



AN ESRI  
TECHNICAL PAPER

June 2026

# ArcGIS Enterprise Hardening Guide

Download latest from [ArcGIS Trust Center](#)

- [Guide](#)
- [Appendices](#)
- [Security Control Spreadsheet](#)

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



**esri**

THE  
SCIENCE  
OF  
WHERE®

Copyright © 2026 Esri  
All rights reserved

## Table of Contents

Introduction .....	2
Security Profile Checklists .....	5
Application Security .....	7
Identity and Access Management.....	14
Supporting Infrastructure .....	26
Data Protection .....	29
Inventory and Maintenance.....	35
Detection and Response .....	43
Training Guidance .....	47
Privacy.....	49
Appendixes.....	56
Document Revision History.....	57

## 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 12.0 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 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 12.1. 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.*

**NOTE:** To provide more focused guidance for the majority of our customers, we have shifted the Appendices to a separate downloadable document and moved all Advanced profile controls Appendix A in it. We have also eliminated multiple separate table listings of the security controls and now provide a spreadsheet so you can sort/filter based on your needs.

## 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](https://trust.esri.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](mailto: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. Note that Esri has started adding application security control settings specified within this guide to some [deployment automation tools such as Chef](#) to ease deployment of **Basic** hardened systems.

**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. As mentioned earlier all Advanced profile controls have been shifted to Appendix A.

**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

## 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.

Detailed secure architecture deployment patterns with ArcGIS Enterprise and supporting security infrastructure components, such as a Standard Secure Enterprise Pattern and a Standard Secure Enterprise Publishing Pattern are located Appendix M.

## Security Profile Checklists

This document provides separate ArcGIS Enterprise security profile checklists for the two profiles:

- **Basic** security profile implementation see **Table 1**
- **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. They are ordered according to relative importance for mitigating security and privacy risks, so if you can't initially implement all, just start at the top of the list and work your way down over time.

**Note:** [Spreadsheet of all controls available for download](#) to ease your reference/filter/prioritizing.

Table 1-**Basic** Security Controls

ID	Control	Owner	Adviser	Privacy	Security
AS-B1	<b>Basic: Configure</b> Portal for ArcGIS Proxy Allow List	SA, GA	Yes	Danger	Danger
SI-B1	<b>Basic: Avoid</b> Forward Proxy Authentication	SA	Yes	Danger	Danger
AS-B2	<b>*Basic: Disable</b> Primary Site Administrator (PSA) account	GA	-	Danger	Danger
AS-B3	<b>Basic: Implement</b> Password Reset Email Notification	SA, GA	-	Danger	Danger
SI-B2	<b>Basic: Implement</b> Web Application Firewall (WAF)	SA	-	Danger	Danger
IM-B1	<b>Basic: Implement</b> Security Patches within One Month	SA, GA	-	Danger	Danger
IA-B1	<b>Basic: Configure</b> All Administrator Accounts with MFA	SA, GA	Yes	Danger	Danger
AS-B4	<b>Basic: Verify</b> Filter Web Content is Enabled for All Feature Services	GA, GU	-	Danger	Danger
AS-B5	<b>Basic: Verify</b> Standardized Queries are Enabled	GA	Yes	Danger	Danger
AS-B6	<b>Basic: Verify</b> Server System Services Secured	GA	-	Danger	Danger
AS-B7	<b>Basic: Verify</b> Token Acquisition via HTTP GET is Disabled	GA	-	Danger	Danger
AS-B8	<b>Basic: Verify</b> Portal for ArcGIS Legend Servlet is Disabled	GA	-	Danger	Danger
AS-B9	<b>Basic: Verify</b> Portal for ArcGIS Print Servlet is Disabled	GA	Yes	Danger	Danger
AS-B10	<b>Basic: Verify</b> Portal for ArcGIS WFS Servlet is Disabled	GA	-	Danger	Danger
IA-B2	<b>Basic: Implement</b> Personal Secrets Management	SA, GA, GU	-	Danger	Danger
IA-B3	<b>Basic: Implement</b> SAML Signed and Encrypted Assertions	SA, GA, GU	-	Danger	Danger
IA-B4	<b>Basic: Implement</b> Group-Based Sharing	GA	-	Danger	Danger
IA-B5	<b>Basic: Manage</b> Content via Role-based Access Control (RBAC)	GA	-	Danger	Danger
DP-B1	<b>Basic: Implement</b> Whole Disk Encryption	SA	-	Danger	Danger
DP-B2	<b>Basic: Verify</b> HTTPS is Enforced	SA	Yes	Danger	Danger
DP-B3	<b>Basic: Implement</b> Signed CA Certificates	SA, GA	-	Danger	Danger
DR-B1	<b>Basic: Manage</b> Webhooks	SA, GA	-	Danger	Danger
IA-B25	<b>Basic: Implement</b> User Authentication for most use cases	GA, GU	-	Danger	Danger
IA-B26	<b>Basic: Implement</b> App Authentication for automation	GA, GU	-	Danger	Danger
IA-B27	<b>Basic: Avoid</b> API Key Authentication for sensitive content	GA, GU	-	Danger	Danger
IA-B28	<b>Basic: Manage</b> SOE, SOI and Geoprocessing Services	GA	Yes	Danger	Danger
AS-B11	<b>Basic: Configure</b> Built-In Accounts Password Policy	GA	Yes	Warning	Danger
AS-B12	<b>Basic: Verify</b> Self-Creation of Built-In User Accounts is Disabled	GA	-	Warning	Danger
IA-B6	<b>Basic: Avoid</b> Embedding User Identities in Scripts	SA, GA, GU	-	Info	Danger
IA-B7	<b>Basic: Avoid</b> Embedding Application Identities in Client Apps	SA, GA, GU	-	Info	Danger
IA-B8	<b>Basic: Avoid</b> Storing Secrets in Source Code	SA, GU	-	Info	Danger
IA-B9	<b>Basic: Disable</b> Members Can Share Content Publicly	GA	Yes	Danger	Info
IA-B10	<b>Basic: Disable</b> Public User Profile Sharing for organization users	GA	Yes	Danger	Info
IA-B11	<b>Basic: Configure</b> Decentralized Profile Visibility	GA	-	Danger	Info
AS-B13	<b>Basic: Verify</b> Nosniff Header Enabled	GA	-	Warning	Warning

AS-B14	<b>Basic: Verify</b> featureServiceXSSFilter to “input”	GA	-	Warning	Warning
AS-B15	<b>Basic: Verify</b> XSSPreventionEnabled to “true”	GA	-	Warning	Warning
AS-B16	<b>*Basic: Disable</b> ArcGIS Portal Directory	GA	-	Warning	Warning
AS-B17	<b>*Basic: Disable</b> ArcGIS Server Services Directory	GA	-	Warning	Warning
AS-B18	<b>Basic: Remove</b> Silverlight and FLEX Policy Files	SA	-	Warning	Warning
AS-B19	<b>Basic: Verify</b> Map Service Dynamic Workspaces/Layers Disabled	GA	-	Warning	Warning
AS-B20	<b>Basic: Implement</b> Group Managed Service Account (gMSA)	SA	-	Warning	Warning
IA-B12	<b>Basic: Implement</b> Centralized User Account Management	SA, GA	Yes	Warning	Warning
IA-B13	<b>Basic: Configure</b> New Member Default Role as Viewer	GA	-	Warning	Warning
IA-B14	<b>Basic: Configure</b> Least Privilege User Types and Roles	GA	-	Warning	Warning
IA-B15	<b>Basic: Configure</b> Default Group Membership Assignments	GA	-	Warning	Warning
IA-B16	<b>Basic: Implement</b> GIS Data Publication Management Process	GA	-	Warning	Warning
IA-B17	<b>Basic: Consider</b> using Feature Layer Views	GA	-	Warning	Warning
IA-B18	<b>Basic: Consider</b> Publication Governance and Delivery Pipelines	SA, GA	-	Warning	Warning
IA-B19	<b>Basic: Consider</b> Defining content access requirements	GA	-	Warning	Warning
IA-B20	<b>Basic: Verify</b> content ownership rights	GA	-	Warning	Warning
IA-B21	<b>Basic: Manage</b> accounts and reduce user permissions	GA	-	Warning	Warning
IA-B22	<b>Basic: Implement</b> permission guardrails	GA	-	Warning	Warning
IA-B23	<b>Basic: Manage</b> Access Based on Employee or Project Life Cycle	SA, GA	-	Warning	Warning
DP-B4	<b>Basic: Implement</b> Backup Strategy and Test Regularly	SA, GA	-	Warning	Warning
DP-B5	<b>Basic: Implement</b> Database Transparent Data Encryption (TDE)	SA, GA	-	Warning	Warning
DP-B6	<b>Basic: Configure</b> HSTS Enforcement	SA	-	Warning	Warning
IM-B2	<b>Basic: Manage</b> Vulnerable Components with Patching	SA, GA	-	Warning	Warning
IM-B3	<b>Basic: Configure</b> Vendor Patch Notification Subscription	SA, GA	-	Warning	Warning
IM-B4	<b>Basic: Manage</b> Configuration Drift	GA	-	Warning	Warning
DR-B2	<b>Basic: Implement</b> Vulnerability Scanning Tools	SA	-	Warning	Warning
DR-B5	<b>Basic: Implement</b> Endpoint Detection and Response	SA	-	Warning	Warning
AS-B21	<b>Basic: Configure</b> Access Notice / Information Banners	SA	-	Info	Warning
SI-B3	<b>Basic: Implement</b> Vendor Security Baselines	SA, GA	-	Info	Warning
SI-B4	<b>Basic: Implement</b> Network segmentation	SA	-	Info	Warning
SI-B5	<b>Basic: Consider</b> Not Using ArcGIS Web Adaptor	SA, GA	-	Info	Warning
DP-B7	<b>Basic: Consider</b> File Geodatabases	SA, GA	-	Info	Warning
IM-B5	<b>Basic: Implement</b> Software Inventory	SA, GA	-	Info	Warning
DR-B3	<b>Basic: Implement</b> SIEM	SA	-	Info	Warning
TG-B1	<b>Basic: Manage</b> Ongoing Awareness Activities	SA, GA, GU	-	Info	Warning
AS-B23	<b>Basic: Configure</b> callbackFunctionsEnabled set to false	GA	-	Info	Warning
AS-B24	<b>Basic: Configure</b> ArcGIS Logging Level	GA	-	Info	Warning
AS-B22	<b>Basic: Consider</b> Disabling Anonymous Access	GA	Yes	Warning	Info
IA-B24	<b>Basic: Disable</b> Show Social Media Links	GA, GU	Yes	Warning	Info
PR-B1	<b>Basic: Consider</b> Data Anonymization	SA	-	Warning	Info
IM-B6	<b>Basic: Manage</b> Only General Availability Product Versions	GA	-	Info	Info
DR-B4	<b>Basic: Implement</b> CSIRT Process	SA	-	Info	Info
TG-B2	<b>Basic: Implement</b> Role-based Training Plans	SA, GA, GU	-	Info	Info

\* Controls with a star should only be completed AFTER other controls implemented.

Legend		
Heading	Description	Template Structure
ID	Unique identifier	{Doc Section: AS, IA, SI, DP, IM, DR, TG, PR} - {Profile: B, A} #
Control	Description of security control	Freertext - Note implement controls prefaced with "*" last
Owner	Responsible for implementing	{Owner: SA, GA, GU}
Adviser	Checked by ArcGIS Security & Privacy Adviser	{Adviser: Yes, -}
Privacy	Relative privacy risk if not implemented	{Privacy: Danger, Warning, Info}
Security	Relative security risk if not implemented	{Security: Danger, Warning, Info}

## 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`)

To improve secure by default settings, starting with ArcGIS Enterprise 12, this setting is now configured by default and a user interface has been added to the home application to ease configuration. 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](#).

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

If using pre-ArcGIS Enterprise 12.0, 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.

**Basic: Verify** XSSPreventionEnabled to “true”

The featureServiceXSSFilter property discussed above can be set to input or inputOutput. The input value is the default; it directs ArcGIS Server to configure all new feature services to scan edits. The inputOutput value directs ArcGIS Server to configure all new feature services to scan edits and returned features.

To override a **specific** service's settings, set XSSPreventionEnabled for that service. To make this change, you must use the ArcGIS Server Administrator Directory, find the service, and edit it. For the basic profile, validate that XSSPreventionEnabled is set to “true” (XSSPreventionEnabled = “true” is the default) for all feature services.

- XSSPreventionEnabled enables scanning for scripts and code in features. Set this to true.
- When XSSPreventionEnabled is set to “true”, XSSPreventionRule automatically defaults to “input”.

**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 limited use cases for some built-in accounts.

**When used, a secure Built-in account must:**

1. Never utilize weak account recovery answers – DANGEROUS
2. Never utilize common administration account names (e.g. Admin, Administrator,...)
3. [Require a strong password policy](#)

ArcGIS password complexity requirements allow you to configure minimum number of characters (default is 8), Uppercase letters, Lowercase letters, Numbers, and Special characters.

Note: 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 and later versions support audit logs in addition to standard logs, see: [Understand audit logs—Portal for ArcGIS | Documentation for ArcGIS Enterprise](#)

## 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 – **At a minimum avoid assigning the service account Admin permissions.** 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. See Appendix O: ArcGIS gMSA Service Account

## 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)

## 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/Developer Identities
- Centralized Identity Management
- User Groups and Attributes
- Permissions Management

### User and Application/Developer 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 App ID/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](#)).

The following table illustrates the available OAuth credentials ArcGIS supports according to valid use cases:

Identity Type	Valid Use Case	Invalid Use Case
<a href="#">User Authentication</a>	Embedded in client applications	Non-interactive (automated) processes
<a href="#">API Key Authentication</a>	Access to premium content	Embedded in client applications
<a href="#">App Authentication</a>	Machine access to private content	Embedded in client applications

**Basic: Implement** User Authentication for most use cases

The lowest risk authentication pattern is User Authentication which makes use of an ArcGIS registered OAuth 2.0 App ID (aka Client ID) to identify an application but requires user-input to supply credentials. This flow is the most common authentication pattern as it enables the application to interact with services under the logged in user's context in alignment with ZTA principles. If you are building an application that a user is expected to login to, use the User Authentication flow. See: [Introduction to user authentication | Documentation | Esri Developer](#)

**Basic: Implement** App Authentication for automation

Application Authentication is the process of exchanging a Client ID & Client Secret for an short lived OAuth Bearer Token (ArcGIS Access Token) to access highly scoped private content. This flow is appropriate for non-interactive flows such as scripts, notebooks, and other server-side automated processes **only**. Avoid embedding Client ID & Client Secrets within client applications that run on user hosts as this practice exposes the Client Secret to compromise. See: [Introduction to app authentication | Documentation | Esri Developer](#)

**Basic: Avoid** API Key Authentication for sensitive content

Due to security risks with the use of API Keys, they are inappropriate for securing sensitive content. API Keys should only be used within applications that seek to consume ArcGIS Premium content and other non-sensitive use cases. API Keys serve the narrow use case in which a developer wishes to make use of premium ArcGIS content (credit bearing services) while paying for access to the content instead of the application user. See: [Introduction to API key authentication | Documentation | Esri Developer](#) . Be aware [legacy API Keys](#) have been retired and should be immediately deleted and replaced with new API Keys.

**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.

**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](#).

**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
  - o 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:
  - o Passwordless authentication (e.g., [Azure Passwordless authentication](#))
  - o [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 2—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

## Centralized Identity Management

A production ArcGIS Enterprise implementation should not establish a separate silo of user accounts but instead utilize centralized identity 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.

## 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.

See [Managing Groups](#) for additional details on configuring Users, Groups, and Items to support group-based sharing.

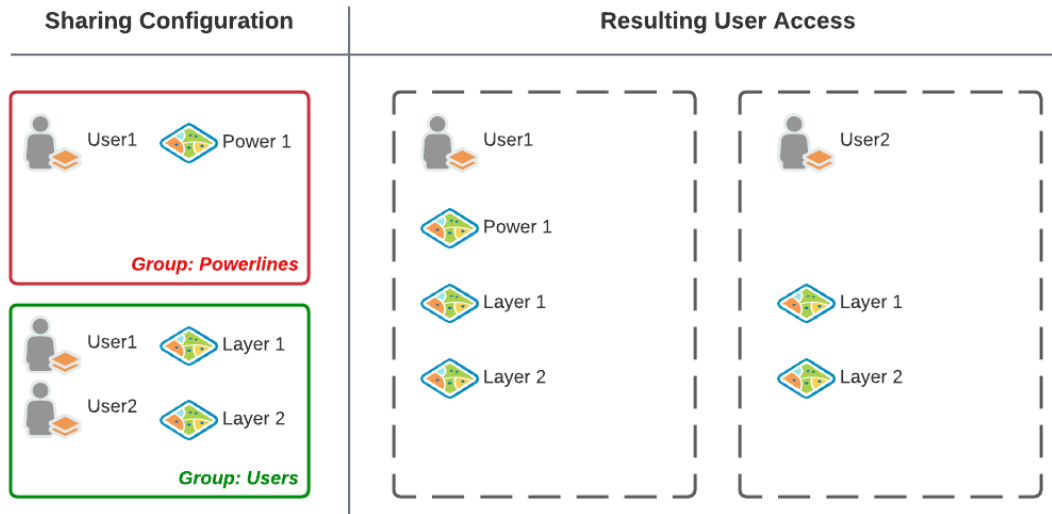


Figure 2—Group-Based Sharing Model

## Privilege Management

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

### 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](#).

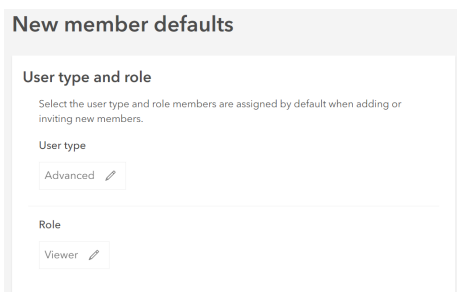


Figure 3—Set New Member Defaults

## 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).



Figure 4—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.

**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.

**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 Responses](#)" 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.

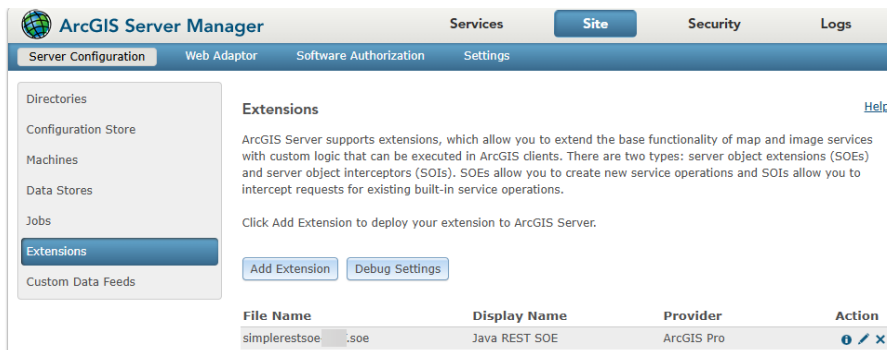
#### **Basic:** Manage SOE, SOI, and Geoprocessing Services

- [Server Object Extensions \(SOE\) and Server Object Interceptors \(SOI\)](#) are relatively rarely utilized by customers to introduce new capabilities or extend and change existing capabilities provided by Map or Image Services. Both SOEs and SOIs allow administrators to introduce custom code or alter the default logic of these service types. SOEs are appropriate if you want to create service operations to extend the base functionality of map and image services (including map and image service extensions, such as feature services). SOIs are suitable for adding new business logic or behavior on top of the existing ArcGIS Server operations in a way that is transparent to existing client applications.
- Geoprocessing Services (GP services) are flexible alternatives to custom Server Object Extensions. ArcGIS Enterprise administrators can publish ArcGIS Geoprocessing tools, models and custom scripts as web services.
- SOEs, SOIs, and GP services can all include powerful functionality. These tools can interact with the underlying host file system or make requests to remote resources using http libraries. They can perform any operation offered by the underlying Java, Python, or .Net framework used to

create the tool. These tools are each executed under the privileges provided to the ArcGIS runas account.

- Publishing GP tools and installing SOEs or SOIs all require administrative privileges by default.
- In the context of preventing configuration drift and given the powerful functionality that SOEs, SOIs, or GP services can offer, it is important that administrators regularly validate that any installed custom tooling is expected and that the intention and functionality of these tools is fully understood.
  - Validation Check: Use ArcGIS Server Manager to understand installed extensions
    - Navigate to [https://\[arcgis-server-host.domain.com\]:6443/manager/site](https://[arcgis-server-host.domain.com]:6443/manager/site)
    - Click “extensions” and review the installed extensions.
    - Validate that these extensions are expected and that their functionality is understood.

**WARNING:** No SOEs or SOIs are deployed by default as part of ArcGIS Enterprise, so if you find such a component, you should confirm if it is needed, and if not remove immediately.



- Validation Check: Use ArcGIS Server Manager to understand published GP services
  - Navigate to [https://\[arcgis-server-host.domain.com\]:6443/manager/](https://[arcgis-server-host.domain.com]:6443/manager/)
  - Browse through the site root and subfolders and examine any Geoprocessing Services
  - These Geoprocessing Services are created by default during site creation and are expected:
    - System folder: See control “Verify Server System Services Are Secured”
    - Utilities folder: GeocodingTools, OfflinePackaging, PrintingTools, RasterUtilities

## 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.

## 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](#).

## 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.

## 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\

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](#)

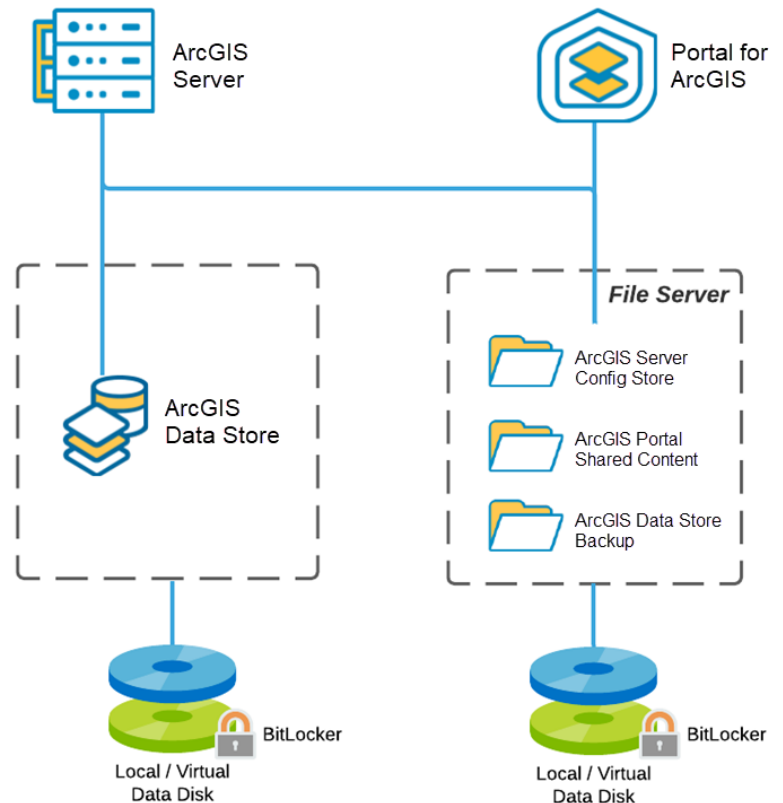


Figure 1—BitLocker Encryption

**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.

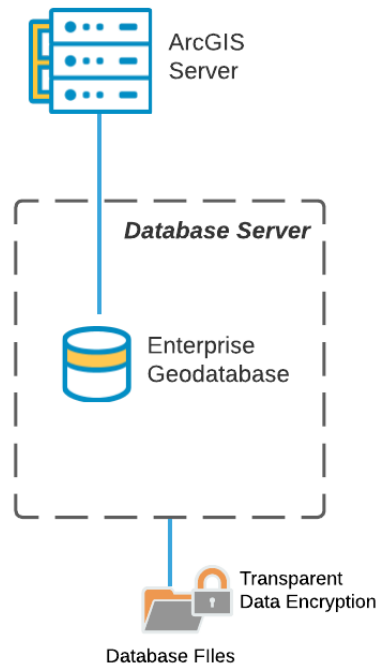


Figure 5—Transparent Data Encryption with Enterprise Geodatabase

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](#) – [ArcGIS SQL Server TDE Support](#)
- [Oracle: Configuring TDE](#)

## 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).

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.

How to configure this setting within Portal for ArcGIS and ArcGIS Server:

- [Enforce strict HTTPS communication—Portal for ArcGIS | Documentation](#)
- [Enforce strict HTTPS communication—ArcGIS Server | Documentation](#)

### **Basic: Implement** Signed CA Certificates

Default deployments of ArcGIS Enterprise 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.

How to deploy CA-signed certificates onto ArcGIS Enterprise:

- 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.

**WARNING:** Maximum certificate lifetimes are decreasing regularly over the next several years (200 days in 2026 and down to 47 days in 2029). We strongly recommend automating certificate updates to minimize outage potential. Note that starting with ArcGIS Enterprise 12.1, when you update a certificate it no longer requires restarting ArcGIS Enterprise, ensuring a smoother automated update workflow.

## 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<sup>1</sup> 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.

---

<sup>1</sup> 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](https://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.

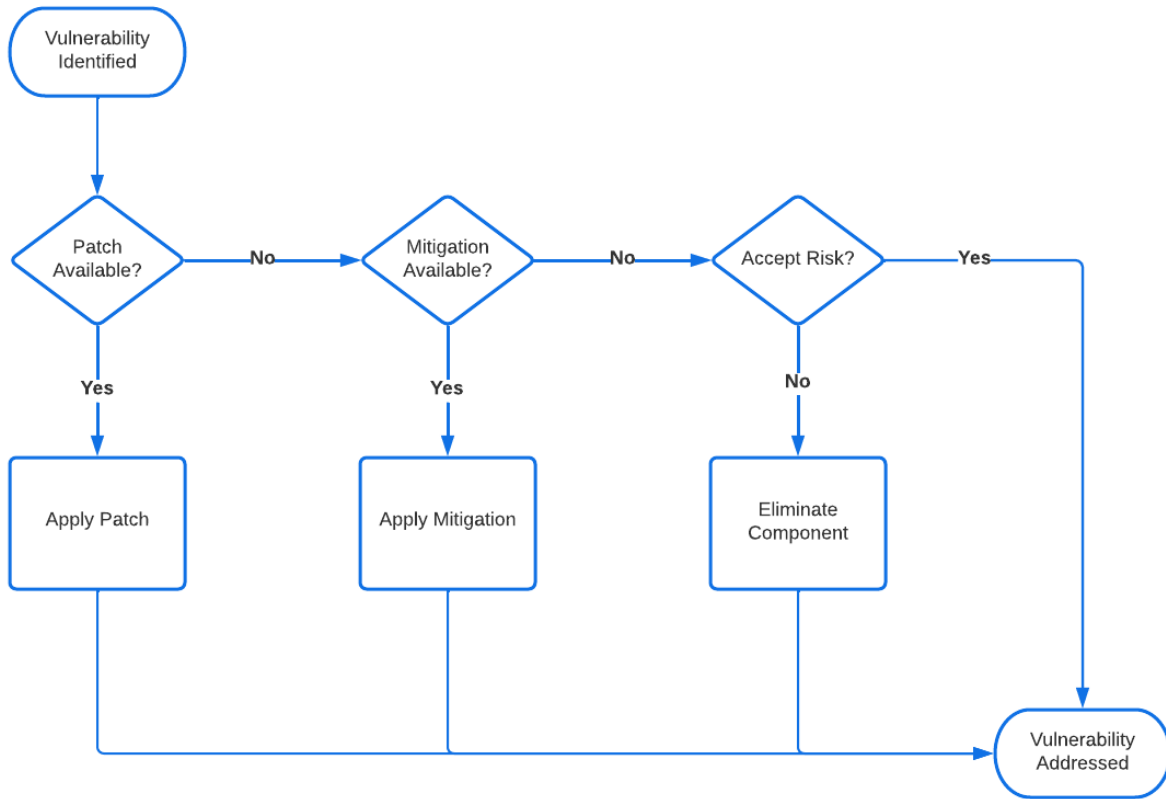


Figure 6—Sample Vulnerability Resolution Workflow

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 want 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 3) to avoid missing a critical software update or security patch:

Table 3—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](#).

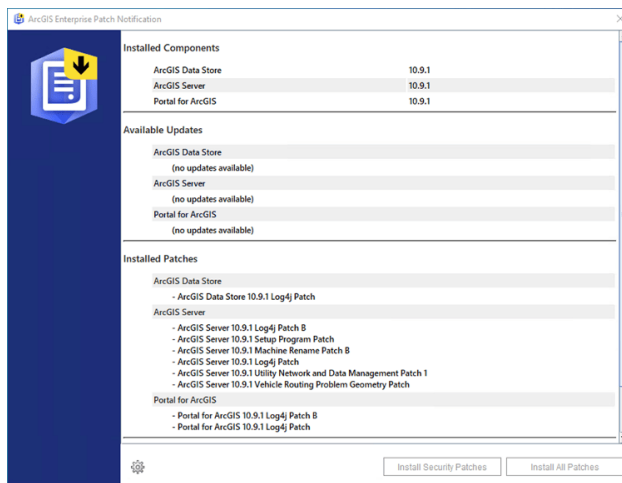


Figure 7—ArcGIS Enterprise Patch Notification Utility

**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](https://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**

██████████.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. <a href="#">More information</a>
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. <a href="#">More information</a>
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. <a href="#">More information</a>
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. <a href="#">More information</a>
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. <a href="#">More information</a>

Figure 8-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**

██████████.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. <a href="#">More information</a>
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. <a href="#">More information</a>
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. <a href="#">More information</a>
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. <a href="#">More information</a>
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. <a href="#">More information</a>

Figure 9-PortalScan.py Security Report

## 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.

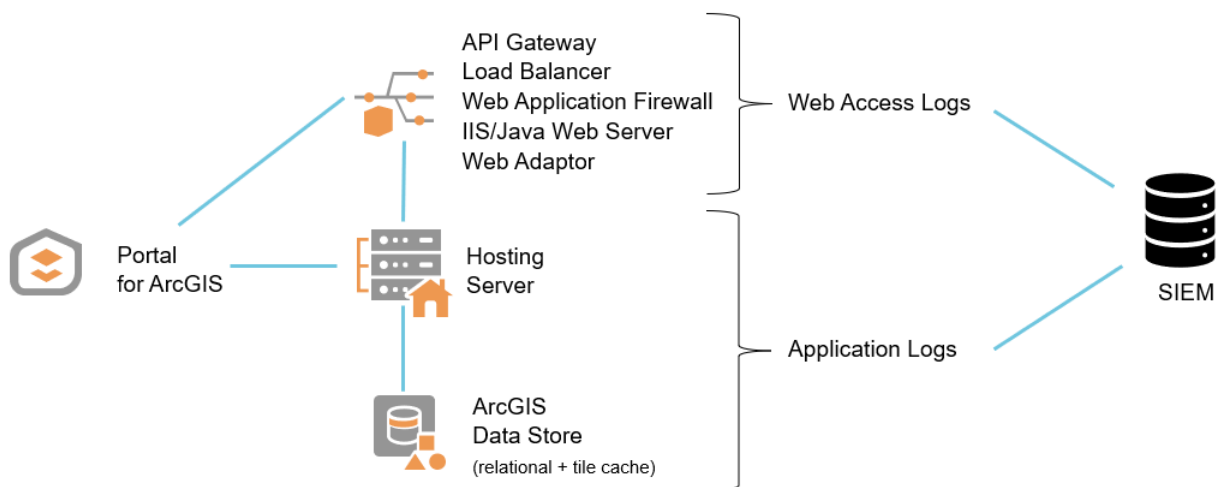


Figure 10—Utilizing a SIEM to Facilitate Correlation Across Logs

**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.<sup>2</sup>

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.<sup>3</sup>

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.

---

<sup>2</sup> Citation: <https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem>

<sup>3</sup> 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, part of our Coordinated Vulnerability Disclosure Document) 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.

## 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 4) to improve workforce security awareness within your organization:

Table 4—Train Users by Role and Responsibility

Role	Learning Plan
All	<a href="#">Stopping Data Leakage</a>
Administrator	<a href="#">ArcGIS Enterprise: Administration Workflows</a>
Administrator	<a href="#">Content Management Techniques</a>
Publisher	<a href="#">Publishing Content and Services</a>

### 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 5 below.

Table 5—Conduct Frequent Awareness Activities

Role	Continuing Education
All roles	<a href="#">Subscribe to ArcGIS Trust Center announcements</a>
	<a href="#">Attend Esri User Conferences</a>
	<a href="#">Review latest ArcGIS Trust Center content</a>

## 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 vulnerability scaing 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

### **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 than 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

██████████—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 6—Alignment of Security and Privacy Principles

Issue/Control	Description	Recommendations
<b>Data Encryption</b>	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.
<b>Authentication and Authorization</b>	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.
<b>Access Logging and Monitoring</b>	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.
<b>Data Minimization</b>	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.
<b>Privacy Settings for Shared Content</b>	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.
<b>Anonymization and Pseudonymization</b>	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.
<b>Retention and Deletion Policies</b>	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.
<b>Privacy Notice and Consent Management</b>	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

Appendices are found in the “ArcGIS Enterprise Hardening Guide: Appendixes” document

Appendix A: **Advanced** Controls & Profile Implementation Checklist

Appendix B: Deployment Diagrams with Ports and Protocols

Appendix C: Web Server Extensions to Allow

Appendix D: HTTP Header Guidance

Appendix E: SIEM Log Shipping Guidance

Appendix F: Case Studies: Misconfiguration Impacts

Appendix G: Security Features by Release

Appendix H: Existing Deployment Control Prioritization

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

Appendix J: Determining Domains to Include for Proxy Allow List

Appendix K: ArcGIS Enterprise 12.1 Ports Utilized Diagram

Appendix L: Software Components

Appendix M: Secure Deployment Patterns cont.

Appendix N: Zero Trust Architecture

Appendix O: ArcGIS gMSA Service Account

Appendix P: Automate ArcGIS Security Patches

Appendix Q: Definitions

## 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

### **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

### **Version 1.19 – Published 3/6/2026**

- Updated recommended ciphers to include AWS and Azure policy references
- Added basic validation check to verify SOE, SOI, and Geoprocessing service installs are expected
- Added New 12.0 security enhancements to Appendix G and removed retired product version
- Update port diagram for Enterprise 12.0 – Appendix K
- AllowedProxy List hyperlink added and secure by default for Enterprise 12 noted
- Basic security profile application security settings added to deployment automation tools
- Delete Legacy API Keys immediately
- Expanded Application/Developer Identity guidance, shifting to Oauth in place of API Keys
- Update Appendix H tables for implementation prioritization order and controls added

### **Version 1.20 – Published 6/11/2026**

- Major structure updates - Assigned all controls identifier, move appendices to separate doc, moved Advanced Profile Controls, Secure Deployment Patterns and ZTA to appendices
- Updated Built-in account policy guidance
- Updated for ArcGIS Enterprise 12.1
- Added certificate update warning