

Technical Deep Dive: ArcGIS Enterprise

Philipp Gintenstorfer

Stefan Jaquemar

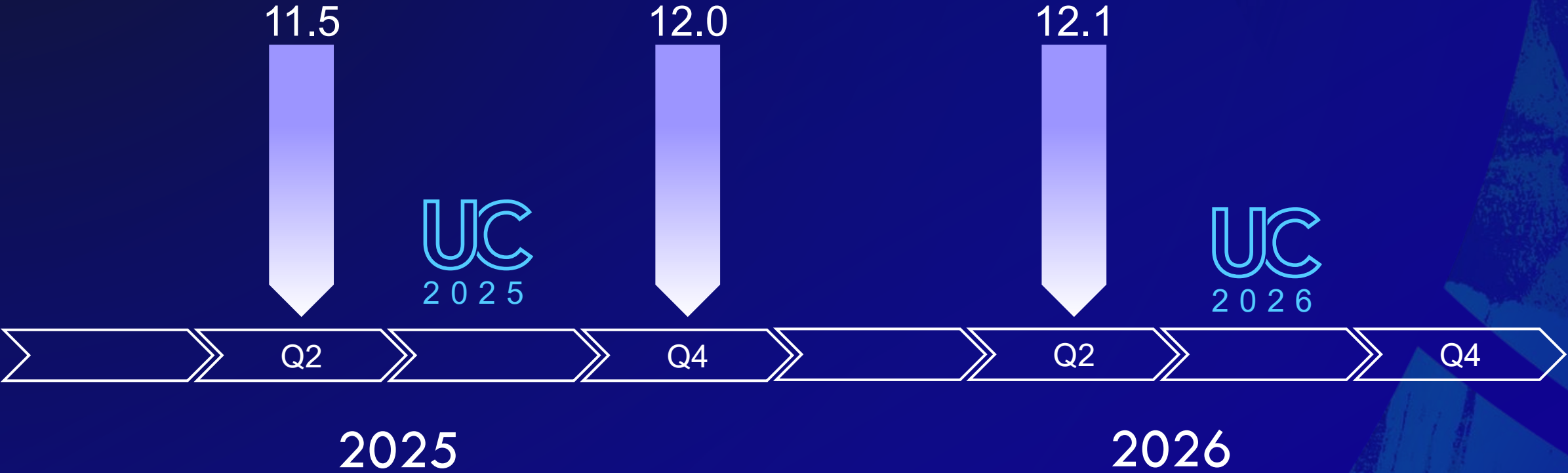
Gerhard “Luigi” Trichtl

*2026 ESRI USER CONFERENCE AUSTRIA
– powered by SynerGIS*

Agenda

- ArcGIS Enterprise – What's New
- ArcGIS Enterprise – Security Best Practice
- ArcGIS Enterprise Q&A
 - Vorabeingereichte Fragen
 - LiveFragen

ArcGIS Enterprise Releases

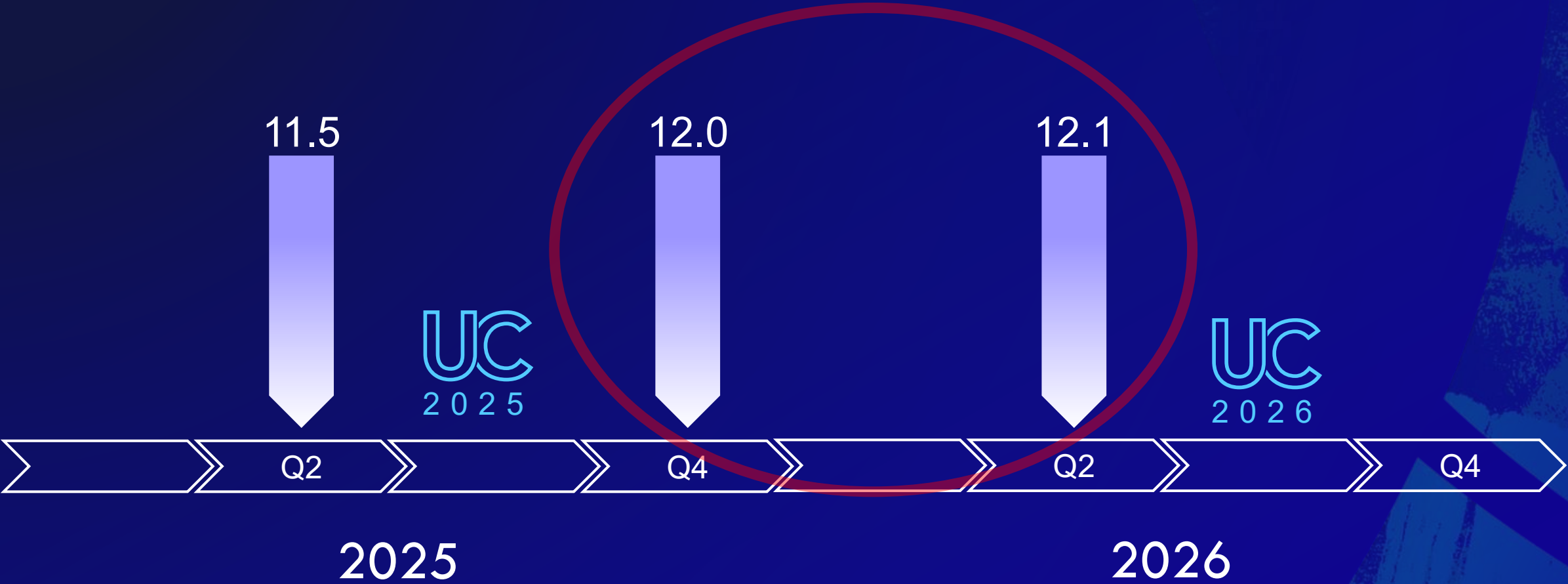


Welche ArcGIS Enterprise Version ist im Einsatz

ArcGIS Enterprise Life Cycle | Esri Support

- Version 12.1, 11.5, 11.3 im Einsatz
- Version 11.1 im Einsatz
 - Stichtag 30. April 2027 bzw. 30. April 2029
- Version 10.9.1 im Einsatz
 - Stichtag 30. Nov. 2027
- Version 12.0, 11.4, 11.2 im Einsatz
 - Stichtag 30. Nov. 2026
- Älter Version im Einsatz?

ArcGIS Enterprise Releases



ArcGIS Enterprise – What's New

Philipp Gintenstorfer

Stefan Jaquemar

2026 ESRI USER CONFERENCE AUSTRIA
– powered by SynerGIS

Agenda

- Änderungen im Lifecycle
- 12.x und Migrationsüberlegungen
- Neuerungen in ArcGIS Enterprise

Änderungen im Lifecycle



Product Lifecycle Phasen

ArcGIS Enterprise - Windows/Linux

	General Availability	Extended Support	Mature	Retirement
Einen Case anlegen	✓	✓	✓	
Online-Supportressourcen	✓	✓	✓	
Softwareupdates und -patches	✓	✓		
Zertifizierung neuer Umgebungen	✓			

ArcGIS Enterprise Product Lifecycle

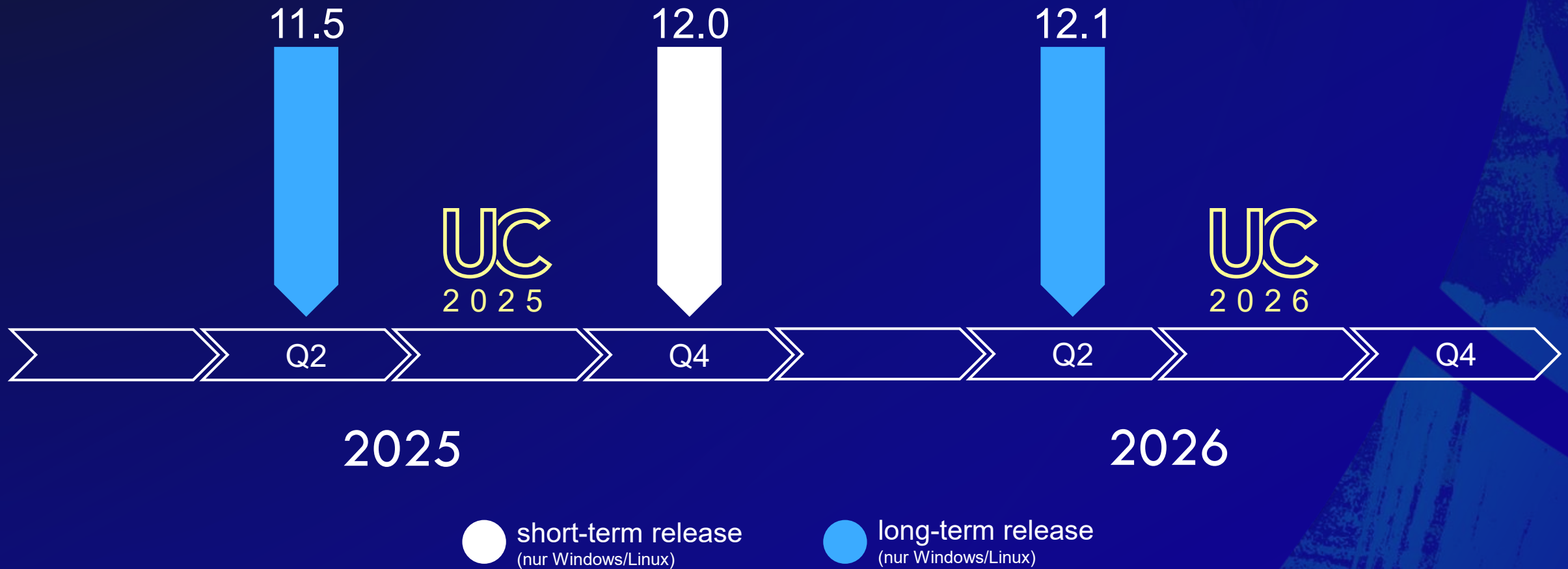
- Bis ArcGIS Enterprise 11.5

	General Availability	Extended Support	Mature	Retired
Short-term support (STS) release	1.5 Jahre	-	1.5 Jahre	3 Jahre
Long-term support (LTS) release	2 Jahre	2 Jahre	2 Jahre	6 Jahre

- Ab ArcGIS Enterprise 12.0

	General Availability	Extended Support	Mature	Retired
Short-term support (STS) Release	~6 Monate (bis zum nächsten Release)	6 Monate	-	~ 1 Jahr
Long-term support (LTS) Release	~1 Jahr (bis zum nächsten LTS Release)	3 Jahre	-	~ 4 Jahre

ArcGIS Enterprise Releases



The background is split into two main sections. The upper section is a solid dark blue with white, intricate topographic contour lines. A curved line separates this from the lower section, which features a photograph of a volcanic landscape. The landscape is dominated by a large, dark, conical volcano in the center, with a plume of dark smoke or ash rising from its summit. The foreground and midground are covered in a field of smaller, rounded volcanic mounds or cinder cones. The sky is a deep, dark purple, and the overall lighting is dramatic, with a strong orange-red glow emanating from the base of the volcano, suggesting an active eruption.

12.x und Migrationsüberlegungen

ArcGIS Enterprise 12.x

ArcGIS Enterprise 12.x enthält keine JavaScript 3.x, sondern JavaScript 4+ Apps.

ArcGIS Enterprise 12.x enthält NICHT: WebAppBuilder, Configurable Apps, Map Viewer Classic.

Auch weitere Features werden retired.

Retirement von *Tile Cache Data Store* und *Metadata Editor classic*

Verwenden Sie ArcGIS Enterprise 11.5, bis Sie bereit für ein Upgrade sind.

Mehr Informationen:



Vorbereitungen zur Migration

ArcGIS Web AppBuilder	ArcGIS Configurable Apps	Map Viewer Classic
Experience Builder ist im Normalfall ein passender Nachfolger. Die Apps müssen vor dem Update auf 12.x abgelöst werden. Für das Upgrade bietet sich der Express Mode an	Instant Apps sind im Normalfall ein passender Nachfolger Viele konfigurierbare App Templates wurden mit Version 11.0 retired. Die Apps müssen vor dem Upgrade auf 12.x migriert werden.	Es ist keine Migration der Items notwendig. Map Viewer ist der moderne Viewer und WebMap Konfigurator. Eventuell ist eine Schulung erforderlich, um sich mit dem Map Viewer vertraut zu machen.

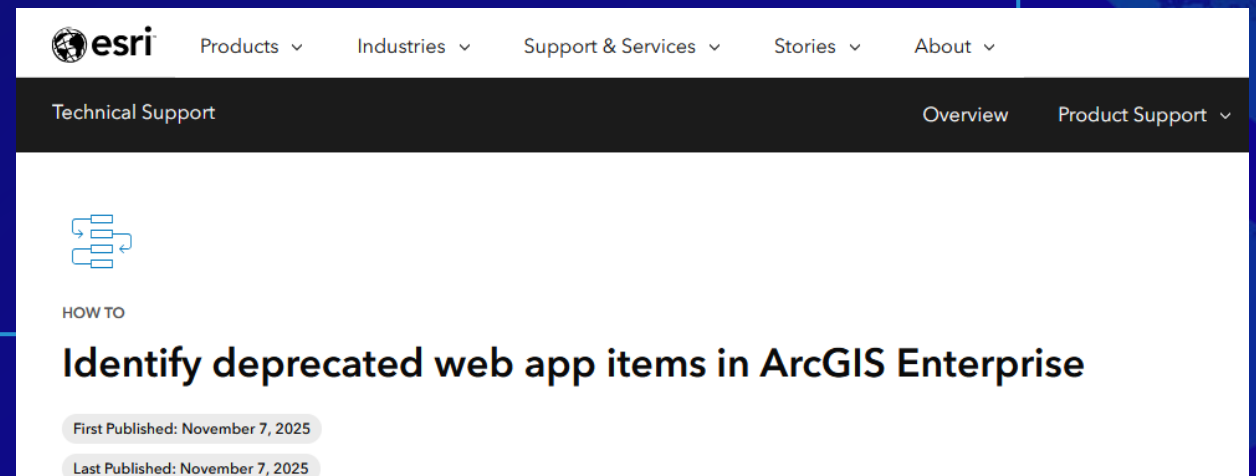
Vorbereitungen zur Migration

retired-apps-cataloger

Script um deprecated Elemente zu erkennen.

<https://support.esri.com/en-us/knowledge-base/script-to-identify-deprecated-web-app-items-in-arcgis-e-000038795>

- Sucht nach "Web Mapping Application" und "AppBuilder Extension" Elementen
- Vergleicht die URLs der Elemente mit einer Liste der bekannten deprecated App Templates
- Ergebnis ist ein CSV-File
- ...



Retirement des Tile Cache Data Store

Der Tile Cache Data Store ist mit 12.0 retired

Der Tile Cache Data Store wurde durch den Object Store ersetzt

Das ArcGIS Enterprise Base Deployment benötigt einen Object Store ab 11.4.

Object Store speichert Hosted Scene Services und andere Systemfunktionen

Hosted Scene Services müssen vor dem Upgrade auf 12.x in den Object Store migriert werden

Es steht eine Migration Utility zur Migration von Hosted Scene Services zur Verfügung

Neuerungen in ArcGIS Enterprise

Neuerungen in ArcGIS Enterprise 12.0 / 12.1 - Auswahl

MapView und Experience Builder: Teilen und zusammenführen

SceneViewer: Unterstützung für Gaussian Splat Layer

Instant Apps: Web Editor template

Experience Builder: Arcade assistant (beta)

Experience Builder: Massenbearbeitung

MapView: Symbolanimation

.NET 10 Support

Individuelles Recht ArcGIS Pro Lizenzen offline zu nehmen

Experience Builder: Map Widget - Locate Tool

Service Management Capabilities für Utility Network Services

Verbesserungen im Response Caching

Benutzer/Inhalt transferieren

Experience Builder: Theme Mode Switcher

Neue Dokumentationswebsite

Living Atlas Update

Distributed Collaboration Updates

Experience Builder: Date Filter

Update to Create/Join/Upgrade experience and Licenses tab

Verbesserungen bei 3D Layern

MapView: What's here? Tool für Custom Geocoders

Metrics API

Service Interceptors

Serververzeichnis in Cloud konfigurierbar

ArcGIS Data Pipelines

Experience Builder: import and export drawings

TLS Zertifikate einspielen ohne Neustart

MapView: Zeitbasierte Layersichtbarkeit

Experience Builder: Copy/Paste Features

Möglichkeit die Portal URL für eine ArcGIS Lizenz zu validieren

Service Interceptors

ArcGIS Velocity

Advanced Editing Tools im Map Viewer

Unterstützung für Shared Templates im Map Viewer

Experience Builder und Web Editor: Kurvensegmente zeichnen

User Type Updates mit neuen Produkten

MapView: Zeitbasierte Layersichtbarkeit

MapView: Daten mit Drag and Drop hinzufügen

ArcGIS Enterprise Metrics API

Wie interagieren die User mit meiner neu angelegten Experience?

Wann ist ein guter Zeitpunkt für ein Wartungsfenster?

Bei welchen Services besteht ein Missverhältnis zwischen konfigurierter Service-Kapazität und tatsächlicher Nutzung?

ArcGIS Enterprise Metrics API

Voraussetzungen

- API Key Credentials mit “Observability” Privileg
- Prometheus Server zum Abgreifen der API
- Visualisierung mit Drittsoftware wie z.B. Grafana

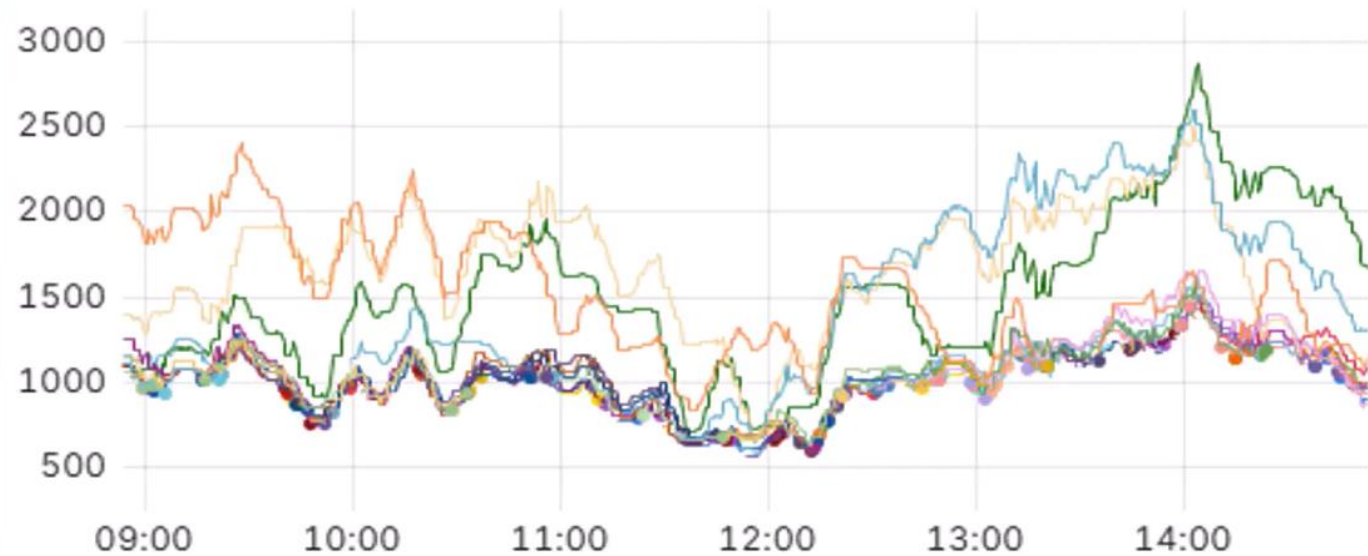


Prometheus



Grafana

Service Requests (req/hr) by User,App



Name	Max ▾	Mean ▴
userName9,arcgisinstantapps	2875	1512
userName9,dashboards	2607	1545
userName9,arcgisonline	2507	1674

Useraktivität pro Applikationstyp

Response Caching

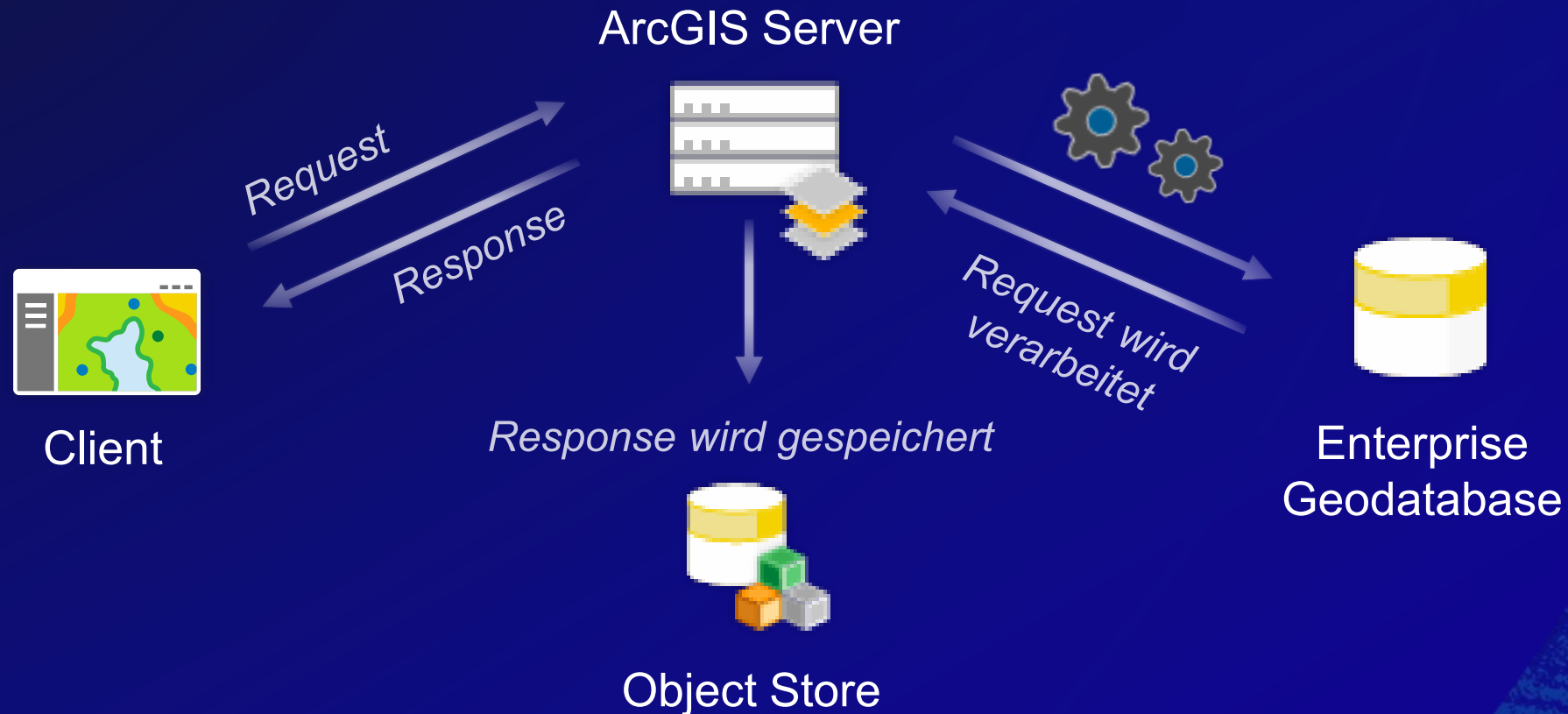
Response caching ist ein Server-Mechanismus, der die Performance von Layern in ArcGIS Enterprise erhöht, indem er die Antworten für Daten, die sich nicht geändert haben, zwischenspeichert.

Identische Requests werden nicht an die Datenbank geschickt.

Bisher in ArcGIS Online und für Hosted Feature Layer in ArcGIS Enterprise verfügbar.

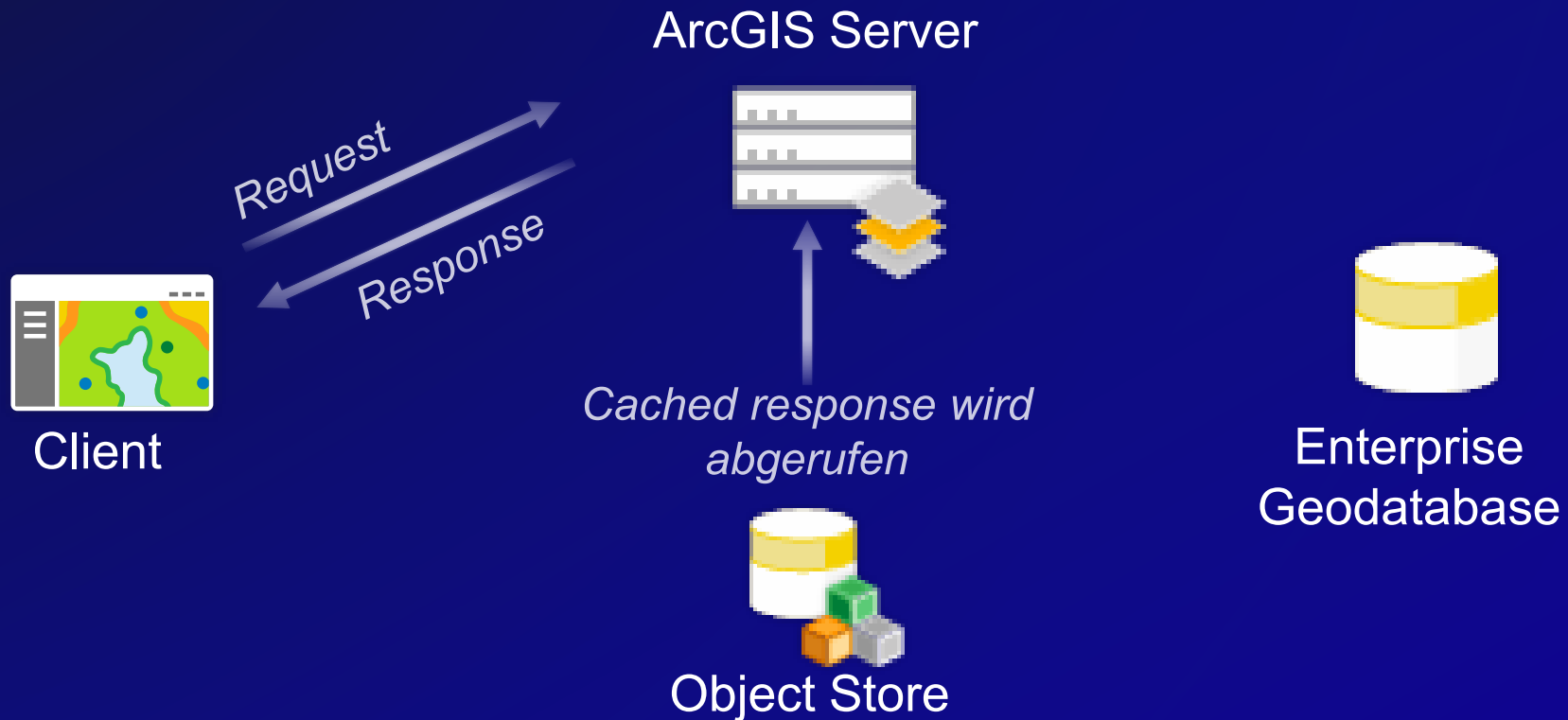
Response Caching

Der Response vom ersten Request wird im Object Store gespeichert (cached).



Response Caching

Nachfolgende Requests der gleichen Daten werden schneller abgerufen.



Response Caching

Neuerungen mit ArcGIS Enterprise 12.1:

- 1 Die Aktivierung kann direkt auf der Elementübersicht im Portal erfolgen.**
Bisher konnte Response Caching nur über die Admin API aktiviert werden.
-

- 2 Response Caching wird auch für Feature Layer und Map Image Layer unterstützt die auf Vektor-Daten aus einer Enterprise Geodatabase referenzieren.**
Bisher war Response Caching nur für Hosted Feature Layer unterstützt.

Mitglieder und Inhalte übertragen

Mitglied übertragen

Inhalt, User Type und Rolle eines Mitglieds können über einen Dialog auf ein anderes Mitglied übertragen werden

Mitglied übertragen

1. Neues Mitglied

2. Inhalt und Gruppen

3. Zusätzliche Einstellungen

Übertragung von

MA

Mark Aurel

m.aurel

Benutzertyp:
Professional

Rolle:
Publisher

☒ Konto beibehalten

☐ Konto löschen

☐ Benutzertyp und Rolle nach der Übertragung ändern

Übertragen zu

ES

Egon Schiele

e.schiele

Benutzertyp und Rolle werden geändert, um eine Übereinstimmung mit m.aurel sicherzustellen

Aktueller Benutzertyp:
Creator

→

Neuer Benutzertyp:
Professional

Aktuelle Rolle:
Benutzer

→

Neue Rolle:
Publisher

Abbrechen

Weiter

Inhalt übertragen

Die Inhalte eines Mitglieds können über einen Dialog auf ein anderes Mitglied übertragen werden

Inhalt übertragen

Neuer Besitzer

ES

Egon Schiele

e.schiele

Zu übertragender Inhalt

4

Alle anzeigen

Optionen für Zielordner

☒ Ordnerstruktur beibehalten

☐ Einen Ordner für den gesamten Inhalt auswählen

Abbrechen

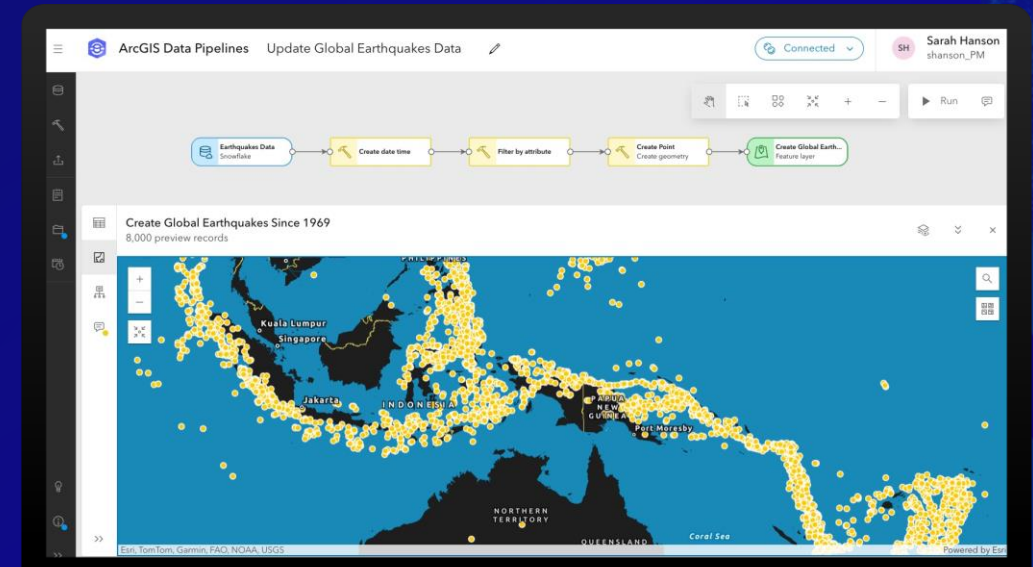
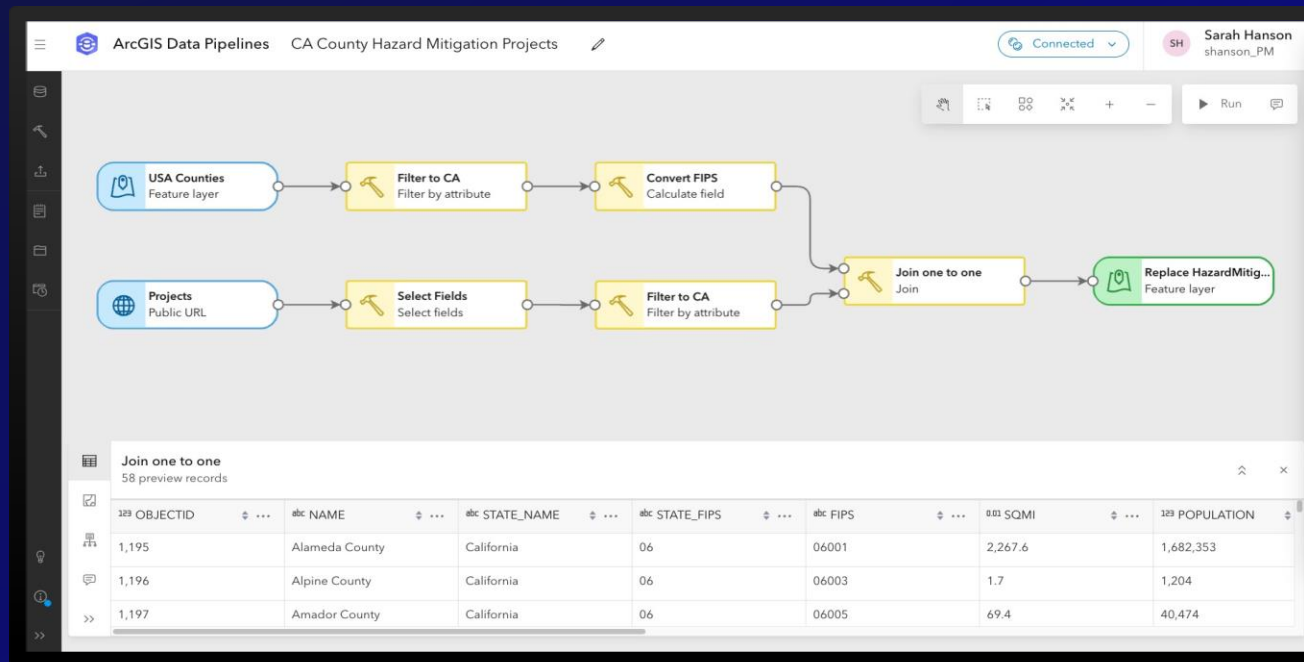
Übertragen



ArcGIS Data Pipelines Server

Mit ArcGIS Enterprise 12.1 verfügbar

ArcGIS Data Pipelines ist eine visuelle, no-code-basierte Datenverarbeitungsfunktion, zur Aufbereitung und Integration von Daten für Karten und Analysen.



ArcGIS Velocity for ArcGIS Enterprise

Mit ArcGIS Enterprise 12.1 verfügbar

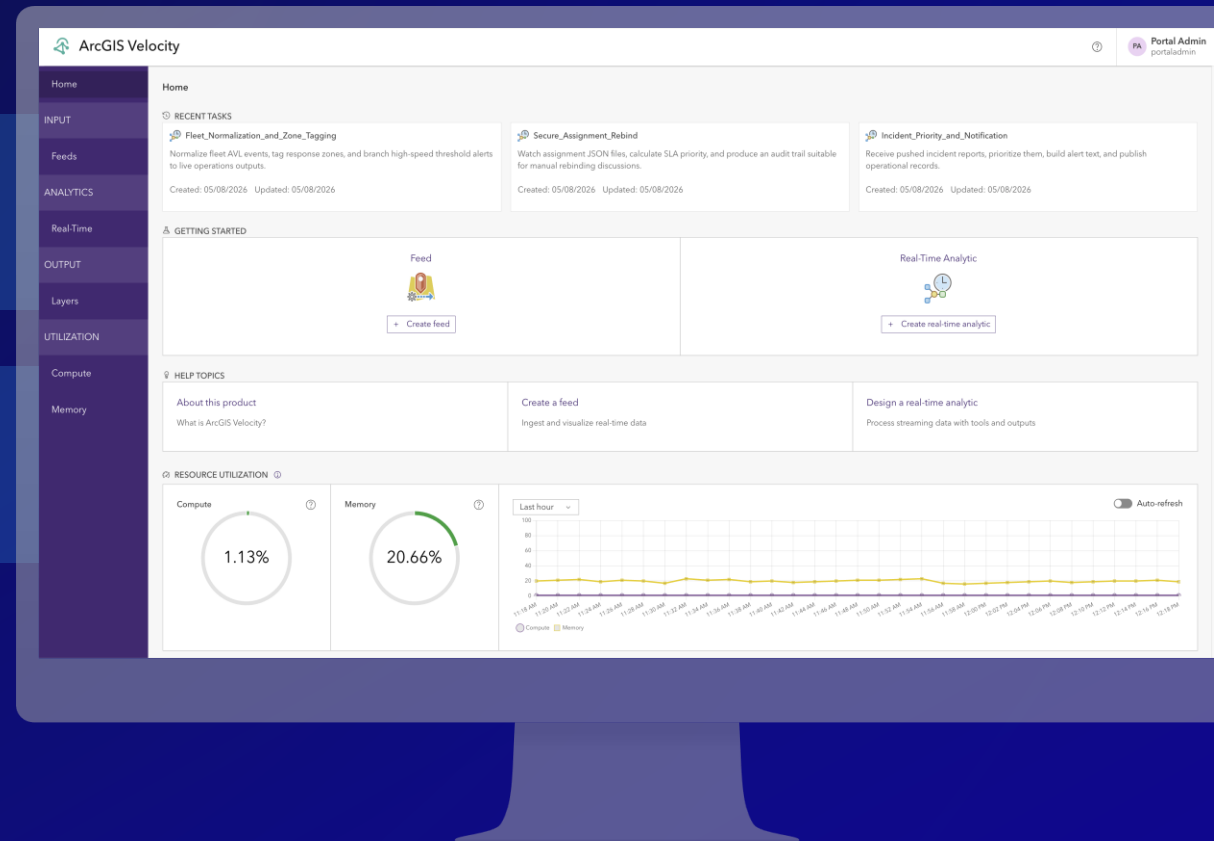


*Erfasst und analysiert
Echtzeitdaten*

*Unterstützt Streams von IoT
Sensoren, Message Brokers
& APIs von Drittanwendungen*

*Single-machine Windows
& Linux Deployments*

*Ersetzt den
GeoEvent Server*

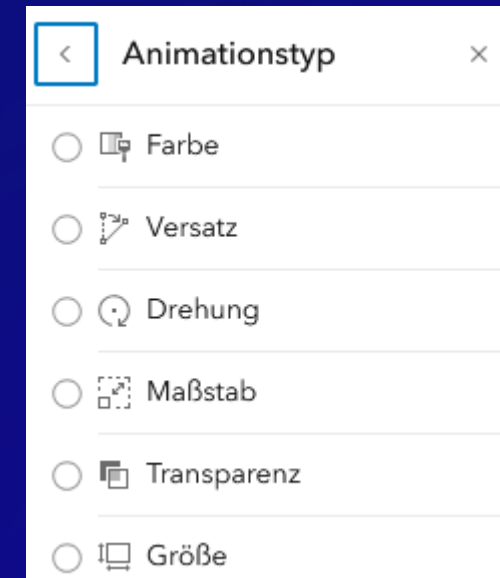
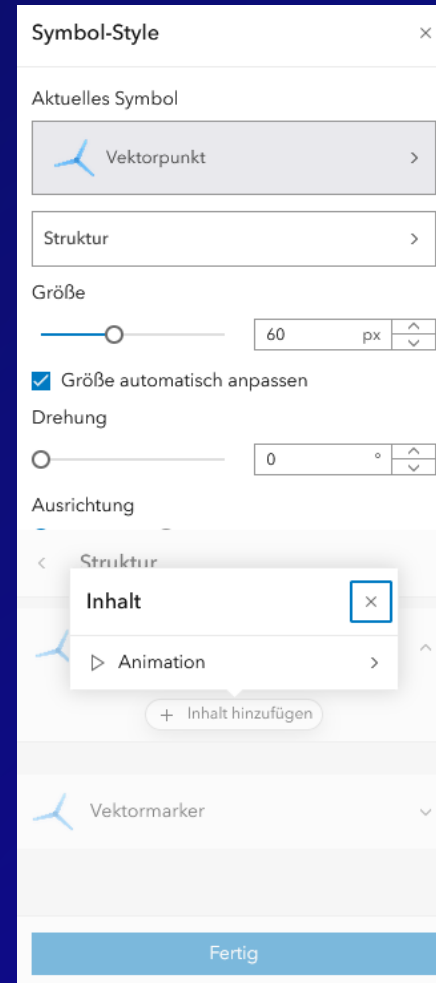


Neuerungen in den Applikationen

- MapViewer: Symbolanimation
- MapViewer: Zeitbasierte Layersichtbarkeit
- MapViewer und Experience Builder: Teilen und zusammenführen
- Experience Builder: Copy/Paste Features
- Experience Builder: Batchbearbeitung
- Experience Builder und Web Editor: Kurvensegmente zeichnen

MapView: Symbolanimation

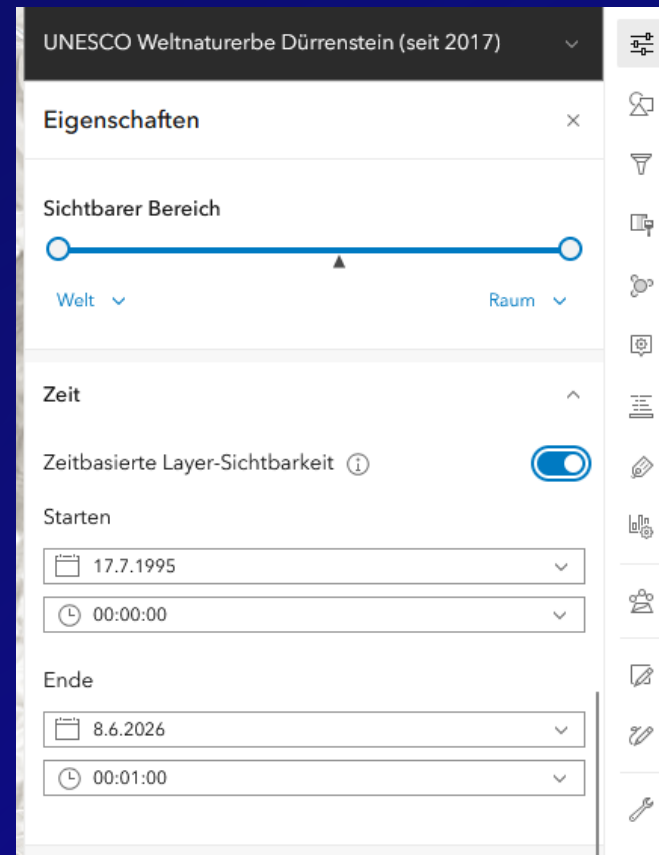
- Auswahl im Symbol-Style-Menü via Struktur -> Animation
- Es stehen verschiedene Animationstypen zur Auswahl



MapView: Zeitbasierte Layersichtbarkeit

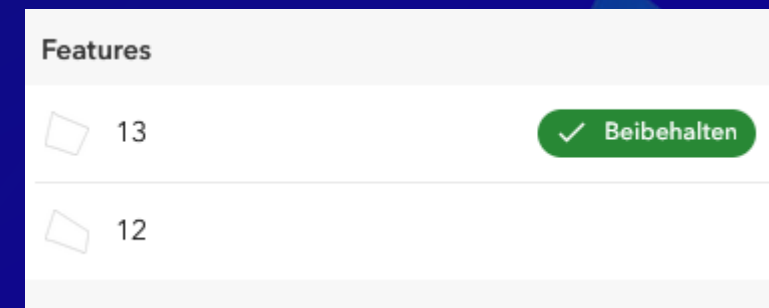
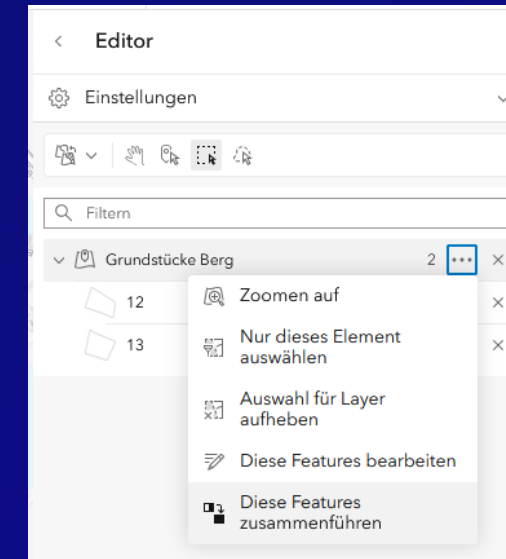
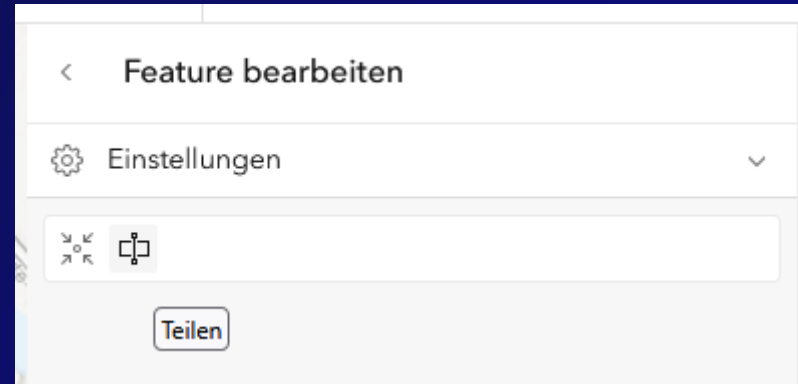
Layer werden nur in einem bestimmten Zeitraum dargestellt, wenn ein Zeitschieberegler konfiguriert ist

Die Konfiguration erfolgt in den Layereigenschaften



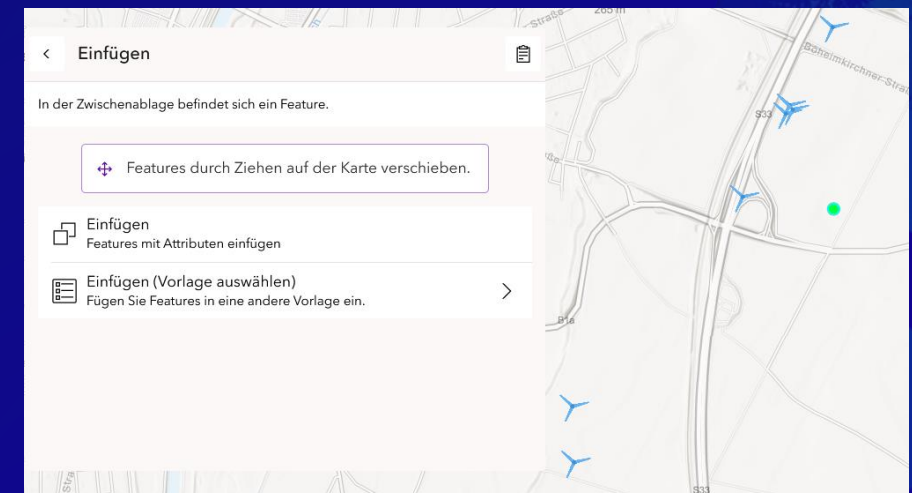
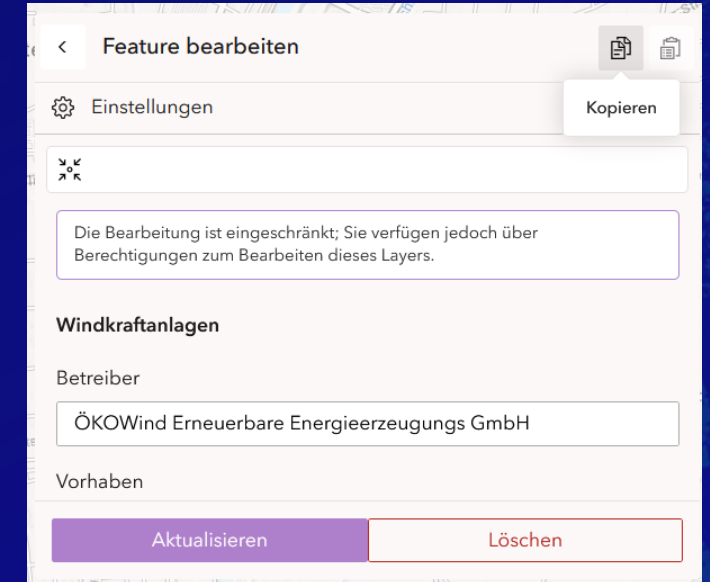
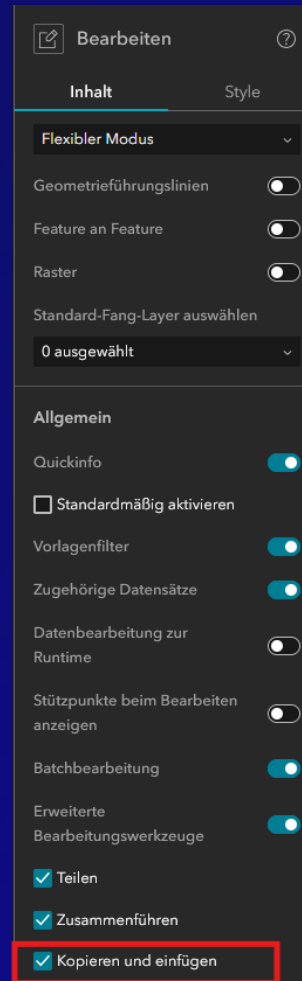
MapView und Experience Builder: Teilen und zusammenführen

- Für das Teilen mittels Teilungslinie muss im Experience Builder “Teilen” aktiviert sein
- Für das Zusammenführen im Experience Builder müssen die “Batchbearbeitung” und “Zusammenführen” aktiviert sein



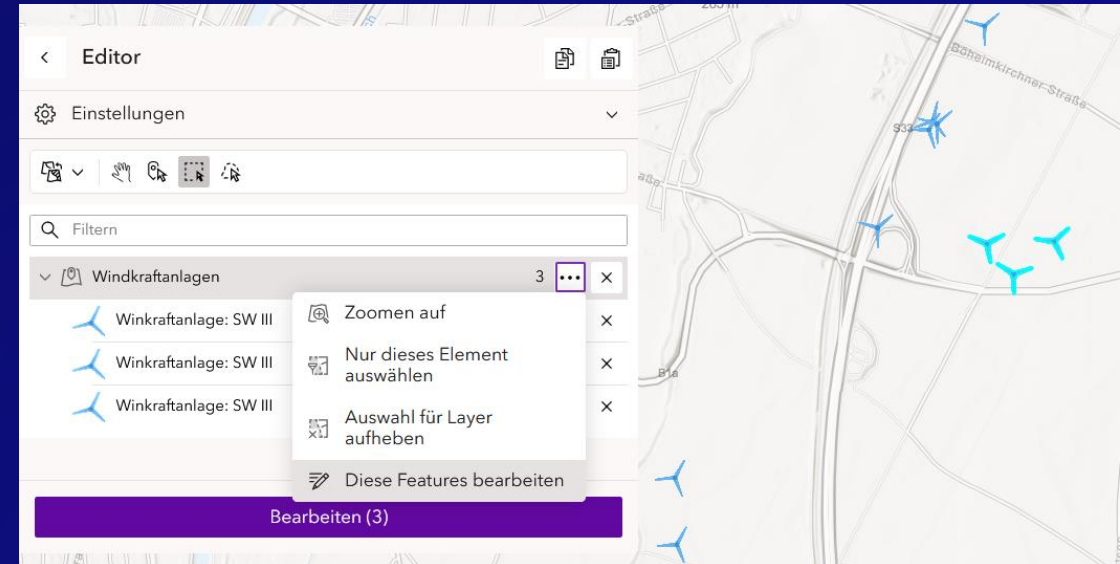
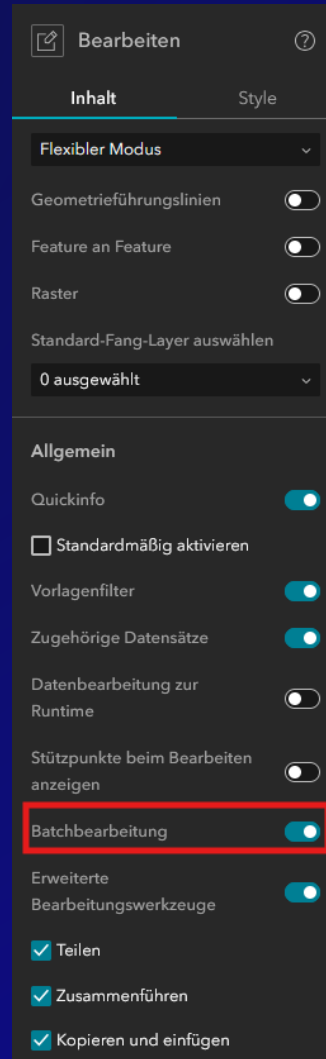
Experience Builder: Copy/Paste Features

- In den Einstellungen muss “Kopieren und Einfügen” aktiviert sein
- Kopiert ein Features mit seinen Attributen an eine neue Position



Experience Builder: Batchbearbeitung

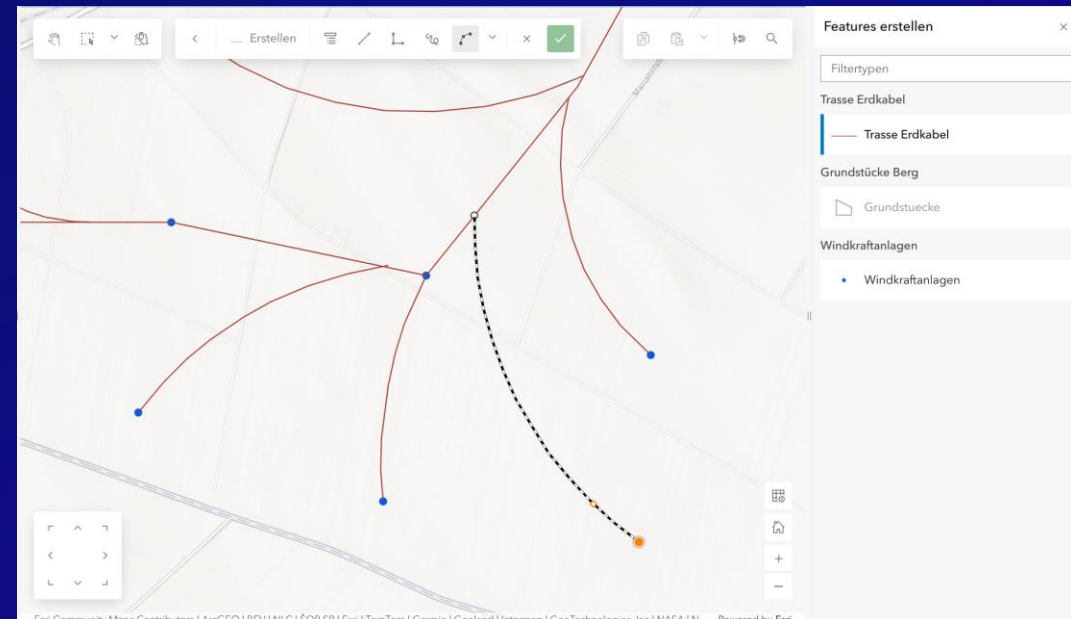
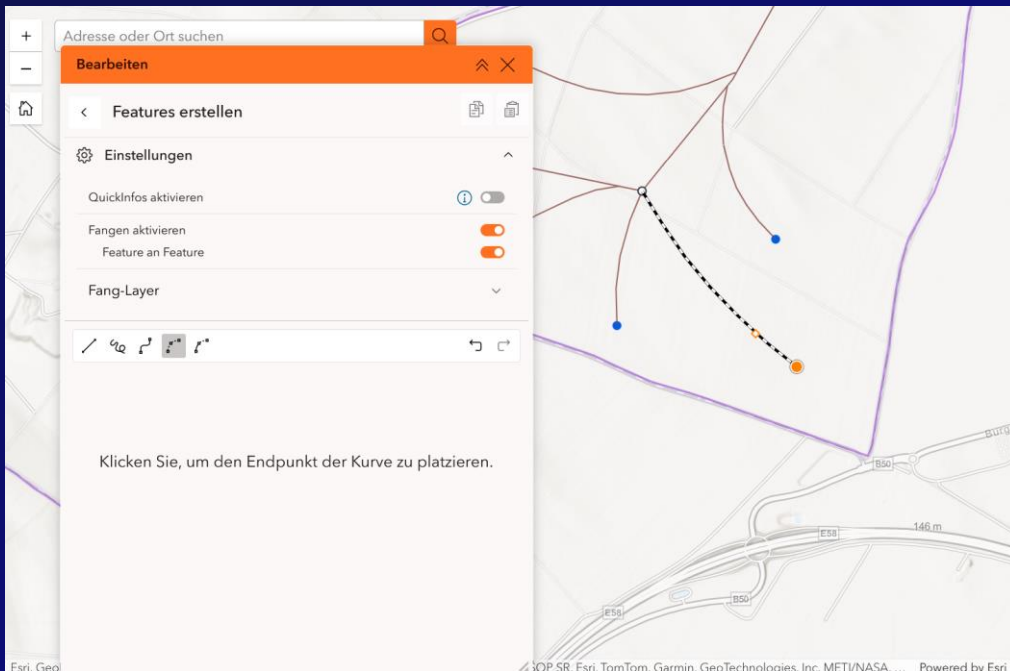
- Parallele Bearbeitung von mehreren Features
- Dazu muss im Experience Builder “Batchbearbeitung” aktiviert sein



Experience Builder und Web Editor: Kurvensegmente zeichnen

- Experience: “Bogensegment” oder “Endpunkt-Bogensegment” bei Linientyp auswählen

- Web Editor: “Bogensegement” bei Linientyp auswählen

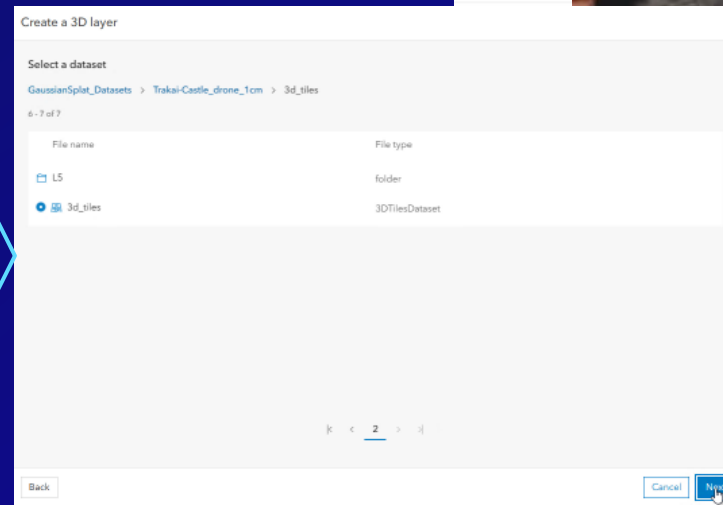
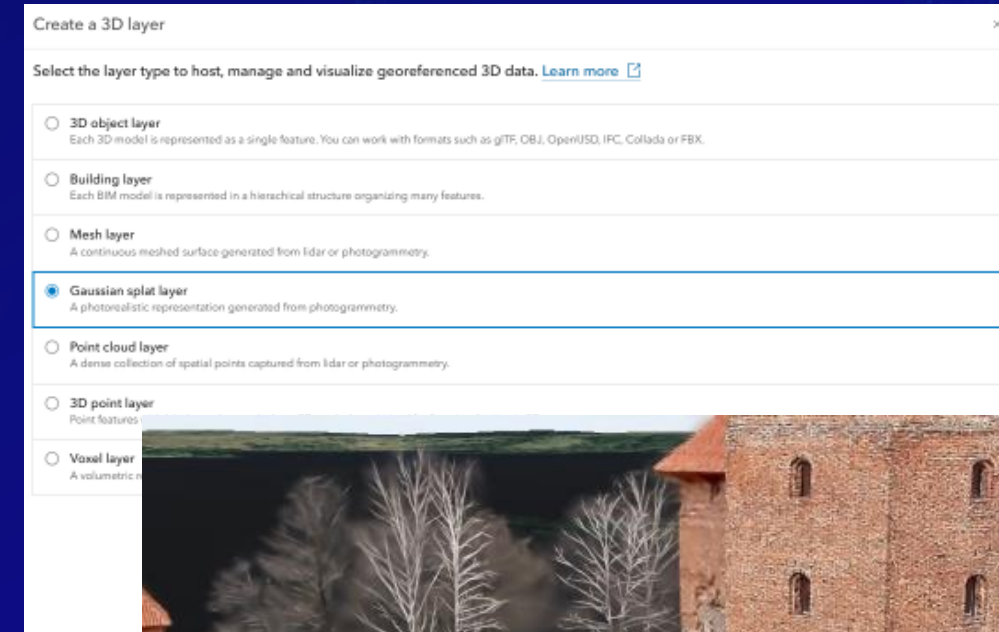


Gaussian Splat Layer

- Hosted Gaussian Splat Layer publizieren
 - Daten liegen im Object Store oder alternativ bei großem Datenvolumen referenziert
 - Visualisieren zusätzlich im Scene Viewer und Experience Builder möglich

[Gaussian Splat Explorer](https://experience.arcgis.com/experience/e2e1e497d13b41cab368c894fd9b3df7)

<https://experience.arcgis.com/experience/e2e1e497d13b41cab368c894fd9b3df7>



Mesh



Gaussian Splats



Captured with Drone, GSD: 0,4" (1 cm),

Mesh



Captured with: Vexcel UltraCam Osprey 4.1 GSD: 1,8" (4cm),
Altitude: ~3,300 ft (~1000m), overlap 80/60%
Data courtesy of GeoFly & City of Stuttgart

Scene1

Gaussian Splats



285 m

9,1930679°E 48,7882444°N 0 m

Selected Features: 0

ArcGIS Enterprise – Security Best Practice

Gerhard “Luigi” Trichtl

*2026 ESRI USER CONFERENCE AUSTRIA
– powered by SynerGIS*

Agenda

ArcGIS Enterprise: Security Best Practices

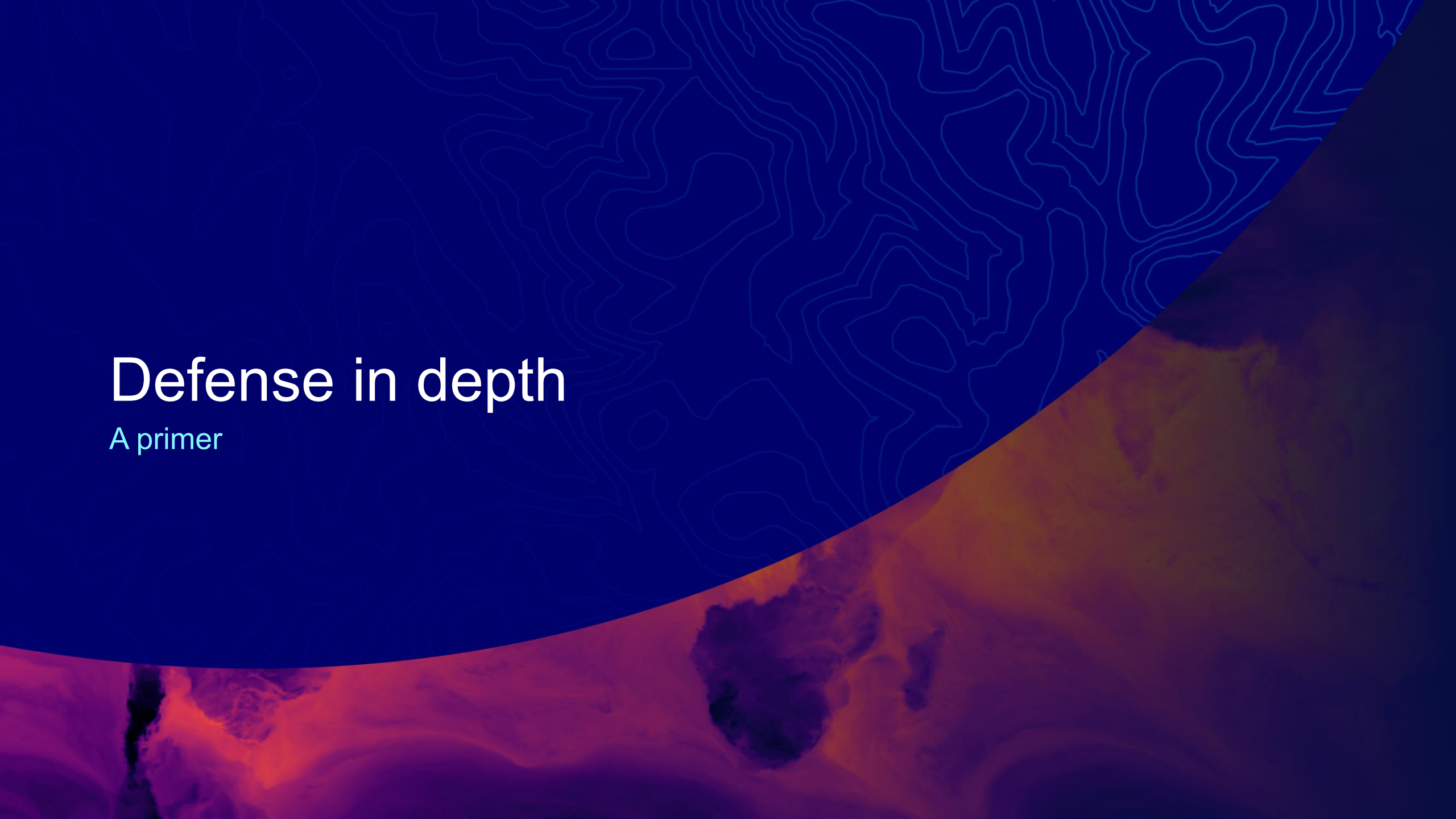
- Focus: Security best practices for ArcGIS Enterprise
- Intro
- Defense in depth
- Security options
- Docs and tools
- Questions



Strongly Recommend:

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





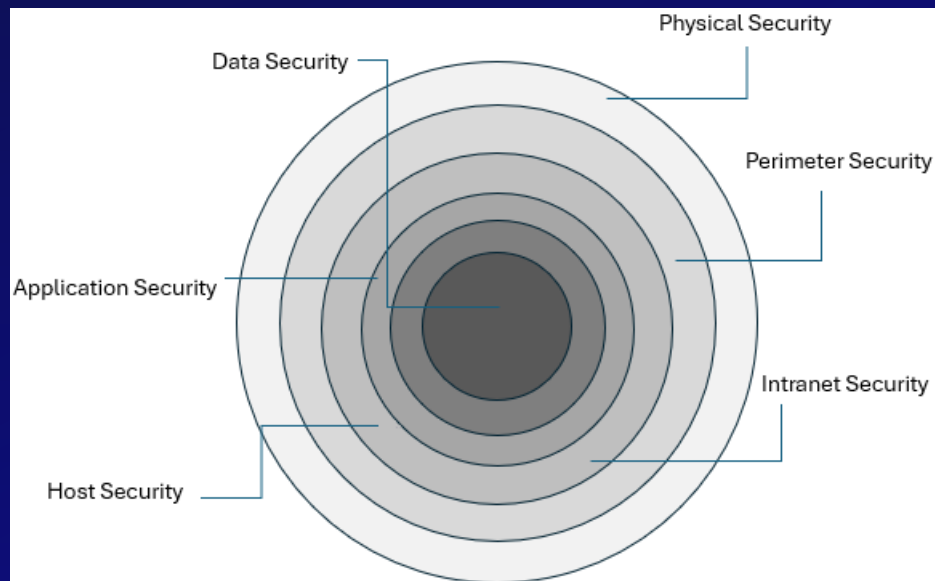
Defense in depth

A primer

Defense In Depth Paradigm

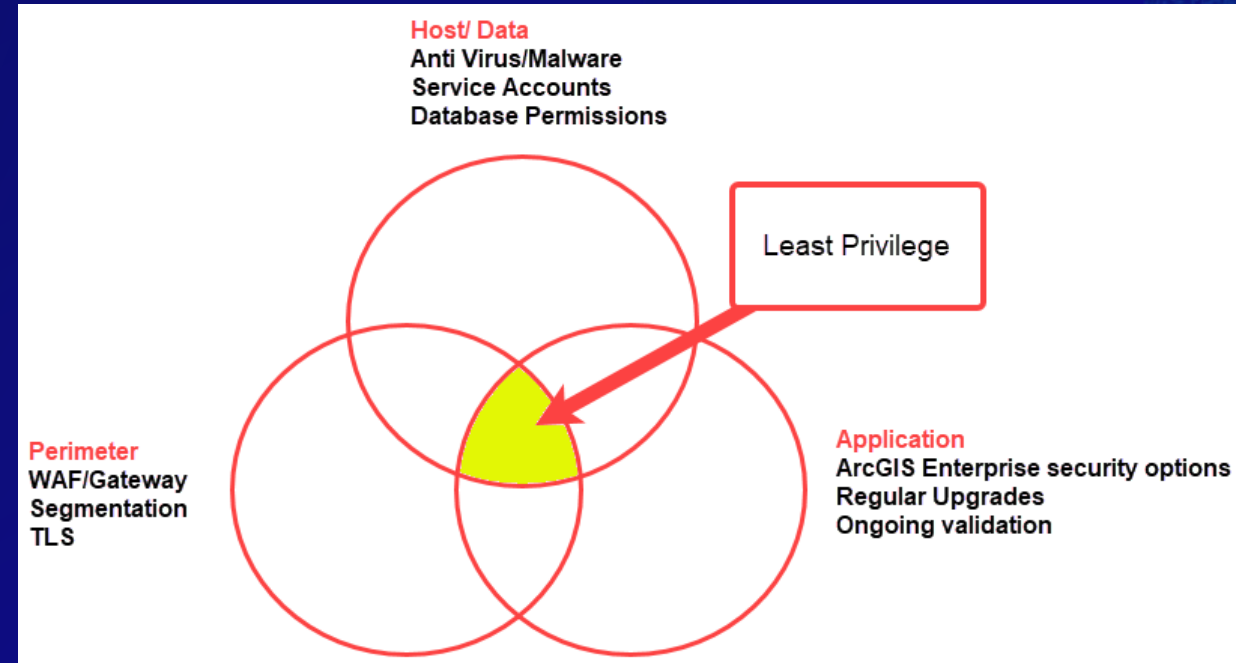
Esri provides tools, but can't compensate for tools beyond the application tier

- Security plans have many “**layers**” – **multiple levels of security**
- Layered security mechanisms increase the security of the system as a whole
- Each feature discussed is considered a “layer”
- WAF, SIEM, Anti-Virus, Encryption, SAML/OIDC identity stores, application config, etc



Fundamentals

- Principle of LEAST privilege
 - **NOT Principle of MOST privilege**
 - Limit admin accounts.
 - Use custom roles
 - Limit Service account permissions
 - Use gMSA (Group Managed Service Accounts)
 - Upgrades are important
 - Updated components/features



Upgrades are important

Patches are also important

Yes, upgrades can be painful

But...

- Updates to 3rd party components with each release
 - Reduce noise from security scans
- Access to new functionality
 - New logging functionality in 11.4/11.5
 - New Content Security Policy support at 11.4/11.5
- Automate patchNotification
 - PatchNotification can be scheduled
 - CRON job or Windows Scheduled task

:: Typical usage:

```
:: > patchnotification.bat -c          # Show patch information
:: > patchnotification.bat -c -i sec  # Install security patches only for
::                                  # installed products
:: > patchnotification.bat -c -i all  # Install all available patches for
::                                  # installed products
```

```
C:\Program Files\ArcGIS\Portal\tools\patchnotification>patchnotification.bat -c
=====
                        ArcGIS Enterprise Patch Notification
=====

Installierte Komponenten

ArcGIS Data Store          11.5
ArcGIS Server              11.5
Portal for ArcGIS          11.5
=====

Verfügbare Aktualisierungen

ArcGIS Data Store
  (keine Aktualisierungen verfügbar)

ArcGIS Server
  - ArcGIS Server Feature Services Security Patch (!)
    https://support.esri.com/en-us/patches-updates/2025/arcgis-server-feature-services-security-patch
    Veröffentlichungsdatum: 07.10.25

Portal for ArcGIS
  - Portal for ArcGIS Mission Manager Location Services and Projection Patch
    https://support.esri.com/en-us/patches-updates/2025/portal-for-arcgis-mission-manager-location-services-and-proje
tion-patch
    Veröffentlichungsdatum: 06.10.25
=====

Installierte Patches
  - Portal for ArcGIS 11.5 Mission Manager Location Services and Projection Patch
  - Portal for ArcGIS 11.5 Web Applications Patch
  - ArcGIS Server 11.5 Branch Versioning Licensing Patch
  - ArcGIS Server 11.5 Calculate Field Patch
  - ArcGIS Server 11.5 Utility Network Patch 1
  - ArcGIS Server 11.5 ArcGIS Pipeline Referencing/ArcGIS Roads and Highways Patch 1
=====

Um eine vollständige Liste der Patches und Service Packs von Esri zu durchsuchen, besuchen Sie die Support-Website von E
sri:
http://support.esri.com/Downloads
```

Security options





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



Copyright © 2026 Esri
All rights reserved

ID	Guide	Section	Profile	Action	Security Control Name
AS-B1	Application Security		Basic	Configure	Portal for ArcGIS Proxy Allow List
SI-B1	Supporting Infrastructure		Basic	Avoid	Forward Proxy Authentication
AS-B2	Application Security		Basic	Disable	Primary Site Administrator (PSA) account
AS-B3	Application Security		Basic	Implement	Password Reset Email Notification
SI-B2	Supporting Infrastructure		Basic	Implement	Web Application Firewall (WAF)
IM-B1	Inventory and Maintenance		Basic	Implement	Security Patches within One Month
IA-B1	Identity and Access		Basic	Configure	All Administrator Accounts with MFA
AS-B4	Application Security		Basic	Verify	Services
AS-B5	Application Security		Basic	Verify	Standardized Queries are Enabled
AS-B6	Application Security		Basic	Verify	Server System Services Secured
AS-B7	Application Security		Basic	Verify	Token Acquisition via HTTP GET is Disabled
AS-B8	Application Security		Basic	Verify	Portal for ArcGIS Legend Servlet is Disabled
AS-B9	Application Security		Basic	Verify	Portal for ArcGIS Print Servlet is Disabled
AS-B10	Application Security		Basic	Verify	Portal for ArcGIS WFS Servlet is Disabled
IA-B2	Identity and Access		Basic	Implement	Personal Secrets Management
IA-B3	Identity and Access		Basic	Implement	SAML Signed and Encrypted Assertions
IA-B4	Identity and Access		Basic	Implement	Group-Based Sharing
IA-B5	Identity and Access		Basic	Manage	Content via Role-based Access Control (RBAC)
DP-B1	Data Protection		Basic	Implement	Whole Disk Encryption
DP-B2	Data Protection		Basic	Verify	HTTPS is Enforced
DP-B3	Data Protection		Basic	Implement	Signed CA Certificates
DR-B1	Detection and Response		Basic	Manage	Webhooks
IA-B25	Identity and Access		Basic	Implement	User Authentication for most developer use cases
IA-B26	Identity and Access		Basic	Implement	App Authentication for automation
IA-B27	Identity and Access		Basic	Avoid	API Key Authentication for sensitive content
IA-B28	Identity and Access		Basic	Manage	SOE, SOI and Geoprocessing Services
AS-B11	Application Security		Basic	Configure	Built-In Accounts Password Policy
AS-B12	Application Security		Basic	Verify	Self-Creation of Built-In User Accounts is Disabled
IA-B6	Identity and Access		Basic	Avoid	Embedding User Identities in Scripts
IA-B7	Identity and Access		Basic	Avoid	Embedding Application Identities in Client Apps
IA-B8	Identity and Access		Basic	Avoid	Storing Secrets in Source Code
IA-B9	Identity and Access		Basic	Disable	Members Can Share Content Publicly
IA-B10	Identity and Access		Basic	Disable	Public User Profile Sharing for organization users
IA-B11	Identity and Access		Basic	Configure	Decentralized Profile Visibility
AS-B13	Application Security		Basic	Verify	Nosniff Header Enabled
AS-B14	Application Security		Basic	Verify	featureServiceXSSFilter to "input"
AS-B15	Application Security		Basic	Verify	XSSPreventionEnabled to "true"
AS-B16	Application Security		Basic	Disable	ArcGIS Portal Directory
AS-B17	Application Security		Basic	Disable	ArcGIS Server Services Directory
AS-B18	Application Security		Basic	Remove	Silverlight and FLEX Policy Files

5 Things you can do today to Harden Any Environment

June 2026 ArcGIS Security Bulletin

- SMTP Server for Password Reset
- MFA / SAML / OIDC
- Disable Initial Admin Account/PSA
- Reduce ArcGIS Server Account Privileges (to default state)
- Upgrade & Patch!

Built-In-User – enforce MFA

AKA: ArcGIS Logins

- When using Built-In-User enhance the Security with MFA
- Now with 12.0 you could enforce it
- Also configure exception Lists e.g. automatic Processes, where you need to sign in and have no option for MFA

Multifactor authentication

Multifactor authentication provides all members with built-in portal accounts in your organization with an extra layer of security by requesting additional information at the time of login to verify that it's you. Email settings must be configured to enable Multifactor authentication. [Learn more about multifactor authentication](#)

For SAML, and OpenID Connect, check with your identity provider.

Enable multifactor authentication for organization.



MFA adoption status

Total adoption

Status for all members with ArcGIS logins



MFA enforcement

Enforcing MFA ensures your members have their accounts secured, improving the security of your organization. When MFA is enforced, members will be required to set up multifactor authentication for their accounts in order to sign in.

 Enforce MFA

MFA exemption list

Exempt some members from being required to set up MFA in order to sign in to their accounts when MFA is enforced.

[Manage exemption list](#)

Members in exemption list: 0

Use SAML or OpenID Connect

AKA: Organization Specific Logins

- Centralized user repository – use your existing identity provider
- Automatically integrates with MFA
 - MFA for ArcGIS accounts also available
 - Requires email server integration
 - Requires two Admin Accounts
- Industry standard
- Can be configured to auto-assign ArcGIS Enterprise Group Membership
- Configuration Details:
 - [Configure a SAML-compliant identity provider with a portal—Portal for ArcGIS | Documentation for ArcGIS Enterprise](#)
 - [Configure OpenID Connect logins—Portal for ArcGIS | Documentation for ArcGIS Enterprise](#)

Security Assertion Markup Language (SAML)

<https://doc.arcgis.com/en/arcgis-online/administer/saml-logins.htm>

- Single Sign On
- Automatically integrates with MFA
- Industry standard



Security Assertion Markup Language (SAML)

<https://doc.arcgis.com/en/arcgis-online/administer/saml-logins.htm>

Home > SSP Cloudlab > Enterprise applications > Enterprise applications | All applications > ArcGIS Online

ArcGIS Online | SAML-based Sign-on

Enterprise Application

[Test this application](#) [Get feedback?](#)

[Upload metadata file](#)

Read the [configuration guide](#) for help integrating ArcGIS Online.

- Basic SAML Configuration** [Edit](#)

Identifier (Entity ID)	softwaresecurity.maps.arcgis.com
Reply URL (Assertion Consumer Service URL)	https://softwaresecurity.maps.arcgis.com/sharing/rest/oauth2/saml/signin
Sign on URL	https://softwaresecurity.maps.arcgis.com
Relay State (Optional)	Optional
Logout URL (Optional)	https://softwaresecurity.maps.arcgis.com/sharing/rest/oauth2/saml/signout
- Attributes & Claims** [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
groups	user.groups
- SAML Certificates** [Edit](#)

Token signing certificate	Active
Status	Active
Thumbprint	A90A32E57EC0249E8162F5A486F4F80C2780128D
Expiration	8/3/2026, 12:23:28 PM
Notification Email	gponto@sspazlaboutlook.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/91f5663a-841b-... Download
Certificate (Base64)	Download
Certificate (Raw)	Download

Federation Metadata XML [Download](#)

Verification certificates (optional)

Required	Yes
----------	-----

Edit SAML login

You can set up your organization so that your users will be able to sign in to ArcGIS using the same username and password that they use with your existing on-premises systems.

Name:

Entra ID (SAML)

Your users will be able to join:

[Automatically](#) [Upon invitation from an administrator](#)

Metadata source for Enterprise Identity Provider:

[URL](#) [File](#) [Parameters specified here](#)

[Choose File](#) No file chosen

> Show advanced settings

Link to download the service provider metadata:

https://softwaresecurity.maps.arcgis.com/sharing/rest/portals/Yb91cD6b0oQRV7uE/sp/metadata?signature=Z2xr [Download](#)

[Download service provider metadata](#)

[Delete login](#) [Save](#) [Cancel](#)

Web Application Firewall (WAF)

<https://trust.esri.com>



930130	Restricted File Access Attempt	Enabled
931100	Possible Remote File Inclusion (RFI) Attack: URL Parameter using IP Address	Disabled
931110	Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameter Name used w/URL Payload	Enabled
931120	Possible Remote File Inclusion (RFI) Attack: URL Payload Used w/Trailing Question Mark Character (?)	Disabled

931130	Pi
932100	Ri
932105	Ri
932106	Ri
932110	Ri
932115	Ri
932120	Ri
932130	Ri
932140	Ri
932150	Ri
932160	Ri
932170	Ri
932171	Ri
932180	Ri
932190	Ri
933100	Pi
933110	Pi
933111	Pi
933120	Pi
933130	Pi
933131	Pi
933140	Pi
933150	Pi
933151	Pi
933160	Pi
933161	Pi
933170	Pi
933180	Pi
933190	Pi
933200	Pi
933210	Pi
941100	Xi
941101	Xi
941110	Xi
941120	Xi

WAF Policy Settings

The following settings should be applied to the WAF Policy/Protection Rules that protects ArcGIS Enterprise for all deployments to ensure ArcGIS Enterprise traffic is correctly inspected while minimizing instances of false blocks/detections.

WAF Exclusions by IP/Network:

The following table outlines suggested WAF Policy exclusions which must be implemented along with the above Core Ruleset rules to allow ArcGIS Enterprise to function when deployed behind a WAF:

Description	Example IP / Network(s)	WAF Protection
ArcGIS Enterprise Network Segment	10.x.x.x/24 172.16.x.x/24	Disabled
ArcGIS Enterprise Outbound Public IPs	54.x.x.x/32	Disabled
Administration Network Segment	10.x.x.x/24 172.16.x.x/24	Disabled
General Private IPs	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 fc00::/7	Enabled
Public IPs	0.0.0.0/0 ::/0	Enabled

Cookie/Querystring parameters:

The following is a list of cookies and querystring parameters that should be excepted from WAF processing as they contain authentication tokens that will lead to false positives:

```
Querystring: "token"
Cookie:      "esri_auth"
Cookie:      "esri_aopc"
```

Enable Body Inspection:

Due to disabling the following 5 rules 941340, 942300, 932105, 942310, 931120, we now recommend enabling body inspection to ensure WAF rules protect from GET and POST request attacks:

```
Inspect request body: "On"
```

The above setting is a major improvement in WAF coverage of your ArcGIS Enterprise deployment and is strongly recommended.

Security Scan Python Scripts

Scans Portal for ArcGIS or ArcGIS Server for security configuration settings and generates an HTML report with recommendations based on security best practices.

Severity levels

- Critical
- Important
- Recommended

Script location

- %AGSPORTAL%\tools\security\portalScan.bat – uses portalScan.py
- %AGSSERVER%\Server\tools\admin\serverScan.py

portalScan.py

enterprise.arcgis.com > Search “portalScan.py”

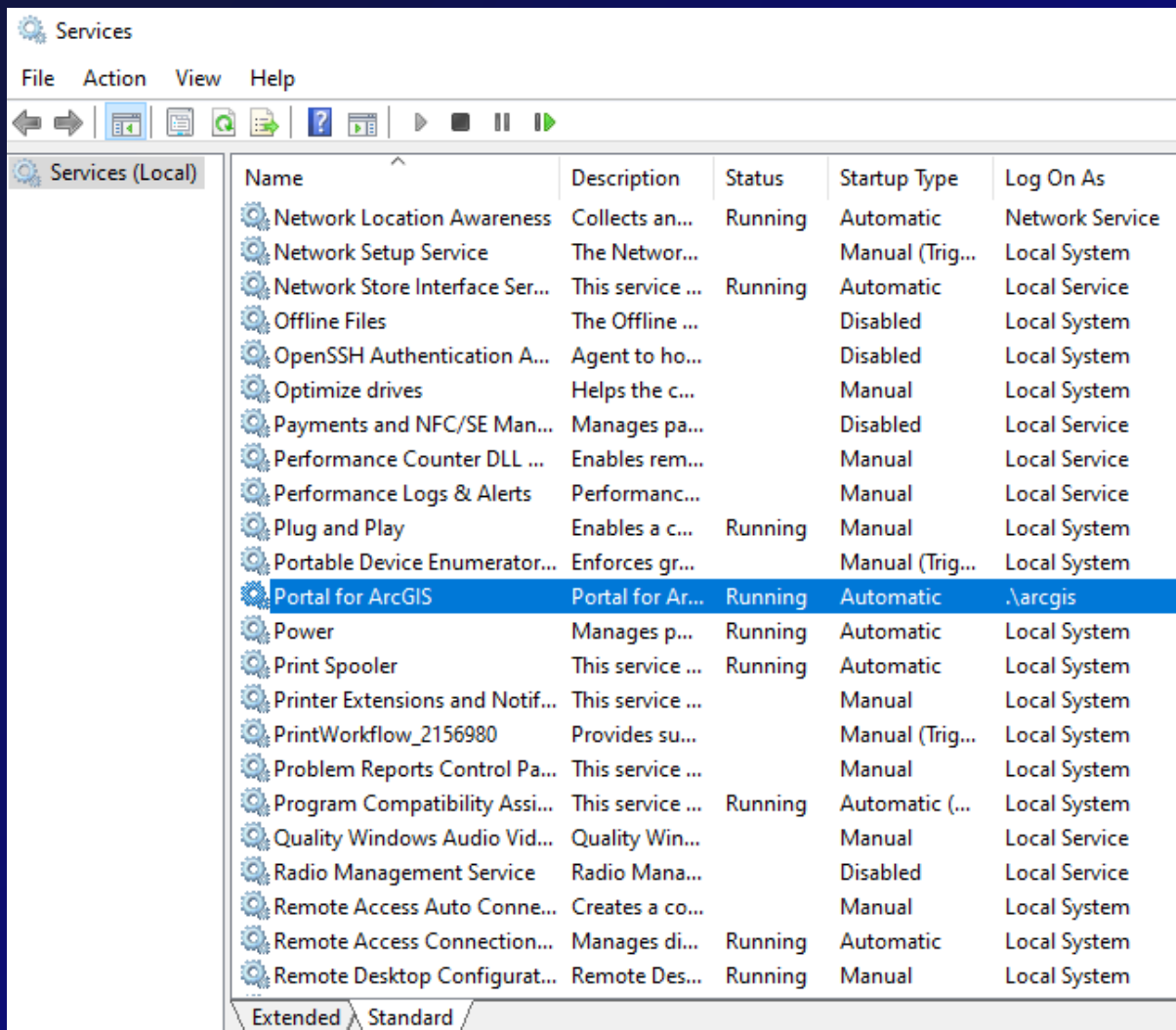
Portal for ArcGIS Security Scan Report - 06/24/26

uc2026.esri.com (12.1)

Potential security items to review

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
PS18	Critical	Service account permissions	Portal for ArcGIS service account - \arcgis This service account is a member of the local Administrators group. This exposes the system to elevated security risks. It is recommended to use a non-administrative account with only the minimum required privileges. More information
PS14	Important	Default print service status	The default print service distributed with your portal is currently enabled. Since the portal is already configured to use a print service from ArcGIS Server, it is recommended to disable the default print service. More information
PS03	Important	Portal services directory	The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. More information
PS06	Recommended	Anonymous access	To prevent any user from accessing the Home application without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information
PS09	Recommended	Cross-domain requests	Cross-domain (CORS) requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. More information
PS17	Recommended	KML service status	The KML service is used by the portal to communicate with KML endpoints. If no KML endpoints will be accessed through any web maps on the portal, it is recommended to disable this service. More information
PS08	Recommended	Portal SSL certificate	To help reduce web browser warnings or other unexpected behavior from clients communicating with your portal, it is recommended to import and use a CA-signed SSL certificate bound to port 7443. More information
PS16	Recommended	RSS service status	The RSS service is used by the portal to communicate with GeoRSS feeds. If no GeoRSS feeds will be accessed through any web maps on the portal, it is recommended to disable this service. More information
PS11	Recommended	Unreachable Federated Server Url	Server Services Url - https://devop00103.esri.com/server The portal is unable to communicate with the federated ArcGIS Server through this services url. This is likely caused by an invalid or untrusted SSL certificate. The root certificate for the CA that signed this certificate may need to be imported into the portal. More information

Portal for ArcGIS / ArcGIS Server Service Account



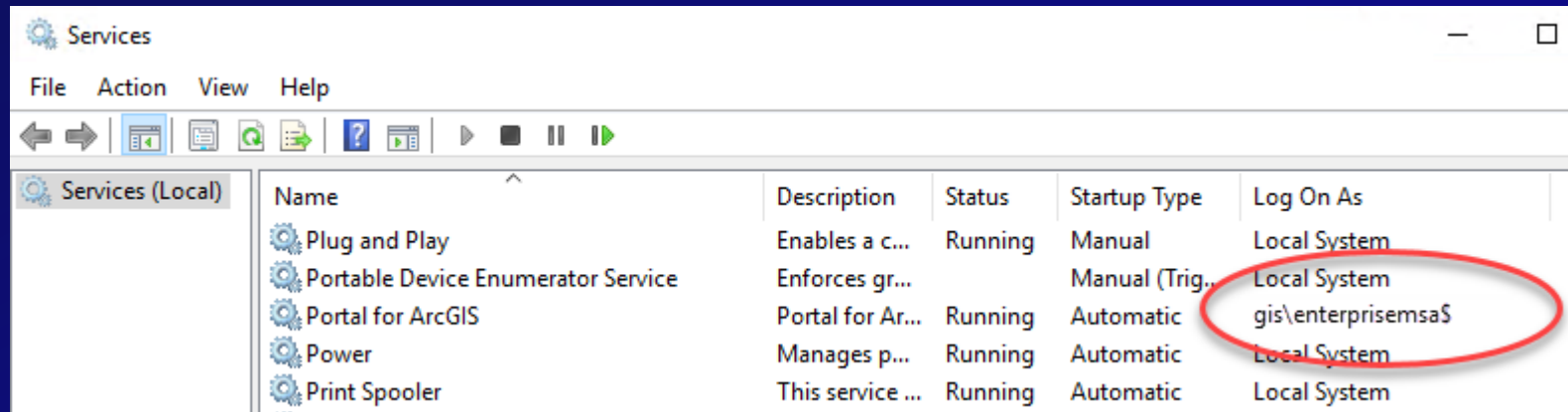
Service Account Types

- Local account
- Domain account
- gMSA (Group managed service account)

What's a gMSA?

Windows only

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



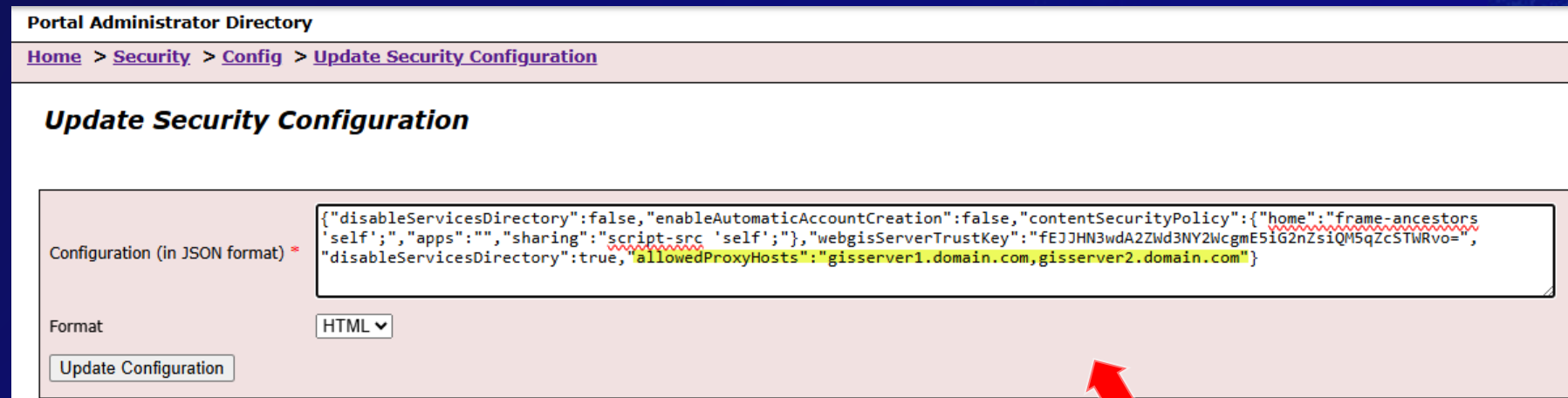
gMSA: Security benefits

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

Restrict Proxy Capability

In 11.5 and earlier

The portal's proxy:
Unrestricted by default



Portal Administrator Directory

[Home](#) > [Security](#) > [Config](#) > [Update Security Configuration](#)

Update Security Configuration

Configuration (in JSON format) *

```
{ "disableServicesDirectory": false, "enableAutomaticAccountCreation": false, "contentSecurityPolicy": { "home": "frame-ancestors 'self';", "apps": "", "sharing": "script-src 'self';", "webgisServerTrustKey": "fEJJHN3wdA2ZWd3NY2WcgmE5iG2nZsiQM5qZcSTWRvo=", "disableServicesDirectory": true, "allowedProxyHosts": "gisservice1.domain.com,gisservice2.domain.com" }
```

Format

- Supports saving credentials for secured servers accessed remotely
- Needed for viewing KML and GeoRSS endpoints
- Define hosts to where Portal can proxy
 - PREVENT Denial of Service (DOS)
 - PREVENT Server-Side Request Forgery (SSRF)

portalScan.py

enterprise.arcgis.com > Search “portalScan.py”

Portal for ArcGIS Security Scan Report - 06/30/25

uc2025.esri.com (11.5)

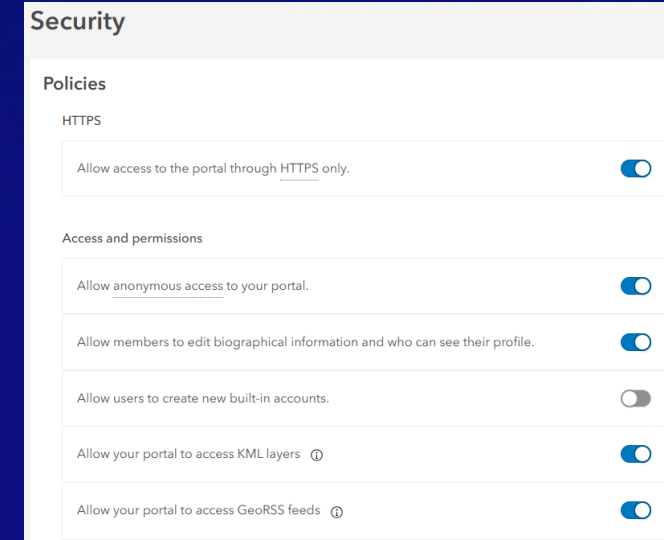
Potential security items to review

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
PS01	Critical	Proxy restrictions	The portal proxy capability is unrestricted. This should be limited to trusted web addresses. More information Suggested "allowedProxyHosts" based on existing maps, services, and configuration settings: droughtmonitor.unl.edu, earthquake.usgs.gov, sampleserver6.arcgisonline.com
PS14	Important	Default print service status	The default print service distributed with your portal is currently enabled. Since the portal is already configured to use a print service from ArcGIS Server, it is recommended to disable the default print service. More information
PS03	Important	Portal services directory	The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. More information
PS06	Recommended	Anonymous access	To prevent any user from accessing the Home application without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information
PS09	Recommended	Cross-domain requests	Cross-domain (CORS) requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. More information
PS17	Recommended	KML service status	The KML service is used by the portal to communicate with KML endpoints. If no KML endpoints will be accessed through any web maps on the portal, it is recommended to disable this service. More information
PS16	Recommended	RSS service status	The RSS service is used by the portal to communicate with GeoRSS feeds. If no GeoRSS feeds will be accessed through any web maps on the portal, it is recommended to disable this service. More information

Security Settings – Improvement within 12.0

Settings now in Portal Home App

- KML & GeoRSS-Layers Konfiguration Option now in the Portal Home App – not only in Admin-Interface
- Allowed Proxy Host – now also in the Portal Home App
 - Automatically within new Installation of 12.x
 - Upgrade from 11.x to 12.x would:
 - Add those if not already existing
 - Check existing Items (as portalscan.py) and would add those as well
 - For earlier Version you might add for using Offline Basemaps within ArcGIS Enterprise the last 3 Hostnames as well



Allowed proxy hosts

Configure a list of hostnames or domains that the Enterprise portal proxy capability is allowed to access. Wildcards are supported using the format (*.*)example.com to allow access to all machines within a specific domain.

[Add hostname](#)

⌐ (*.*)arcgis.com	x
⌐ (*.*)arcgisonline.com	x
⌐ gisupdates.esri.com	x
⌐ lws-job-results-prd0-apse2.s3.amazonaws.com	x
⌐ lws-job-results-prd0-euw1.s3.amazonaws.com	x
⌐ lws-job-results-prd0-use1.s3.amazonaws.com	x

Restrict public sharing

- Limits who can share with “Everyone”
 - Does not change sharing level on existing items
 - Admins can ALWAYS share publicly
 - **Suggestion: Set content review policy to prevent unintended sharing, allow admin to share public.**

Access and permissions

Allow anonymous access to your portal.	☒
Allow members to edit biographical information and who can see their profile.	☒
Allow users to create new built-in accounts.	☐
Allow your portal to access KML layers ⓘ	☒
Allow your portal to access GeoRSS feeds ⓘ	☒

Sharing and searching

Members who are not administrators can make their content, groups, and profile public. ⓘ	☒
Show social media links on item and group pages.	☐

portalScan.py

enterprise.arcgis.com > Search “portalScan.py”

Portal for ArcGIS Security Scan Report - 06/30/25

uc2025.esri.com (11.5)

Potential security items to review

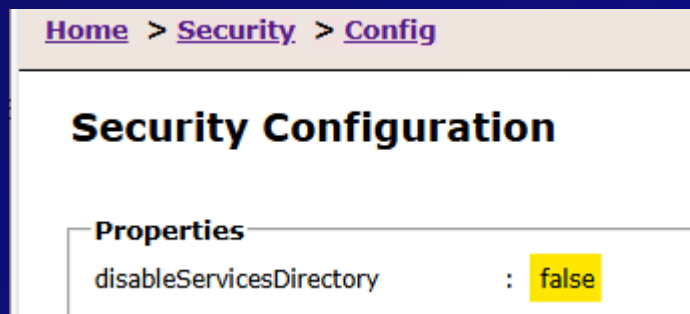
<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>									
PS01	Critical	Proxy restrictions	The portal proxy capability is unrestricted. This should be limited to trusted web addresses. More information Suggested "allowedProxyHosts" based on existing maps, services, and configuration settings: droughtmonitor.unl.edu, earthquake.usgs.gov, sampleserver6.arcgisonline.com									
PS14	Important	Default print service status	The default print service distributed with your portal is currently enabled. Since the portal is already configured to use a print service from ArcGIS Server, it is recommended to disable the default print service. More information									
PS03	Important	Portal services directory	The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. More information									
PS06	Recommended	Anonymous access	To prevent any user from accessing the Home application without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information									
PS09	Recommended	Cross-domain requests	Cross-domain (CORS) requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. More information									
PS17	Recommended	KML service status	The KML service is used by the portal to communicate with KML endpoints. If no KML endpoints will be accessed through any web maps on the portal, it is recommended to disable this service. More information									
PS12	Recommended	Public content	The portal is configured so members cannot share content publicly but the following items are currently shared with everyone and may need to be updated. <table><tr><th>Item Name</th><th>Item Type</th><th>Owner</th></tr><tr><td>California</td><td>Feature Service</td><td>admin</td></tr><tr><td>California Map</td><td>Web Map</td><td>admin</td></tr></table>	Item Name	Item Type	Owner	California	Feature Service	admin	California Map	Web Map	admin
Item Name	Item Type	Owner										
California	Feature Service	admin										
California Map	Web Map	admin										
PS16	Recommended	RSS service status	The RSS service is used by the portal to communicate with GeoRSS feeds. If no GeoRSS feeds will be accessed through any web maps on the portal, it is recommended to disable this service. More information									

Disable Services Directories

Reduces Potential Attack Surface

- Prevents service listing by bots / search engines
- Does NOT limit functionality – just hides HTML form driven view
- Recommend to not expose:
 - ArcGIS Portal Directory
 - ArcGIS Server REST Services Directory
- Use Case Dependent Option

Portal for ArcGIS



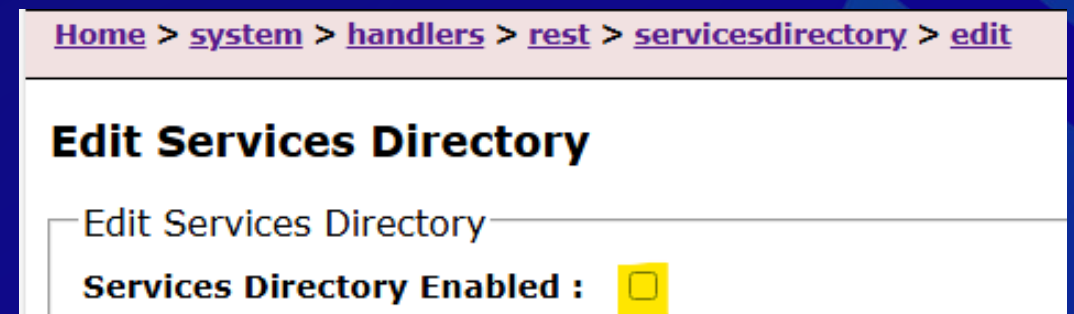
Home > Security > Config

Security Configuration

Properties

disableServicesDirectory	:	false
--------------------------	---	-------

ArcGIS Server



Home > system > handlers > rest > servicesdirectory > edit

Edit Services Directory

Edit Services Directory

Services Directory Enabled : ☐

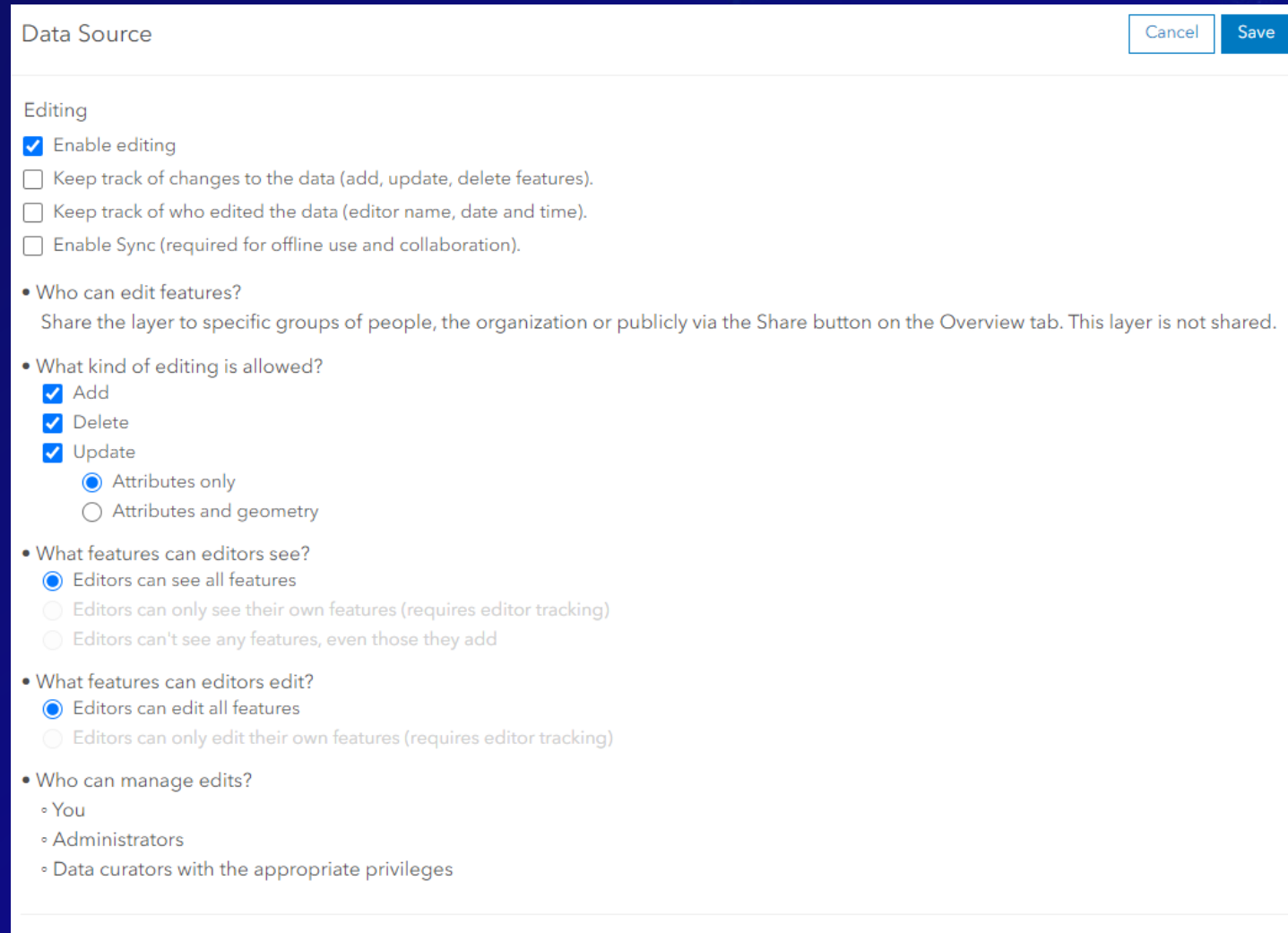
Content Security Policy

If you choose to expose the services directory...

- CSP allows another level of protection against cross-site-scripting (XSS)
- Consistent with defense in depth approach
- The default CSP will block potential XSS attacks against
 - ArcGIS Portal Directory (11.5)
 - ArcGIS Server REST Services Directory (11.5)
 - ArcGIS Portal Admin REST-Interface (12.0)
 - ArcGIS Server Admin-Interface (12.0)

Feature Layer Security and Editing

- Users who can always edit
 - Owner
 - Admins
 - Members of Groups w/ Update capability
- Enable Editing: Defaults
 - Anyone who can access the service can edit
 - Add, update and delete features
 - Only update feature attributes
 - See and edit all features



The screenshot shows the 'Data Source' configuration window with the following settings:

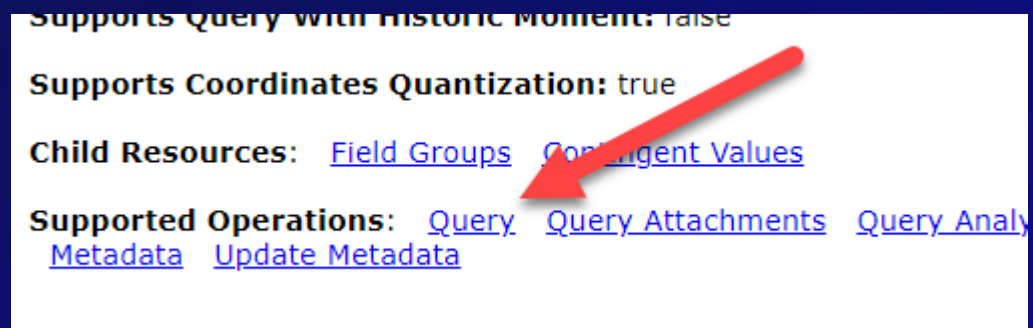
- Editing**
 - ☒ Enable editing
 - ☐ Keep track of changes to the data (add, update, delete features).
 - ☐ Keep track of who edited the data (editor name, date and time).
 - ☐ Enable Sync (required for offline use and collaboration).
- Who can edit features?**

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

Buttons: Cancel, Save

Feature Layer Security and Editing

- Considerations for Sensitive Content
 - Disable delete and update
 - Enable “Editors can’t see features, even those they add”
 - This disables “Query” capability on the service
 - If users can query features, they can see data



Data Source

Editing

☒ Enable editing

☐ Keep track of changes to the data (add, update, delete features).

☐ Keep track of who edited the data (editor name, date and time).

☐ Enable Sync (required for offline use and collaboration).

• Who can edit features?
Share the layer to specific groups of people, the organization or publicly via the Share button

• What kind of editing is allowed?

☐ Add

☐ Delete

☐ Update

• What features can editors see?

☐ Editors can see all features

☐ Editors can only see their own features (requires editor tracking)

☒ Editors can't see any features, even those they add

• What features can editors edit?

☒ Editors can edit all features

☐ Editors can only edit their own features (requires editor tracking)

• Who can manage edits?

- You
- Administrators
- Data curators with the appropriate privileges

Two red arrows point from the text "Disables 'query'" to the "Delete" and "Update" checkboxes in the "What kind of editing is allowed?" section.

Use Hosted Feature Service Views

What is a view?

- Allows publishers to control which data a user sees.
- View definition:
 - Spatial Extent
 - Define visible fields
 - NOT the same as an attribute filter

Why use a view?

- Restrict sensitive information to authorized users
- Show non-sensitive information to wider audience
- Create apps for different audiences
- All referencing same data source

serverScan.py

enterprise.arcgis.com > Search “serverScan.py”

ArcGIS Server Security Scan Report - 06/30/25

uc2025.esri.com (11.5)

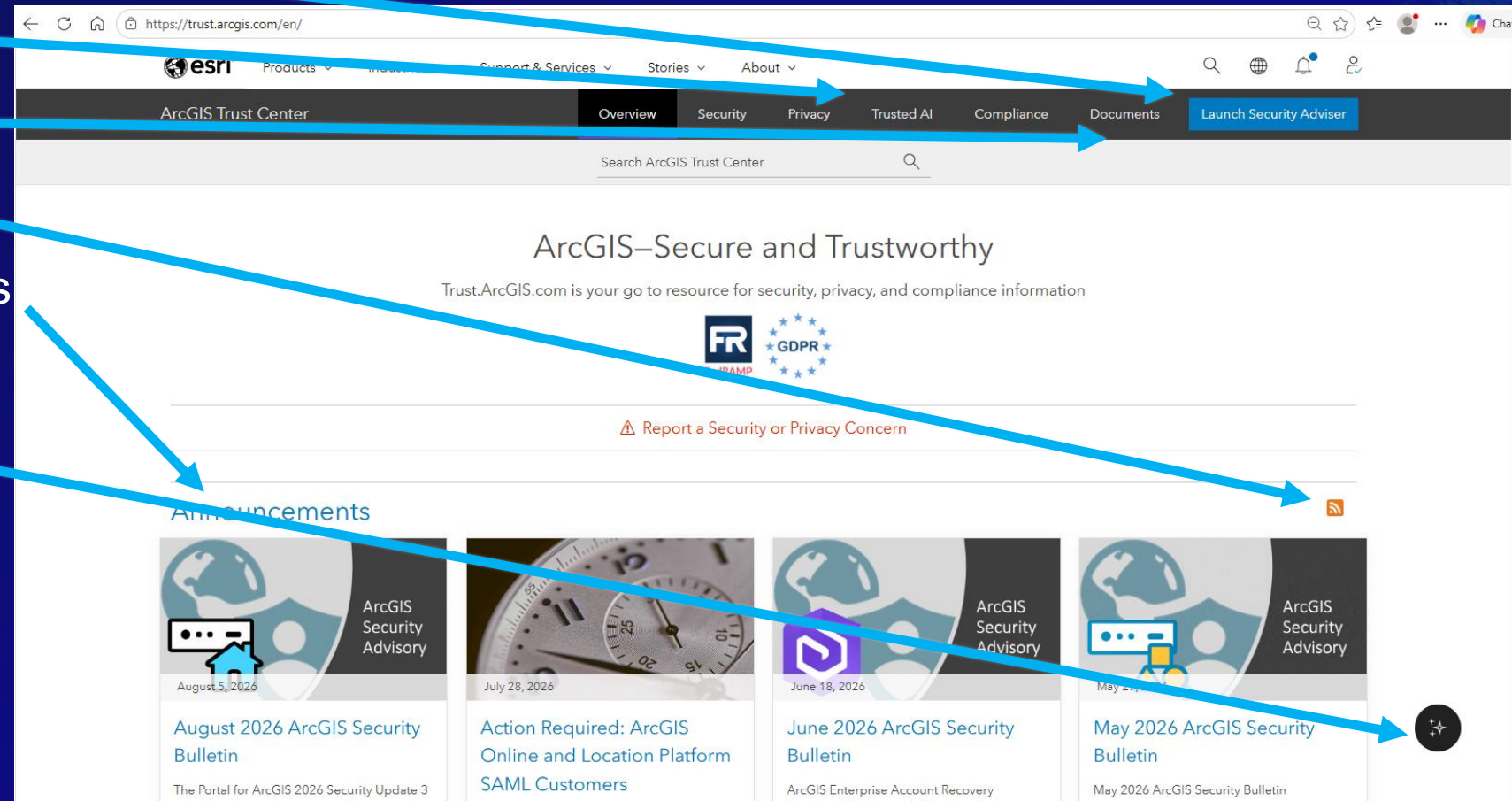
Potential security items to review

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
SS08	Important	Cross-domain requests	Cross-domain requests for REST endpoints are unrestricted. To reduce the possibility of an unknown application sending malicious requests to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. More information
SS08	Important	Cross-domain requests	Cross-domain requests for SOAP endpoints are unrestricted; this applies to OGC endpoints (WMS, WFS, etc.) that are exposed as well. To reduce the possibility of an unknown application sending malicious requests to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. More information
SS07	Important	Rest services directory	The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks. More information
SS12	Recommended	Feature service operations	Feature service: Hosted/Airports This feature service has the update and/or delete operations enabled and is open to anonymous access. This allows the feature service data to be changed and/or deleted without authentication.
SS11	Recommended	PSA account status	The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your configuration. More information

Trust.ArcGIS.com

...your go to resource for security, privacy, and compliance information

- Security and Privacy Advisor
- Trusted AI
- Technical papers
- Subscribe to RSS
- Announcements/Advisories
- AI Chatbot





ArcGIS Security and Privacy Adviser

Best Practice Validation and Discovery Tool



Sign In to ArcGIS Online



Sign In to ArcGIS Enterprise

We welcome feedback [here](#) for this tool, which falls outside of standard customer support.

Refresh

Help

Custom Server Functionality: No issues found		Custom Server Functionality
Server Object Extensions and Intercepts		+
Custom GeoProcessing Services		+
Portaladmin Configuration: No issues found		
Forward Proxy Authentication		▼
Restrict Portal Proxy Capability		▼
		Export CSV
Shared Credentials: No issues found		Shared Credentials Scan
Legacy API Keys		▼
Embedded Credentials		▼
Organization Security Settings: Critical Issues		Organization Security Settings
Access and Permissions		▼
Sharing and Searching		▼
Password Policy		▼
Logins		▼
Allowed Origins		▼
Allowed Portal Access		▼
Multi-Factor Authentication		▼
Trusted Servers		▼
		Export CSV

Well Architected Framework

ArcGIS Architecture Center

OverviewSystem PatternsArchitecture PracticesLibrary

Search ArcGIS Architecture Center

ArcGIS Architecture Center

Design and implement enterprise systems with ArcGIS that meet your organization's business needs.

Get started

Learn about the mission behind the ArcGIS Well-Architected Framework and characteristics of ArcGIS as an information system.



About the ArcGIS Well-Architected Framework

The ArcGIS Well-Architected Framework is intended to help organizations design, deploy, and operate ArcGIS as an enterprise system. Working in today's IT landscape requires context, expertise, and collaboration.

[Learn more](#)



An overview of ArcGIS

New to ArcGIS? Learn about the characteristics of ArcGIS as an information system, how it's designed, how it supports different deployment and operational models, and how it aligns with your IT landscape.

[Learn more](#)



Architecture

The process of a variety of topics, including an overview of approaching a solution design.

[Learn more](#)

architecture.arcgis.com



Observability
Monitoring, etc.



Automation
DevOps, etc.



Reliability
Backup, HA/DR, etc.



Security
Auth, Identity, etc.



Performance & Scalability
Caching, tuning, etc.



Integration
Systems, Data, etc.

PatchNotification-Tool-Limitationen

- BUG-000142951 : The Patch Notification tool does not honor the cumulative patches
- BUG-000160275 : ArcGIS Web Adaptor is not identified by the patchnotification tool (Check for ArcGIS Enterprise Updates).
- ENH-000186533 : Request for ArcGIS Patch Notification Utility to send email updates when patches are available
- Sollte jemand dieses Probleme haben – bitte info an g.trichtl@mysynergis.com

ArcGIS Enterprise – Q&A

SynerGIS-Team

*2026 ESRI USER CONFERENCE AUSTRIA
– powered by SynerGIS*

An aerial photograph of a river valley, showing a winding river and surrounding terrain. The image is partially covered by a large blue diagonal overlay that extends from the bottom left towards the top right.

synergis



esri™ Official
Distributor