS Admin	-
9	Consider Disabling KML and GeoRSS Servlets	Advanced	GIS Admin	-
10	Configure Access Notice and/or Information Banners	Basic	GIS Admin	-
11	Configure Password Policy for Built-In Accounts	Basic	GIS Admin	Utilize Built-In accounts
12	Verify Standardized Queries Are Enabled	Basic	GIS Admin	-
13	Verify Nosniff Header Enabled	Basic	GIS Admin	-
14	Reduce Default Token Expiration to Align with Organization Policy	Advanced	GIS Admin System Admin	-
15	Implement Centralized User Account Management	Basic	System Admin GIS Admin	-
16	Disable Public Sharing by Default	Basic	GIS Admin	-

Order	Task	Basic/Advanced	Responsible Role	Prerequisites
17	Disable Public Sharing	**Basic**	GIS Admin	-
18	Enable SAML-Based Group Membership	**Advanced**	GIS Admin System Admin	Implement SAML
19	Implement SAML-Signed and Encrypted Assertions	**Basic**	System Admin GIS Admin	-
20	Disable ArcGIS Logins/Allow SAML Login Only	**Advanced**	GIS Admin	Implement SAML into ArcGIS Enterprise
21	Choose to Enable or Disable Item Comments	**Advanced**	GIS Admin	-
22	Consider Custom Roles	**Advanced**	GIS Admin	-
23	Configure New Member Default Role as Viewer	**Basic**	GIS Admin	-
24	Utilize Central Profile Policy	**Advanced**	GIS Admin	-
25	Implement Administrative Network Segments	**Basic**	System Admin GIS Admin	-
26	Configure Portal for ArcGIS Proxy Allow List	**Basic**	GIS Admin	-
27	Implement Email Notification for Password Reset Workflows	**Basic**	System Admin GIS Admin	Provide or identify SMTP server
28	Configure Hardened TLS Algorithms	**Advanced**	System Admin	-
29	Implement Signed CA Certificates	**Basic**	System Admin GIS Admin	Obtain CA signed certificate(s)
30	Revoke Public Access to the Enterprise Geodatabase	**Advanced**	System Admin	-
31	Consider ArcGIS Monitor	**Advanced**	GIS Admin System Admin	-
32	Disable Primary Site Administrator Account (ArcGIS Server)	**Basic**	GIS Admin	Create a new primary admin account
33	Remove Initial Admin Account (Portal for ArcGIS)	Advanced	GIS Admin	Create a new admin account
34	Disable ArcGIS Server Services Directory	**Basic**	GIS Admin	-
35	Disable ArcGIS Portal Directory	**Basic**	GIS Admin	-

*Table 14—Maintenance **Advanced** Profile Controls*

#	Task	Basic/Adv	Responsible Role	Prerequisites
1	Verify Filter Web Content Is Enabled for All Feature Services	**Basic**	GIS Admin GIS User	-
2	Verify XSSPreventionEnabled Is Enabled for All Feature Services	**Basic**	GIS Admin	
3	Configure XSSPreventionRule to inputOutput	**Advanced**	GIS Admin	xssPreventionEnabled=true
4	Disable callbackFunctionsEnabled	**Basic**	GIS Admin	
5	Verify Server System Services Secured	**Basic**	GIS Admin	-
6	Avoid Embedding User Identities in Scripts	**Basic**	GIS Admin GIS User System Admin	-
7	Avoid Embedding Application Identities in Client Applications	**Basic**	GIS Admin GIS User System Admin	-
8	Avoid Storing Secrets in Source Code	**Basic**	System Admin GIS User	-
9	Configure All Administrator Accounts with Multifactor Authentication	**Basic**	System Admin	-
10	Enforce SAML/OIDC Identity Provider Lockouts Against Brute Force Attacks	**Advanced**	System Admin	Implement SAML
11	Utilize an Identity Provider That Supports Strong Credential Flow	**Advanced**	System Admin	-
12	Certificate-Based Authentication (PKI/PIV/CAC)	**Advanced**	System Admin	-
13	Implement Group-Based Sharing	**Basic**	GIS Admin	-
14	Configure Least Privilege User Types and Roles	**Basic**	GIS Admin	-
15	Configure Decentralized Profile Visibility	**Basic**	GIS Admin	-
16	Manage Content via Role-Based Access Control	**Basic**	GIS Admin	-

17	Configure Default Group Membership Assignments	Basic	GIS Admin	-
18	Manage Distributed Collaboration Securely	Advanced	GIS Admin	-
19	Implement GIS Data Publication Management Process	Advanced	GIS Admin	-
20	Configure Organizational Policies to Prevent Over Sharing	Advanced	GIS Admin System Admin	-
21	Disable Public User Profile Sharing for Organization Users	Basic	GIS Admin	
22	Disable Show Social Media Links on Item and Group Pages"	Basic	GIS Admin GIS User	-
23	Consider Using Scoping Feature Layer Capabilities by Using Feature Layer Views	Basic	GIS Admin	
24	Consider Establishing Governance around Publication Processes and Delivery Pipelines	Basic	GIS Admin System Admin	
25	Consider Defining Content Access Requirements	Basic	GIS Admin	-
26	Verify Content Ownership Rights	Basic	GIS Admin	-
27	Manage Accounts and Reduce User Permissions	Basic	GIS Admin	-
28	Implement Permission Guardrails	Basic	GIS Admin	-
29	Manage Access Based on Employee or Project Life Cycle	Basic	GIS Admin	-
30	Define a Content Security Policy	Advanced	GIS Admin System Admin	-
31	Implement Backup Strategy and Test Regularly	Basic	GIS Admin System Admin	-
32	Consider File Geodatabases	Basic	GIS Admin System Admin	-
33	Implement Database Transparent Data Encryption	Basic	System Admin GIS Admin	-
34	Implement FIPS 140-2 Encryption if Required	Advanced	System Admin GIS Admin	-

35	Implement Data Segmentation	Advanced	System Admin GIS Admin	-
36	Disable Mixed Mode SQL Server Authentication	Advanced	System Admin GIS Admin	-
37	Implement Whole Disk Encryption for Content and Configuration Stores	Basic	System Admin	-
38	Implement and Maintain Software Inventory	Basic	System Admin GIS Admin	-
39	Manage Only General Availability Product Versions	Basic	GIS Admin	-
40	Configure Subscription to Vendor Patch Notifications	Basic	GIS Admin	-
41	Implement Security Patches within One Month	Basic	GIS Admin	-
42	Manage Configuration Drift	Basic	GIS Admin	-
43	Automate Software Inventory	Advanced	System Admin GIS Admin	-
44	Remove Superfluous Components	Advanced	System Admin	-
45	Implement Security Information and Event Management	Basic	System Admin	-
46	Manage Webhooks	Basic	GIS Admin System Admin	-
47	Implement a CSIRT Process	Basic	System Admin	-
48	Implement Training Users by Role and Responsibility	Basic	System Admin GIS Admin GIS User	-
49	Manage Frequent and Ongoing Awareness Activities	Basic	System Admin GIS Admin GIS User	-
50	Disable or Location Lock Clients with EUEI Analytics	Advanced	System Admin GIS Admin	-
51	Implement Vulnerability Scanning Tools	Basic	System Admin	-
52	Manage Vulnerable Components with Patching	Basic	GIS Admin System Admin	-
53	Verify Log Folder Security Permissions	Advanced	System Admin GIS Admin	-

Appendix B: Deployment Diagrams with Ports and Protocols

We have provided detailed port information along with supporting diagrams for three common deployment patterns:

- Single-machine ArcGIS Enterprise Infrastructure*
- Multimachine ArcGIS Enterprise Infrastructure
- Securing Highly Available ArcGIS Enterprise Infrastructure

***Notes:**

- The single-machine pattern should *not* be utilized to support production operations of an internet-facing deployment of ArcGIS Enterprise. It is appropriate for internal-only, small-scale usage or testing and development purposes.
- RDP and SSH are NOT required by ArcGIS Enterprise, but were added to the systems where they are commonly utilized for administration of the system. Only add these ports for your organization’s particular operational needs.

Securing Single-Machine ArcGIS Enterprise Infrastructure

For deployments of limited scale, development, and testing, ArcGIS Enterprise may be deployed on a single physical or virtual machine following the pattern below:

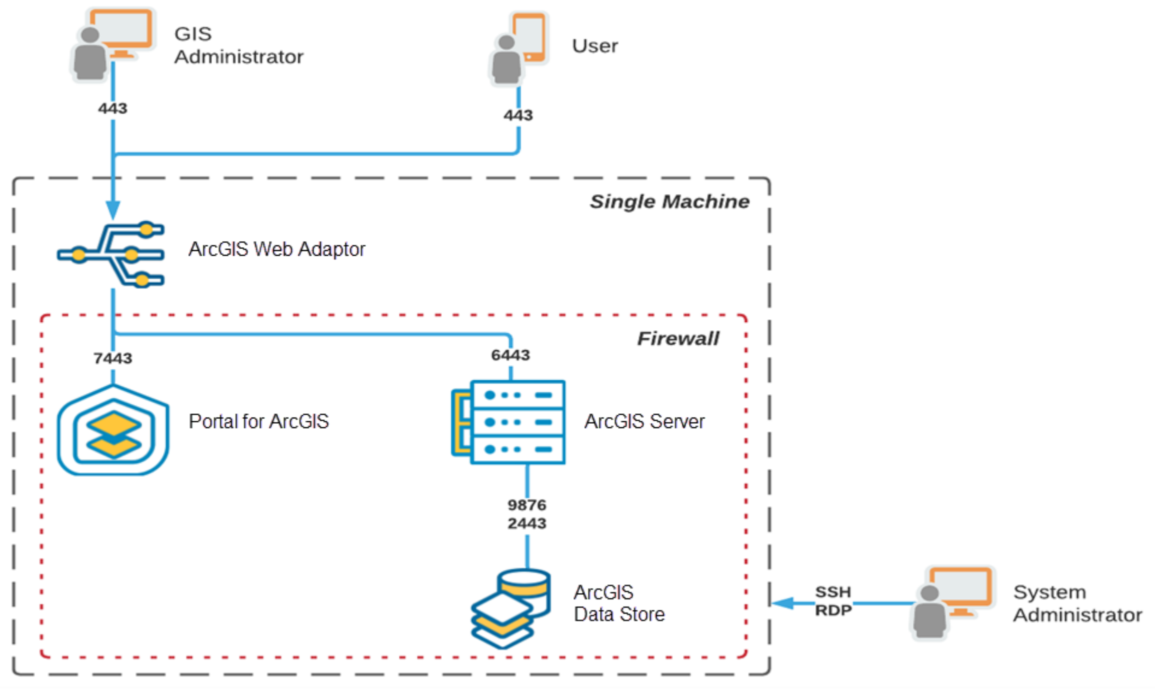


Figure 23—ArcGIS Enterprise Single Machine Deployment

ArcGIS Web Adaptor hosted on IIS/Tomcat on HTTPS (TCP 443) is the main point of ingress for GIS Users and the GIS Administrator.

Table 15—Local Firewall Configuration of Single Machine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	HTTPS	TCP 443	0.0.0.0/0, ::0
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>

- All ArcGIS Enterprise components are deployed on the same host.
- System Administrator administers host over RDP or SSH (or via another secure agent).

Securing Multimachine ArcGIS Enterprise Infrastructure

ArcGIS Enterprise is commonly deployed across multiple servers or virtual machines to meet the scale of production workloads. Here all ArcGIS Enterprise components; Web Adaptor, Portal for ArcGIS, ArcGIS Server, and ArcGIS Data Store are distributed to dedicated servers:

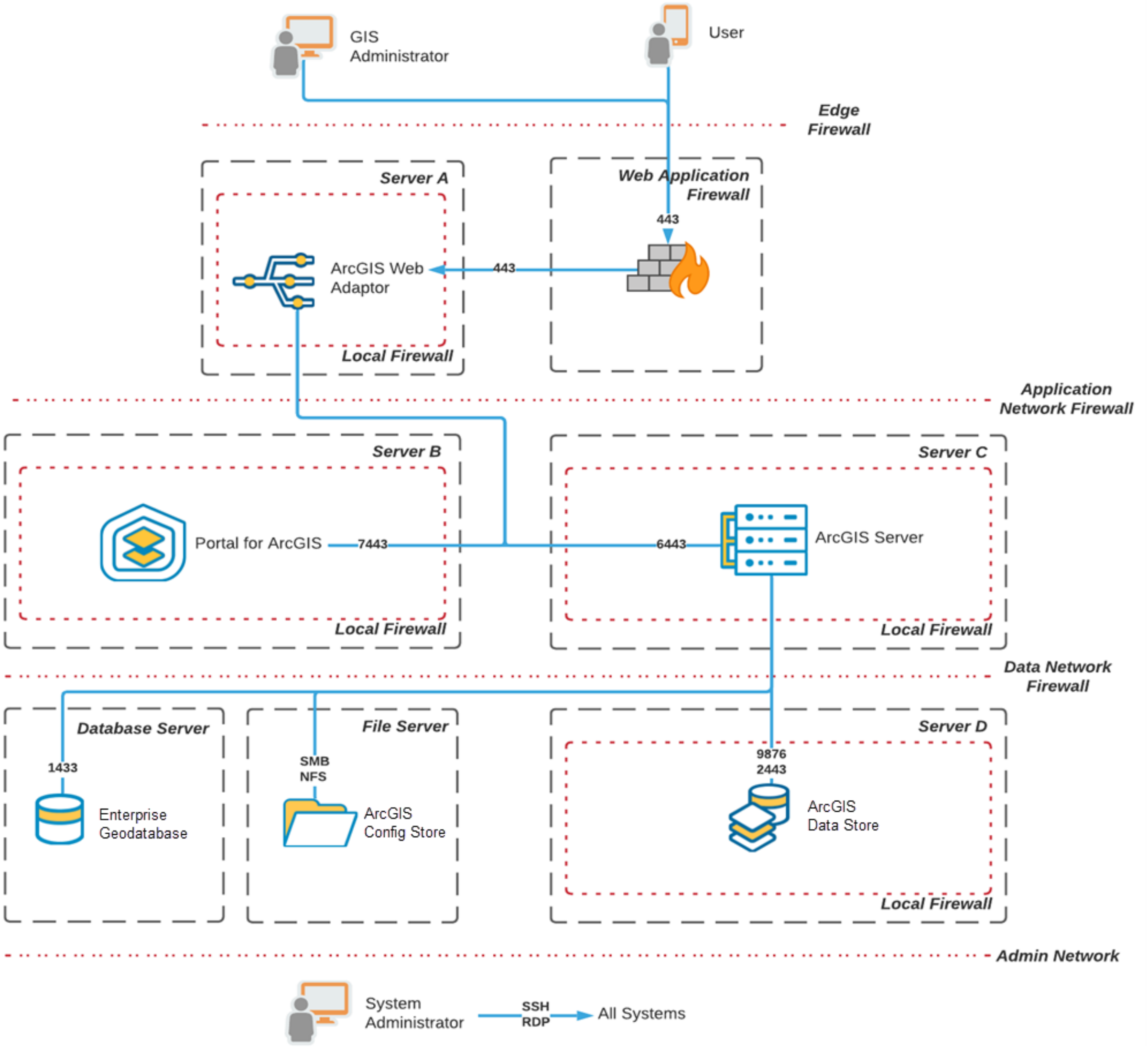


Figure 24—ArcGIS Enterprise on Multiple Machines

The pattern above describes the following component configuration:

- **Web Application Firewall**
  - Main ingress for GIS Users and GIS Administrators
  - Configured according to ArcGIS Enterprise Web Application Filter Rules
  - Routes requests to the Web Adaptor component

- **Server A—Web Adaptor *(Optional)***
  - Hosted on IIS or supported Java application server
  - Can be replaced by a Load Balancer

Table 16—Web Adaptor Local Firewall Configuration Multimachine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	HTTPS	TCP 443	0.0.0.0/0, ::0
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>

- **Server B—Portal for ArcGIS**
  - Hosts Portal for ArcGIS component
  - Ports used by Portal for ArcGIS

Table 17—Portal Local firewall configuration Multimachine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>
ALLOW	HTTPS	TCP 7443	<Edge Network>
ALLOW	HTTPS	TCP 7443	<Administrative Network>

- **Server C—ArcGIS Server**
  - Hosts ArcGIS Server component(s)
  - Can be scaled horizontally to handle load (Server C1…Cn).
  - Ports used by ArcGIS Server

Table 18—Server Local Firewall Configuration Multimachine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>
ALLOW	HTTPS	TCP 6443	<Edge Network>
ALLOW	HTTPS	TCP 6443	<Administrative Network>

- **Server D—ArcGIS Data Store**
    - Hosts ArcGIS Data Store component
    - Ports used by ArcGIS Data Store

Table 19—Data Store Local Firewall Configuration Multimachine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>
ALLOW	TCP	TCP 9876	<Data Network>
ALLOW	HTTPS	TCP 2443	<Data Network>
ALLOW	TCP	TCP 9876	<Application Network>
ALLOW	HTTPS	TCP 2443	<Application Network>
ALLOW	ALL	ALL	<Local>

- **File Server**
    - Hosts ArcGIS Config Store
    - Required to provide a shared storage space when scaling the ArcGIS Server or Portal for ArcGIS components beyond a single server.
    - Hosts file data

Table 20—File Server Local Firewall Configuration Multimachine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	SMB	TCP 445	<Application Network>
ALLOW	SMB	TCP 139	<Application Network>
ALLOW	SMB	UDP 138	<Application Network>
ALLOW	SMB	UDP 139	<Application Network>
ALLOW	NFS	TCP 111	<Application Network>
ALLOW	NFS	UDP 111	<Application Network>
ALLOW	NFS	TCP 2049	<Application Network>
ALLOW	NFS	UDP 2049	<Application Network>

- **Database Server *(Optional)***
    - Hosts Enterprise Geodatabase component
    - A separate enterprise geodatabase server is not required for ArcGIS Enterprise if ArcGIS Data Store is present.

Table 21—Database Server Local Firewall Configuration Multimachine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	<RDBMS>	<RDBMS>	<Application Network>

- **Edge Firewall**

Table 22—Edge Firewall Local Firewall Configuration Multimachine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	HTTPS	TCP 443	0.0.0.0/0, ::0
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>

- **Application Network Firewall**

Table 23—Application Network Firewall Configuration Multimachine Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	HTTPS	TCP 6443	<Edge Network>
ALLOW	HTTPS	TCP 6443	<Application Network>
ALLOW	HTTPS	TCP 7443	<Edge Network>
ALLOW	HTTPS	TCP 7443	<Application Network>
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>

- **Data Network Firewall**
  - System Administrator administers host over RDP or SSH (or via another secure agent)

Table 24—Data Network Firewall Configuration Multimedia Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	TCP	TCP 9876	<Application Network>
ALLOW	UDP	UDP 9876	<Application Network>
ALLOW	TCP	TCP 9876	<Data Network>
ALLOW	UDP	UDP 9876	<Data Network>
ALLOW	SMB	TCP 445	<Application Network>
ALLOW	SMB	TCP 139	<Application Network>
ALLOW	NFS	TCP 111	<Application Network>
ALLOW	NFS	UDP 111	<Application Network>
ALLOW	NFS	TCP 2049	<Application Network>
ALLOW	NFS	UDP 2049	<Application Network>
ALLOW	<RDBMS>	<RDBMS>	<Application Network>
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>

Securing Highly Available ArcGIS Enterprise Infrastructure

Production workloads classified as critical infrastructure are best suited for ArcGIS Enterprise High Availability patterns. In a high availability pattern, enterprise components: Portal for ArcGIS, ArcGIS Server, and ArcGIS Data Store are both distributed and replicated to dedicated servers on the next page.

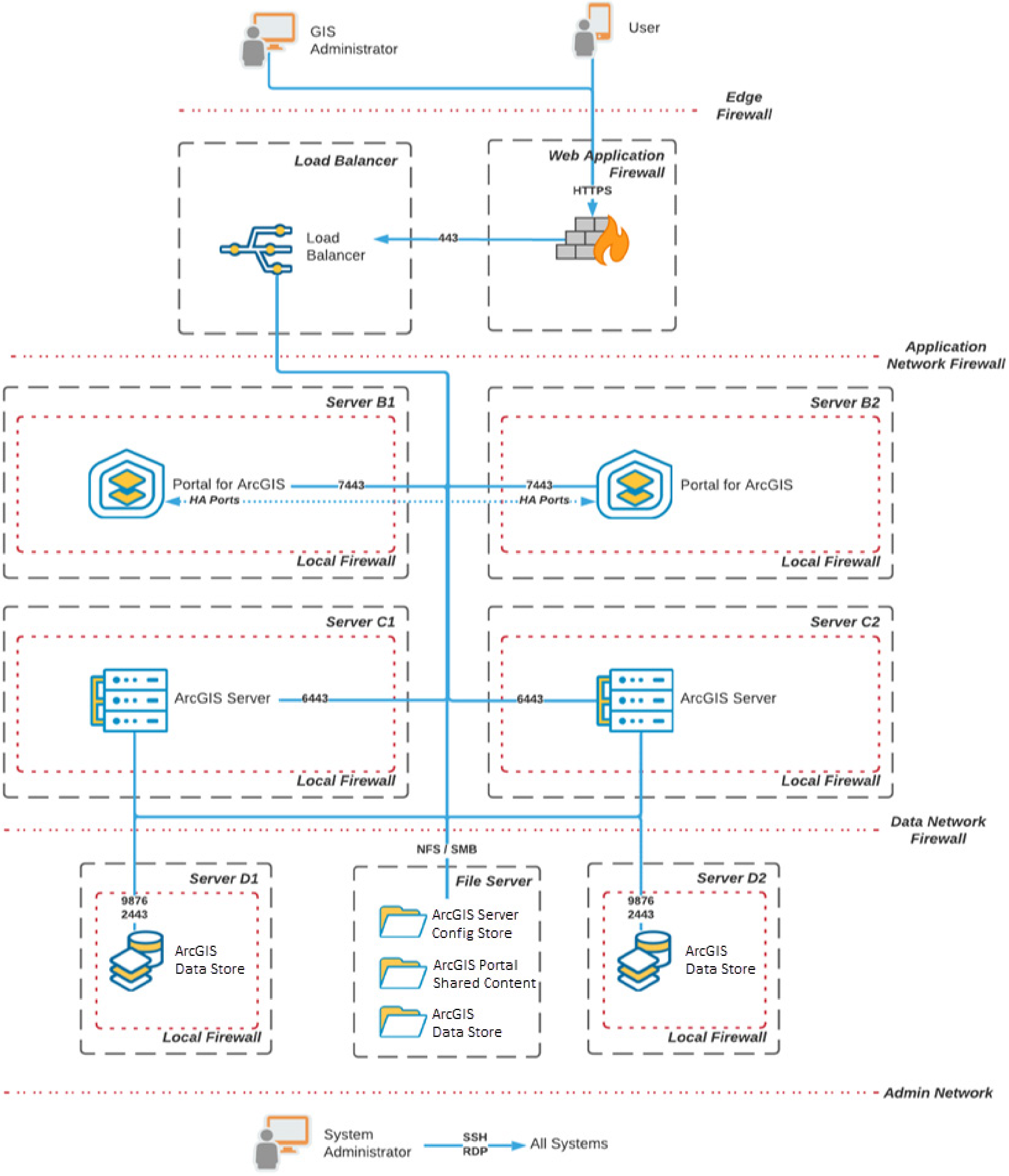


Figure 25—ArcGIS Enterprise High Availability

The preceding pattern describes the following component configuration:

- **Web Application Firewall**
    - Main ingress for GIS Users and GIS Administrators
    - Configured according to ArcGIS Enterprise Web Application Filter Rules
    - Routes requests to Load Balancer

- **Load Balancer**
    - Replaces Web Adaptor as a Scalable Layer 4 or Layer 7 distributed proxy
    - Routes Portal requests to HA Portal Servers (Server B1 & Server B2) over TCP 7443
    - Routes Server requests to HA ArcGIS Servers (Server C1 & Server C2) over TCP 6443

- **Server B1 and B2—Portal for ArcGIS**
    - Hosts Portal for ArcGIS component
    - Configured for high availability

Table 25—Portal Local Firewall Configuration HA Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>
ALLOW	HTTPS	TCP 7443	<Edge Network>
ALLOW	HTTPS	TCP 7443	<Administrative Network>
ALLOW	TCP	HA Ports	<Application Network>
ALLOW	ALL	ALL	<Local>

- **Server C1 and C2—ArcGIS Server**
    - Hosts ArcGIS Server component
    - Configured as a multimachine site
    - Federated with Portal and Configured as a hosting server

Table 26—Server Local Firewall Configuration HA Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>
ALLOW	HTTPS	TCP 6443	<Edge Network>
ALLOW	HTTPS	TCP 6443	<Administrative Network>
ALLOW	ALL	ALL	<Local>

- **Server D1 and D2—ArcGIS Data Store**
    - Hosts ArcGIS Data Store component
    - Configured as standby data store

Table 27—Data Store Local Firewall Configuration HA Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>
ALLOW	TCP	TCP 9876	<Data Network>
ALLOW	HTTPS	TCP 2443	<Data Network>
ALLOW	TCP	TCP 9876	<Application Network>
ALLOW	HTTPS	TCP 2443	<Application Network>
ALLOW	ALL	ALL	<Local>
ALLOW	TCP	TCP 50432	<Local>
ALLOW	HTTP	TCP 29080	<Local>
ALLOW	HTTPS	TCP 29081	<Local>
ALLOW	TCP	TCP 29082	<Local>
ALLOW	TCP	TCP 9220	<Local>
ALLOW	TCP	TCP 9320	<Local>
ALLOW	HTTPS	TCP 6443	<Application Network>
ALLOW	TCP	TCP 9829	<Local>
ALLOW	TCP	TCP 9828	<Local>
ALLOW	TCP	TCP 9831	<Local>
ALLOW	TCP	TCP 9820	<Local>
ALLOW	TCP	TCP 9830	<Local>
ALLOW	TCP	TCP 9840	<Local>
ALLOW	TCP	TCP 9880	<Local>
ALLOW	TCP	TCP 29874	<Local>
ALLOW	TCP	TCP 29876	<Local>
ALLOW	TCP	TCP 29882	<Local>
ALLOW	TCP	TCP 29875	<Local>
ALLOW	TCP	TCP 29877	<Local>
ALLOW	TCP	TCP 29883	<Local>
ALLOW	TCP	TCP 29860-29863	<Local>
ALLOW	TCP	TCP 29858-29859	<Local>
ALLOW	TCP	TCP 25672	<Local>
ALLOW	TCP	TCP 44369	<Local>
ALLOW	TCP	TCP 29858	<Local>
ALLOW	TCP	TCP 45671-45672	<Local>

- **File Server**
  - Hosts ArcGIS Config Store
  - Hosts Data Store Backup Store

- Hosts file data

Table 28—File Server Local Firewall Configuration HA Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	SMB	TCP 445	<Application Network>
ALLOW	SMB	TCP 139	<Application Network>
ALLOW	SMB	UDP 138	<Application Network>
ALLOW	SMB	UDP 139	<Application Network>
ALLOW	NFS	TCP 111	<Application Network>
ALLOW	NFS	UDP 111	<Application Network>
ALLOW	NFS	TCP 2049	<Application Network>
ALLOW	NFS	UDP 2049	<Application Network>

- **Edge Firewall**

Table 29—Edge Firewall Configuration HA Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	HTTPS	TCP 443	0.0.0.0/0, ::0

- **Application Network Firewall**

Table 30—Application Network Firewall Configuration HA Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	HTTPS	TCP 6443	<Edge Network>
ALLOW	HTTPS	TCP 6443	<Application Network>
ALLOW	HTTPS	TCP 7443	<Edge Network>
ALLOW	HTTPS	TCP 7443	<Application Network>
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>

- **Data Network Firewall**
    - System Administrator administers host over RDP or SSH (or via another secure agent)

Table 31—Data Network Firewall Configuration HA Deployment

ACTION	PROTOCOL	PORT	SOURCE
ALLOW	TCP	TCP 9876	<Application Network>
ALLOW	UDP	UDP 9876	<Application Network>
ALLOW	TCP	TCP 9876	<Data Network>
ALLOW	UDP	UDP 9876	<Data Network>
ALLOW	SMB	TCP 445	<Application Network>
ALLOW	SMB	TCP 139	<Application Network>
ALLOW	NFS	TCP 111	<Application Network>
ALLOW	NFS	UDP 111	<Application Network>
ALLOW	NFS	TCP 2049	<Application Network>
ALLOW	NFS	UDP 2049	<Application Network>
ALLOW	<RDBMS>	<RDBMS>	<Application Network>
ALLOW	RDP	TCP 3389	<Administrative Network>
ALLOW	RDP	UDP 3389	<Administrative Network>
ALLOW	SSH	TCP 22	<Administrative Network>

- See Appendix K: ArcGIS Enterprise Ports Utilized Diagram for both data network and edge network port details.
- More details concerning ArcGIS Enterprise port requirements is available in the documentation - Ports used by ArcGIS Enterprise components

Appendix C: Web Server Extensions to Allow

Note: We do not recommend user leveraging Organization Specific logins where userNames are defined in a format firstname.lastname@domain attempt to define allowed web server extensions. IIS limits interpret the “dot” in a format like firstname.lastname@domain as identifying an extension.

.3dd	.ico	.nmf	.svg.surveyaddi	.featureserver
.3vr	.insightswbk	.numbers	.swf.svg	.imageserver
.3ws	.ipynb	.ogg	.sxd .swf	.geometryserver
.aptx	.jl	.oic	.tex.sxd	.symbolserver
.as	.jpeg	.otf	.tif.tex	.dpserver
.aspx	.jpg	.pages	.tiff.tif	.workspaceserver
.babelrc	.js	.pagx	.tld.tiff	.geodataserver
.bmp	.jsbeautifyrc	.parquet	.tpk.tld	.vectortileserver
.bpk	.jshintrc	.pbf	.tpkx.tpk	.knowledgegraphserver
.css	.json	.pdf	.ts.tpkx	.geocodeserver
.csv	.jsp	.pitem	.tsx.ts	.Geoenrichmentserver
.cur	.key	.pmf	.ttf.tsx	.relationalcatalogserver
.dlpk	.kml	.png	.vm.ttf	.sceneserver
.doc	.kmz	.ppkx	.vm	.opdashboardaddin
.docx	.lapk	.ppt	.vsd	
.dtd	.less	.pptx	.vtpk.vsd	
.eaz	.lpk	.proconfigX	.wasm.vtpk	
.ecd	.lpkx	.psd	.webm.wasm	
.eot	.lyr	.rb	.wmpk.webm	
.epk	.lyrx	.rft.json	.woff.wmpk	
.eslintrc	.map	.rft.xml	.woff2.woff	
.esriaddin	.mapx	.rpk	.wpk.woff2	
.esriaddinx	.MF	.rptx	.wsv.wpk	
.fla	.mmpk	.rtf	.xls.wsv	
.gcpk	.mov	.scss	.xlsx.xls	
.geojson	.mp	.sd	.xml.xlsx	
.gif	.mpk	.sh	.xsd.xml	
.gpk	.mpkx	.slpk	.xsl.xsd	
.gpkg	.msd	.smd	.zip.xsl	
.hbs	.mspk	.spk	.zip .zip	
.htm	.mxd	.styl	JSON	
PJSON	.ncfg	.stylx	.gpserver	
.html	.nmc	.surveyaddinn	.mapserver	

Appendix D: HTTP Header Guidance

What is an HTTP header?

HTTP headers are part of the HTTP specification. They represent the name or value pairs that are displayed in the request and response headers for HTTP requests and responses. Request headers send information to the remote server about the method the browser is using to send data, the path to the requested resource, the page that is linked to the resource requested, the type size of the data being sent, etc. A response header provides information regarding the success of the request, the type and size of the data requested, the location a redirect sends the browser to, cookies the site sets for the browser, instructions for how the browser should authenticate to a resource, and how a browser should behave when interacting with a given site. Not all browsers support all HTTP headers. This document speaks to both request and response headers used in ArcGIS Enterprise.

What is an HTTP Security Header?

HTTP Security Headers provide explicit instructions to a browser regarding how it should interact with a website. For instance, some headers establish a requirement that HTTPS be always used with a site or instruct a browser to not try to guess the content type of data and to just trust what is declared. Other headers disallow the browser from opening remote pages or forms in an HTML frame. Essentially, these headers define whether a set of security precautions should be activated or deactivated on the browser while interacting with a website or application. For reference and definitions of specific headers, consult the OWASP Secure Headers Project.

Which HTTP headers does ArcGIS Enterprise support?

ArcGIS Online and ArcGIS Enterprise administrators frequently have questions regarding Esri's use and support of various HTTP headers.

Header Name	Value	Version Implemented
Strict-Transport-Security (HSTS)	max-age=31536000	10.6.1+

- Implemented in ArcGIS 10.6.1+ when HTTPS is required and HSTS is enabled.
- Some security scanners flag HSTS as a failure because Preload is not included. References:
- enterprise.arcgis.com/en/server/latest/administer/linux/enforce-strict-https-communication.htm
- enterprise.arcgis.com/en/portal/latest/administer/linux/enforce-strict-https-communication.htm

Header Name	Value	Version Implemented
X-Frame-Options	SAMEORIGIN	All

- The X-Frame-Options header is set for all OAuth resources (anywhere credentials are passed).
- Not set in bundled documentation or in the Portal for ArcGIS Map Viewer or Scene Viewer™ as these resources are intended to be framed in an application residing in a separate origin.
- If resources participating in a web map (or the web map is secured), X-Frame-Options SAMEORIGIN is set at the OAuth level, preventing framing.

Header Name	Value	Version Implemented
X-XSS-Protection	1; mode=block	All

- X-XSS-Protection is deprecated and not respected in modern browsers in favor of CSP

Header Name	Value	Version Implemented
X-Content-Type-Options	NOSNIFF	10.7+

- There are additional filters at the API and server levels to sanitize inputs into the application.
- Attempting to manually enforce X-Content-Type-Options by introducing the header via a proxy is known to cause issues with Esri clients prior to 10.7 due to a mismatch of expected content types.

Reference:

- enterprise.arcgis.com/en/server/latest/administer/windows/disable-the-no-sniff-header.htm

Header Name	Value	Version Implemented
Access-Control-Allow-Origin	*	10.5+

- Enabled by default for all CORS requests to ArcGIS Online, Portal for ArcGIS, and ArcGIS Server.
- The value of the origins ArcGIS Enterprise is allowed to send cross-domain responses to is user-supplied and must match the value for the Origin request header.

References:

- enterprise.arcgis.com/en/server/latest/administer/linux/restricting-cross-domain-requests-to-arcgis-server.htm
- enterprise.arcgis.com/en/portal/latest/administer/linux/restrict-cross-domain-requests-to-your-portal.htm

Header Name	Value	Version Implemented
Content-Security-Policy	User-defined	Defined by user at web tier

- Review the in-depth discussion in this document for CSP implementation considerations.

Header Name	Value	Version Implemented
Origin: (Request Header)	Domain	Defined by user at web tier

- The Origin header indicates the origin of the cross-site access request or CORS preflight request.
- In any access control request, the Origin header is always set.
- The value of the Origin header is compared against the values presented in the Access-Control-Allow-Origin header in a CORS request. If the values match, the request is allowed.

Reference:

- developer.mozilla.org/en-US/docs/Web/HTTP/CORS

Header Name	Value	Version Implemented
X-Esri-Authorization (Request Header)	Token	10.5+

- When building custom ArcGIS client applications that use GET requests to access web services secured using ArcGIS token-based authentication, it is recommended that the token be sent in the X-Esri-Authorization header instead of a query parameter.
- This prevents intermediaries on the network, such as proxies, gateways, or load balancers from being able to obtain the token.

Reference:

- enterprise.arcgis.com/en/server/latest/administer/linux/accessing-arcgis-token-secured-web-services.htm

Header Name	Value	Version Implemented
Referer (Request Header)	referer	*

- The Referer request header contains the address of the previous web page from which a link to the currently requested page was followed.
- The Referer header allows servers to identify where people are visiting them from.

References:

- developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer
- enterprise.arcgis.com/en/server/latest/administer/linux/acquiring-arcgis-tokens.htm

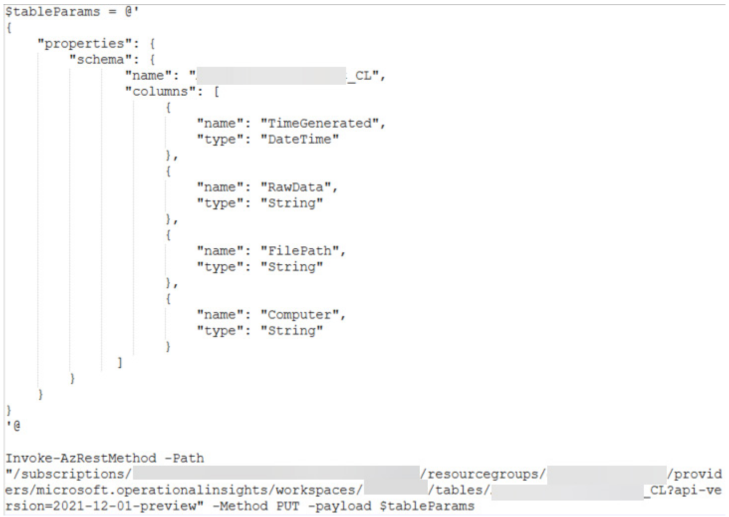
Appendix E: SIEM Log Shipping Guidance

Effective auditing of ArcGIS Enterprise starts with shipping logs to a SIEM system such as Splunk, Microsoft Sentinel, Elastic LogStash, or other event management platforms. External log collection and correlation provide the following benefits:

- **Correlation and Forensics—**SIEM solutions provide powerful query and correlation capabilities similar to a relational SQL database, allowing for correlation of events across ArcGIS Enterprise and related components including load balancer access logs, database event logs, and web application logs where applicable.
- **Nonrepudiation**—Events collected on the SIEM provide a source of truth independent of any issues with or compromise of ArcGIS Enterprise. Should an attacker attempt to evade detection by clearing the ArcGIS Server or Portal for ArcGIS event logs, those events will remain on the SIEM for discovery, tracking, and auditing.
- **Storage—**With a SIEM implementation in place, ArcGIS Enterprise logs can be configured to automatically clear on a rapid cycle (e.g., 30 days), avoiding any storage problems that may occur with long-term log storage on disk.

The following configuration should be in place to support effective log collection and auditing:

1. Configure the Portal for ArcGIS' logging level to at least INFO – See Basic: Configure Logging Level.
2. Configure the ArcGIS Server' logging level to at least INFO. – See Basic: Configure Logging Level.
3. Deploy SIEM log agents on each application host (e.g., https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-agent)
4. Configure one or more custom tables within the SIEM to store logs as "RawData/Text" (e.g., https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-log-text?tabs=portal#custom-table). For example, this code will create a table to store ArcGIS Portal logs:



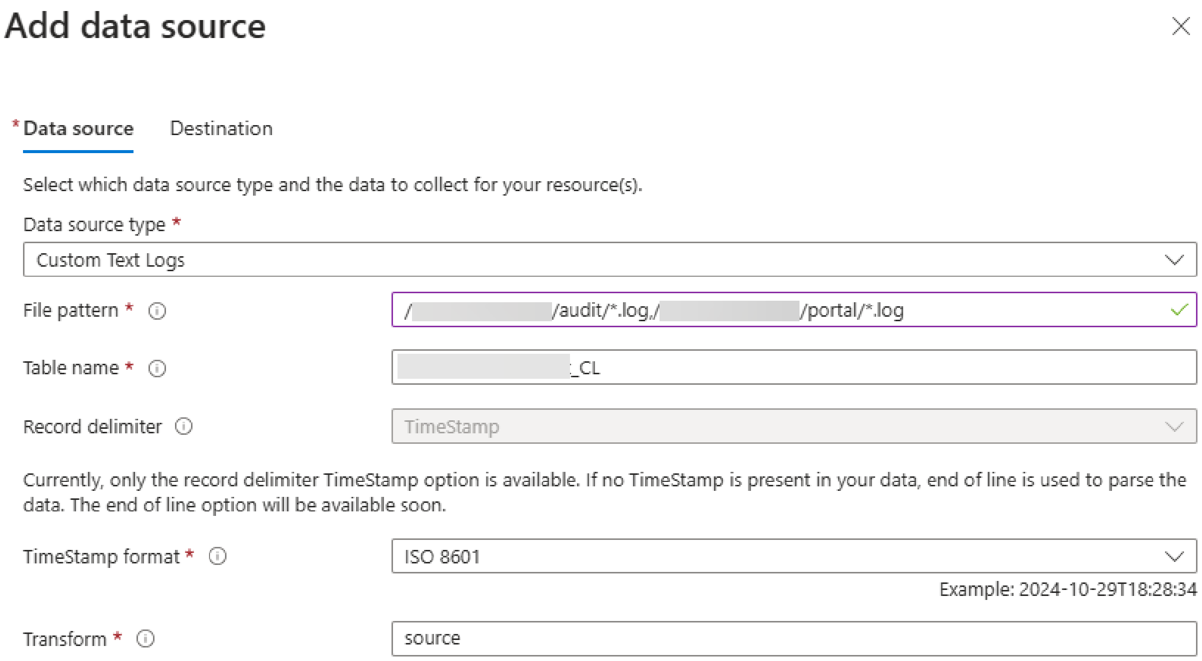
```
$tableParams = @'
{
    "properties": {
        "schema": {
               "name": "[redacted]_CL",
               "columns": [
                    {
                        "name": "TimeGenerated",
                        "type": "DateTime"
                    },
                    {
                        "name": "RawData",
                        "type": "String"
                    },
                    {
                        "name": "FilePath",
                        "type": "String"
                    },
                    {
                        "name": "Computer",
                        "type": "String"
                    }
               ]
        }
    }
}
'@

Invoke-AzRestMethod -Path
"/subscriptions/[redacted]/resourcegroups/[redacted]/provid
ers/microsoft.operationalinsights/workspaces/[redacted]/tables/[redacted]_CL?api-ve
rsion=2021-12-01-preview" -Method PUT -payload $tableParams
```

5. Instruct SIEM agents to read the following log areas (on disk) as a "RawData/Text" log (e.g., https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-manage):
   a. Portal for ArcGIS:
      i. `<INSTALL_PATH>/logs/<HOSTNAME>/portal/*.log`

   ii. `<INSTALL_PATH>/logs/<HOSTNAME>/audit/*.log` *(new @ v11.4)*

b. ArcGIS Server:
   i. `<INSTALL_PATH>/logs/<HOSTNAME>/server/*.log`
   ii. `<INSTALL_PATH>/logs/<HOSTNAME>/audit/*.log` *(new @ v11.4)*

c. ArcGIS Data Store:
   i. `<INSTALL_PATH>/logs/<HOSTNAME>/server/*.log`
   ii. `<INSTALL_PATH>/logs/<HOSTNAME>/audit/*.log` *(new @ v11.4)*



Add data source

*Data source | Destination

Select which data source type and the data to collect for your resource(s).

Data source type *: Custom Text Logs

File pattern *: /[redacted]/audit/*.log,/[redacted]/portal/*.log ✓

Table name *: [redacted]_CL

Record delimiter: TimeStamp

Currently, only the record delimiter TimeStamp option is available. If no TimeStamp is present in your data, end of line is used to parse the data. The end of line option will be available soon.

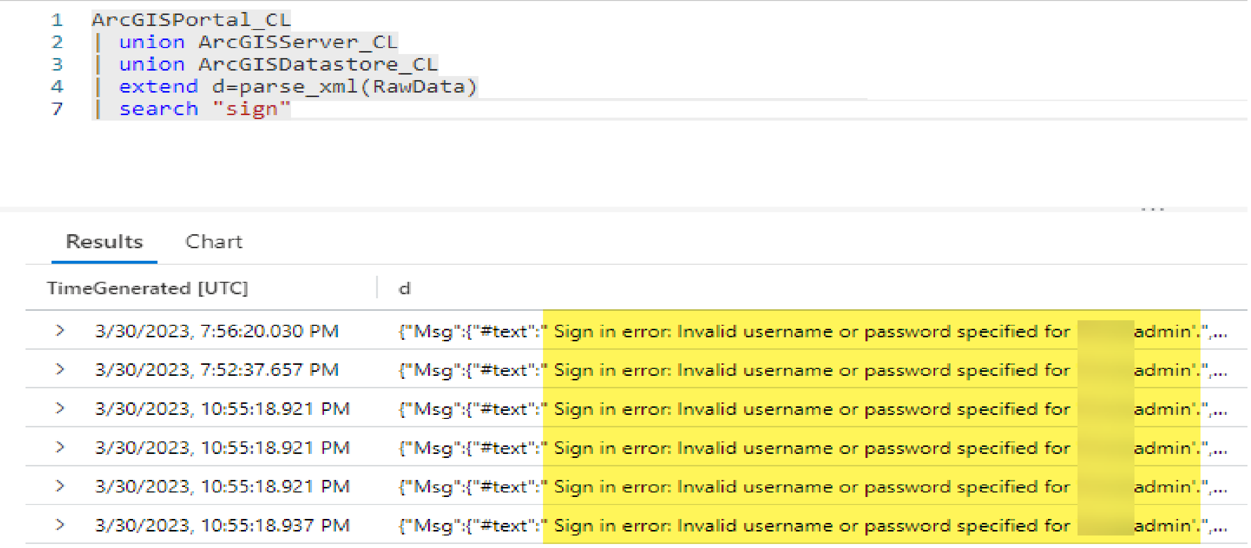
TimeStamp format *: ISO 8601

Example: 2024-10-29T18:28:34

Transform *: source

Generally this process should be repeated for each component (ArcGIS Server, Portal for ArcGIS, and ArcGIS Datastore), which will yield 3 distinct logging tables. All hosts can then be configured to ship logs to the same application table.

Once logs are shipped to the SIEM, a variety of query, reporting, and alerting options emerge including monitoring for frequent invalid logins or high-risk accounts as with the following query that finds sign-in events across multiple log sources:

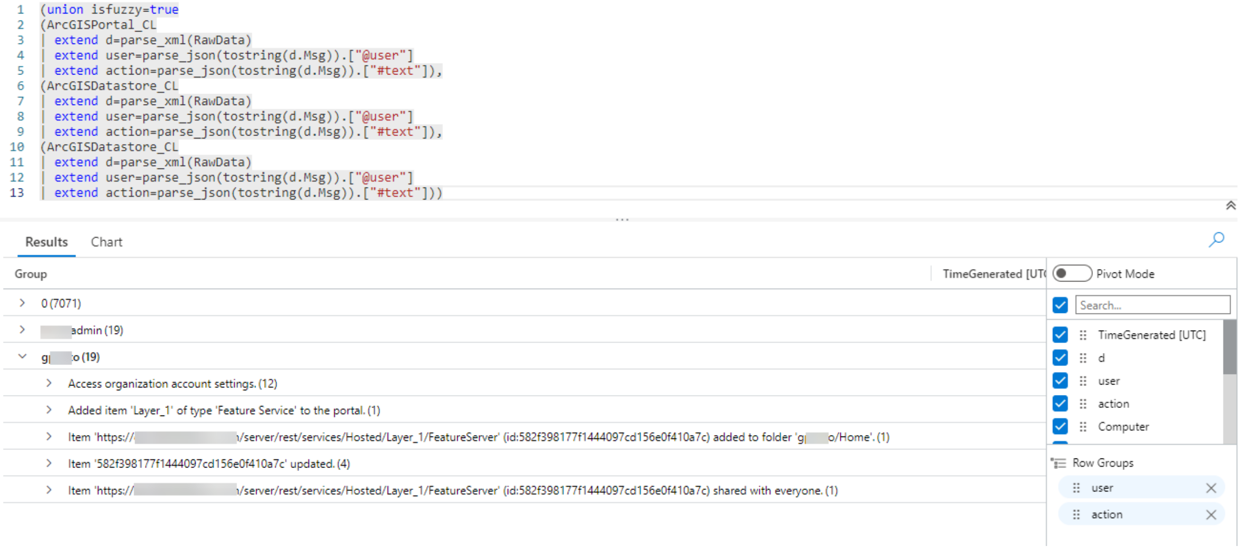


```
ArcGISPortal_CL
| union ArcGISServer_CL
| union ArcGISDatastore_CL
| extend d=parse_xml(RawData)
| search "sign"
```

Results Chart

	TimeGenerated [UTC]	d
>	3/30/2023, 7:56:20.030 PM	{"Msg":{"#text":" Sign in error: Invalid username or password specified for [redacted]admin'.",...
>	3/30/2023, 7:52:37.657 PM	{"Msg":{"#text":" Sign in error: Invalid username or password specified for [redacted]admin'.",...
>	3/30/2023, 10:55:18.921 PM	{"Msg":{"#text":" Sign in error: Invalid username or password specified for [redacted]admin'.",...
>	3/30/2023, 10:55:18.921 PM	{"Msg":{"#text":" Sign in error: Invalid username or password specified for [redacted]admin'.",...
>	3/30/2023, 10:55:18.921 PM	{"Msg":{"#text":" Sign in error: Invalid username or password specified for [redacted]admin'.",...
>	3/30/2023, 10:55:18.937 PM	{"Msg":{"#text":" Sign in error: Invalid username or password specified for [redacted]admin'.",...

Monitoring user activity in SIEM tools like Microsoft Sentinel is eased through KQL (Kusto Query Language) parsing and query structures:

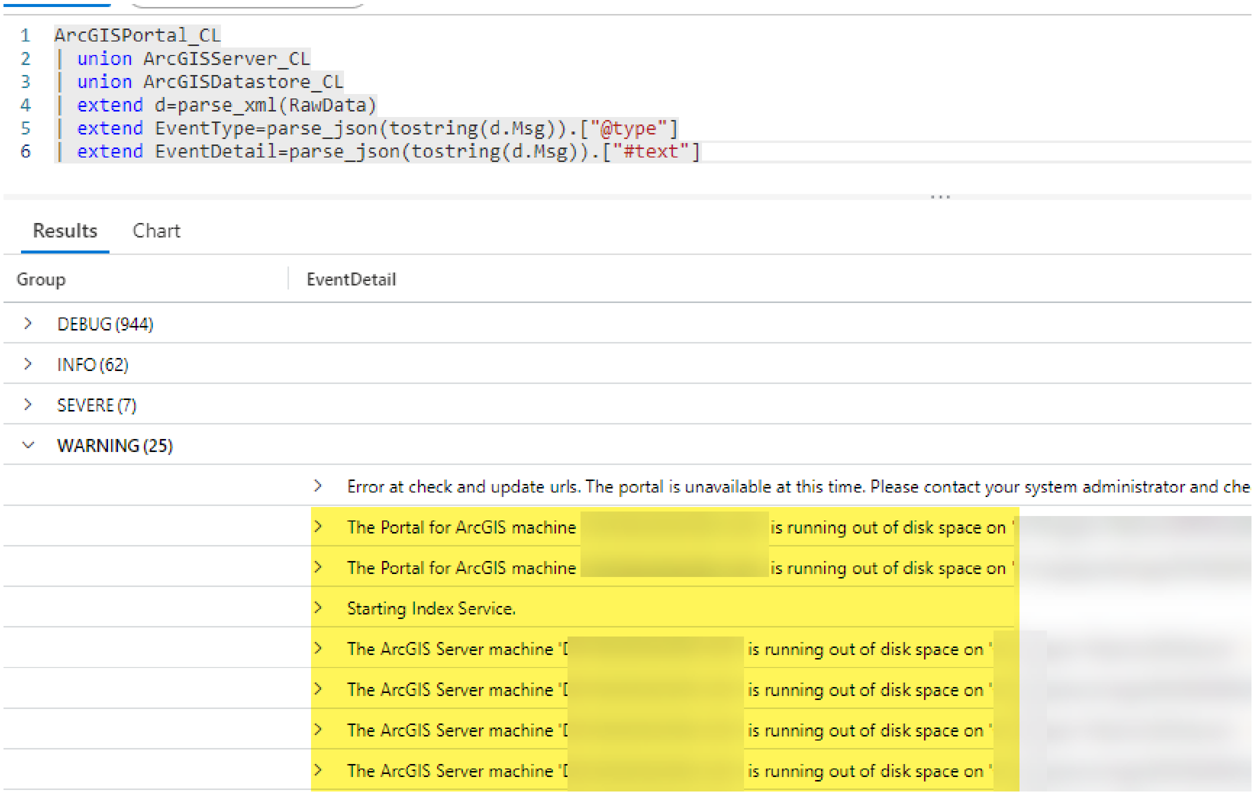


```
(union isfuzzy=true
(ArcGISPortal_CL
| extend d=parse_xml(RawData)
| extend user=parse_json(tostring(d.Msg)).["@user"]
| extend action=parse_json(tostring(d.Msg)).["#text"]),
(ArcGISDatastore_CL
| extend d=parse_xml(RawData)
| extend user=parse_json(tostring(d.Msg)).["@user"]
| extend action=parse_json(tostring(d.Msg)).["#text"]),
(ArcGISDatastore_CL
| extend d=parse_xml(RawData)
| extend user=parse_json(tostring(d.Msg)).["@user"]
| extend action=parse_json(tostring(d.Msg)).["#text"]))
```

Results Chart

```
Group                                                                                    TimeGenerated [UT(
>  0 (7071)
>  [redacted]admin (19)
v  g[redacted]o (19)
     >  Access organization account settings. (12)
     >  Added item 'Layer_1' of type 'Feature Service' to the portal. (1)
     >  Item 'https://[redacted]/server/rest/services/Hosted/Layer_1/FeatureServer' (id:582f398177f1444097cd156e0f410a7c) added to folder 'g[redacted]o/Home'. (1)
     >  Item '582f398177f1444097cd156e0f410a7c' updated. (4)
     >  Item 'https://[redacted]/server/rest/services/Hosted/Layer_1/FeatureServer' (id:582f398177f1444097cd156e0f410a7c) shared with everyone. (1)
```

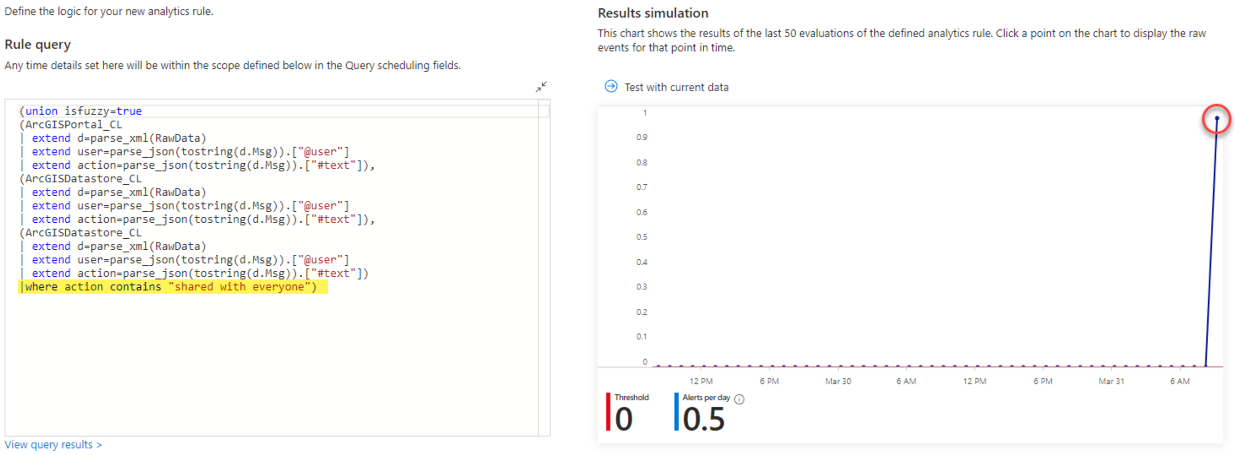
It is also possible to parse the log structure output from ArcGIS Enterprise to expose actionable operational events that could affect the availability of ArcGIS Enterprise:



```
ArcGISPortal_CL
| union ArcGISServer_CL
| union ArcGISDatastore_CL
| extend d=parse_xml(RawData)
| extend EventType=parse_json(tostring(d.Msg)).["@type"]
| extend EventDetail=parse_json(tostring(d.Msg)).["#text"]
```

Group	EventDetail
DEBUG (944)	
INFO (62)	
SEVERE (7)	
WARNING (25)	
	Error at check and update urls. The portal is unavailable at this time. Please contact your system administrator and che
	The Portal for ArcGIS machine [redacted] is running out of disk space on ' [redacted]
	The Portal for ArcGIS machine [redacted] is running out of disk space on ' [redacted]
	Starting Index Service.
	The ArcGIS Server machine '[redacted] is running out of disk space on ' [redacted]
	The ArcGIS Server machine '[redacted] is running out of disk space on ' [redacted]
	The ArcGIS Server machine '[redacted] is running out of disk space on ' [redacted]
	The ArcGIS Server machine '[redacted] is running out of disk space on ' [redacted]

Beyond just querying and threat hunting, these queries can be organized by advanced tools such as Microsoft Sentinel to generate Incidents for security and operations teams to take action against potential threats:



Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
(union isfuzzy=true
(ArcGISPortal_CL
| extend d=parse_xml(RawData)
| extend user=parse_json(tostring(d.Msg)).["@user"]
| extend action=parse_json(tostring(d.Msg)).["#text"]),
(ArcGISDatastore_CL
| extend d=parse_xml(RawData)
| extend user=parse_json(tostring(d.Msg)).["@user"]
| extend action=parse_json(tostring(d.Msg)).["#text"]),
(ArcGISDatastore_CL
| extend d=parse_xml(RawData)
| extend user=parse_json(tostring(d.Msg)).["@user"]
| extend action=parse_json(tostring(d.Msg)).["#text"])
|where action contains "shared with everyone")
```

Results simulation

This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

The above query will create an incident any time a service is shared with everyone—the most common source of unexpected data spillage.

The above guidance utilized Microsoft Sentinel to demonstrate SIEM ingestion capabilities with ArcGIS Enterprise, documented in the following:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-custom-logs
- https://learn.microsoft.com/en-us/azure/azure-monitor/logs/parse-text
- https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom

  However, this is possible with any modern SIEM system that supports file-based data ingestion and structured query reporting.

Appendix F: Case Studies: Misconfiguration Impacts

Case Study 1: Smalltown USA School District

- A GIS Publisher is tasked with publishing a spreadsheet containing student names, addresses, and parent contact details to ArcGIS Enterprise. These are converted to hosted feature layers and analyzed to create centralized bus stops within walking distance from each address. Details for each stop then support creating efficient routes for school buses to follow.
- Unrecognized by the GIS Publisher, in addition to potentially sensitive information (PII) associated with members of each household, some records contain details related to the disabilities of exceptional children (PHI) that is not strictly necessary for bus drivers to be aware of to perform their job function.
  - The GIS Publisher uploads the dataset and performs geocoding and other analyses to generate efficient stops and routing. They create a web mapping application, share the web map and the application with the public, and share the links to the application broadly.
- The next day, the school district administrators were surprised to learn of complaints from parents of school -age children in their district. They are upset that their family's PII and PHI are accessible to the public, and they have contacted the local media.
- The school district administrators must now manage the aftermath of this leak.

Case Study 2: Underwater Resource Exploration, Inc.

- A contractor for Bigtime Underwater Resource Exploration, Inc., is hired to collect locations and attributes associated with proprietary assets critical to their operations. These sensitive details are operationally critical and would be devastating to the company were these details leaked to competitors.
- ArcGIS Enterprise and ArcGIS Client applications are leveraged to assist with data collection, feature storage, analysis, presentation, and sharing.
- The contractor needs to share some nonsensitive fields in the data that they have collected with other stakeholders who are not authorized with credentials to access ArcGIS Enterprise.
  - To support this requirement, the contractor creates a web map using the original feature layer that represents the entirety of the collected data and configures pop-ups to hide sensitive fields and only show selected fields when features are clicked.
  - Because the contractor believes the sensitive fields are hidden at the data source *and* in the configured web map, they share the content with the public so that the external stakeholders may review it.
- The next day, the contractor is surprised to learn of complaints from their employer that sensitive proprietary information has been shared with the public and may have been exported by their competitors. They are threatening to sue the contractor for breach of contract.

Case Study 3: National Police Force

- A contact form created with ArcGIS Survey123 was used to gauge the interest of officers in attending a webinar provided by their host organization. The form collected information such as the officers' full names, regiments, professional email addresses, positions/roles, ranks, telephone numbers, and unit postal addresses.
- While Survey123 offers a secure by default stance, the provided defaults were overridden. and the Survey123 result layer was configured to be accessible by the public, which exposed the sensitive details that were collected.
- The exposed layer was discovered by a media group that discusses hacking, information security, and technology. The media group wrote an embarrassing exposé highlighting and describing the unintentionally leaked PII details.
  Training and a robust ArcGIS content publication review flow would have prevented the above issues.

Appendix G: Security Features by Release

Each release of ArcGIS Enterprise brings new security improvements as a direct response to the evolving security landscape of web services. The table below delineates each security feature incorporated into the key components that make up ArcGIS Enterprise (Portal for ArcGIS, ArcGIS Server, and ArcGIS Data Store).

Table 32—ArcGIS Enterprise Security Features by Release

Product	*Version*	*Security Features*
ArcGIS Data Store	11.5	Following ports no longer required on object store machines TCP 9840, 9830, 9820 – HTTP 9880, 29882, 29878, 29876, 29874 – HTTPS 29883, 29877, 29875
ArcGIS Data Store	11.5	Replacing SSL cert for relational data store no longer fails when SAN and CN different
ArcGIS Data Store	11.4	Support for HTTP Strict Transport Security (HSTS) headers
ArcGIS Data Store	11.2	Opensearch utilizes HTTPS
ArcGIS Data Store	11.2	Object store backup support added
ArcGIS Data Store	11.1	Add a timestamp to the db log in ArcGIS Data Store
ArcGIS Data Store	11.0	Support for service webhooks added
ArcGIS Data Store	11.0	Installer improved to only place files on machine that are selected by customer
ArcGIS Data Store	11.0	New utility to clean up unused files on disk
ArcGIS Data Store	11.0	Improve IPv6 support
ArcGIS Data Store	11.0	3rd party component updates
ArcGIS Data Store	10.9.1	3rd party component updates
ArcGIS Data Store	10.9.1	Use sha256 checksums for patches
ArcGIS Data Store	10.9.1	Patch Notification tool validates patch checksums
ArcGIS Data Store	10.9.1	TLS 1.3 support
ArcGIS Data Store	10.9.1	Native support for ECDHE based cipher suites
ArcGIS Data Store	10.9.1	Improved tile cache data store signature algorithm for certificate
ArcGIS Data Store	10.8.1	3rd party component updates
ArcGIS Data Store	10.8.1	Improved cipher support for tile cache data stores
ArcGIS Data Store	10.7.1	Default HTTPS
ArcGIS Data Store	10.7.1	Default TLS 1.2
ArcGIS Data Store	10.7.1	Disable default support for DHE ciphers
Portal for ArcGIS	11.5	Manage delete protection settings for multiple items owned by same org member
Portal for ArcGIS	11.5	Add database data store that accesses data in Snowflake using key-pair auth.
Portal for ArcGIS	11.5	New Content Security Policy (CSP) enforcement for sharing directory reduces XSS attacks
Portal for ArcGIS	11.5	Check certificate and cipher compatibility when making changes
Portal for ArcGIS	11.4	Support for defining a Content-Security-Policy header in for embedded web applications.
Portal for ArcGIS	11.4	Portal for ArcGIS security scan script to provide suggestions for allowedProxyHosts
Portal for ArcGIS	11.4	Add support for CHACHA cipher suites
Portal for ArcGIS	11.4	SIEM readable audit logs
Portal for ArcGIS	11.4	Customize username values when manually adding OpenID Connect (OIDC) accounts
Portal for ArcGIS	11.4	Classification schema administration allows data classification based on sensitivity levels

Portal for ArcGIS	11.3	The .NET 8-based ArcGIS Web Adaptor (IIS) requires ASP.NET Core Runtime - Windows Hosting Bundle 8.x
Portal for ArcGIS	11.3	Block members' access to some of the applications that are included with user types and that cannot be controlled through licenses, settings, or privileges
Portal for ArcGIS	11.3	Custom role that allows members to create and manage administrative reports
Portal for ArcGIS	11.3	New authentication methods are available when you add a cloud storage data store in Microsoft Azure
Portal for ArcGIS	11.3	Pre-invite OpenID Connect users from Microsoft Entra ID
Portal for ArcGIS	11.3	Use Microsoft Graph API to retrieve Microsoft Entra SAML group memberships > than 150
Portal for ArcGIS	11.3	Automatically import the root and intermediate certificates from a web server certificate’s trust chain as trusted root/intermediate authorities
Portal for ArcGIS	11.2	Delete member transfers content to another member
Portal for ArcGIS	11.2	Additional cloud-native authentication methods for data stores
Portal for ArcGIS	11.2	Allow access to secured services via forward proxy using authentication
Portal for ArcGIS	11.2	Administrator can configure default username format for adding built-in members
Portal for ArcGIS	11.1	Install and configure a new .NET 6 based ArcGIS Web Adaptor (IIS Only).
Portal for ArcGIS	11.1	Assign member categories when adding new members to the organization or specify a default set of member categories to automatically assign to new members when they join.
Portal for ArcGIS	11.1	Error handling processes when adding members in bulk to your organization using a .csv file improved.
Portal for ArcGIS	11.1	Configure member categories for the organization with Manage categories privilege.
Portal for ArcGIS	11.1	Scan your portal for Active Directory or LDAP members that no longer have active domain accounts using the AD_LDAP_Users.py Python script.
Portal for ArcGIS	11.1	Change the ownership of a report schedule to another default administrator.
Portal for ArcGIS	11.1	New privilege: Share member content with organization
Portal for ArcGIS	11.1	New privilege: Share member content with public
Portal for ArcGIS	11.0	Update log4j to address security vulnerabilities.
Portal for ArcGIS	11.0	Configure advanced portal options through the ArcGIS Portal Directory (Sharing API)
Portal for ArcGIS	11.0	Restrict member access to only approved external apps for enhanced security in the organization.
Portal for ArcGIS	11.0	Schedule administrative reports to run automatically
Portal for ArcGIS	11.0	Scan your portal for operational health issues using the included operationalHealth.py Python script.
Portal for ArcGIS	11.0	Specify a list of 3rd party apps approved for member access
Portal for ArcGIS	11.0	Allow approved 3rd party apps in app launcher
Portal for ArcGIS	10.9.1	Improved default encryption algorithm support
Portal for ArcGIS	10.9.1	MFA support for built-in logins
Portal for ArcGIS	10.9.1	support for SASL communication with Active Directory
Portal for ArcGIS	10.9.1	Improvements to non-proxy hosts property
Portal for ArcGIS	10.9.1	Provide admin option to enable or disable KML and RSS servlet
Portal for ArcGIS	10.9.1	Disable portal Legends and Print Servlets
Portal for ArcGIS	10.9.1	httpOnly attribute set on authorization cookie
Portal for ArcGIS	10.9.1	admin option to disable the WFS servlet
Portal for ArcGIS	10.9.1	Use strong encryption to obfuscate credentials displayed in system security properties
Portal for ArcGIS	10.9.1	TLS 1.3 support
Portal for ArcGIS	10.9.1	3rd party component updates

Portal for ArcGIS	10.9.1	Improvements to portalScan.py
Portal for ArcGIS	10.9.1	Use sha256 checksums for patches
Portal for ArcGIS	10.9.1	PatchNotification tool validates patch checksums
Portal for ArcGIS	10.9.1	Various Security Bug fixes
Portal for ArcGIS	10.9.1	Removed reliance on plain-text esri_auth cookie in favor of esri_aopc cookie
Portal for ArcGIS	10.9.1	Improved enterprise email functionality
Portal for ArcGIS	10.9.1	Improvements to forward proxy connection string encryption
Portal for ArcGIS	10.9.1	Improvements for webhooks trigger events
Portal for ArcGIS	10.8.1	Support for X-Content-Type-Options: NOSNIFF introduced
Portal for ArcGIS	10.8.1	Support Admin Privileges for custom roles
Portal for ArcGIS	10.8.1	Webhooks introduced to monitor activity for your portal items, users, and groups
Portal for ArcGIS	10.8.1	Default HTTPS
Portal for ArcGIS	10.8.1	Native HSTS Support
Portal for ArcGIS	10.8.1	TLS 1.2 required by default
Portal for ArcGIS	10.8.1	Enterprise logins: LDAP/AD: enforce encrypted communication between Portal for ArcGIS and Active Directory
Portal for ArcGIS	10.8.1	Org Specific logins: SAML
Portal for ArcGIS	10.8.1	Support for X-Esri-Authorization Header
Portal for ArcGIS	10.8.1	Support for defining allowed CORS origins
Portal for ArcGIS	10.8.1	Support for limiting sharing proxy destinations
Portal for ArcGIS	10.8.1	ArcGIS Crypto Toolkit integration
Portal for ArcGIS	10.8.1	Disable default support for DHE ciphers
Portal for ArcGIS	10.8.1	portalScan.py
Portal for ArcGIS	10.8.1	MFA support for SAML logins via SAML provider
Portal for ArcGIS	10.8.1	maxTokenExpirationMinutes parameter to serve as both the default and max token expiration times for both the sharing/generateToken and oauth2/sign-in requests
Portal for ArcGIS	10.8.1	Support group membership managed by SAML provider
Portal for ArcGIS	10.8.1	Password strength meter introduced
Portal for ArcGIS	10.8.1	Organization Specific Logins: Add support for OpenID connect
Portal for ArcGIS	10.8.1	MFA support via OpenID connect provider
Portal for ArcGIS	10.8.1	Improved default encryption algorithm support
Portal for ArcGIS	10.8.1	Managed Service Account Support
Portal for ArcGIS	10.8.1	Fine grained privilege support in custom roles
Portal for ArcGIS	10.8.1	Incorporate banned password list
Portal for ArcGIS	10.8.1	Enterprise email integration introduced
Portal for ArcGIS	10.8.1	Support for ArcGIS HTML Sanitizer
Portal for ArcGIS	10.8.1	3rd party component updates
Portal for ArcGIS	10.8.1	Improvements to portalScan.py
Portal for ArcGIS	10.8.1	Various Security Bug fixes
Portal for ArcGIS	10.8.1	Improvements for webhooks trigger events
Portal for ArcGIS	10.8.1	Ability to configure access notices
Portal for ArcGIS	10.8.1	Ability to configure information banner
Portal for ArcGIS	10.7.1	Support for X-Content-Type-Options: NOSNIFF introduced
Portal for ArcGIS	10.7.1	Support Admin Privileges for custom roles

Portal for ArcGIS	10.7.1	Webhooks introduced to monitor activity for your portal items, users, and groups
Portal for ArcGIS	10.7.1	Default HTTPS
Portal for ArcGIS	10.7.1	Native HSTS Support
Portal for ArcGIS	10.7.1	TLS 1.2 required by default
Portal for ArcGIS	10.7.1	Enterprise logins: LDAP/AD: enforce encrypted communication between Portal for ArcGIS and Active Directory
Portal for ArcGIS	10.7.1	Org Specific logins: SAML
Portal for ArcGIS	10.7.1	Support for X-Esri-Authorization Header
Portal for ArcGIS	10.7.1	Support for defining allowed CORS origins
Portal for ArcGIS	10.7.1	Support for limiting sharing proxy destinations
Portal for ArcGIS	10.7.1	ArcGIS Crypto Toolkit integration
Portal for ArcGIS	10.7.1	Disable default support for DHE ciphers
Portal for ArcGIS	10.7.1	portalScan.py
Portal for ArcGIS	10.7.1	MFA support for SAML logins via SAML provider
Portal for ArcGIS	10.7.1	maxTokenExpirationMinutes parameter to serve as both the default and max token expiration times for both the sharing/generateToken and oauth2/signin requests
Portal for ArcGIS	10.7.1	Support group membership managed by SAML provider
Portal for ArcGIS	10.7.1	Password strength meter introduced
ArcGIS Server	11.5	Audit logs available for Server – Useful for SIEM event security awareness
ArcGIS Server	11.5	Add support for defining a Content-Security-Policy header for rest/services pages
ArcGIS Server	11.5	Support oAuth login in the Server administrator directory for federated servers
ArcGIS Server	11.4	GeoAnalytics Server retired
ArcGIS Server	11.4	Add support for CHACHA cipher suites
ArcGIS Server	11.3	Automatically import the root and intermediate certificates from a web server certificate's trust chain as trusted root/intermediate authorities
ArcGIS Server	11.2	HSTS Support added to ArcGIS Workflow Manager Server
ArcGIS Server	11.2	Linux deployments no longer incorrectly flag files as malware
ArcGIS Server	11.1	ArcMapServiceCheck tool generates an HTML report that provides details on the status of services using the ArcMap runtime that existed prior upgrading to ArcGIS Server 11+
ArcGIS Server	11.0	Update log4j to address security vulnerabilities.
ArcGIS Server	11.0	Enable or disable the ability to make JSONP callback requests
ArcGIS Server	11.0	End of support for ArcMap-based workflows which require Python 2.7.x
ArcGIS Server	11.0	Support for the use of PKCE during the authorization code exchange added
ArcGIS Server	11.0	CORS restrictions honored for SOAP web services
ArcGIS Server	11.0	CORS restrictions honored for OGC web services
ArcGIS Server	10.9.1	Improved default encryption algorithm support
ArcGIS Server	10.9.1	TLS 1.3 support
ArcGIS Server	10.9.1	3rd party component updates
ArcGIS Server	10.9.1	Improvements to serverScan.py
ArcGIS Server	10.9.1	Use sha256 checksums for patches
ArcGIS Server	10.9.1	Patch Notification tool validates patch checksums
ArcGIS Server	10.9.1	Various Security Bug fixes
ArcGIS Server	10.9.1	New option to NOT install Python 2.7 (ArcMap service runtime)
ArcGIS Server	10.8.1	Improved default encryption algorithm support

ArcGIS Server	10.8.1	Managed Service Account Support
ArcGIS Server	10.8.1	3rd party component updates
ArcGIS Server	10.8.1	Removed FLEX and Silverlight policy files
ArcGIS Server	10.8.1	Improvements to serverScan.py
ArcGIS Server	10.8.1	Various Security Bug fixes
ArcGIS Server	10.8.1	Support for ArcGIS HTML Sanitizer
ArcGIS Server	10.8.1	Support xssPreventionEnabled
ArcGIS Server	10.7.1	X-Content-Type-Options: NOSNIFF
ArcGIS Server	10.7.1	Default HTTPS only
ArcGIS Server	10.7.1	Default TLS 1.2 only
ArcGIS Server	10.7.1	Support for X-Esri-Authorization Header
ArcGIS Server	10.7.1	Native HSTS Support
ArcGIS Server	10.7.1	serverScan.py
ArcGIS Server	10.7.1	Disable default support for DHE ciphers
ArcGIS Server	10.7.1	XSSPrevention Rule introduced
ArcGIS Server	10.7.1	Standardized queries

Appendix H: Existing Deployment Control Prioritization

Existing ArcGIS Enterprise deployments should roll out security hardening controls in an incremental manner, ideally starting with the highest severity items being addressed first. As there are over 100 security controls in this guide, we've provided the following tables to help your rollout planning. Most customers will find the Basic profile security controls appropriate for ArcGIS Enterprise operations, but even if your organization determines the Advanced profile is your long-term objective, you will want to implement the Basic profile security controls first.

Secondarily, we have categorized the relative security and privacy severity of each control for a typical customer's ArcGIS Enterprise deployment. Controls are ranked Danger, Warning, and Info, with Danger being the most severe items to address first and so on down to Info. This means you can address the most severe concern by initially implementing just the first 20 controls in the table!

Descriptions for the table fields are as follows:

- **Guide Section –** An abbreviation for the corresponding section of this document the control can be found.
- **Security Control Name –** The action to be taken and security control name.
- **Esri or 3rd Party** – The control can be satisfied by configuring Esri's ArcGIS Enterprise, separately by a 3rd party offering, or by "Both" ArcGIS Enterprise and 3rd party offerings.
- **Default** – If the control is satisfied by the default configuration of ArcGIS Enterprise then "Yes" is listed, otherwise "No". Because configuration drift is a common significant issue for all software deployments, verifying settings are in place for your deployment is important even if the default is appropriate.
- **Portal Scan** – If the Portal for ArcGIS security control is checked by this tool, the corresponding rule identifier is listed (see details within the Maintenance and Inventory portalscan.py section).
- **Server Scan** - If the ArcGIS Server security control is checked by this tool, the corresponding rule identifier is listed (see details within the Maintenance and Inventory serverscan.py section).
- **Security Adviser** – The Security & Privacy Adviser tool is available within the ArcGIS Trust Center, controls checked by this tool are listed as Yes (see details within the Maintenance and Inventory Security & Privacy Adviser Tool section).
- **Privacy & Security** – Labeled with the criticality for a typical ArcGIS Enterprise deployment.

Getting Started

With this information, you can now work your way top down implementing the **Basic** profile controls listed in Table 33 below, so instead of trying to implement 100+ security controls at the same time, you can start with the top 27 critical controls (listed as Danger), then work through Warning, then Info, depending on your organizations risk posture.

The **Basic** profile controls are adequate security assurance for the majority of Esri customers with minimal usability impact. However, if your organization requires more rigorous compliance controls that result in reduced capability and usability, the **Advanced** profile controls can also be deployed based on criticality as listed in Table 34 below.

*Table 33-**BASIC** Profile Security Controls Sorted by Severity*

Guide Section	Security Control Name	Esri or 3rd Party	Default	Portal Scan	Server Scan	Security Advisor	Privacy	Security
App Sec	Implement Email Notification for Password Reset Workflows	Both	No	-	-	-	Danger	Danger
App Sec	Verify “Filter Web Content” is Enabled for all Feature Services	Esri	Yes	-	SS05	-	Danger	Danger
App Sec	Verify Standardized Queries are Enabled	Esri	Yes	-	SS02	Yes	Danger	Danger
App Sec	Verify Server System Services Secured	Esri	Yes	-	SS06 & SS15	-	Danger	Danger
App Sec	Verify Token Acquisition via HTTP GET is Disabled	Esri	Yes	PS02	SS03	-	Danger	Danger
App Sec	Verify Portal for ArcGIS Legend Servlet is Disabled	Esri	No	-	-	-	Danger	Danger
App Sec	Verify Portal for ArcGIS Print Servlet is Disabled	Esri	No	-	-	-	Danger	Danger
App Sec	Verify Portal for ArcGIS WFS Servlet is Disabled	Esri	No	-	-	-	Danger	Danger
ID & Access	Implement Personal Secrets Management	3rd Party	No	-	-	-	Danger	Danger
ID & Access	Configure All Administrator Accounts with Multi-Factor	Both	No	-	-	Yes	Danger	Danger
ID & Access	Implement SAML Signed and Encrypted Assertions	Both	No	PS13	-	-	Danger	Danger
ID & Access	Implement Group-Based Sharing	Esri	Yes	-	-	-	Danger	Danger
ID & Access	Manage Content via Role-based Access Control (RBAC)	Esri	Yes	-	-	-	Danger	Danger
Data Prot	Implement Whole Disk Encryption	3rd Party	No	-	-	-	Danger	Danger
Data Prot	Verify HTTPS is Enforced	Both	Yes	PS04	SS01	Yes	Danger	Danger
Data Prot	Implement Signed CA Certificates	3rd Party	No	PS08	SS14	-	Danger	Danger
Inv & Maint	Implement Security Patches within One Month	Both	No	-	-	-	Danger	Danger
Detect & Resp	Manage Webhooks	Esri	No	-	-	-	Danger	Danger
App Sec	Configure Password Policy for Built-in Accounts	Esri	Yes	-	-	Yes	Warning	Danger
App Sec	Verify Self-Creation of Built-In User Accounts is Disabled	Esri	Yes	PS05	-	-	Warning	Danger
ID & Access	Avoid Embedding User Identities in Scripts	3rd Party	No	-	-	-	Info	Danger
ID & Access	Avoid Embedding Application Identities in Client Applications	3rd Party	No	-	-	-	Info	Danger
ID & Access	Avoid Storing Secrets in Source Code	3rd Party	No	-	-	-	Info	Danger
Support Infra	Implement Web Application Firewall (WAF)	3rd Party	No	-	-	-	Info	Danger
ID & Access	Disable Public Sharing by Default	Esri	Yes	PS12	-	Yes	Danger	Info
ID & Access	Disable Public User Profile Sharing for organization users	Esri	No	-	-	Yes	Danger	Info
ID & Access	Configure Decentralized Profile Visibility	Esri	No	-	-	-	Danger	Info
App Sec	Verify Nosniff Header Enabled	Esri	Yes	-	-	-	Warning	Warning
App Sec	Disable Portal for ArcGIS Directory	Esri	No	PS03	-	-	Warning	Warning
App Sec	Disable ArcGIS Server Services Directory	Esri	No	-	SS07	-	Warning	Warning
App Sec	Remove Silverlight and FLEX Policy Files	Esri	Yes	-	-	-	Warning	Warning
App Sec	Verify Dynamic Workspaces/Layers for Map Services is Disabled	Esri	Yes	-	SS09	-	Warning	Warning
App Sec	Implement Group Managed Service Account (gMSA)	3rd Party	No	-	-	-	Warning	Warning
App Sec	Disable Primary Site Administrator (PSA) account (ArcGIS Server)	Esri	No	-	SS11	-	Warning	Warning
ID & Access	Implement Centralized User Account Management	3rd Party	No	-	-	Yes	Warning	Warning
ID & Access	Implement Custom Roles	Esri	No	-	-	-	Warning	Warning
ID & Access	Configure New Member Default Role as Viewer	Esri	No	-	-	-	Warning	Warning
ID & Access	Configure Least Privilege User Types and Roles	Esri	No	-	-	-	Warning	Warning
ID & Access	Configure Default Group Membership Assignments	Esri	No	-	-	-	Warning	Warning
ID & Access	Implement GIS Data Publication Management Process	Both	No	-	-	-	Warning	Warning
ID & Access	Consider using Feature Layer Views	Esri	No	-	-	-	Warning	Warning
ID & Access	Consider Publication Governance Delivery Pipelines	Both	No	-	-	-	Warning	Warning
ID & Access	Consider Defining content access requirements	Both	No	-	-	-	Warning	Warning
ID & Access	Verify content ownership rights	Both	No	-	-	-	Warning	Warning
ID & Access	Manage accounts and reduce user permissions	Both	No	-	-	-	Warning	Warning
ID & Access	Implement permission guardrails	Both	No	-	-	-	Warning	Warning
ID & Access	Manage access based on employee or project lifecycle	Both	No	-	-	-	Warning	Warning
Data Prot	Implement Backup Strategy and Test Regularly	Both	No	-	-	-	Warning	Warning
Data Prot	Implement Database Transparent Data Encryption (TDE)	3rd Party	No	-	-	-	Warning	Warning
Data Prot	Configure HTTP Strict Transport Security (HSTS) Enforcement	Both	No	-	-	-	Warning	Warning
Inv & Maint	Manage Vulnerable Components with Patching	Both	No	-	-	-	Warning	Warning
Inv & Maint	Configure Subscription to Vendor Patch Notifications	Esri	No	-	-	-	Warning	Warning
Inv & Maint	Manage Configuration Drift	Both	No	-	-	-	Warning	Warning
Detect & Resp	Implement Vulnerability Scanning Tools	3rd Party	No	-	-	-	Warning	Warning
App Sec	Configure Access Notice and/or Information Banners	Esri	No	-	-	-	Info	Warning
Support Infra	Implement Vendor Security Baselines	Both	No	-	-	-	Info	Warning
Support Infra	Implement Network segmentation	3rd Party	No	-	-	-	Info	Warning
Support Infra	Consider Not Utilizing the ArcGIS Web Adaptor	3rd Party	No	-	-	-	Info	Warning
Data Prot	Consider File Geodatabases	Esri	No	-	-	-	Info	Warning
Inv & Maint	Implement and Maintain Software Inventory	3rd Party	No	-	-	-	Info	Warning
Detect & Resp	Implement Security information and Event Management (SIEM)	3rd Party	No	-	-	-	Info	Warning
Train Guid	Manage frequent and ongoing awareness activities	Both	No	-	-	-	Info	Warning
App Sec	Consider Disabling Anonymous Access	Esri	No	PS06	-	Yes	Warning	Info
ID & Access	Disable “show social media links on item and group pages”	Esri	Yes	-	-	Yes	Warning	Info
Privacy	Consider Data Anonymization	Both	No	-	-	-	Warning	Info
Inv & Maint	Manage Only General Availability (GA) Product Versions	Both	No	-	-	-	Info	Info
Detect & Resp	Implement a CSIRT Process	3rd Party	No	-	-	-	Info	Info
Train Guid	Implement Training users by role and responsibility	Both	No	-	-	-	Info	Info

*Table 34-**ADVANCED** Profile Security Controls Sorted by Severity*

Guide Section	Security Control Name	Esri or 3rd Party	Default	Portal Scan	Server Scan	Security Advisor	Privacy	Security
ID & Access	Implement Organization Secrets Management	3rd Party	No	-	-	-	Danger	Danger
ID & Access	Configure All User Accounts with MFA	Both	No	-	-	Yes	Danger	Danger
Data Prot	Configure Hardened TLS Algorithms	Both	Yes	PS04	SS01	Yes	Danger	Danger
ID & Access	Manage Distributed Collaborations Securely	Esri	No	-	-	-	Warning	Danger
Support Infra	Configure Portal for ArcGIS Proxy Allow List – Client-side	Esri	No	PS01	-	-	Warning	Danger
ID & Access	Implement Developer IDE-integrated Secrets Management	3rd Party	No	-	-	-	Info	Danger
App Sec	Verify Utility Service External System Dependencies Approved	Esri	Yes			-	Danger	Info
ID & Access	Implement a Central Profile Policy	Esri	No	-	-	-	Danger	Info
App Sec	Configure token expiration to align to organization policy	Esri	Yes	-	-	-	Warning	Warning
App Sec	Consider Disabling KML and GeoRSS Servlets	Esri	No	-	-	-	Warning	Warning
App Sec	Remove Initial Admin (IAA) Account (Portal for ArcGIS)	Esri	No	-	-	-	Warning	Warning
ID & Access	Disable ArcGIS Logins	Esri	No	-	-	Yes	Warning	Warning
ID & Access	Configure SAML/OIDC Identity Provider Lockouts	3rd Party	Yes	-	-	-	Warning	Warning
ID & Access	Configure SAML Group Membership	Both	No	-	-	-	Warning	Warning
ID & Access	Consider Disabling Item Comments	Esri	No	-	-	-	Warning	Warning
Support Infra	Configure Cross-Origin-Resource-Sharing (CORS) Allow List	Esri	No	PS09	SS08	Yes	Warning	Warning
Support Infra	Implement Content-Security-Policy (CSP)	3rd Party	No	-	-	-	Warning	Warning
Data Prot	Implement Data Segmentation	Both	No	-	-	-	Warning	Warning
Data Prot	Disable “Mixed Mode” SQL Server Authentication	3rd Party	No	-	-	-	Warning	Warning
Detect & Resp	Consider ArcGIS Monitor	Esri	No	-	-	-	Warning	Warning
ID & Access	Implement Identity Provider Strong Credential Flow	3rd Party	No	-	-	-	Info	Warning
ID & Access	Implement Certificate-based Authentication (PKI/PIV/CAC)	3rd Party	No	-	-	-	Info	Warning
Support Infra	Implement Advanced Benchmarks	Both	No	-	-	-	Info	Warning
Support Infra	Consider Identity Secure Web Gateways (SWG)	3rd Party	No	-	-	-	Info	Warning
Support Infra	Consider Allow Listing File Extensions	3rd Party	No	-	-	-	Info	Warning
Support Infra	Implement Intermachine Network Restrictions	3rd Party	No	-	-	-	Info	Warning
Support Infra	Implement Network Intrusion Detection System (NIDS)	3rd Party	No	-	-	-	Info	Warning
Support Infra	Implement Administrative Network Segments	Both	No	-	-	-	Info	Warning
Prvicacy	Disable or Location Lock Clients with EUEI Analytics	Esri	Yes	-	-	Yes	Warning	Info
Support Infra	Disable Web Tier Technology Identifiers and Banners	3rd Party	Yes	-	-	-	Info	Info
Data Prot	Consider FIPS 140-2 Encryption	Both	No	-	-	-	Info	Info
Data Prot	Consider Server Object Interceptors (SOI) for Unique	Esri	No	-	-	-	Info	Info
Data Prot	Remove “PUBLIC” access to Enterprise Geodatabase	Both	No	-	-	-	Info	Info
Inv & Maint	Manage Software Inventory through Automation	Both	No	-	-	-	Info	Info
Inv & Maint	Remove Superfluous Components	Both	No	-	-	-	Info	Info
Inv & Maint	Implement Separation of Monolithic Systems	Both	No	-	-	-	Info	Info

Appendix I: Load-balancer Rules When NOT Utilizing Web Adaptor

When not utilizing the web adaptor it is important to properly configure the load balancer rules. This workflow will describe how to properly configure the Azure Application Gateway – a layer 7 load balancer - with a single machine ArcGIS Enterprise deployment in Azure.

Considerations:

1. It is recommended that this workflow is done prior to federating the ArcGIS Enterprise deployment.
   - It is possible to successfully integrate the workflow after federating; however, there is a higher risk for unforeseen errors to occur.
2. This workflow requires a DNS alias
3. Ensure that all necessary ArcGIS Enterprise ports are open on the host machine. Refer to Appendix K for more information.

Summary of the workflow:

Option 1 Automated:

1. Utilize the ArcGIS Enterprise Cloudbuilder to automate the creation of an ArcGIS Enterprise deployment that uses a load balancer.
   a. Note that some configuration options may be limited, such as flexibility with the DNS alias.

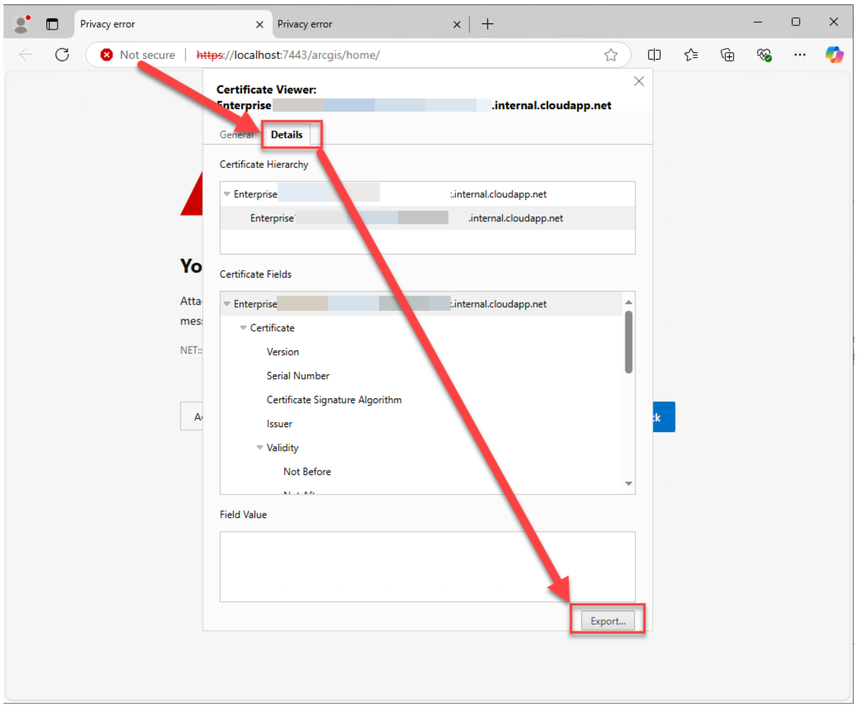
Option 2 Manual:

1. Deploy the host. Ensure all required ports are open.
   a. Manual configuration allows more flexible deployments.
      i. The detailed workflow represents manual deployment activities.
2. Configure the necessary DNS records.
3. Install and configure the Portal for ArcGIS and ArcGIS Enterprise Server.
4. Retrieve the necessary certificates.
5. Create and configure the Azure application gateway.
6. Change the ArcGIS Enterprise Web Context URLs
7. If federated – change the ArcGIS Server URLs.

Detailed workflow:

1. Install and configure the ArcGIS Enterprise deployment
2. Ensure the machine hosting ArcGIS Enterprise has the necessary ArcGIS Enterprise Ports open.
3. Configure the necessary DNS records. Once the Application Gateways public IP address is created associate it with the A Record.
4. Obtain a certificate file in .pfx format. A .pfx file, or Personal Information Exchange file, is a binary file that stores an SSL certificate and its private key. The Certificate’s CN attribute should match the DNS alias you’ve chosen. This will be needed when creating the Azure Application Gateway.
5. Download the ArcGIS Enterprise root certificates.

- There will be 2 certificates needed, 1 for the ArcGIS Enterprise Portal and 1 for the ArcGIS Server. These will be needed in later steps when configuring the Application Gateway. To download the machine's root certificate, do the following:
- Sign into the machine where ArcGIS Enterprise is hosted.
- Open a browser and search "https://localhost:7443/arcgis/home/" to access Portal for ArcGIS



Certificate Viewer: Enterprise[redacted].internal.cloudapp.net

Certificate Hierarchy

Enterprise[redacted].internal.cloudapp.net

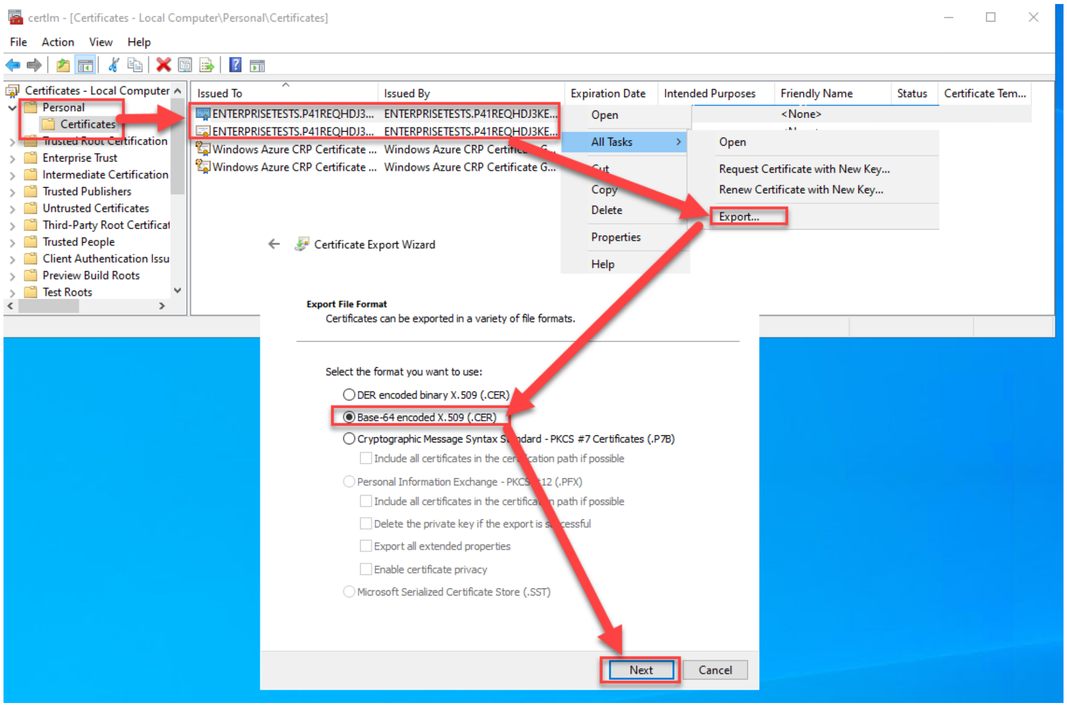
Enterprise[redacted].internal.cloudapp.net

Certificate Fields

Enterprise[redacted].internal.cloudapp.net
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before

Field Value

- Open the certificates details in the browser > Click the "Details" tab > Click the "Export" button and download the certificate.
- Right-Click the certificate downloaded > select "Install certificate" > install the certificate in the "Personal" certificate store.


certlm - [Certificates - Local Computer\Personal\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issu
Preview Build Roots
Test Roots
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
Status
Certificate Tem...
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Export...
Certificate Export Wizard
Next
Cancel

Issued To	Issued By	Friendly Name
ENTERPRISETESTS.P41REQHDJ3...	ENTERPRISETESTS.P41REQHDJ3KE...	<None>
ENTERPRISETESTS.P41REQHDJ3...	ENTERPRISETESTS.P41REQHDJ3KE...	
Windows Azure CRP Certificate ...	Windows Azure CRP Certifi... G...	
Windows Azure CRP Certificate ...	Windows Azure CRP Certificate G...	

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax S...dard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the cer...cation path if possible
○ Personal Information Exchange - PKCS ...12 (.PFX)
□ Include all certificates in the certifica...n path if possible
□ Delete the private key if the export is s...cessful
□ Export all extended properties
□ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

- Open the Windows Certificate Manager > navigate to the “Personal” certificate store > export the certificate in a Base-64 encoded X.509 (.CER) format.
    - i. *It is helpful to name the certificate after its respective ArcGIS Enterprise component i.e “PortalBackend.cer” or “ServerBackend.cer”*
- Repeat steps c-e to download the root certificate of the ArcGIS Server by navigating to the “https://localhost:6443/arcgis/manager/” site.

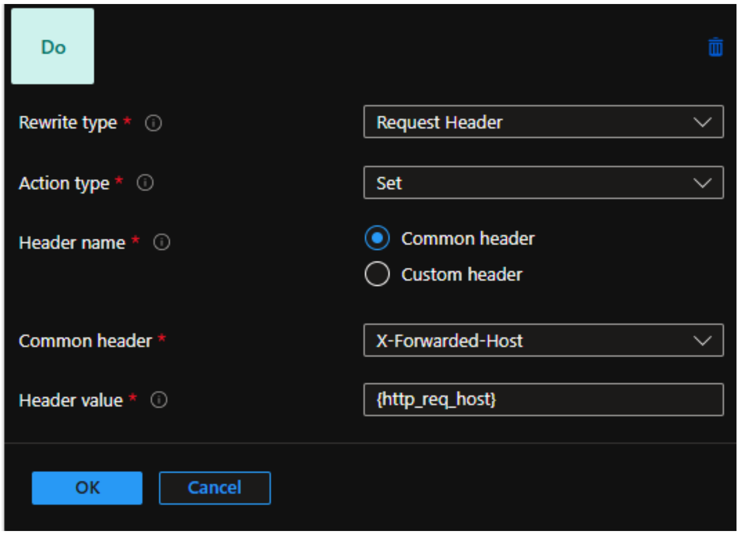
6. Using the Azure Portal, create an Application Gateway for the virtual machine with the following settings:
    - Ensure the Application gateway is in the same virtual network as the ArcGIS Enterprise machine, but in a different subnet.
    - Create a unique public IP address for the application gateway
    - Add 2 Backend Pools.
        - i. Pool 1 named: “PortalBackend”
        - ii. Pool 2 named “ServerBackend”
    - Configure both backend pools with the “Target Type” set to “IP address or FQDN”, and the “Target” set to the FQDN of the virtual machine:
    - Add a routing rule named “EnterpriseRequestRoutingRule” with the following details:
        - i. Set “Priority” to “10”
        - ii. Configure the Listener for the routing rule.
            1. Add a Listener named “HttpsListner”
            2. Set the “Frontend IP” to “Public IPv4”
            3. Set the “Protocol” to “HTTPS”
            4. Upload the DNS certificate created earlier
            5. Set the “Listener Type” to “Multi site” - “Single” and input the DNS alias created as the “Host name”
        - iii. Configure the Backend Targets for the routing rule

1. Set the “Target Type” to “Backend Pool”
2. Set the “Backend target” to the “ServerBackend” created earlier
3. For “Backend settings” add 2 new setting with the following configurations:
    a. Backend Setting 1:
        i. Name the backend setting “PortalHttpsSetting”
        ii. Set the “Backend protocol” to “HTTPS”
        iii. Set the “Backend port” to 7443
        iv. In “Upload Root CA certificate” upload the ArcGIS Portal certificate downloaded earlier
        v. Set “Connection draining” to “Enabled”
        vi. Set the “Request time-out” to “180”
        vii. Set “Override backend path” to “/arcgis/”
        viii. Set “Override with host name” to “Yes”
        ix. Set “Host name override” to “Pick host name from backend target”
        x. Set “Create custom Probes” to “Yes”
    b. Backend Setting 2:
        i. Name the backend setting “ServerHttpsSetting”
        ii. Set the “Backend protocol” to “HTTPS”
        iii. Set the “Backend port” to 6443
        iv. In “Upload Root CA certificate” upload the ArcGIS Server certificate downloaded earlier
        v. Set “Connection draining” to “Enabled”
        vi. Set the “Request time-out” to “180”
        vii. Set “Override backend path” to “/arcgis/”
        viii. Set “Override with host name” to “Yes”
        ix. Set “Host name override” to “Pick host name from backend target”
        x. Set “Create custom Probes” to “Yes”
4. Configure the “Path-based rules” for the routing rule by doing the following:
    a. Path Rule 1 Settings:
        i. When on the “Add a routing rule” page select “Add multiple targets to create a routing rule”
        ii. Set the “Target Type” to “Backend Pool”
        iii. Set the “Path” to “/server/*”
        iv. Set the “Target name” to “serverPathRule”
        v. Set the “Backend setting” to “ServerHttpsSetting”
        vi. Set the “Backend target” to “ServerBackend”
    b. Path Rule 2 Settings:
        i. When on the “Add a routing rule” page select “Add multiple targets to create a routing rule”
        ii. Set the “Target Type” to “Backend Pool”

iii. Set the "Path" to "/portal/*,/portal"
iv. Set the "Target name" to "portalPathRule"
v. Set the "Backend setting" to the "PortalHttpsSetting" that was created earlier
vi. Set the "Backend target" to the "PortalBackend"

- Add another routing rule named "HttpToHttpsRequestRoutingRule" with the following Settings:
  i. Set "Priority" to "20"
  ii. Configure the Listener for the routing rule.
    1. Add a Listener named "HttpListner"
    2. Set the "Frontend IP" to "Public IPv4"
    3. Set the "Protocol" to "HTTP"
    4. Set the "Listener Type" to "Multi site" - "Single" and input the DNS alias created as the "Host name"
  iii. Configure the Backend Targets for the routing rule
    1. Set the "Target type" to "Redirection"
    2. Set the "Redirection Type" to "Permanent"
    3. Set the "Redirection Target" to "Listener"
    4. Set the "Target Listener" to the "HttpsListner" created earlier
    5. Click "Add"
- Create the Application Gateway

7. After the Application Gateway is created configure the Rewrite rules with the following settings:
   - **Rewrite Rule 1:**
     i. Name the Rewrite rule "ServerRewriteRuleSet"
     ii. Set the "Associated routing rules" to ONLY select the "ServerPathRule" that was created earlier
     iii. In the "Rewrite rule configuration" page Add a rewrite rule named "XForwardHostRewrite" with these settings:



Do

Rewrite type * Request Header

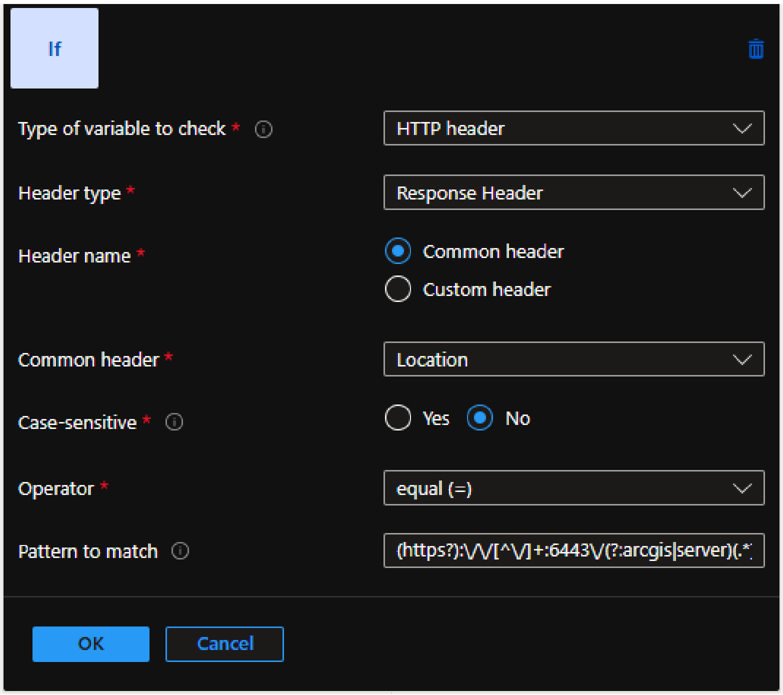
Action type * Set

Header name * ● Common header ○ Custom header

Common header * X-Forwarded-Host

Header value * {http_req_host}

     iv. Add another rewrite rule named "ServerRewrite" with the following settings:



If

Type of variable to check * HTTP header

Header type * Response Header

Header name * ● Common header ○ Custom header

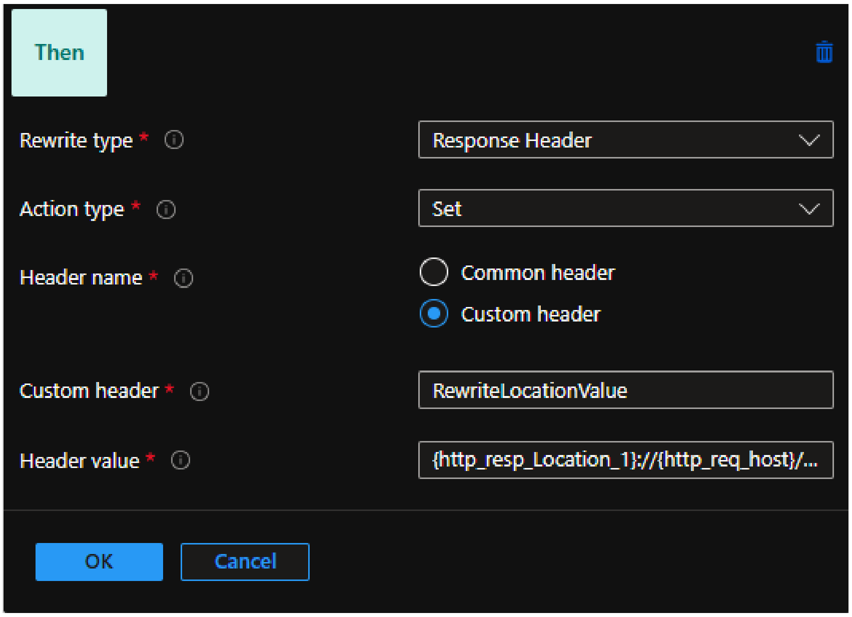
Common header * Location

Case-sensitive * ○ Yes ● No

Operator * equal (=)

Pattern to match (https?):\/\/[^\/]+:6443\/(?:arcgis|server)(.*

v. Where the “Pattern to Match” is set to “(https?):\/\/[^\/]+:6443\/(?:arcgis|server)(.*)$”



Then

Rewrite type * Response Header

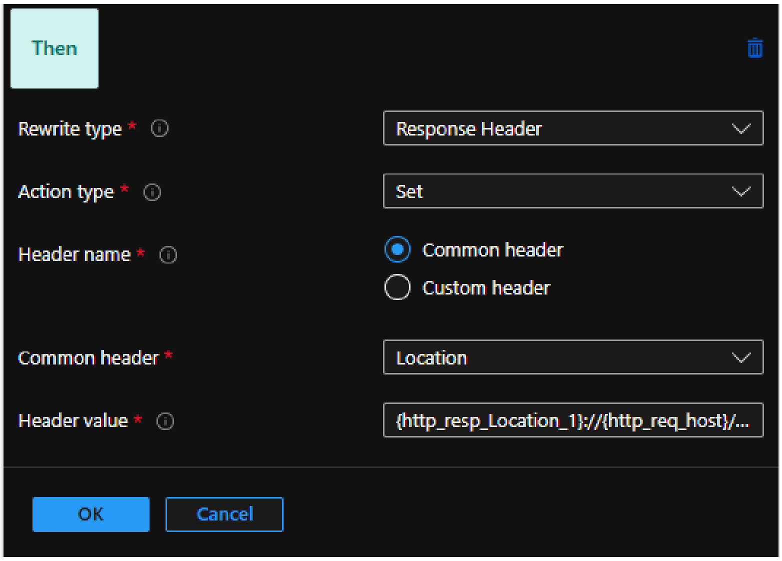
Action type * Set

Header name * ○ Common header ● Custom header

Custom header * RewriteLocationValue

Header value * {http_resp_Location_1}://{http_req_host}/...

vi. Where the “Header value” is set to “{http_resp_Location_1}://{http_req_host}/server{http_resp_Location_2}”



Then

Rewrite type * Response Header

Action type * Set

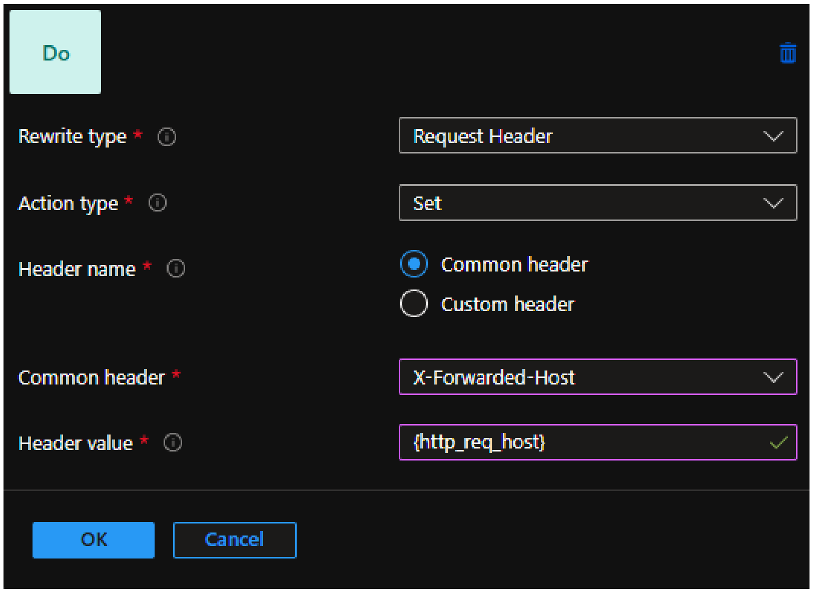
Header name * ● Common header ○ Custom header

Common header * Location

Header value * {http_resp_Location_1}://{http_req_host}/...

vii. Where the "Header value" is set to "{http_resp_Location_1}://{http_req_host}/server{http_resp_Location_2}"

- **Rewrite Rule 2:**
    i. Name the Rewrite rule "PortalRewriteRuleSet"
    ii. Set the "Associated routing rules" to ONLY select the "PortalPathRule" that was created earlier
    iii. In the "Rewrite rule configuration" page Add a rewrite rule named "XForwardHostRewrite" with the following settings:



Do

Rewrite type * Request Header

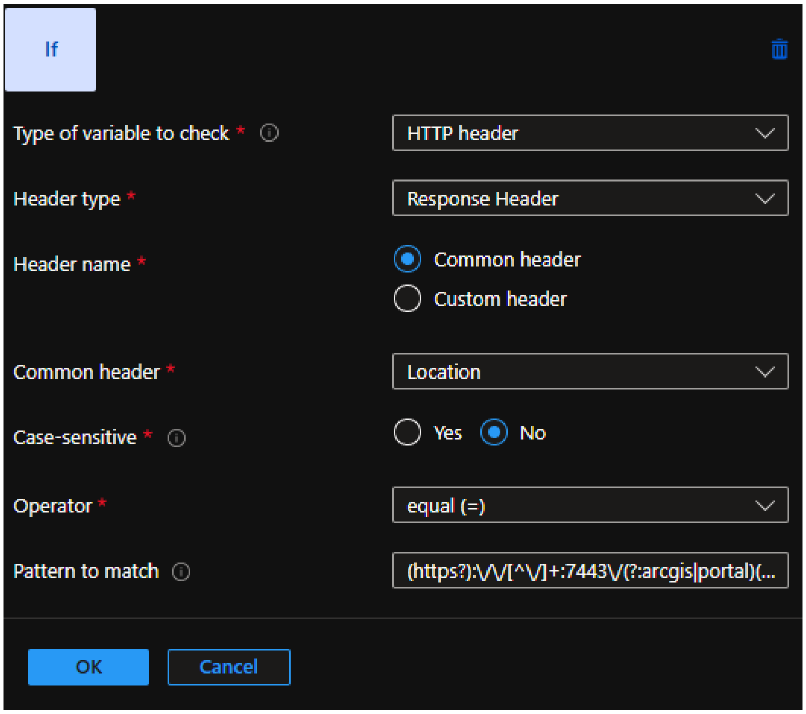
Action type * Set

Header name * ● Common header ○ Custom header

Common header * X-Forwarded-Host

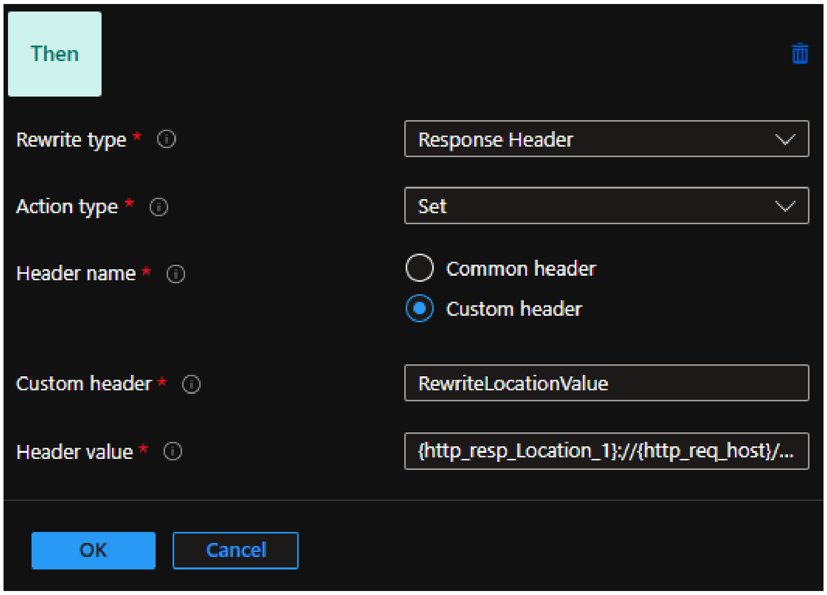
Header value * {http_req_host}

iv. Add another rewrite rule named "PortalRewrite" with the following settings:



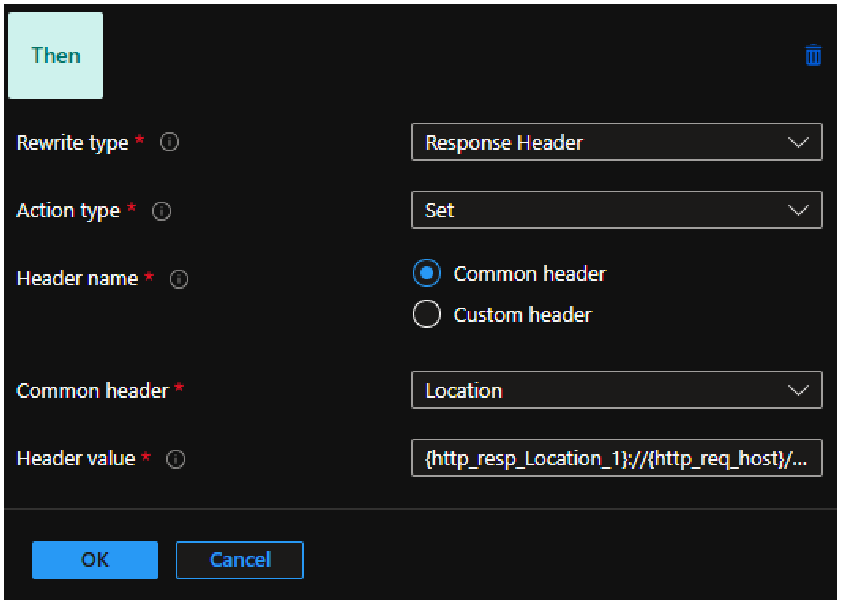
Type of variable to check *	HTTP header
Header type *	Response Header
Header name *	● Common header ○ Custom header
Common header *	Location
Case-sensitive *	○ Yes ● No
Operator *	equal (=)
Pattern to match	(https?):\/\/[^\/]+:7443\/(?:arcgis|portal)(...

v. Where the "Pattern to match" is set to "(https?):\/\/[^\/]+:7443\/(?:arcgis|portal)(.*)$"



Rewrite type *	Response Header
Action type *	Set
Header name *	○ Common header ● Custom header
Custom header *	RewriteLocationValue
Header value *	{http_resp_Location_1}://{http_req_host}/...

vi. Where the "Header value" is set to "{http_resp_Location_1}://{http_req_host}/portal{http_resp_Location_2}"



Then

Rewrite type * : Response Header

Action type * : Set

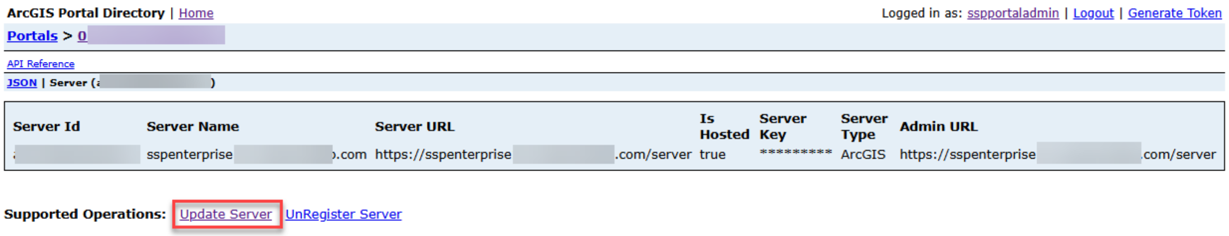
Header name * : ● Common header ○ Custom header

Common header * : Location

Header value * : {http_resp_Location_1}://{http_req_host}/...

vii. Where the "Header value" is set to "{http_resp_Location_1}://{http_req_host}/portal{http_resp_Location_2}"

8. Configure the Azure Application Gateways health probes to point to the ArcGIS Enterprise health endpoints:
   - Portals Health Probe:
     i. Set the "Path" to "/arcgis/portaladmin/healthCheck"
   - Servers Health Probe:
     i. Set the "Path" to "/arcgis/rest/info/healthcheck"
   - *Note: The health probes will fail until all steps are complete.*
9. Configure ArcGIS Enterprise Settings:
   - Change the Web Context in the portaladmin and the server admin endpoints:
     i. For Portal:
        1. Navigate to the "https://FQDN:7443/arcgis/portaladmin/system/properties" url
        2. Update the properties with the following: {"WebContextURL":"https://DNS/portal","privatePortalURL":"https://DNS/portal"}
     ii. For Server:
        1. Navigate to the "https://FQDN:6443/arcgis/server/admin/system/properties/update" site
        2. Update the properties with: {"WebContextURL": https://DNS/server}



ArcGIS Portal Directory | Home

Logged in as: sspportaladmin | Logout | Generate Token

Portals > 0[redacted]

API Reference

JSON | Server ([redacted])

Server Id	Server Name	Server URL	Is Hosted	Server Key	Server Type	Admin URL
[redacted]	sspenterprise[redacted].com	https://sspenterprise[redacted].com/server	true	*********	ArcGIS	https://sspenterprise[redacted].com/server

Supported Operations: Update Server UnRegister Server

NOTE: If the ArcGIS Enterprise deployment is federated it is required to also change the Server URLs located in https://FQDN:7443/arcgis/sharing/rest/portals/<orgID>/servers/<ServerID>/update

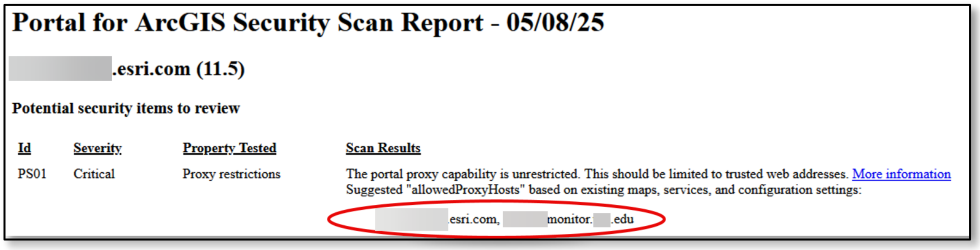
iii. Update the Server name, Server URL, and Admin URL with the DNS alias used in the Server Web context URL. For example, “https://<DNS>/server”

Appendix J: Determining Domains to Include for Proxy Allow List

Configuring the Proxy Allow List for your Enterprise deployment is critical, however, not including domain entries for the three scenarios the allow list is used could result in disruption of service access with those domains. Therefore, we have provided detailed implementation guidance for determining what domains should be added to allowedProxyHosts below.

Use portalScan.py Security Scan Script

If you have ArcGIS Enterprise 11.4 or later and you are comfortable executing Python scripts, we have a short-cut for identifying the FQDN's that should be added to the allow list. Esri includes with Portal for ArcGIS 11.4 and later a Python script, portalScan.py, that scans for common security issues. If the allowedProxyHosts property is not populated for a system, it lists FQDN's that should be allow listed as shown below:



Portal for ArcGIS Security Scan Report - 05/08/25

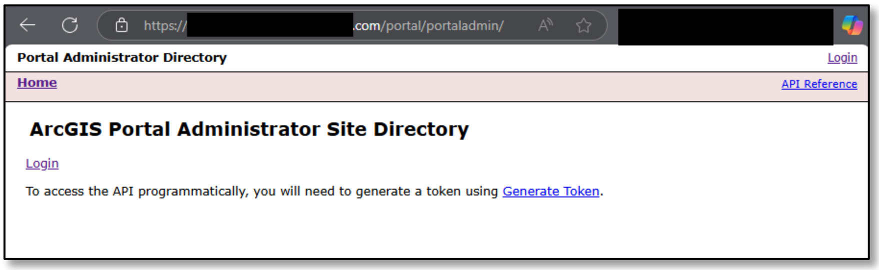
[redacted].esri.com (11.5)

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 Suggested "allowedProxyHosts" based on existing maps, services, and configuration settings: [redacted]esri.com, [redacted]monitor.[redacted].edu

Check if AllowProxyHost Entry Already Exists

Validate if your system has an allowedProxyHosts entry by opening a web browser and sign in to the Portal Administrator Directory as an Administrator of your organization. The URL is formatted as https://organization.domain.com/<Portal>/portaladmin.



https://[redacted].com/portal/portaladmin/ [redacted]

Portal Administrator Directory

Login

Home

API Reference

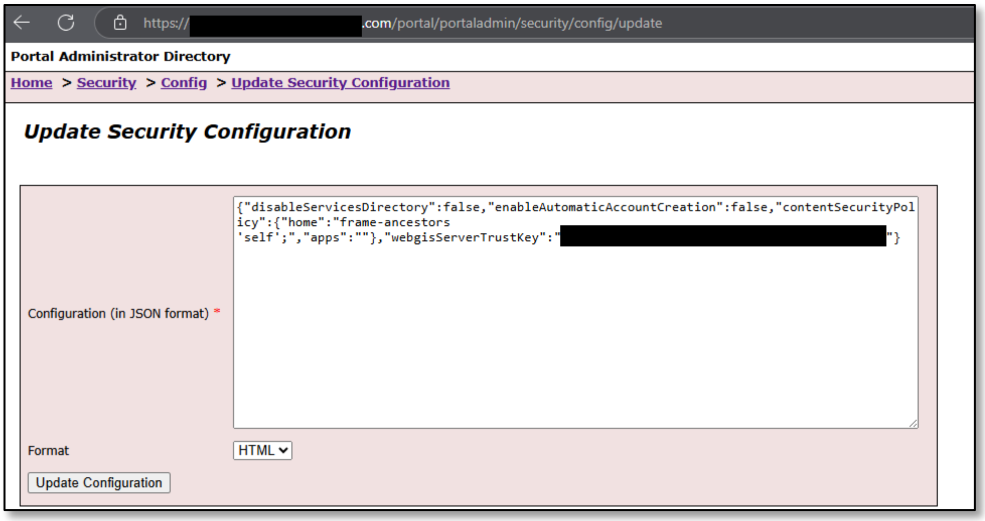
ArcGIS Portal Administrator Site Directory

Login

To access the API programmatically, you will need to generate a token using Generate Token.

Once logged in, then Click Security > Config > Update Security Configuration.

A default ArcGIS Enterprise 11.4 Configuration is shown below (notice no allowedProxyHosts entry). If you already have domains assigned to allowedProxyHosts, then your system is secured as recommended.



https://[redacted].com/portal/portaladmin/security/config/update

Portal Administrator Directory

Home > Security > Config > Update Security Configuration

Update Security Configuration

Configuration (in JSON format) *

```
{"disableServicesDirectory":false,"enableAutomaticAccountCreation":false,"contentSecurityPolicy":{"home":"frame-ancestors 'self';","apps":""},"webgisServerTrustKey":"[redacted]"}
```

Format: HTML

Update Configuration

Copy Configuration Text to Editor

If you don't see allowedProxyHosts in the Configuration window, then we recommend copy and pasting the configuration text to Notepad or similar plaintext editor and save the file to be able to recover original configuration text if necessary.

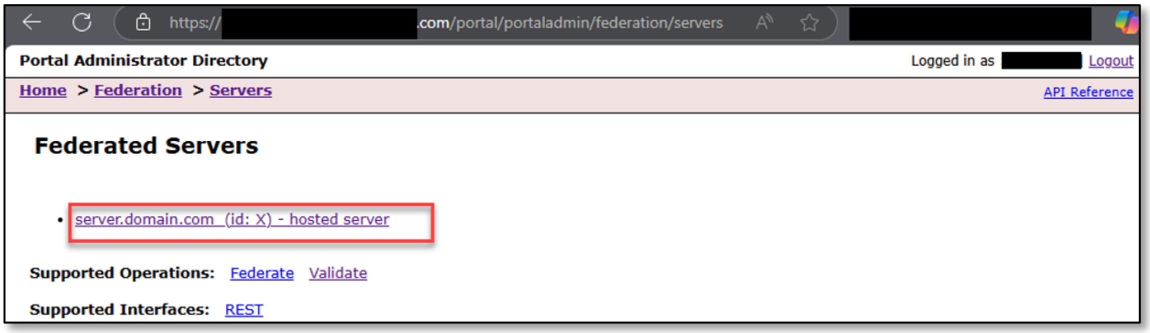
Copy and paste the below allowedProxyHosts property to the Notepad file before the ending bracket "}"

```
        , "allowedProxyHosts": "
```

Yes, that is a comma at the beginning as a separator between the property entries. Yes, that is a quote at the end, as you will be entering the domains / FQDN's you want to allow list there. Every entry will need to be separated by a comma. There are three scenarios requiring entries to be added to the allow list – Admin URL domains, External ArcGIS Enterprise service domains with embedded credentials, and legacy CORS support domains – We walk you through those below:

Admin URL Domains:

1. Open another browser windows and go the to the Portal Administrator Directory Servers page at: https://organization.domain.com/<Portal>/portaladmin/federation/servers
2. Select the hosted server link as shown below:



https://[redacted].com/portal/portaladmin/federation/servers [redacted]

Portal Administrator Directory — Logged in as [redacted] Logout

Home > Federation > Servers — API Reference

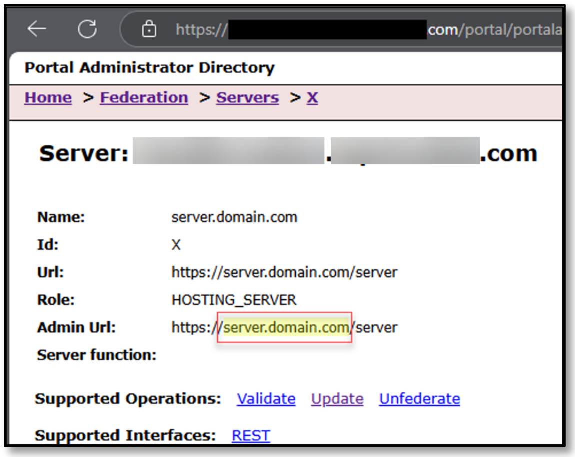
Federated Servers

- server.domain.com (id: X) - hosted server

Supported Operations: Federate Validate

Supported Interfaces: REST

3. Examine the "Admin Url" FQDN from the Servers screen below and add to the allow list.



https://[redacted]com/portal/portala

Portal Administrator Directory

Home > Federation > Servers > X

Server: [redacted].[redacted].com

Name: server.domain.com
Id: X
Url: https://server.domain.com/server
Role: HOSTING_SERVER
Admin Url: https://server.domain.com/server
Server function:

Supported Operations: Validate Update Unfederate

Supported Interfaces: REST

Within the Notepad configuration text, populate the `allowProxyHosts` value with the fully qualified domain name of each Admin URL an example domain is shown below:

```
{
<…Additional Configuration Parameters…>,
"allowedProxyHosts": "server.domain.com,(.*).domain.com"
}
```

External ArcGIS Enterprise service domains with embedded credentials

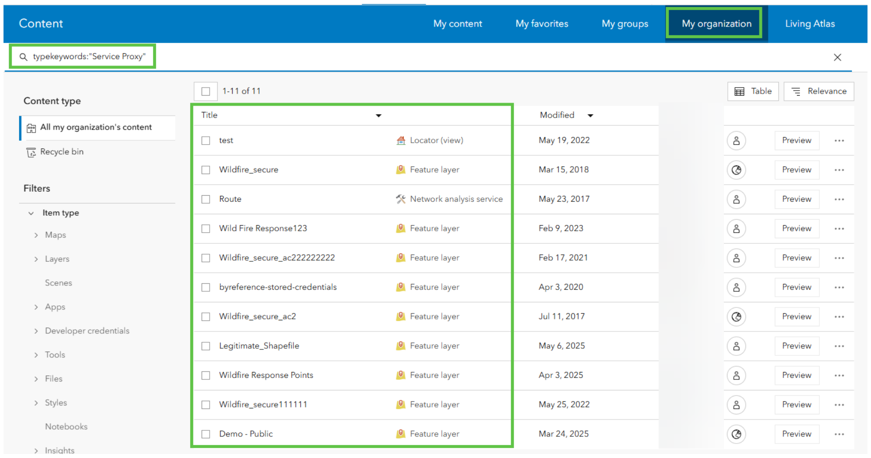
Organizations that make use of this feature: ArcGIS Server web services > Secure Services | Documentation for ArcGIS Enterprise to add external ArcGIS Server services as items and store credentials as part of the connection, must add domain names associated with these services to the `allowedProxyHosts` list as either a wildcard or explicit entry (Fully Qualified Domain Name – FQDN). Note that external domain GeoRSS and KML references should also be allow listed as part of this step. We recommend utilizing FQDN's for the strongest security (as feasible).

WARNING: Customers should strongly consider implementing Collaboration with the external services instead of embedding credentials. Collaboration is significantly more secure, you are more likely in alignment with the external service providers terms, and no allowedProxyHosts entries are necessary for such external services.

To find all items which reference external ArcGIS Server services with stored credentials, do the following:

1. Login to the ArcGIS Enterprise Portal Home application with administrator privileges.
2. Execute this search:
```
https://{organization.domain.com}/{portal}/home/content.html?sortField=relevance&sortOrder=desc&searchTerm=typekeywords%3A%22Service+Proxy%22&view=table#org
```

3. This will return all ArcGIS Server service items with stored credentials.

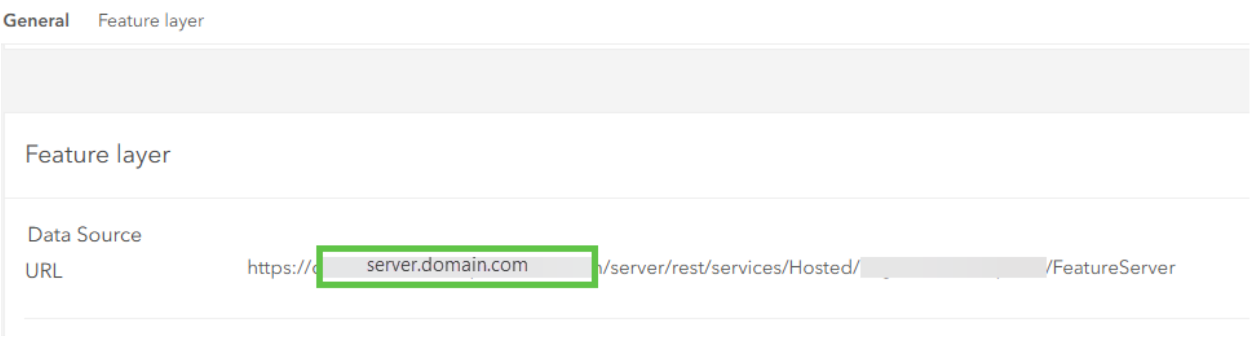


typekeywords:"Service Proxy"

1-11 of 11

Title		Modified		
test	Locator (view)	May 19, 2022	Preview	···
Wildfire_secure	Feature layer	Mar 15, 2018	Preview	···
Route	Network analysis service	May 23, 2017	Preview	···
Wild Fire Response123	Feature layer	Feb 9, 2023	Preview	···
Wildfire_secure_ac222222222	Feature layer	Feb 17, 2021	Preview	···
byreference-stored-credentials	Feature layer	Apr 3, 2020	Preview	···
Wildfire_secure_ac2	Feature layer	Jul 11, 2017	Preview	···
Legitimate_Shapefile	Feature layer	May 6, 2025	Preview	···
Wildfire Response Points	Feature layer	Apr 3, 2025	Preview	···
Wildfire_secure111111	Feature layer	May 25, 2022	Preview	···
Demo - Public	Feature layer	Mar 24, 2025	Preview	···

4. Inspect each Item's > Settings > Layer properties. Document the fully qualified domain name of the "Data Source URL" value of each item:



Feature layer

Data Source URL https://[redacted]server.domain.com[redacted]/server/rest/services/Hosted/[redacted]/FeatureServer

5. Within the Notepad configuration text, add the additional domains to the `allowProxyHosts` value with a comma separated list of each the fully qualified domain names of each service (most secure) and/or a wildcard prefixed (.*) domain of each service (broader/less secure).

```
{
<…Additional Configuration Parameters…>,
"allowedProxyHosts": "server.domain.com,(.*).domain.com"
}
```

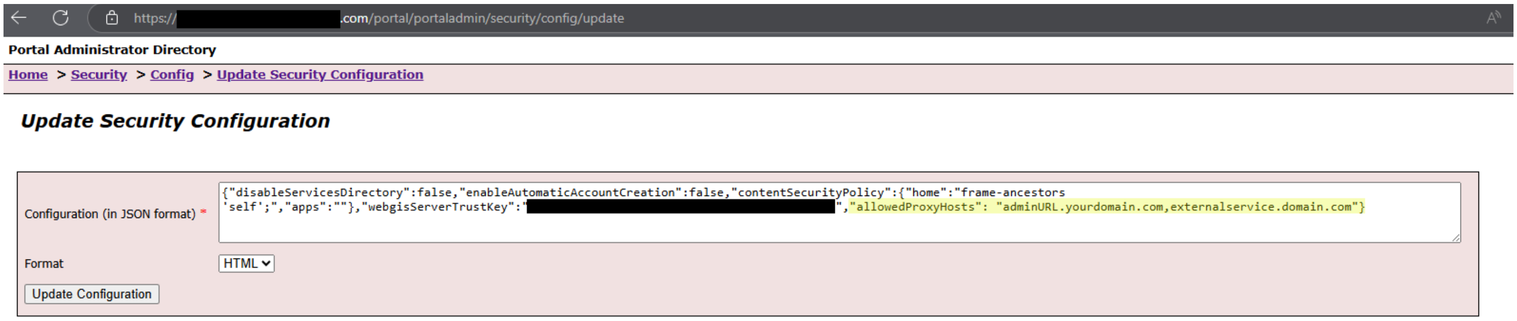
Legacy CORS support domains

Legacy web services and web clients that did not support Cross Origin Resource Sharing (CORS) may attempt to use Portal's proxy capability to work around CORS rules. We strongly recommend eliminating any services or clients that do not support CORS instead of adding them to the allow list.

Complete Configuration and Update

Once your domain entries are completed in Notepad, make sure there is a closing quote at the end followed by bracket, then copy all the configuration text from Notepad and paste over all of the Configuration text within the Portal Administrator Directory interface and click "Update Configuration".

Note, it typically takes 1-2 minutes for the update to complete. Your configuration should be similar in structure to the screenshot below, however be aware the Property entries listed vary depending on the version of ArcGIS Enterprise you are using. For example, contentSecurityPolicy is new starting with 11.4, so if you have an older version, you will not see such a property.



https://[redacted].com/portal/portaladmin/security/config/update

Portal Administrator Directory

Home > Security > Config > Update Security Configuration

Update Security Configuration

Configuration (in JSON format) *

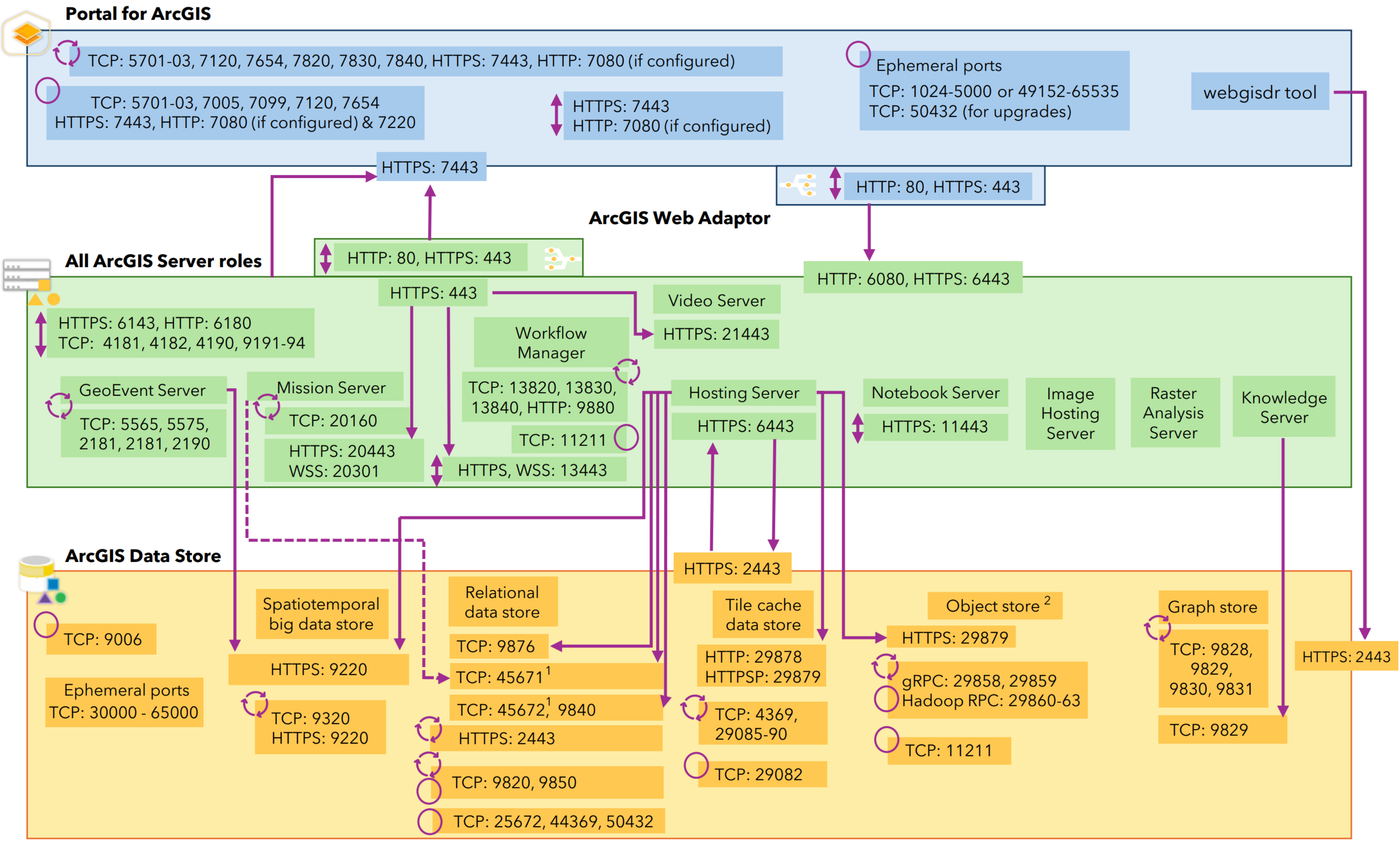
```
{"disableServicesDirectory":false,"enableAutomaticAccountCreation":false,"contentSecurityPolicy":{"home":"frame-ancestors
'self';","apps":""},"webgisServerTrustKey":"[redacted]","allowedProxyHosts": "adminURL.yourdomain.com,externalservice.domain.com"}
```

Format: HTML

Upon applying the above settings the Portal's proxy capability will be correctly configured to:

- Allow connections to federated ArcGIS Server service hosts
- Allow item registration and credential embedding vs unfederated ArcGIS Server hosts
- Allow external KML and GeoRSS references
- Disallow CORS workaround hacks

Appendix K: ArcGIS Enterprise 11.5 Ports Utilized Diagram



↻ Ports used for communication between machines in the same ArcGIS Server site, portal, or individual data store.

○ Ports must be available on each machine. No external communication is needed.

↑ Single direction communication between components or sites.

↕ Inbound & outbound communication between components or sites.

[1] These ports are also needed to communicate with federated ArcGIS Server sites that use web hooks.

[2] When you use ArcGIS tools to deploy on Amazon Web Services or Microsoft Azure, the object store may use a cloud service location instead of ArcGIS Data Store.

Appendix L: Definitions

C.I.A.: The basics of information security—confidentiality, integrity, and availability

Configuration Drift: When change management procedures are not effective, an environment's configuration may gradually change and become inconsistent with originally defined requirements

Data Breach: A data or information breach is an event caused by a cyberattack by an unauthorized user

Data Leak (or Spill): A data or information leak (or spill) occurs when sensitive data is unknowingly and unintentionally exposed to the public

Group: Mechanism used to organize and share items, often related to a region, subject, or project

ISO: International Organization for Standardization

Items: Contents made available through an ArcGIS Enterprise organization. Items include content such as files, layers (services), maps, scenes, apps, tools, and templates

Least Privilege: People and processes must be able to access or perform only the information, actions, and resources necessary to perform their role functions

Member: ArcGIS Enterprise user account

NIST: National Institute of Standards and Technology

PHI: personal health information

Phishing-resistant MFA: Highly secure authentication method designed to fortify user accounts against phishing attacks. Unlike traditional MFA, which can still be vulnerable to phishing attempts, this approach incorporates multiple layers of protection to ensure enhanced security

PII: personally identifiable information

Privilege creep: New permissions are added, but permissions no longer required remain

Privileges: Confer specific rights to the ArcGIS Enterprise members of the role

Proprietary Information: Organization created or discovered information that has commercial value

QA/QC: quality assurance/quality control

Roles: ArcGIS Enterprise privilege assignments via default or custom roles

STIG: Security Technical Implementation Guide – Standardized security hardening guidance utilized by defense as well as many federal organizations

SWG/IAP: secure web gateway/identity aware proxy

User Types: ArcGIS Enterprise licensing assignments. Allows access to specific apps and determines the privileges that *can* be granted to the member through roles

ZTA: zero trust architecture—An evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources

Appendix M: Document Revision History

Version 1.10 – Published 1/30/24

- Initial public release

Version 1.11 – Published 4/19/24

- Added Enterprise 11.2 security improvements
- Minor updates/corrections based on customer feedback

Version 1.13 – Published 2/24/25

- Added Enterprise 11.3 & 11.4 security improvements
- Added Appendix J Azure Load Balancer configuration guidance for no Web Adaptor
- Added supplementary guidance to Web Server Extension requirement Appendix
- Updated Appendix F Log Shipping guidance, including new 11.4 security logging capabilities
- Added new 11.4 contentSecurityPolicy option to "Implement Content Security Policy" section
- Updated User Types for 2024 changes
- Other minor updates

Version 1.16 – Published 5/8/25

- Added clarifications for working with Anti-Virus Engine Aggregator false positives
- Added xssPreventionEnabled and xssPreventionRule option
- Extend guidance in Appendix J for configuring load balancers without Web Adaptors
- Shifted AllowProxyHosts from Advanced to Basic and added appendix to determine domains
- New security control added - Basic: Avoid Forward Proxy Authentication

Version 1.17 – Published 6/10/25

- Updated Implement Advanced Baseline details for current STIG guidance
- Added new 11.5 security enhancements to Appendix G
- Updated Ports Diagram – Appendix K for ArcGIS Enterprise 11.5

Version 1.18 – Published 7/7/2025

- Updated allowed extensions
- Final gap analysis of DISA ArcGIS Server STIG and Enterprise hardening guide completed
- Added log permission security control "Verify Log Folder Security Permissions"
- Added reference to DISA STIG Control APSC-DV-002970