ArcGIS Online:

Ensuring Security and Privacy with FedRAMP, AI, ZTA, and beyond

Michael Young – CISO-Products

Pete Buwembo – Principal Product Security Engineer

Esri Software Security & Privacy

Agenda

- Compliance
- Shared Responsibility Model
- Tools
- Trusted AI
- Zero Trust Architecture (ZTA)
- Summary
- Q & A

Compliance

Compliance

FedRAMP – ArcGIS Online

- ArcGIS Online FedRAMP Authorized 7 years!
    - Initial 2018 FedRAMP Tailored Low Rev 4
- 2024 – Moderate
    - NIST 800-53 Rev 5 Controls
        - Supply chain
        - Red team
    - Cross-agency Collaborative ConMon
    - New Customer Responsibilities
    - Expands coverage to PII, CUI and CDI requirements

Stronger security & privacy assurance means agencies can expand use case scenarios of ArcGIS Online!

Compliance

FedRAMP – Esri Managed Cloud Services (EMCS) – Advanced Plus

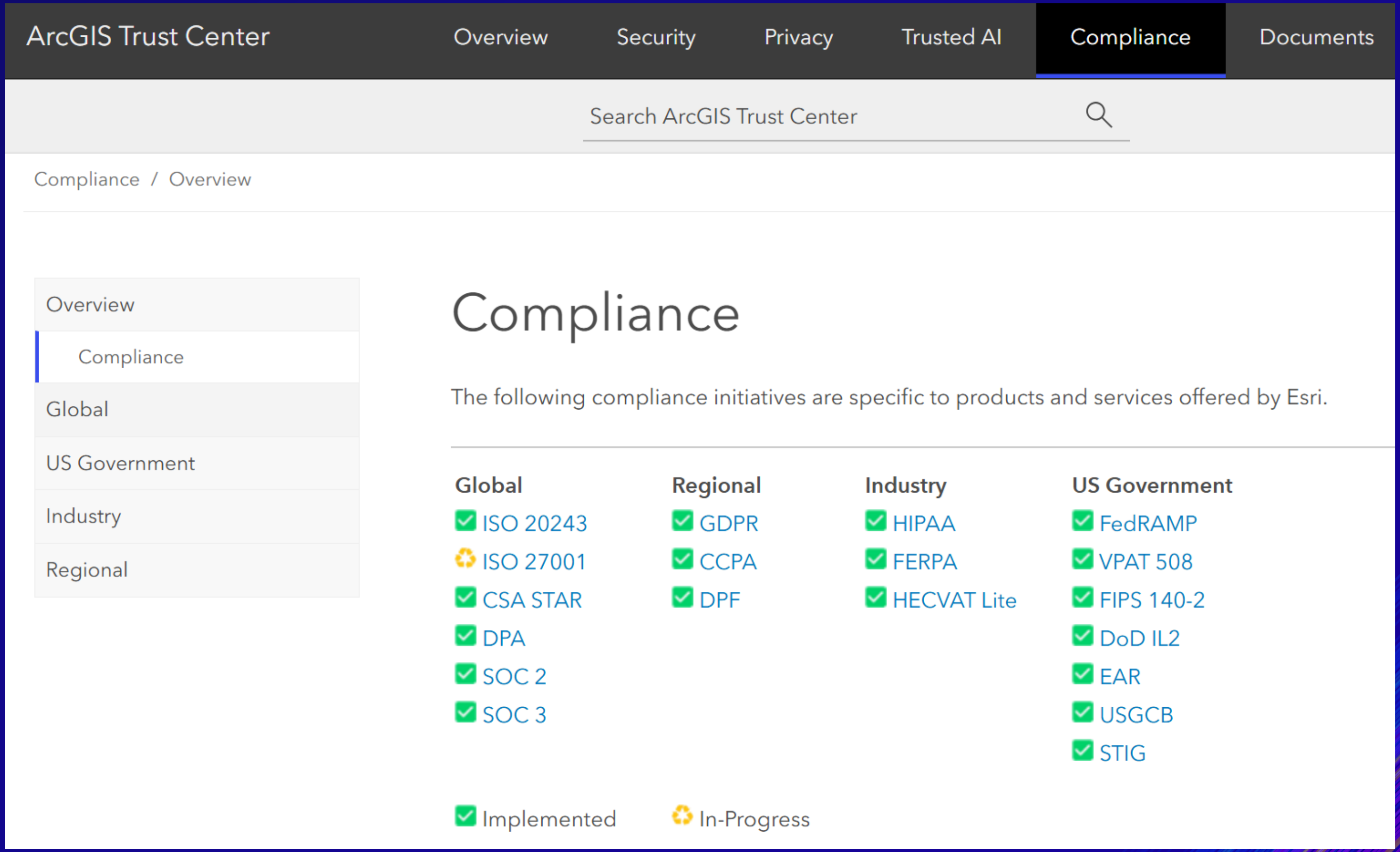
- EMCS FedRAMP Authorized 2015
- What is the difference?
  - EMCS Adv. +
    - Single Tenant (Dedicated) ArcGIS Enterprise
  - ArcGIS Online
    - Multi-Tenant (SaaS)

FedRAMP

Compliance

Beyond FedRAMP

- Privacy regulations
- Health care (HIPAA)
  - Eligible services expanding
  - BAA Available
- Accessibility (VPAT / WCAG)
- DoD Public Data (IL2) Reciprocity
  - Welcome discussing DoD IL4 demands



ArcGIS Trust Center

Compliance

The following compliance initiatives are specific to products and services offered by Esri.

Global

✓ ISO 20243
○ ISO 27001
✓ CSA STAR
✓ DPA
✓ SOC 2
✓ SOC 3

Regional

✓ GDPR
✓ CCPA
✓ DPF

Industry

✓ HIPAA
✓ FERPA
✓ HECVAT Lite

US Government

✓ FedRAMP
✓ VPAT 508
✓ FIPS 140-2
✓ DoD IL2
✓ EAR
✓ USGCB
✓ STIG

✓ Implemented ○ In-Progress

Check out the ArcGIS Trust Center Compliance page to explore more!

Shared Responsibility Model

Shared Responsibility Model

Esri Responsibilities

- Secure Development & Supply Chain
- Product Incident Response
- Certifications / Authorizations
- Customer Guidance

Shared Responsibility Model

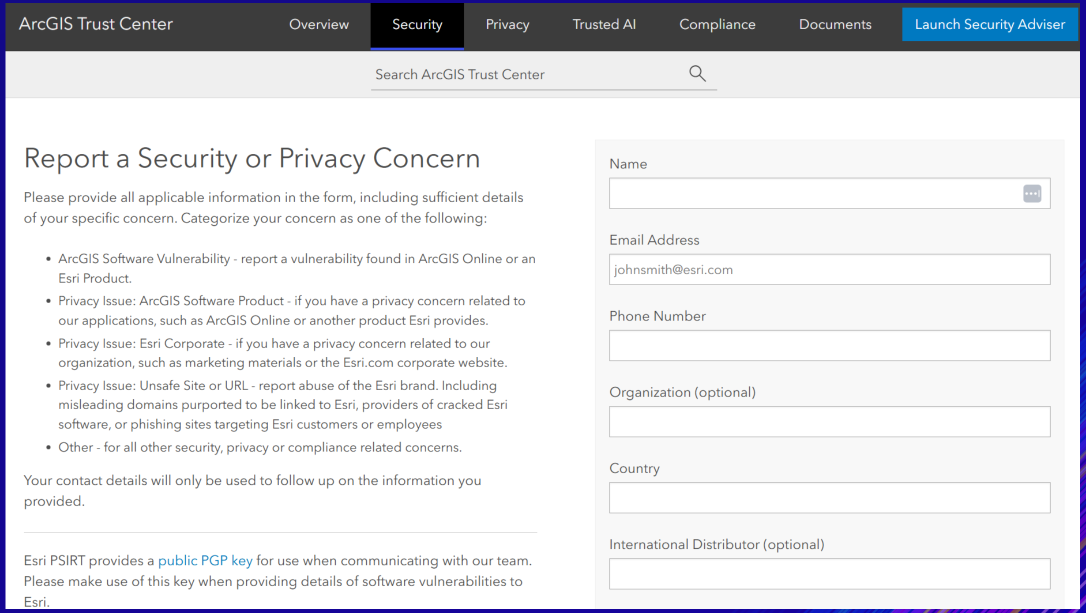
Esri Responsibilities

- Secure Development & Supply Chain
  - CISA Secure Development Attestation Completed in 2024
    - Posted to RSAA – https://SoftwareSecurity.CISA.gov

RSAA
Repository for Software Attestations and Artifacts

- Product Incident Response
  - FIRST structured PSIRT program
  - CVE Numbering Authority
  - Report incidents via Trust Center

FIRST™
Improving Security Together



Report a Security or Privacy Concern

Please provide all applicable information in the form, including sufficient details of your specific concern. Categorize your concern as one of the following:

- ArcGIS Software Vulnerability - report a vulnerability found in ArcGIS Online or an Esri Product.
- Privacy Issue: ArcGIS Software Product - if you have a privacy concern related to our applications, such as ArcGIS Online or another product Esri provides.
- Privacy Issue: Esri Corporate - if you have a privacy concern related to our organization, such as marketing materials or the Esri.com corporate website.
- Privacy Issue: Unsafe Site or URL - report abuse of the Esri brand. Including misleading domains purported to be linked to Esri, providers of cracked Esri software, or phishing sites targeting Esri customers or employees
- Other - for all other security, privacy or compliance related concerns.

Your contact details will only be used to follow up on the information you provided.

Esri PSIRT provides a public PGP key for use when communicating with our team. Please make use of this key when providing details of software vulnerabilities to Esri.

Name

Email Address
johnsmith@esri.com

Phone Number

Organization (optional)

Country

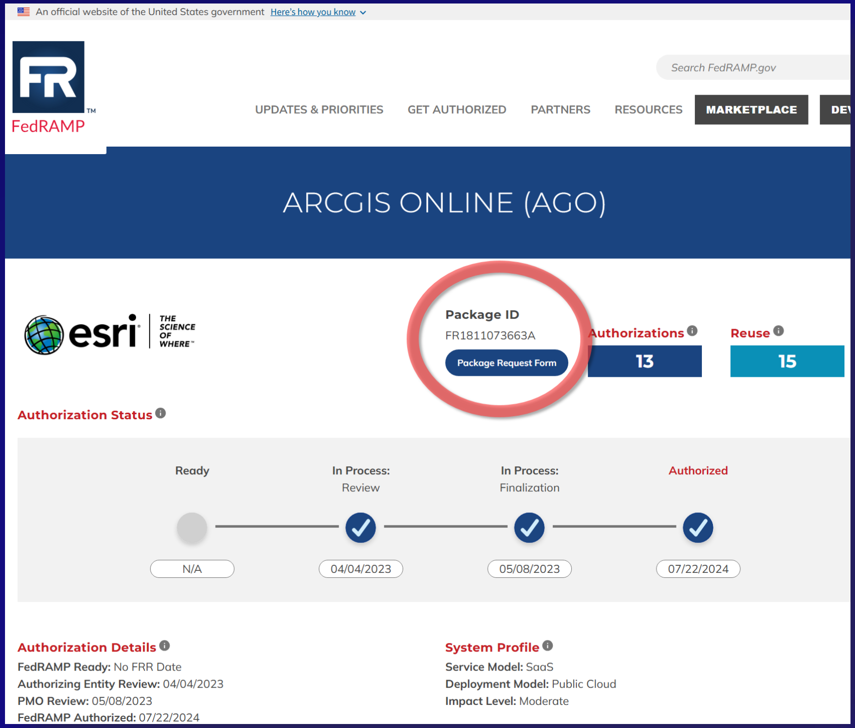
International Distributor (optional)

Shared Responsibility Model

Esri Responsibilities

- Certifications & Authorizations
  - Package available via FedRAMP Marketplace
  - MarketPlace.FedRAMP.gov

- Customer Guidance
  - ArcGIS Trust Center
    - Security & Privacy Advisor Tool
    - Mobile
    - Surveys
    - Hardening guides



ARCGIS ONLINE (AGO)

Package ID
FR1811073663A

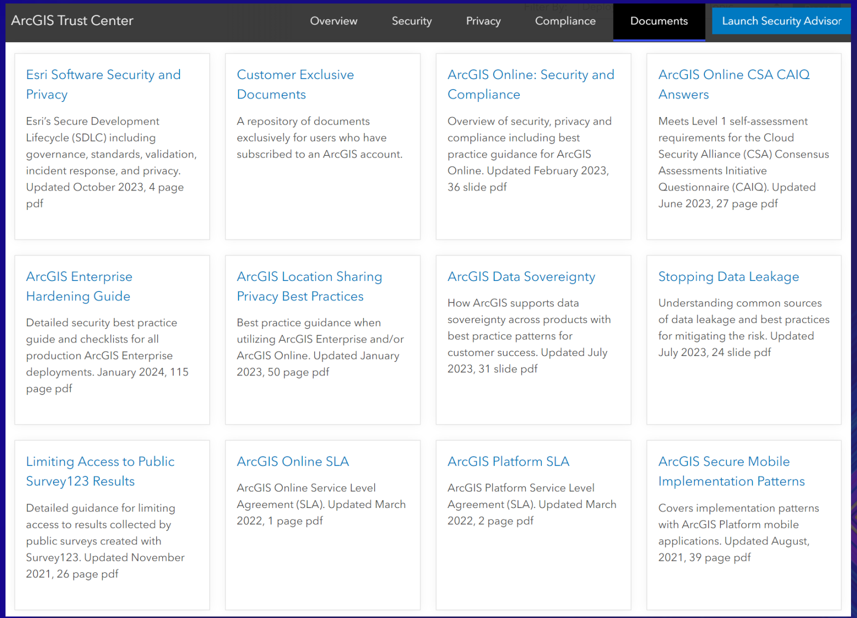
Authorizations	Reuse
13	15

Authorization Status

Ready	In Process: Review	In Process: Finalization	Authorized
N/A	04/04/2023	05/08/2023	07/22/2024

Authorization Details
FedRAMP Ready: No FRR Date
Authorizing Entity Review: 04/04/2023
PMO Review: 05/08/2023
FedRAMP Authorized: 07/22/2024

System Profile
Service Model: SaaS
Deployment Model: Public Cloud
Impact Level: Moderate



Esri Software Security and Privacy
Esri's Secure Development Lifecycle (SDLC) including governance, standards, validation, incident response, and privacy. Updated October 2023, 4 page pdf

Customer Exclusive Documents
A repository of documents exclusively for users who have subscribed to an ArcGIS account.

ArcGIS Online: Security and Compliance
Overview of security, privacy and compliance including best practice guidance for ArcGIS Online. Updated February 2023, 36 slide pdf

ArcGIS Online CSA CAIQ Answers
Meets Level 1 self-assessment requirements for the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). Updated June 2023, 27 page pdf

ArcGIS Enterprise Hardening Guide
Detailed security best practice guide and checklists for all production ArcGIS Enterprise deployments. January 2024, 115 page pdf

ArcGIS Location Sharing Privacy Best Practices
Best practice guidance when utilizing ArcGIS Enterprise and/or ArcGIS Online. Updated January 2023, 50 page pdf

ArcGIS Data Sovereignty
How ArcGIS supports data sovereignty across products with best practice patterns for customer success. Updated July 2023, 31 slide pdf

Stopping Data Leakage
Understanding common sources of data leakage and best practices for mitigating the risk. Updated July 2023, 24 slide pdf

Limiting Access to Public Survey123 Results
Detailed guidance for limiting access to results collected by public surveys created with Survey123. Updated November 2021, 26 page pdf

ArcGIS Online SLA
ArcGIS Online Service Level Agreement (SLA). Updated March 2022, 1 page pdf

ArcGIS Platform SLA
ArcGIS Platform Service Level Agreement (SLA). Updated March 2022, 2 page pdf

ArcGIS Secure Mobile Implementation Patterns
Covers implementation patterns with ArcGIS Platform mobile applications. Updated August, 2021, 39 page pdf

Shared Responsibility Model

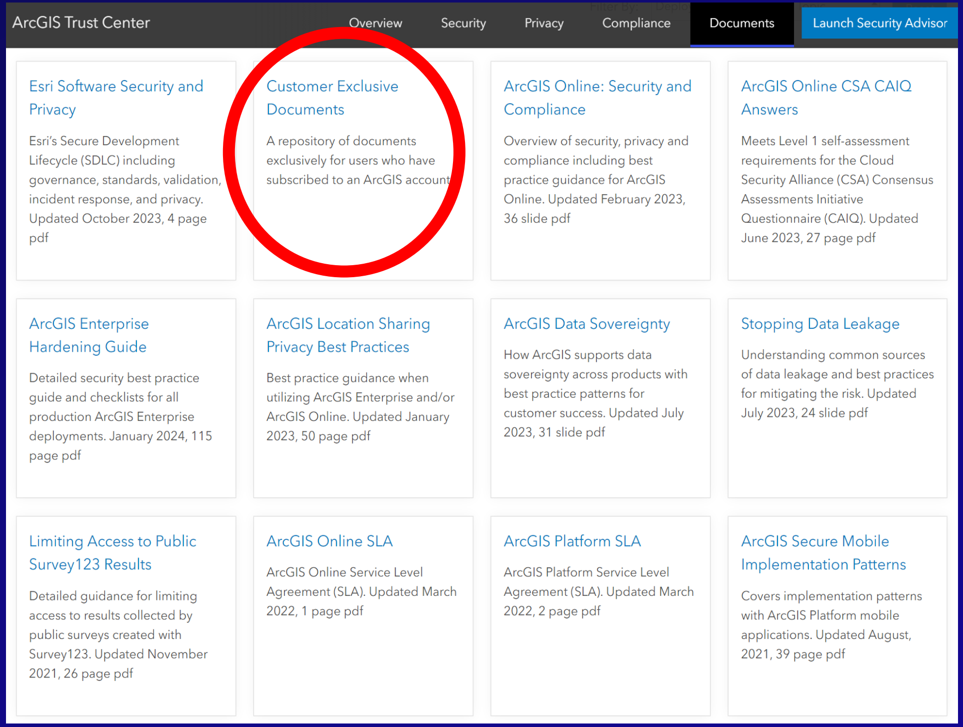
Agency Responsibilities

- Configure
- Maintain

Shared Responsibility Model

Agency Responsibilities - ***Configure***

- Configure Organization settings in alignment with Customer Responsibility Matrix (CRM)
  - CRM in FedRAMP package and ArcGIS Trust Center Customer Exclusive Documents



Esri Software Security and Privacy

Esri's Secure Development Lifecycle (SDLC) including governance, standards, validation, incident response, and privacy. Updated October 2023, 4 page pdf

Customer Exclusive Documents

A repository of documents exclusively for users who have subscribed to an ArcGIS account

ArcGIS Online: Security and Compliance

Overview of security, privacy and compliance including best practice guidance for ArcGIS Online. Updated February 2023, 36 slide pdf

ArcGIS Online CSA CAIQ Answers

Meets Level 1 self-assessment requirements for the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). Updated June 2023, 27 page pdf

ArcGIS Enterprise Hardening Guide

Detailed security best practice guide and checklists for all production ArcGIS Enterprise deployments. January 2024, 115 page pdf

ArcGIS Location Sharing Privacy Best Practices

Best practice guidance when utilizing ArcGIS Enterprise and/or ArcGIS Online. Updated January 2023, 50 page pdf

ArcGIS Data Sovereignty

How ArcGIS supports data sovereignty across products with best practice patterns for customer success. Updated July 2023, 31 slide pdf

Stopping Data Leakage

Understanding common sources of data leakage and best practices for mitigating the risk. Updated July 2023, 24 slide pdf

Limiting Access to Public Survey123 Results

Detailed guidance for limiting access to results collected by public surveys created with Survey123. Updated November 2021, 26 page pdf

ArcGIS Online SLA

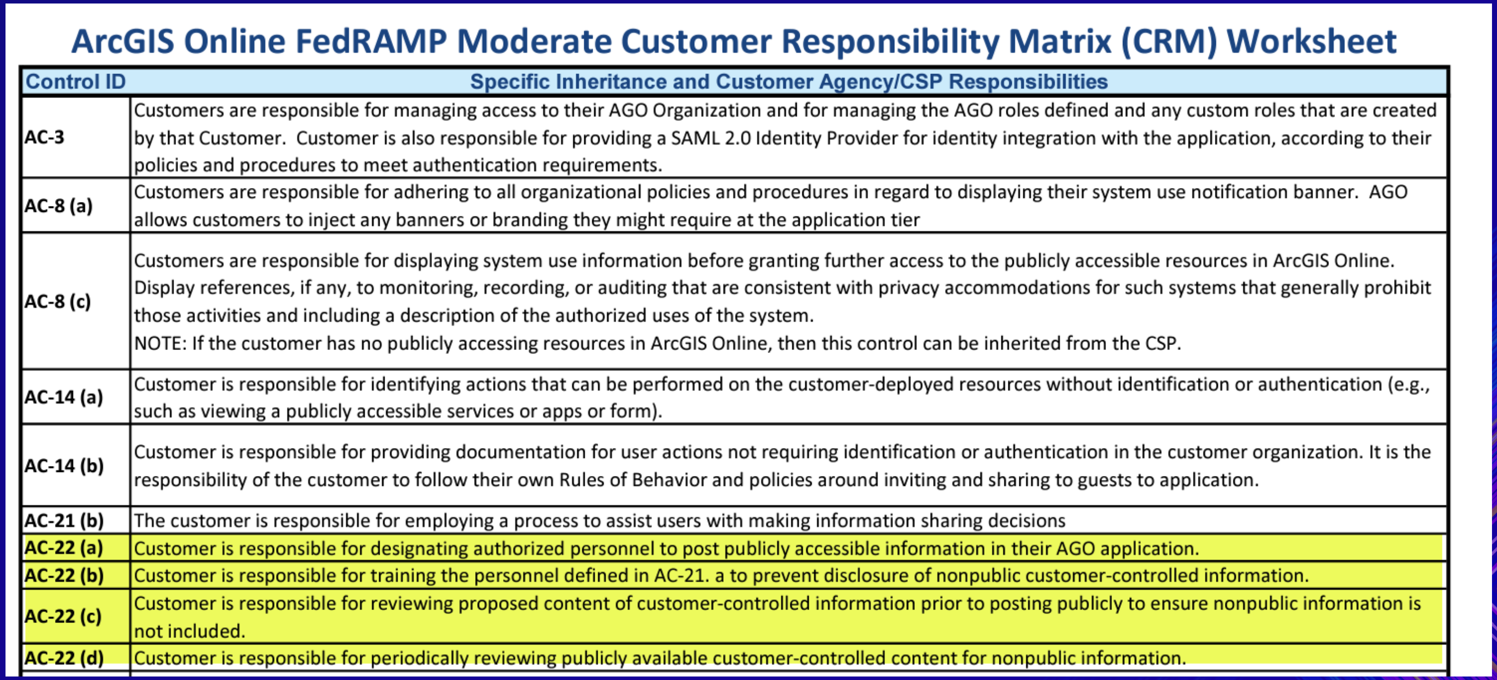
ArcGIS Online Service Level Agreement (SLA). Updated March 2022, 1 page pdf

ArcGIS Platform SLA

ArcGIS Platform Service Level Agreement (SLA). Updated March 2022, 2 page pdf

ArcGIS Secure Mobile Implementation Patterns

Covers implementation patterns with ArcGIS Platform mobile applications. Updated August, 2021, 39 page pdf



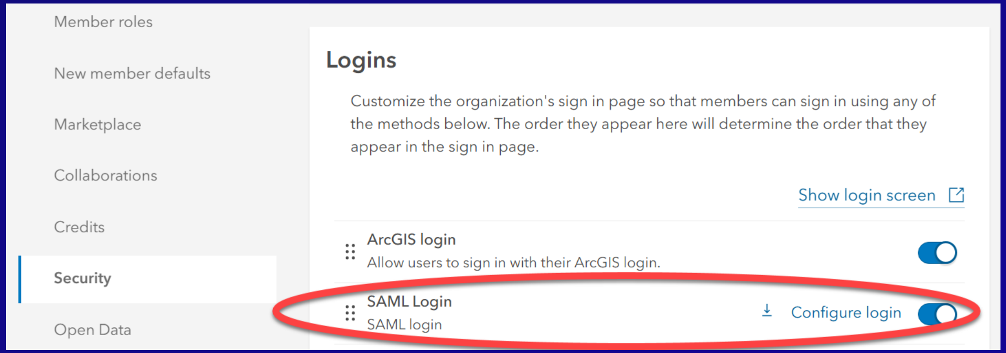
ArcGIS Online FedRAMP Moderate Customer Responsibility Matrix (CRM) Worksheet

Control ID	Specific Inheritance and Customer Agency/CSP Responsibilities
AC-3	Customers are responsible for managing access to their AGO Organization and for managing the AGO roles defined and any custom roles that are created by that Customer. Customer is also responsible for providing a SAML 2.0 Identity Provider for identity integration with the application, according to their policies and procedures to meet authentication requirements.
AC-8 (a)	Customers are responsible for adhering to all organizational policies and procedures in regard to displaying their system use notification banner. AGO allows customers to inject any banners or branding they might require at the application tier
AC-8 (c)	Customers are responsible for displaying system use information before granting further access to the publicly accessible resources in ArcGIS Online. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities and including a description of the authorized uses of the system. NOTE: If the customer has no publicly accessing resources in ArcGIS Online, then this control can be inherited from the CSP.
AC-14 (a)	Customer is responsible for identifying actions that can be performed on the customer-deployed resources without identification or authentication (e.g., such as viewing a publicly accessible services or apps or form).
AC-14 (b)	Customer is responsible for providing documentation for user actions not requiring identification or authentication in the customer organization. It is the responsibility of the customer to follow their own Rules of Behavior and policies around inviting and sharing to guests to application.
AC-21 (b)	The customer is responsible for employing a process to assist users with making information sharing decisions
AC-22 (a)	Customer is responsible for designating authorized personnel to post publicly accessible information in their AGO application.
AC-22 (b)	Customer is responsible for training the personnel defined in AC-21. a to prevent disclosure of nonpublic customer-controlled information.
AC-22 (c)	Customer is responsible for reviewing proposed content of customer-controlled information prior to posting publicly to ensure nonpublic information is not included.
AC-22 (d)	Customer is responsible for periodically reviewing publicly available customer-controlled content for nonpublic information.

Shared Responsibility Model

Agency Responsibilities - ***Configure***

- Example Customer Responsibility Configuration Items
  - Utilize Centralized Identity Management for User Accounts
    - Manage users and groups with your domain tools
    - Typical SAML 2
  - Enforce MFA for accounts
    - Manage MFA exceptions for services

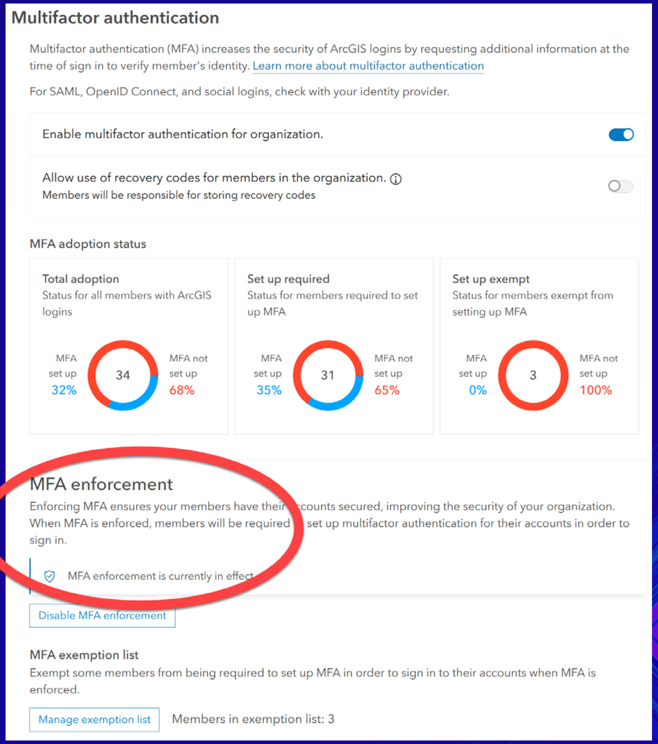


Logins

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

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

SAML Login
SAML login



Multifactor authentication

Multifactor authentication (MFA) increases the security of ArcGIS logins by requesting additional information at the time of sign in to verify member's identity. Learn more about multifactor authentication

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

Enable multifactor authentication for organization.

Allow use of recovery codes for members in the organization.
Members will be responsible for storing recovery codes

MFA adoption status

Total adoption	Set up required	Set up exempt
Status for all members with ArcGIS logins	Status for members required to set up MFA	Status for members exempt from setting up MFA
34	31	3
MFA set up 32%	MFA set up 35%	MFA set up 0%
MFA not set up 68%	MFA not set up 65%	MFA not set up 100%

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.

MFA enforcement is currently in effect

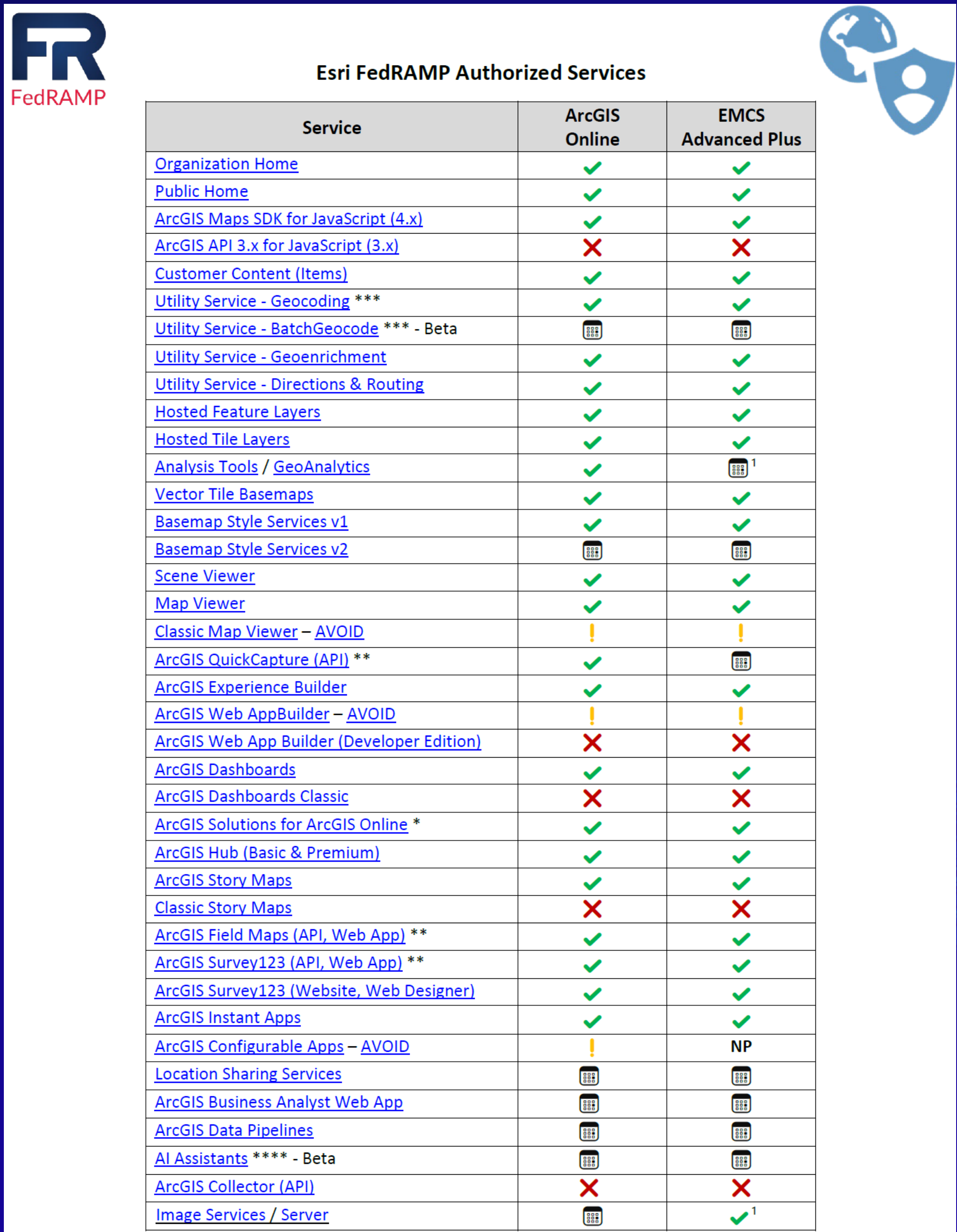
MFA exemption list
Exempt some members from being required to set up MFA in order to sign in to their accounts when MFA is enforced.

Members in exemption list: 3

Shared Responsibility Model

Agency Responsibilities - ***Maintain***

- Participate in monthly ConMon Meetings
  - Make your agency’s voice heard
- Check Authorized Services Listing
  - Now includes ArcGIS Online & EMCS services
  - Use blocker for deprecated capabilities
  - Consider your AI and Beta settings
- Use Validation Tools
  - Check for application configuration drift
  - Security & Privacy Adviser



Esri FedRAMP Authorized Services

Service	ArcGIS Online	EMCS Advanced Plus
Organization Home	✓	✓
Public Home	✓	✓
ArcGIS Maps SDK for JavaScript (4.x)	✓	✓
ArcGIS API 3.x for JavaScript (3.x)	✗	✗
Customer Content (Items)	✓	✓
Utility Service - Geocoding ***	✓	✓
Utility Service - BatchGeocode *** - Beta	📅	📅
Utility Service - Geoenrichment	✓	✓
Utility Service - Directions & Routing	✓	✓
Hosted Feature Layers	✓	✓
Hosted Tile Layers	✓	✓
Analysis Tools / GeoAnalytics	✓	📅[1]
Vector Tile Basemaps	✓	✓
Basemap Style Services v1	✓	✓
Basemap Style Services v2	📅	📅
Scene Viewer	✓	✓
Map Viewer	✓	✓
Classic Map Viewer – AVOID	!	!
ArcGIS QuickCapture (API) **	✓	📅
ArcGIS Experience Builder	✓	✓
ArcGIS Web AppBuilder – AVOID	!	!
ArcGIS Web App Builder (Developer Edition)	✗	✗
ArcGIS Dashboards	✓	✓
ArcGIS Dashboards Classic	✗	✗
ArcGIS Solutions for ArcGIS Online *	✓	✓
ArcGIS Hub (Basic & Premium)	✓	✓
ArcGIS Story Maps	✓	✓
Classic Story Maps	✗	✗
ArcGIS Field Maps (API, Web App) **	✓	✓
ArcGIS Survey123 (API, Web App) **	✓	✓
ArcGIS Survey123 (Website, Web Designer)	✓	✓
ArcGIS Instant Apps	✓	✓
ArcGIS Configurable Apps – AVOID	!	NP
Location Sharing Services	📅	📅
ArcGIS Business Analyst Web App	📅	📅
ArcGIS Data Pipelines	📅	📅
AI Assistants **** - Beta	📅	📅
ArcGIS Collector (API)	✗	✗
Image Services / Server	📅	✓[1]

Tools

ArcGIS Security and Privacy Adviser

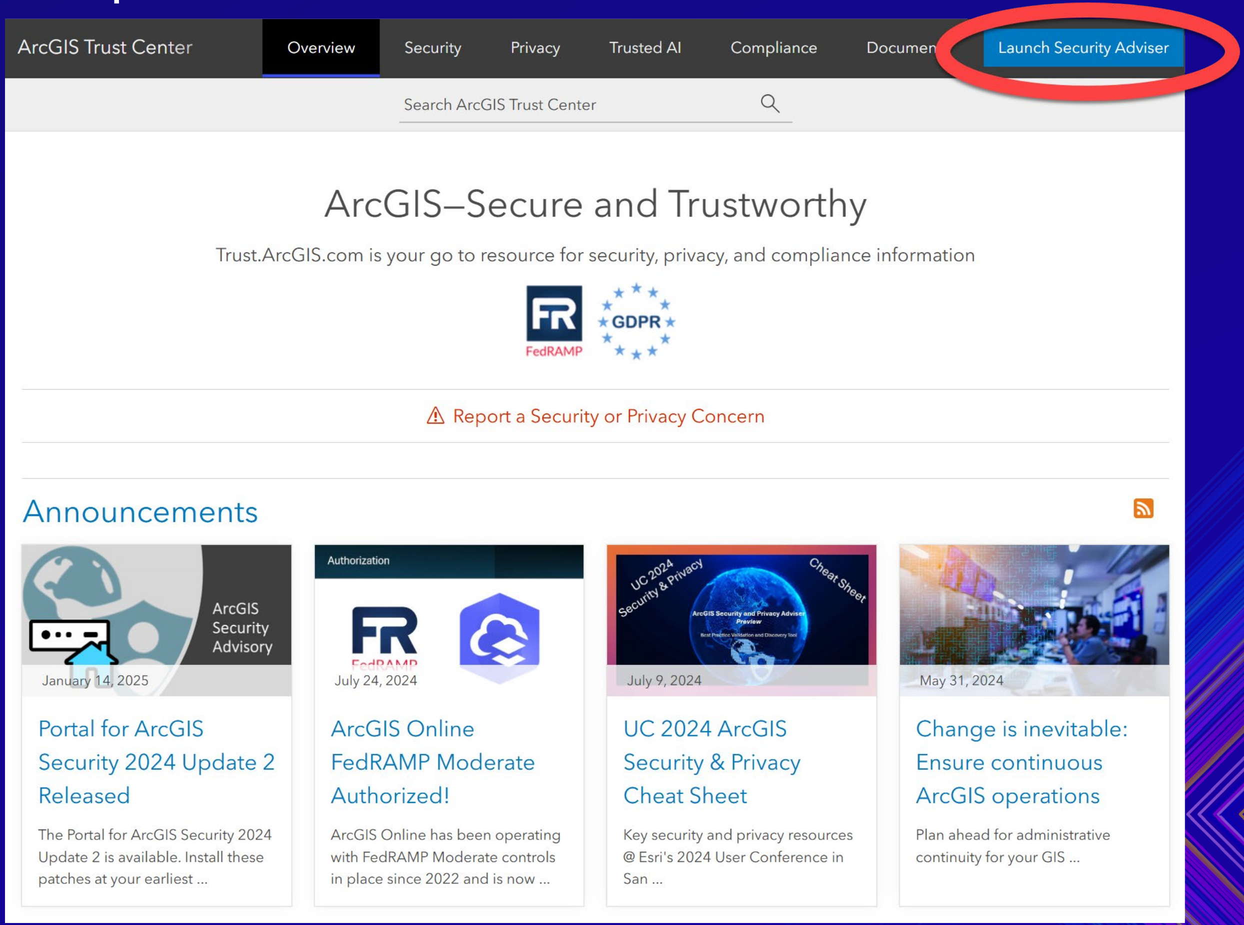
Best Practice Validation and Discovery Tool

Tools

ArcGIS Security & Privacy Adviser

- Ensure systems configured in alignment with best practices

- Use ArcGIS Security & Privacy Advisor
  - Where? ArcGIS Trust Center home page
  - What? Scan ArcGIS Online or Enterprise
  - Who? Requires Admin role
  - Cost? Free
  - Setup? ArcGIS Online - None
  - Time? Less then 1 minute



ArcGIS Trust Center | Overview | Security | Privacy | Trusted AI | Compliance | Documen | Launch Security Adviser

Search ArcGIS Trust Center

ArcGIS–Secure and Trustworthy

Trust.ArcGIS.com is your go to resource for security, privacy, and compliance information

⚠ Report a Security or Privacy Concern

Announcements

January 14, 2025
Portal for ArcGIS Security 2024 Update 2 Released
The Portal for ArcGIS Security 2024 Update 2 is available. Install these patches at your earliest ...

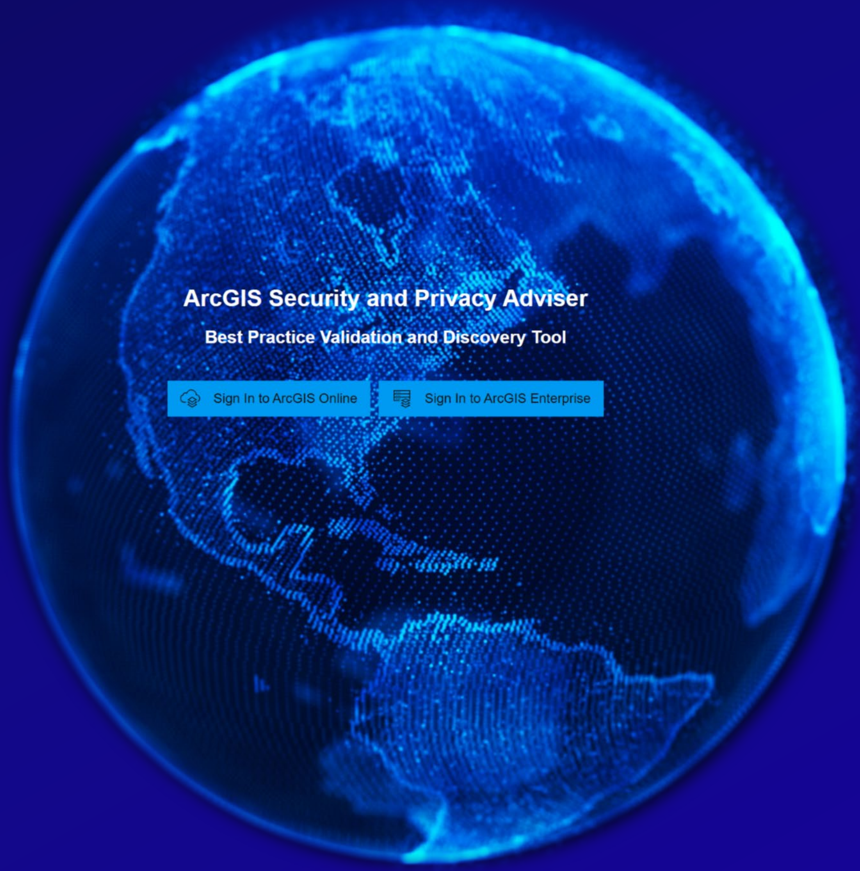
July 24, 2024
ArcGIS Online FedRAMP Moderate Authorized!
ArcGIS Online has been operating with FedRAMP Moderate controls in place since 2022 and is now ...

July 9, 2024
UC 2024 ArcGIS Security & Privacy Cheat Sheet
Key security and privacy resources @ Esri's 2024 User Conference in San ...

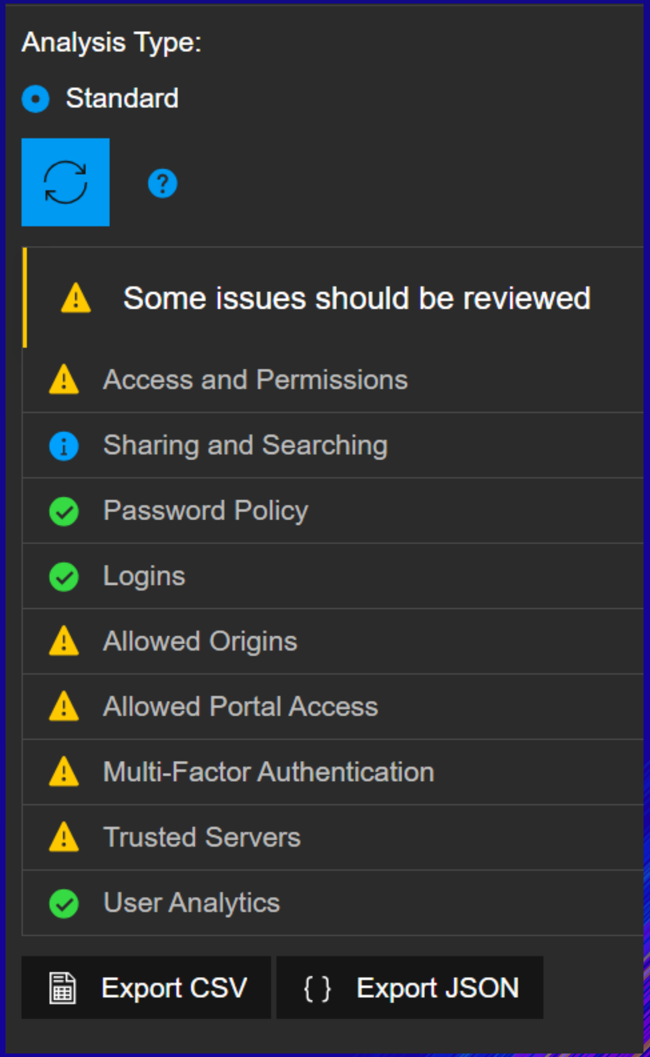
May 31, 2024
Change is inevitable: Ensure continuous ArcGIS operations
Plan ahead for administrative continuity for your GIS ...

Tools

Using Security & Privacy Adviser


ArcGIS Security and Privacy Adviser

Best Practice Validation and Discovery Tool


Analysis Type:

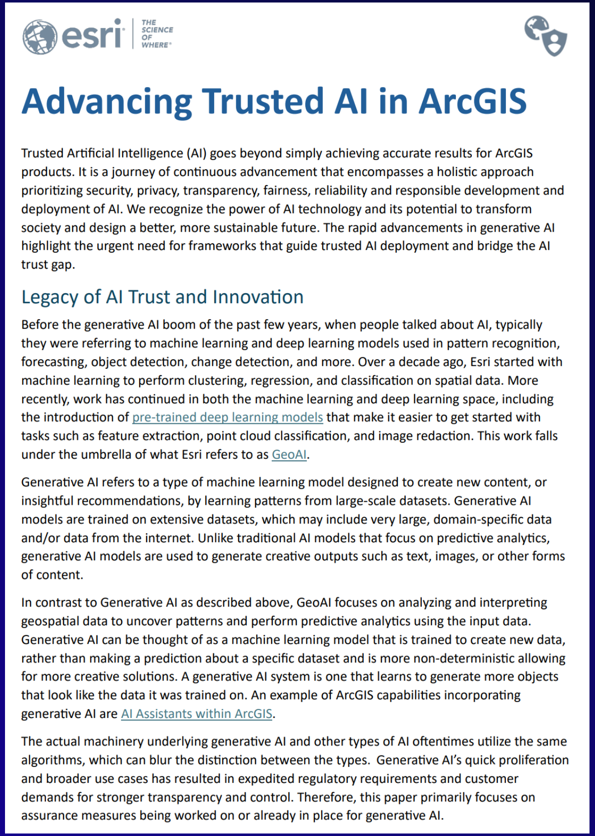
● Standard

⚠ Some issues should be reviewed

- ⚠ Access and Permissions
- ⓘ Sharing and Searching
- ✓ Password Policy
- ✓ Logins
- ⚠ Allowed Origins
- ⚠ Allowed Portal Access
- ⚠ Multi-Factor Authentication
- ⚠ Trusted Servers
- ✓ User Analytics

Address Red (Dangerous) items immediately

Trusted AI



esri THE SCIENCE OF WHERE

Advancing Trusted AI in ArcGIS

Trusted Artificial Intelligence (AI) goes beyond simply achieving accurate results for ArcGIS products. It is a journey of continuous advancement that encompasses a holistic approach prioritizing security, privacy, transparency, fairness, reliability and responsible development and deployment of AI. We recognize the power of AI technology and its potential to transform society and design a better, more sustainable future. The rapid advancements in generative AI highlight the urgent need for frameworks that guide trusted AI deployment and bridge the AI trust gap.

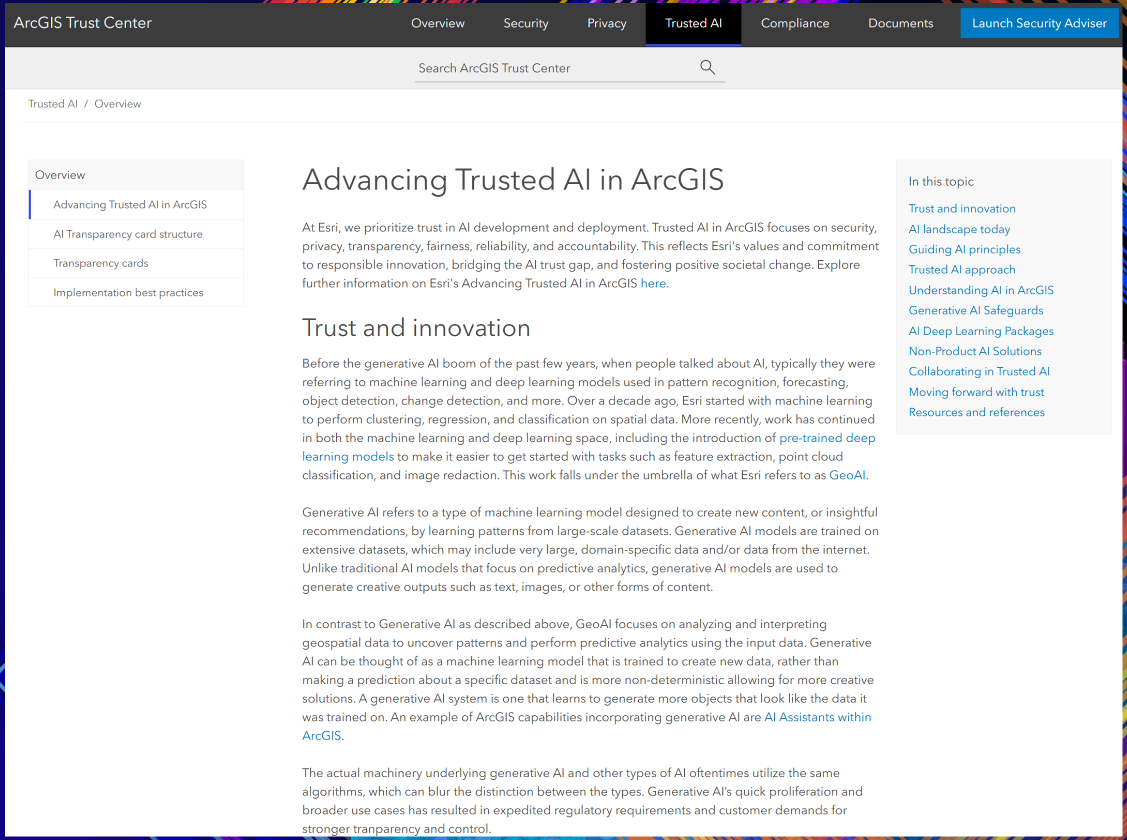
Legacy of AI Trust and Innovation

Before the generative AI boom of the past few years, when people talked about AI, typically they were referring to machine learning and deep learning models used in pattern recognition, forecasting, object detection, change detection, and more. Over a decade ago, Esri started with machine learning to perform clustering, regression, and classification on spatial data. More recently, work has continued in both the machine learning and deep learning space, including the introduction of pre-trained deep learning models that make it easier to get started with tasks such as feature extraction, point cloud classification, and image redaction. This work falls under the umbrella of what Esri refers to as GeoAI.

Generative AI refers to a type of machine learning model designed to create new content, or insightful recommendations, by learning patterns from large-scale datasets. Generative AI models are trained on extensive datasets, which may include very large, domain-specific data and/or data from the internet. Unlike traditional AI models that focus on predictive analytics, generative AI models are used to generate creative outputs such as text, images, or other forms of content.

In contrast to Generative AI as described above, GeoAI focuses on analyzing and interpreting geospatial data to uncover patterns and perform predictive analytics using the input data. Generative AI can be thought of as a machine learning model that is trained to create new data, rather than making a prediction about a specific dataset and is more non-deterministic allowing for more creative solutions. A generative AI system is one that learns to generate more objects that look like the data it was trained on. An example of ArcGIS capabilities incorporating generative AI are AI Assistants within ArcGIS.

The actual machinery underlying generative AI and other types of AI oftentimes utilize the same algorithms, which can blur the distinction between the types. Generative AI's quick proliferation and broader use cases has resulted in expedited regulatory requirements and customer demands for stronger transparency and control. Therefore, this paper primarily focuses on assurance measures being worked on or already in place for generative AI.



Advancing Trusted AI in ArcGIS

At Esri, we prioritize trust in AI development and deployment. Trusted AI in ArcGIS focuses on security, privacy, transparency, fairness, reliability, and accountability. This reflects Esri's values and commitment to responsible innovation, bridging the AI trust gap, and fostering positive societal change. Explore further information on Esri's Advancing Trusted AI in ArcGIS here.

Trust and innovation

Before the generative AI boom of the past few years, when people talked about AI, typically they were referring to machine learning and deep learning models used in pattern recognition, forecasting, object detection, change detection, and more. Over a decade ago, Esri started with machine learning to perform clustering, regression, and classification on spatial data. More recently, work has continued in both the machine learning and deep learning space, including the introduction of pre-trained deep learning models to make it easier to get started with tasks such as feature extraction, point cloud classification, and image redaction. This work falls under the umbrella of what Esri refers to as GeoAI.

Generative AI refers to a type of machine learning model designed to create new content, or insightful recommendations, by learning patterns from large-scale datasets. Generative AI models are trained on extensive datasets, which may include very large, domain-specific data and/or data from the internet. Unlike traditional AI models that focus on predictive analytics, generative AI models are used to generate creative outputs such as text, images, or other forms of content.

In contrast to Generative AI as described above, GeoAI focuses on analyzing and interpreting geospatial data to uncover patterns and perform predictive analytics using the input data. Generative AI can be thought of as a machine learning model that is trained to create new data, rather than making a prediction about a specific dataset and is more non-deterministic allowing for more creative solutions. A generative AI system is one that learns to generate more objects that look like the data it was trained on. An example of ArcGIS capabilities incorporating generative AI are AI Assistants within ArcGIS.

The actual machinery underlying generative AI and other types of AI oftentimes utilize the same algorithms, which can blur the distinction between the types. Generative AI's quick proliferation and broader use cases has resulted in expedited regulatory requirements and customer demands for stronger tranparency and control.

Trusted AI

- Esri started providing machine learning capabilities over a decade ago
  - Introduced pre-trained deep learning models – GeoAI

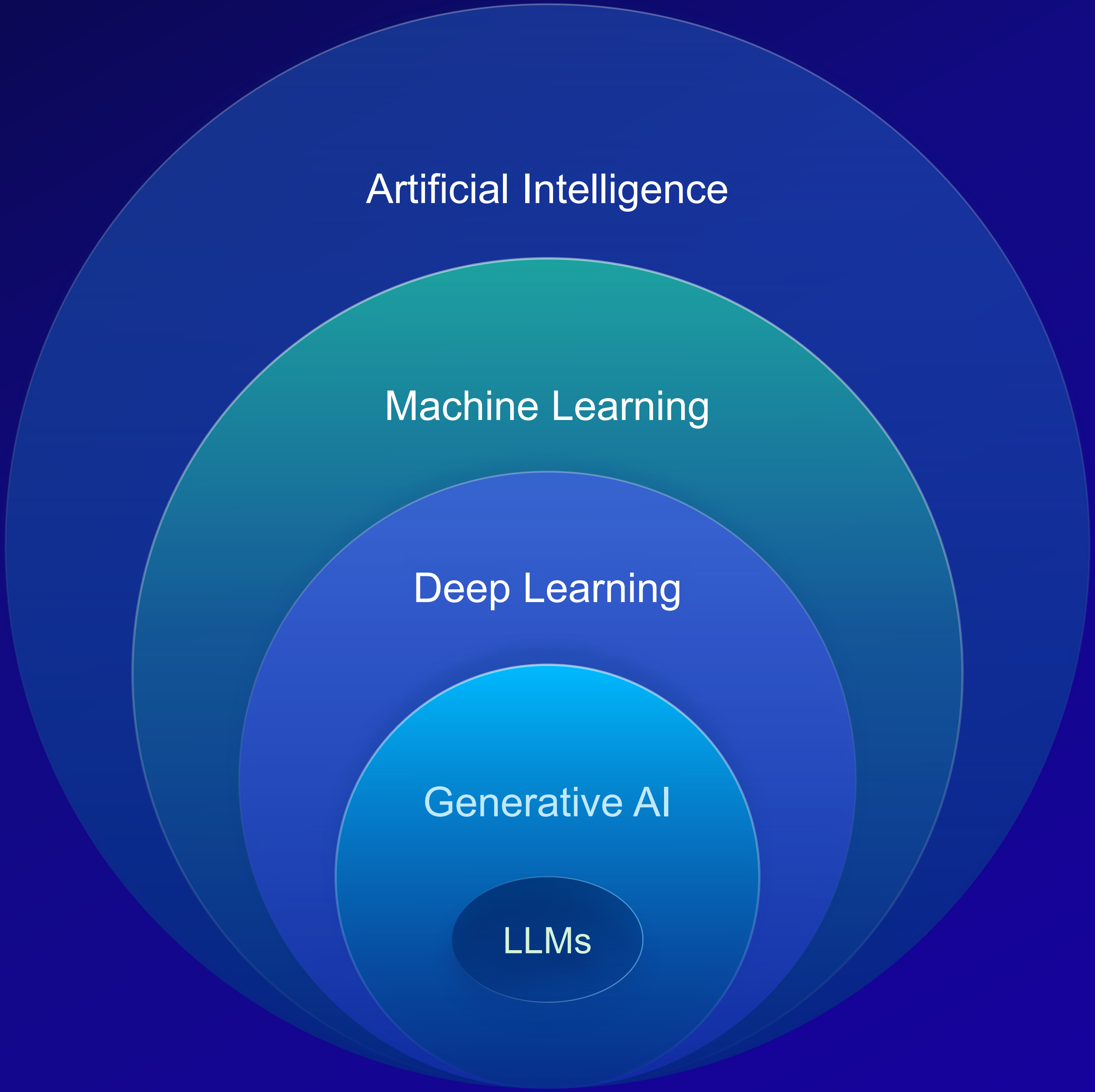
- Esri is introducing Generative-AI capabilities as part new “AI Assistants”
  - Generative-AI brings new opportunities to expand geospatial service value
  - Customers demand transparency due to corresponding risks if not appropriately designed and managed

- Creating a Trusted AI is a shared responsibility between Esri and our customers
  - NEW “*Trusted AI*” section of ArcGIS Trust Center

Before jumping into new site content, let’s cover some AI basics

Trusted AI

AI Basics



Trusted AI

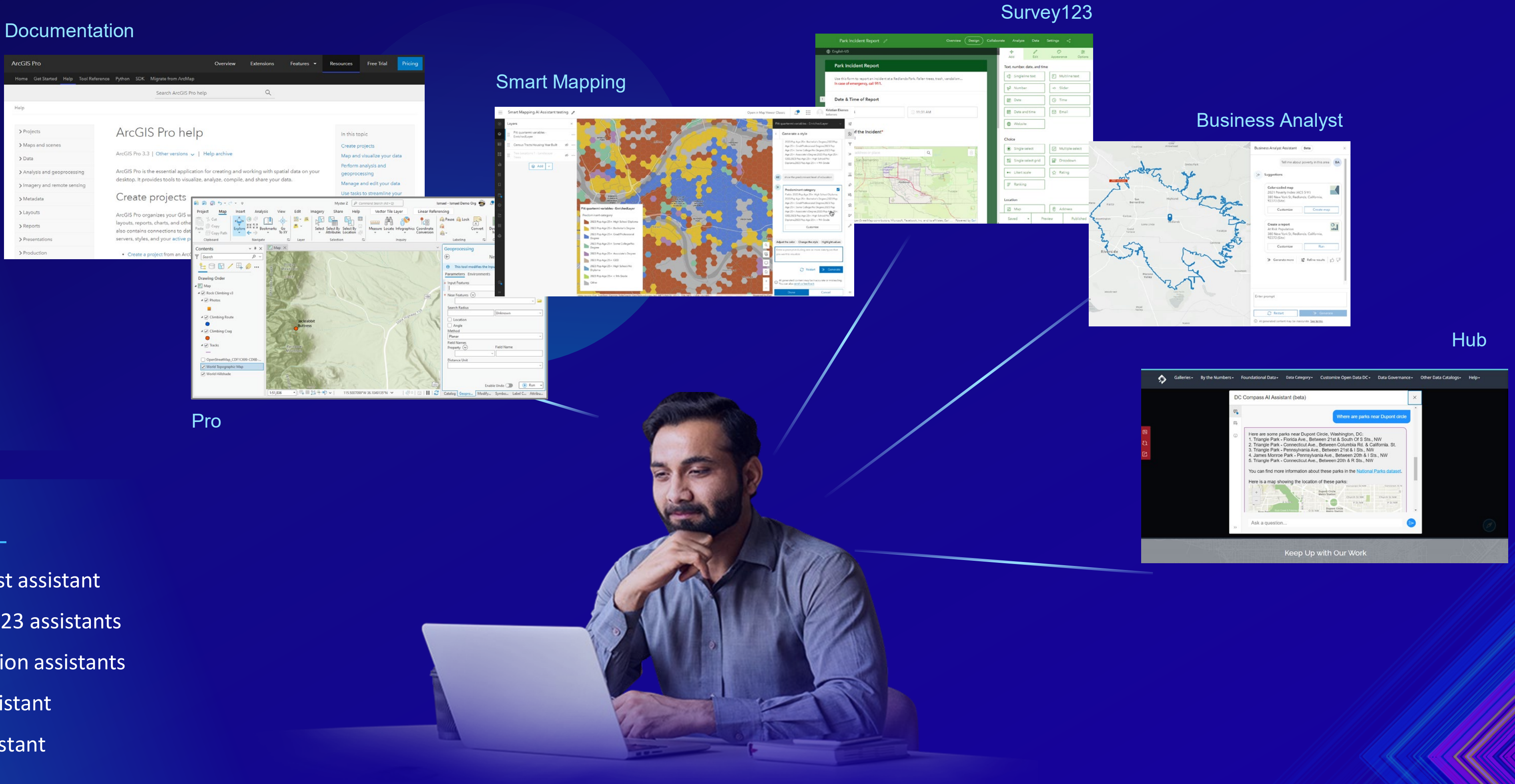
AI Assistants in ArcGIS

Assistants for…

- Mapping
- Analysis
- App Creation
- Data Management
- Administration
- Search
- Learning
- …

In Beta now

- Business Analyst assistant
- ArcGIS Survey123 assistants
- ArcGIS Translation assistants
- ArcGIS Hub assistant
- ArcGIS Pro assistant



ArcGIS Pro help

ArcGIS Pro is the essential application for creating and working with spatial data on your desktop. It provides tools to visualize, analyze, compile, and share your data.

Create projects

DC Compass AI Assistant (beta)

Where are parks near Dupont circle

Here are some parks near Dupont Circle, Washington, DC:
1. Triangle Park - Florida Ave., Between 21st & South Of S Sts., NW
2. Triangle Park - Connecticut Ave., Between Columbia Rd. & California. St.
3. Triangle Park - Pennsylvania Ave., Between 21st & I Sts., NW
4. James Monroe Park - Pennsylvania Ave., Between 20th & I Sts., NW
5. Triangle Park - Connecticut Ave., Between 20th & R Sts., NW

You can find more information about these parks in the National Parks dataset.

Here is a map showing the location of these parks:

Ask a question...

Trusted AI

Esri’s Principles

Security
Committed to safeguarding security and mitigating risks

Privacy
Prioritize protecting user data and ensuring the privacy of AI

Accountability
Governance, responsibility, and human oversight

Transparency
Clear visibility about our AI models

Fairness
Upholding the principles of fairness, ethics, and societal responsibility

Reliability
AI is carefully tested and validated to be consistent

Trusted AI

Esri Commitments

AI Assistants

- Not enabled by default; users or administrators must opt-in to utilize them

Data Privacy & Security Measures

- User data and prompts not utilized to train AI models
  - Feedback – prompts are stored
- When third-party AI services are employed by Esri, enterprise-class AI instances are used

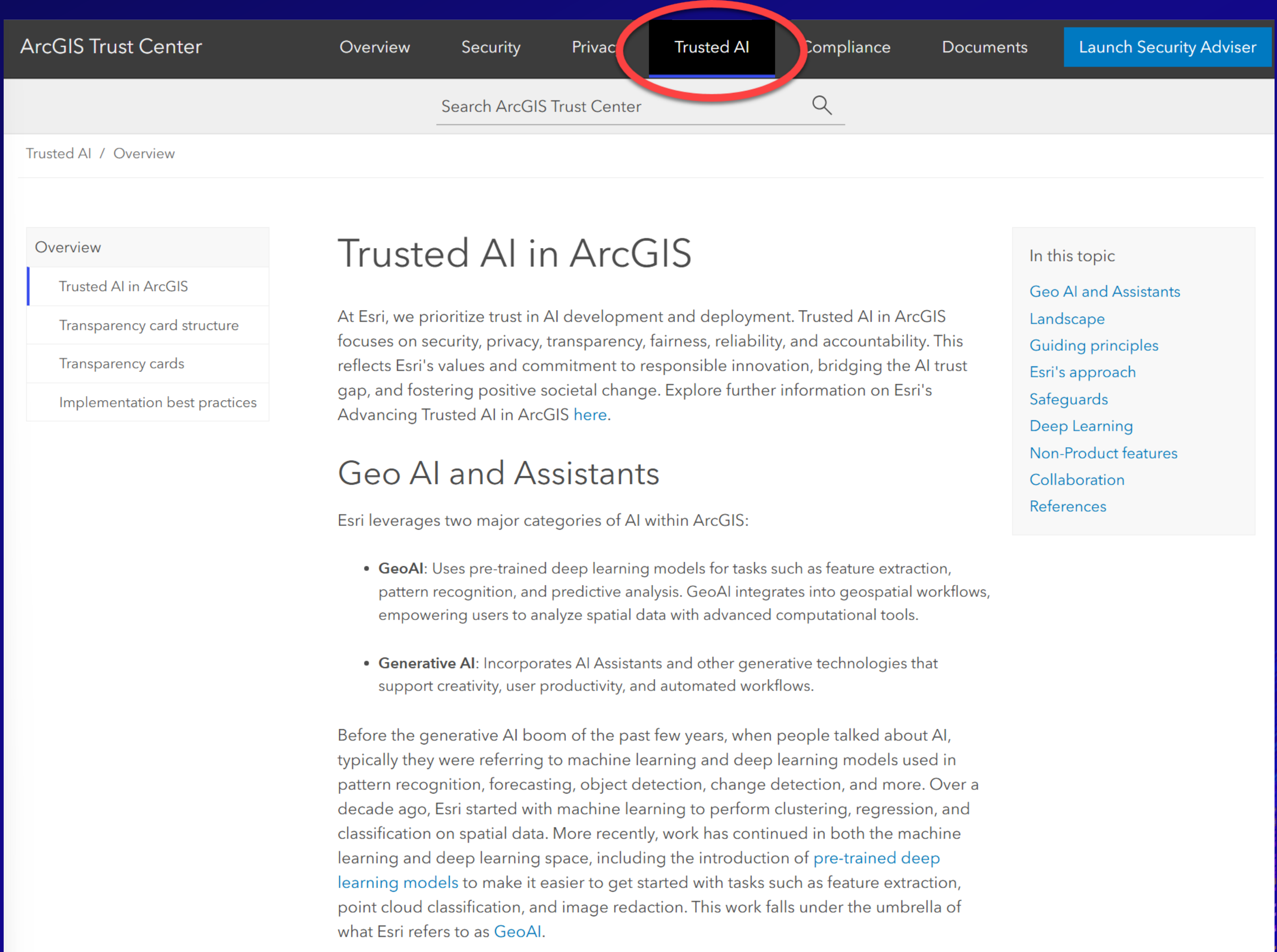
Oversight & Limitation

- Outputs may vary in accuracy; customers are advised to validate results
- Tools such AI Transparency Cards can be leveraged

Trusted AI

NEW Site!

- Where?
  - ArcGIS Trust Center
- When?
  - Live Feb 20, 2025
- Why?
  - Single-stop for AI questions
- Four areas
  - Overview
  - Card Structure
  - Transparency Cards
  - Best Practices



Trusted AI in ArcGIS

At Esri, we prioritize trust in AI development and deployment. Trusted AI in ArcGIS focuses on security, privacy, transparency, fairness, reliability, and accountability. This reflects Esri's values and commitment to responsible innovation, bridging the AI trust gap, and fostering positive societal change. Explore further information on Esri's Advancing Trusted AI in ArcGIS here.

Geo AI and Assistants

Esri leverages two major categories of AI within ArcGIS:

- **GeoAI**: Uses pre-trained deep learning models for tasks such as feature extraction, pattern recognition, and predictive analysis. GeoAI integrates into geospatial workflows, empowering users to analyze spatial data with advanced computational tools.
- **Generative AI**: Incorporates AI Assistants and other generative technologies that support creativity, user productivity, and automated workflows.

Before the generative AI boom of the past few years, when people talked about AI, typically they were referring to machine learning and deep learning models used in pattern recognition, forecasting, object detection, change detection, and more. Over a decade ago, Esri started with machine learning to perform clustering, regression, and classification on spatial data. More recently, work has continued in both the machine learning and deep learning space, including the introduction of pre-trained deep learning models to make it easier to get started with tasks such as feature extraction, point cloud classification, and image redaction. This work falls under the umbrella of what Esri refers to as GeoAI.

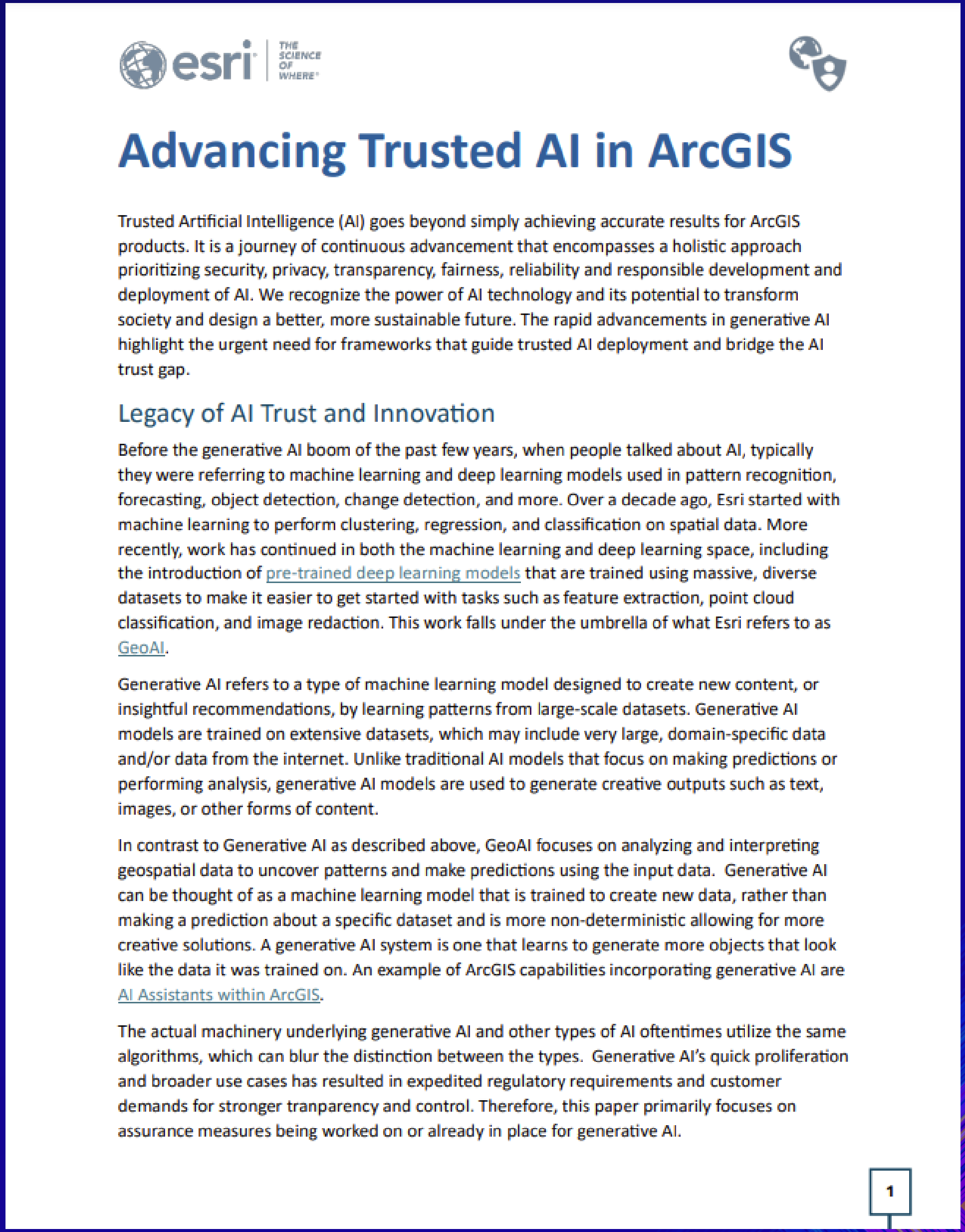
Trust.ArcGIS.com

Trusted AI

Overview

- Advancing Trusted AI in ArcGIS
  - Comprehensive information on Esri's AI practices
  - GeoAI / Assistants
  - AI Principles (Secure, Transparent…)
  - Customer choice (Opt-in)
  - Governance (AI Board)

- Understanding AI Models and AI-backed features
  - Model Cards
    - Deep-Learning models
  - Transparency Cards
    - Esri features utilizing Generative AI



esri THE SCIENCE OF WHERE

Advancing Trusted AI in ArcGIS

Trusted Artificial Intelligence (AI) goes beyond simply achieving accurate results for ArcGIS products. It is a journey of continuous advancement that encompasses a holistic approach prioritizing security, privacy, transparency, fairness, reliability and responsible development and deployment of AI. We recognize the power of AI technology and its potential to transform society and design a better, more sustainable future. The rapid advancements in generative AI highlight the urgent need for frameworks that guide trusted AI deployment and bridge the AI trust gap.

Legacy of AI Trust and Innovation

Before the generative AI boom of the past few years, when people talked about AI, typically they were referring to machine learning and deep learning models used in pattern recognition, forecasting, object detection, change detection, and more. Over a decade ago, Esri started with machine learning to perform clustering, regression, and classification on spatial data. More recently, work has continued in both the machine learning and deep learning space, including the introduction of pre-trained deep learning models that are trained using massive, diverse datasets to make it easier to get started with tasks such as feature extraction, point cloud classification, and image redaction. This work falls under the umbrella of what Esri refers to as GeoAI.

Generative AI refers to a type of machine learning model designed to create new content, or insightful recommendations, by learning patterns from large-scale datasets. Generative AI models are trained on extensive datasets, which may include very large, domain-specific data and/or data from the internet. Unlike traditional AI models that focus on making predictions or performing analysis, generative AI models are used to generate creative outputs such as text, images, or other forms of content.

In contrast to Generative AI as described above, GeoAI focuses on analyzing and interpreting geospatial data to uncover patterns and make predictions using the input data. Generative AI can be thought of as a machine learning model that is trained to create new data, rather than making a prediction about a specific dataset and is more non-deterministic allowing for more creative solutions. A generative AI system is one that learns to generate more objects that look like the data it was trained on. An example of ArcGIS capabilities incorporating generative AI are AI Assistants within ArcGIS.

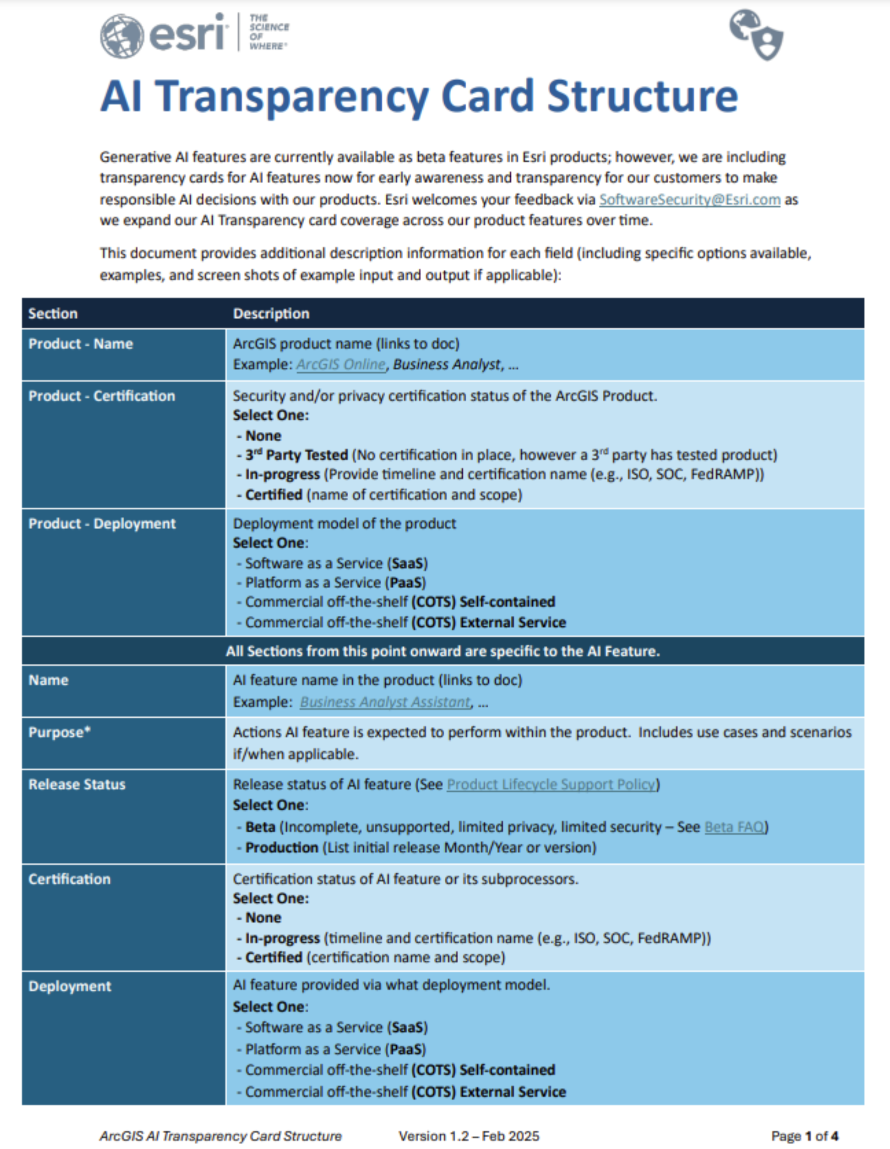
The actual machinery underlying generative AI and other types of AI oftentimes utilize the same algorithms, which can blur the distinction between the types. Generative AI's quick proliferation and broader use cases has resulted in expedited regulatory requirements and customer demands for stronger tranparency and control. Therefore, this paper primarily focuses on assurance measures being worked on or already in place for generative AI.

Trusted AI

Card Structures

- AI Transparency Card Structure document
  - Detailed lookup table for Transparency Cards
  - Descriptions for each field and associated options
  - Four pages
  - Result - Succinct 2-page cards for each AI Assistant

- Deep-learning Model cards
  - Based on Hugging-Face / FedRAMP structure
  - Focus is on AI Model itself
  - Available within Living Atlas DLTK downloads



esri THE SCIENCE OF WHERE

AI Transparency Card Structure

Generative AI features are currently available as beta features in Esri products; however, we are including transparency cards for AI features now for early awareness and transparency for our customers to make responsible AI decisions with our products. Esri welcomes your feedback via SoftwareSecurity@Esri.com as we expand our AI Transparency card coverage across our product features over time.

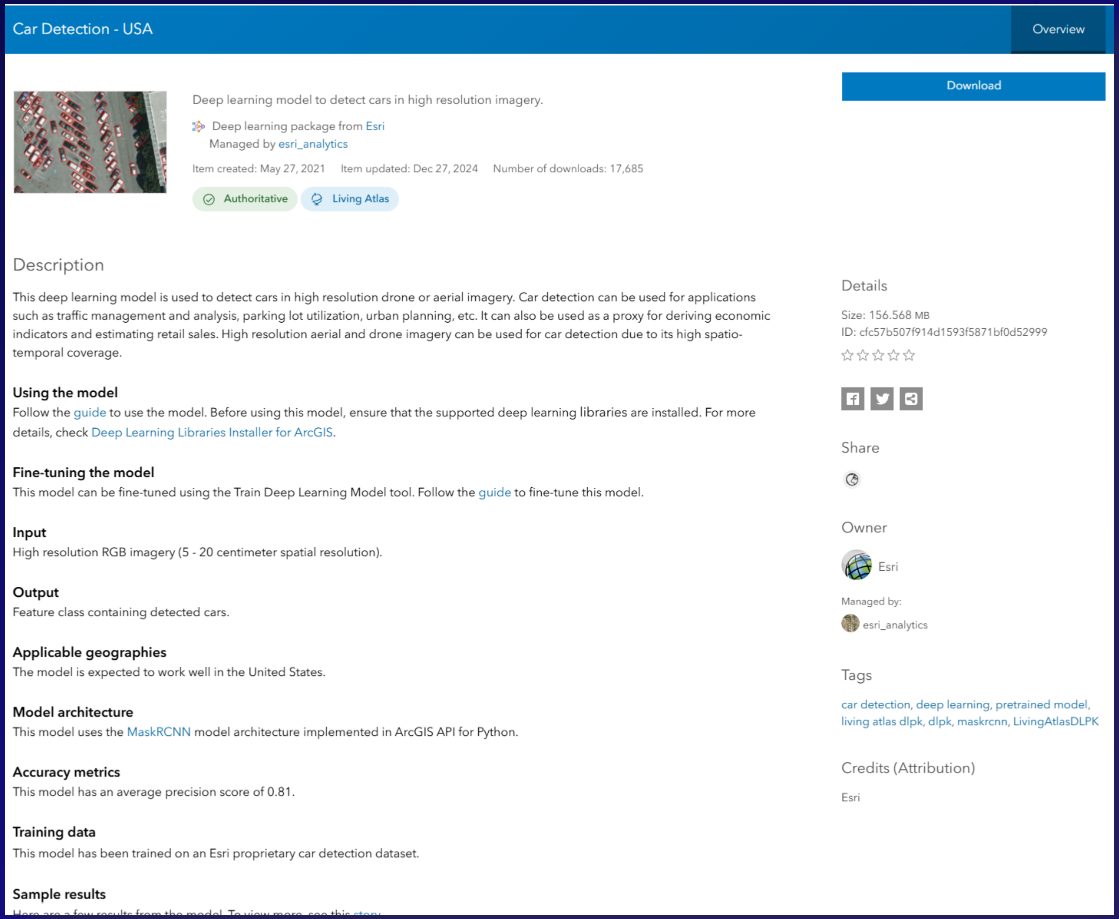
This document provides additional description information for each field (including specific options available, examples, and screen shots of example input and output if applicable):

Section	Description
Product - Name	ArcGIS product name (links to doc) Example: *ArcGIS Online*, ***Business Analyst***, …
Product - Certification	Security and/or privacy certification status of the ArcGIS Product. **Select One:** - **None** - **3rd Party Tested** (No certification in place, however a 3rd party has tested product) - **In-progress** (Provide timeline and certification name (e.g., ISO, SOC, FedRAMP)) - **Certified** (name of certification and scope)
Product - Deployment	Deployment model of the product **Select One**: - Software as a Service (**SaaS**) - Platform as a Service (**PaaS**) - Commercial off-the-shelf **(COTS) Self-contained** - Commercial off-the-shelf **(COTS) External Service**
All Sections from this point onward are specific to the AI Feature.	
Name	AI feature name in the product (links to doc) Example: *Business Analyst Assistant*, …
Purpose*	Actions AI feature is expected to perform within the product. Includes use cases and scenarios if/when applicable.
Release Status	Release status of AI feature (See Product Lifecycle Support Policy) **Select One**: - **Beta** (Incomplete, unsupported, limited privacy, limited security – See Beta FAQ) - **Production** (List initial release Month/Year or version)
Certification	Certification status of AI feature or its subprocessors. **Select One:** - **None** - **In-progress** (timeline and certification name (e.g., ISO, SOC, FedRAMP)) - **Certified** (certification name and scope)
Deployment	AI feature provided via what deployment model. **Select One**: - Software as a Service (**SaaS**) - Platform as a Service (**PaaS**) - Commercial off-the-shelf **(COTS) Self-contained** - Commercial off-the-shelf **(COTS) External Service**

ArcGIS AI Transparency Card Structure Version 1.2 – Feb 2025 Page **1** of **4**

Trusted AI

Two Types of Cards



Car Detection - USA

Deep learning model to detect cars in high resolution imagery.

Deep learning package from Esri
Managed by esri_analytics

Item created: May 27, 2021 Item updated: Dec 27, 2024 Number of downloads: 17,685

Authoritative Living Atlas

Description

This deep learning model is used to detect cars in high resolution drone or aerial imagery. Car detection can be used for applications such as traffic management and analysis, parking lot utilization, urban planning, etc. It can also be used as a proxy for deriving economic indicators and estimating retail sales. High resolution aerial and drone imagery can be used for car detection due to its high spatio-temporal coverage.

Using the model
Follow the guide to use the model. Before using this model, ensure that the supported deep learning libraries are installed. For more details, check Deep Learning Libraries Installer for ArcGIS.

Fine-tuning the model
This model can be fine-tuned using the Train Deep Learning Model tool. Follow the guide to fine-tune this model.

Input
High resolution RGB imagery (5 - 20 centimeter spatial resolution).

Output
Feature class containing detected cars.

Applicable geographies
The model is expected to work well in the United States.

Model architecture
This model uses the MaskRCNN model architecture implemented in ArcGIS API for Python.

Accuracy metrics
This model has an average precision score of 0.81.

Training data
This model has been trained on an Esri proprietary car detection dataset.

Sample results
Here are a few results from the model. To view more, see this story.

Details

Size: 156.568 MB
ID: cfc57b507f914d1593f5871bf0d52999

☆☆☆☆☆

Share

Owner

Esri

Managed by:

esri_analytics

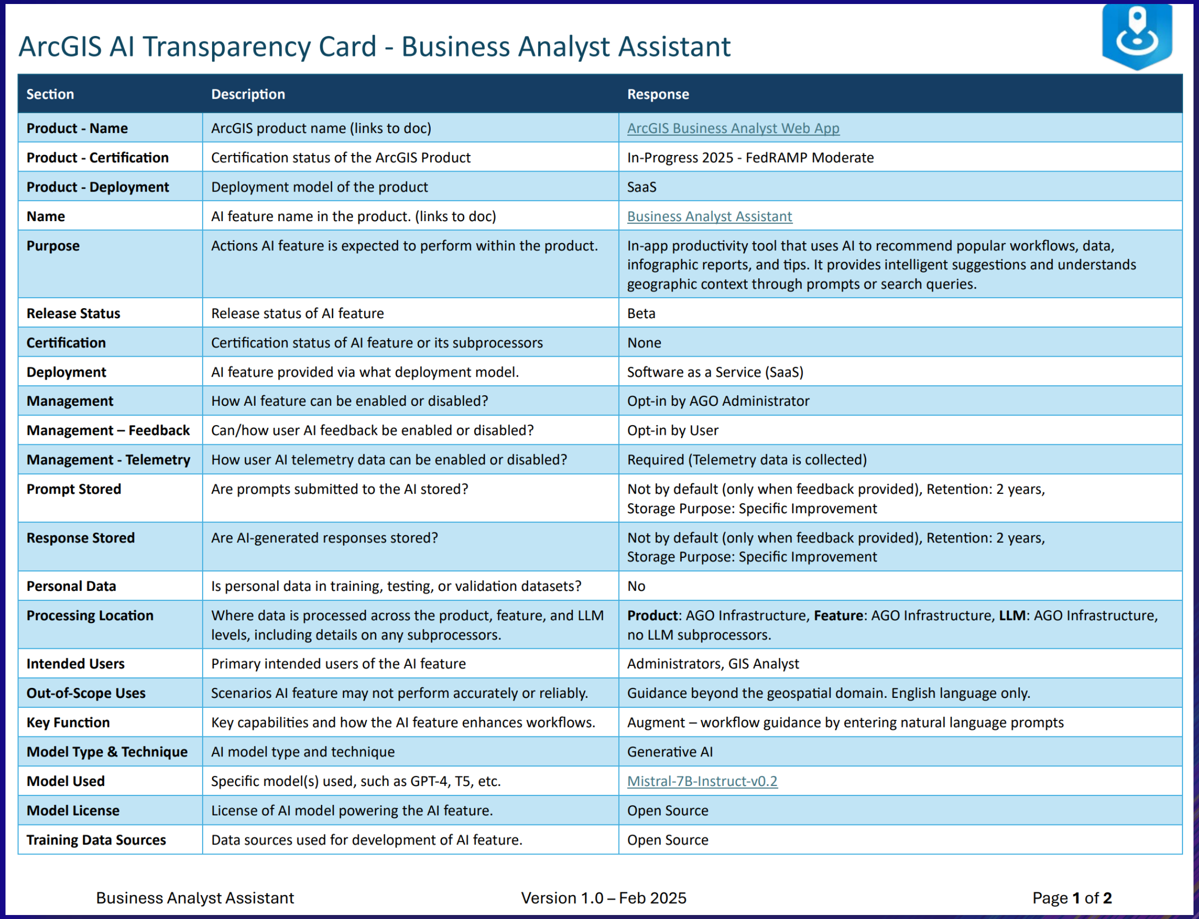
Tags

car detection, deep learning, pretrained model, living atlas dlpk, dlpk, maskrcnn, LivingAtlasDLPK

Credits (Attribution)

Esri

Deep Learning Model Cards



ArcGIS AI Transparency Card - Business Analyst Assistant

Section	Description	Response
Product - Name	ArcGIS product name (links to doc)	ArcGIS Business Analyst Web App
Product - Certification	Certification status of the ArcGIS Product	In-Progress 2025 - FedRAMP Moderate
Product - Deployment	Deployment model of the product	SaaS
Name	AI feature name in the product. (links to doc)	Business Analyst Assistant
Purpose	Actions AI feature is expected to perform within the product.	In-app productivity tool that uses AI to recommend popular workflows, data, infographic reports, and tips. It provides intelligent suggestions and understands geographic context through prompts or search queries.
Release Status	Release status of AI feature	Beta
Certification	Certification status of AI feature or its subprocessors	None
Deployment	AI feature provided via what deployment model.	Software as a Service (SaaS)
Management	How AI feature can be enabled or disabled?	Opt-in by AGO Administrator
Management – Feedback	Can/how user AI feedback be enabled or disabled?	Opt-in by User
Management - Telemetry	How user AI telemetry data can be enabled or disabled?	Required (Telemetry data is collected)
Prompt Stored	Are prompts submitted to the AI stored?	Not by default (only when feedback provided), Retention: 2 years, Storage Purpose: Specific Improvement
Response Stored	Are AI-generated responses stored?	Not by default (only when feedback provided), Retention: 2 years, Storage Purpose: Specific Improvement
Personal Data	Is personal data in training, testing, or validation datasets?	No
Processing Location	Where data is processed across the product, feature, and LLM levels, including details on any subprocessors.	**Product**: AGO Infrastructure, **Feature**: AGO Infrastructure, **LLM**: AGO Infrastructure, no LLM subprocessors.
Intended Users	Primary intended users of the AI feature	Administrators, GIS Analyst
Out-of-Scope Uses	Scenarios AI feature may not perform accurately or reliably.	Guidance beyond the geospatial domain. English language only.
Key Function	Key capabilities and how the AI feature enhances workflows.	Augment – workflow guidance by entering natural language prompts
Model Type & Technique	AI model type and technique	Generative AI
Model Used	Specific model(s) used, such as GPT-4, T5, etc.	Mistral-7B-Instruct-v0.2
Model License	License of AI model powering the AI feature.	Open Source
Training Data Sources	Data sources used for development of AI feature.	Open Source

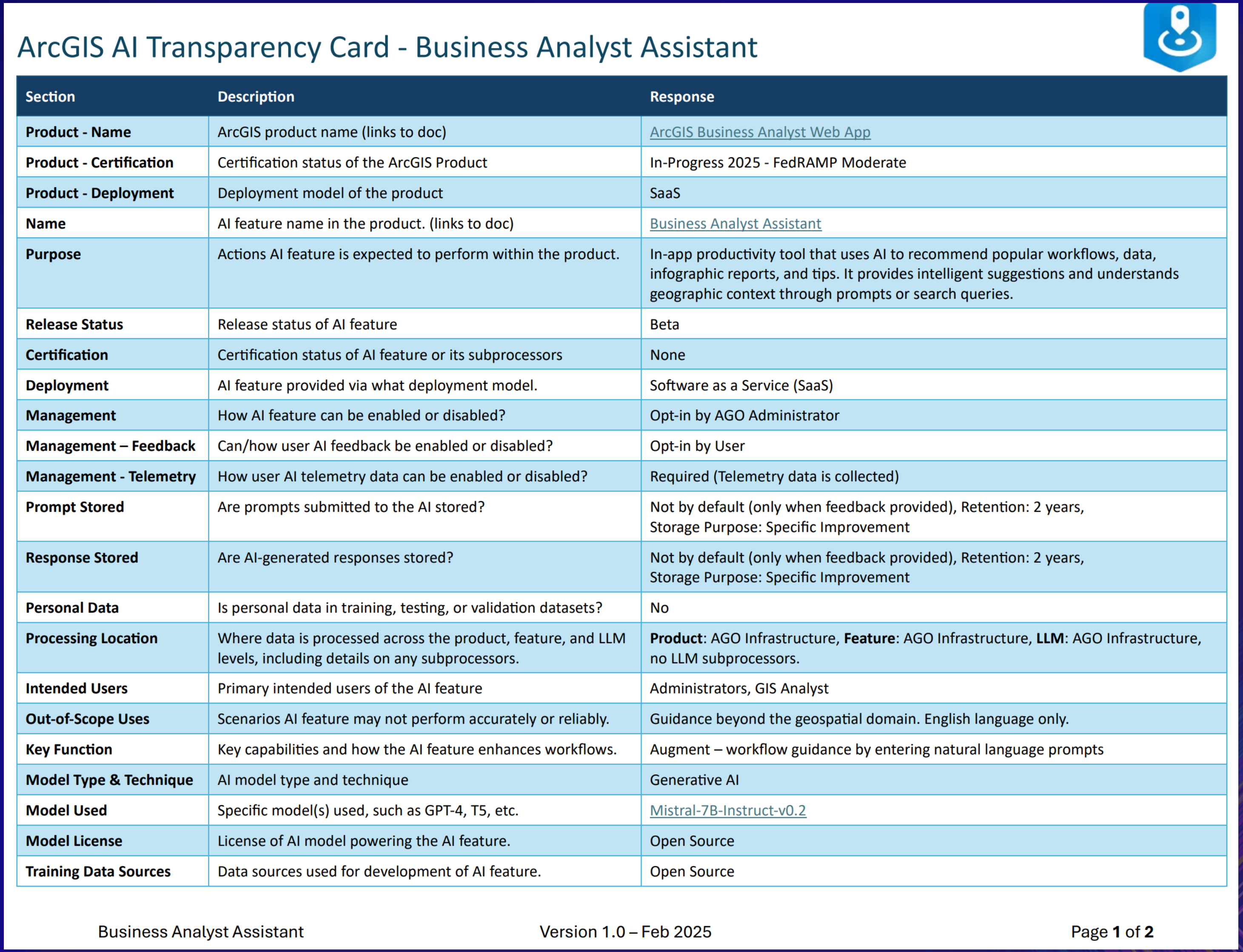
Business Analyst Assistant Version 1.0 – Feb 2025 Page **1** of **2**

AI Assistant Transparency Cards

Trusted AI

AI Transparency Cards

- Generative AI backed features results in a broader set of concerns NOT addressed by AI Model cards
- Resulted in AI Transparency Cards
- Contains information such as
  - Data handling and sources
  - Privacy/security safeguards
- Empowers customers to make risk-based decisions concerning features



ArcGIS AI Transparency Card - Business Analyst Assistant

Section	Description	Response
Product - Name	ArcGIS product name (links to doc)	ArcGIS Business Analyst Web App
Product - Certification	Certification status of the ArcGIS Product	In-Progress 2025 - FedRAMP Moderate
Product - Deployment	Deployment model of the product	SaaS
Name	AI feature name in the product. (links to doc)	Business Analyst Assistant
Purpose	Actions AI feature is expected to perform within the product.	In-app productivity tool that uses AI to recommend popular workflows, data, infographic reports, and tips. It provides intelligent suggestions and understands geographic context through prompts or search queries.
Release Status	Release status of AI feature	Beta
Certification	Certification status of AI feature or its subprocessors	None
Deployment	AI feature provided via what deployment model.	Software as a Service (SaaS)
Management	How AI feature can be enabled or disabled?	Opt-in by AGO Administrator
Management – Feedback	Can/how user AI feedback be enabled or disabled?	Opt-in by User
Management - Telemetry	How user AI telemetry data can be enabled or disabled?	Required (Telemetry data is collected)
Prompt Stored	Are prompts submitted to the AI stored?	Not by default (only when feedback provided), Retention: 2 years, Storage Purpose: Specific Improvement
Response Stored	Are AI-generated responses stored?	Not by default (only when feedback provided), Retention: 2 years, Storage Purpose: Specific Improvement
Personal Data	Is personal data in training, testing, or validation datasets?	No
Processing Location	Where data is processed across the product, feature, and LLM levels, including details on any subprocessors.	**Product**: AGO Infrastructure, **Feature**: AGO Infrastructure, **LLM**: AGO Infrastructure, no LLM subprocessors.
Intended Users	Primary intended users of the AI feature	Administrators, GIS Analyst
Out-of-Scope Uses	Scenarios AI feature may not perform accurately or reliably.	Guidance beyond the geospatial domain. English language only.
Key Function	Key capabilities and how the AI feature enhances workflows.	Augment – workflow guidance by entering natural language prompts
Model Type & Technique	AI model type and technique	Generative AI
Model Used	Specific model(s) used, such as GPT-4, T5, etc.	Mistral-7B-Instruct-v0.2
Model License	License of AI model powering the AI feature.	Open Source
Training Data Sources	Data sources used for development of AI feature.	Open Source

Business Analyst Assistant Version 1.0 – Feb 2025 Page **1** of **2**

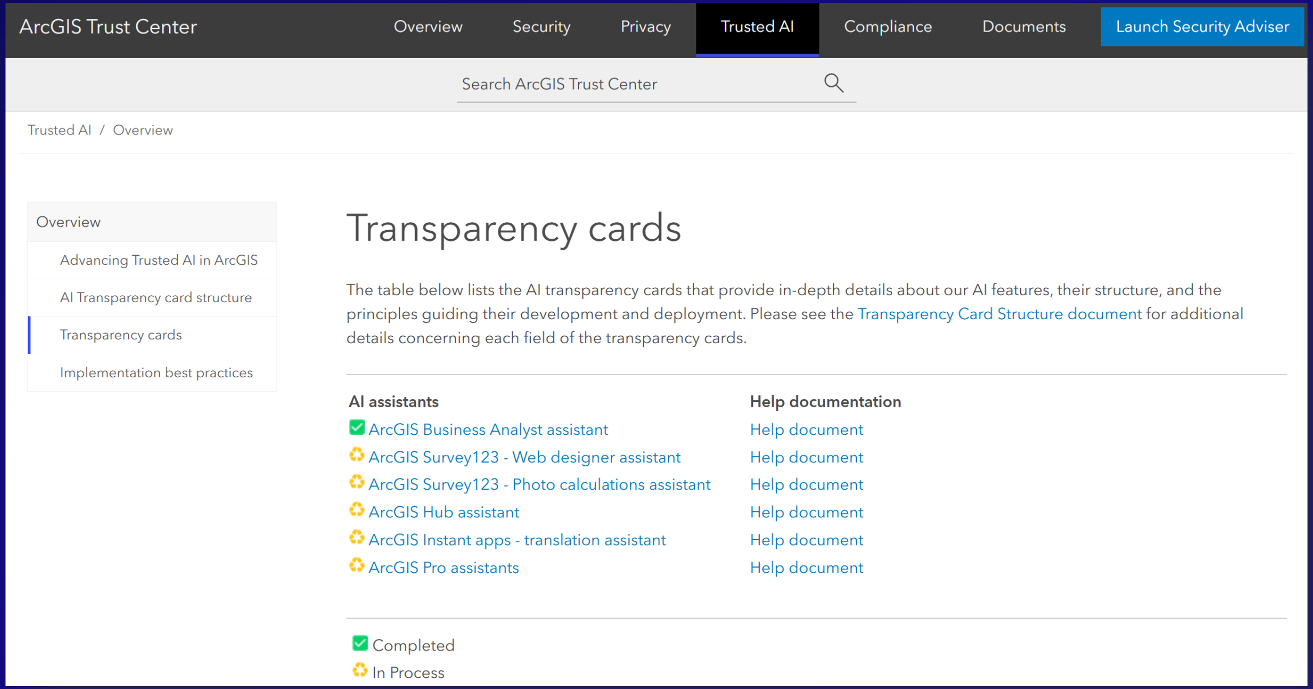
Trusted AI

Implementation Best Practices

- Shared Responsibility

- Esri responsibilities
  - Transparency & Model Cards
  - Communicate what Esri’s done

- Customer responsibilities
  - Implementation Best Practices section
  - Summarizes customer responsibilities
    - Settings
    - Monitoring
    - Training
    - Validation

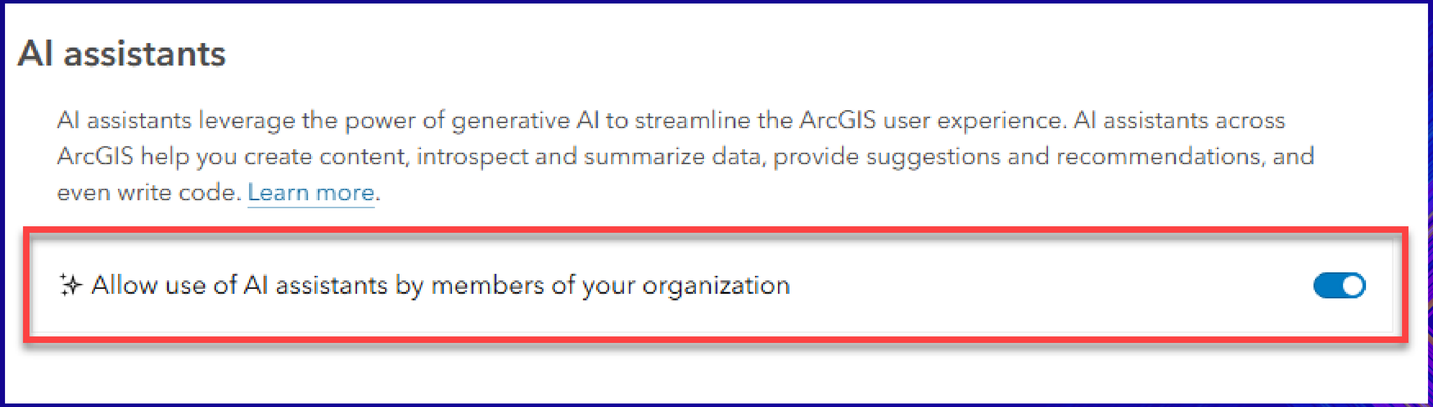


Transparency cards

The table below lists the AI transparency cards that provide in-depth details about our AI features, their structure, and the principles guiding their development and deployment. Please see the Transparency Card Structure document for additional details concerning each field of the transparency cards.

AI assistants	Help documentation
☑ ArcGIS Business Analyst assistant	Help document
♻ ArcGIS Survey123 - Web designer assistant	Help document
♻ ArcGIS Survey123 - Photo calculations assistant	Help document
♻ ArcGIS Hub assistant	Help document
♻ ArcGIS Instant apps - translation assistant	Help document
♻ ArcGIS Pro assistants	Help document

☑ Completed
♻ In Process



AI assistants

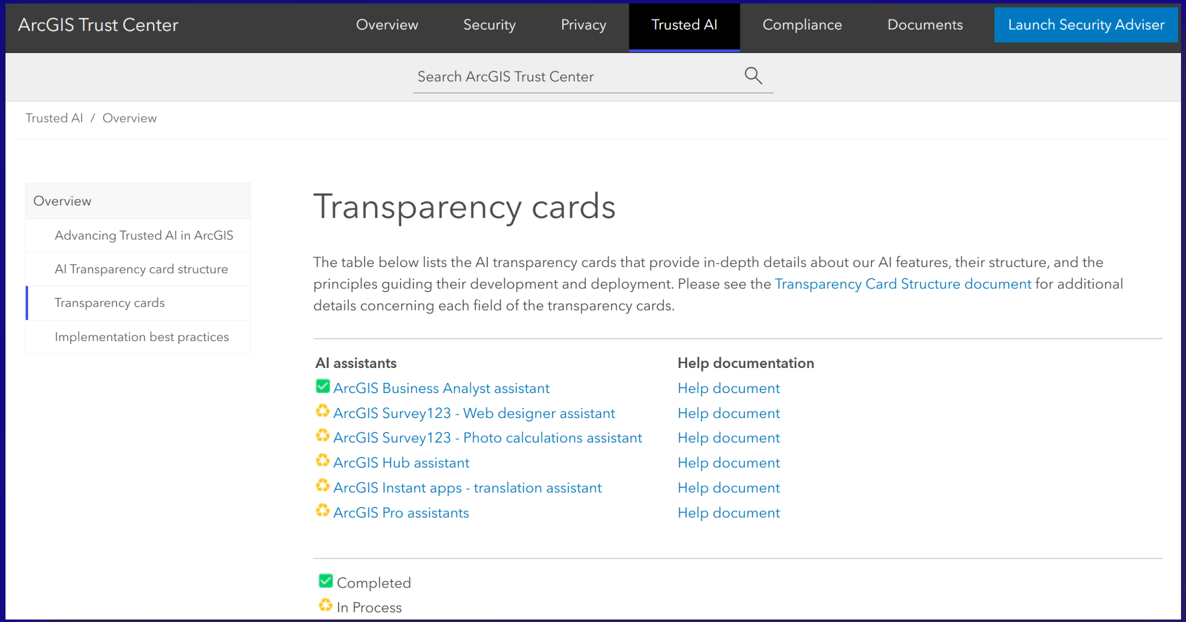
AI assistants leverage the power of generative AI to streamline the ArcGIS user experience. AI assistants across ArcGIS help you create content, introspect and summarize data, provide suggestions and recommendations, and even write code. Learn more.

Allow use of AI assistants by members of your organization ●

Trusted AI

Summary

- ArcGIS Trust Center new “Trusted AI” section
  - One stop shop for agencies to get Artificial Intelligence answers
  - Extensive information now available
  - Designed to evolve based on customer feedback/demands
  - Links to relevant AI materials across Esri pages



ArcGIS Trust Center

Overview | Security | Privacy | Trusted AI | Compliance | Documents | Launch Security Adviser

Search ArcGIS Trust Center

Trusted AI / Overview

- Overview
  - Advancing Trusted AI in ArcGIS
  - AI Transparency card structure
  - Transparency cards
  - Implementation best practices

Transparency cards

The table below lists the AI transparency cards that provide in-depth details about our AI features, their structure, and the principles guiding their development and deployment. Please see the Transparency Card Structure document for additional details concerning each field of the transparency cards.

AI assistants	Help documentation
☑ ArcGIS Business Analyst assistant	Help document
⟳ ArcGIS Survey123 - Web designer assistant	Help document
⟳ ArcGIS Survey123 - Photo calculations assistant	Help document
⟳ ArcGIS Hub assistant	Help document
⟳ ArcGIS Instant apps - translation assistant	Help document
⟳ ArcGIS Pro assistants	Help document

☑ Completed

⟳ In Process

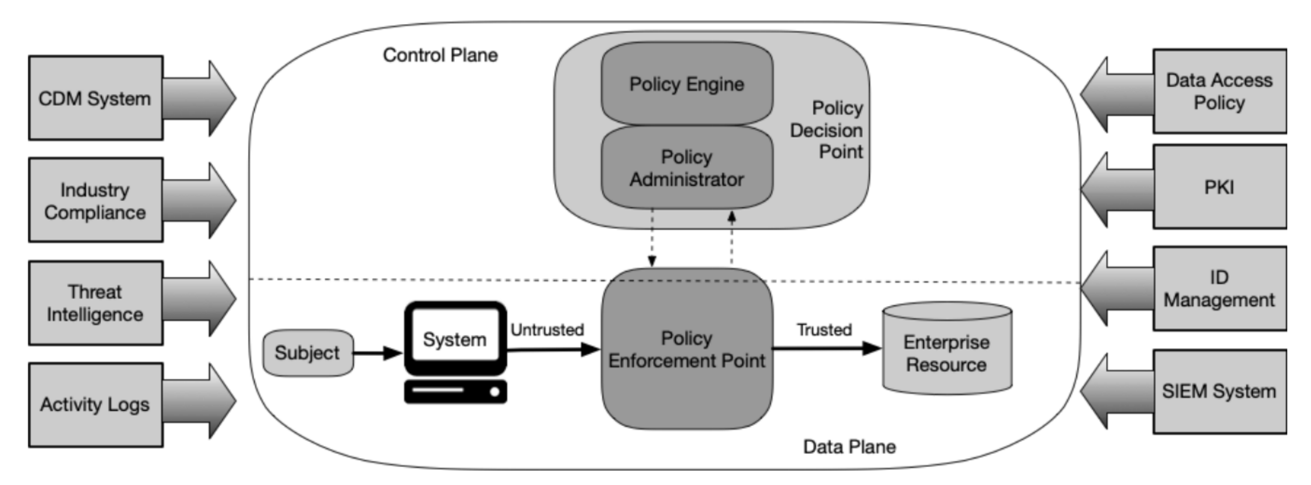
Zero Trust Architecture (ZTA)

Image generated by Microsoft Copilot.

Zero Trust Architecture

- Strong security value, but strong marketing hype still

- Focus on ZTA foundations first
  - Zero Trust Maturity Model from CISA
  - ZTA implementation target for US agencies was EOY 2024
  - ZTA Foundations in Enterprise Hardening Guide applicable for ArcGIS Online



NIST SP 800-207 – Core Zero Trust Components

Zero Trust Architecture

Three Foundational Components Your Agency Should Have in Place By Now

- Phishing resistant MFA
  - Non-Phishing resistant MFA - Ex: code sent to your phone
  - Phishing resistant MFA – Ex: Biometrics, hardware tokens, PKI based MFA, or Windows Hello etc.

- Conditional access
  - Setup Identity Provider (IdP)
  - Define conditional access policies
  - Configure AGO (SAML Logins)

- Categorization sensitive datasets

Zero Trust Architecture

Guidance - Phishing Resistant MFA

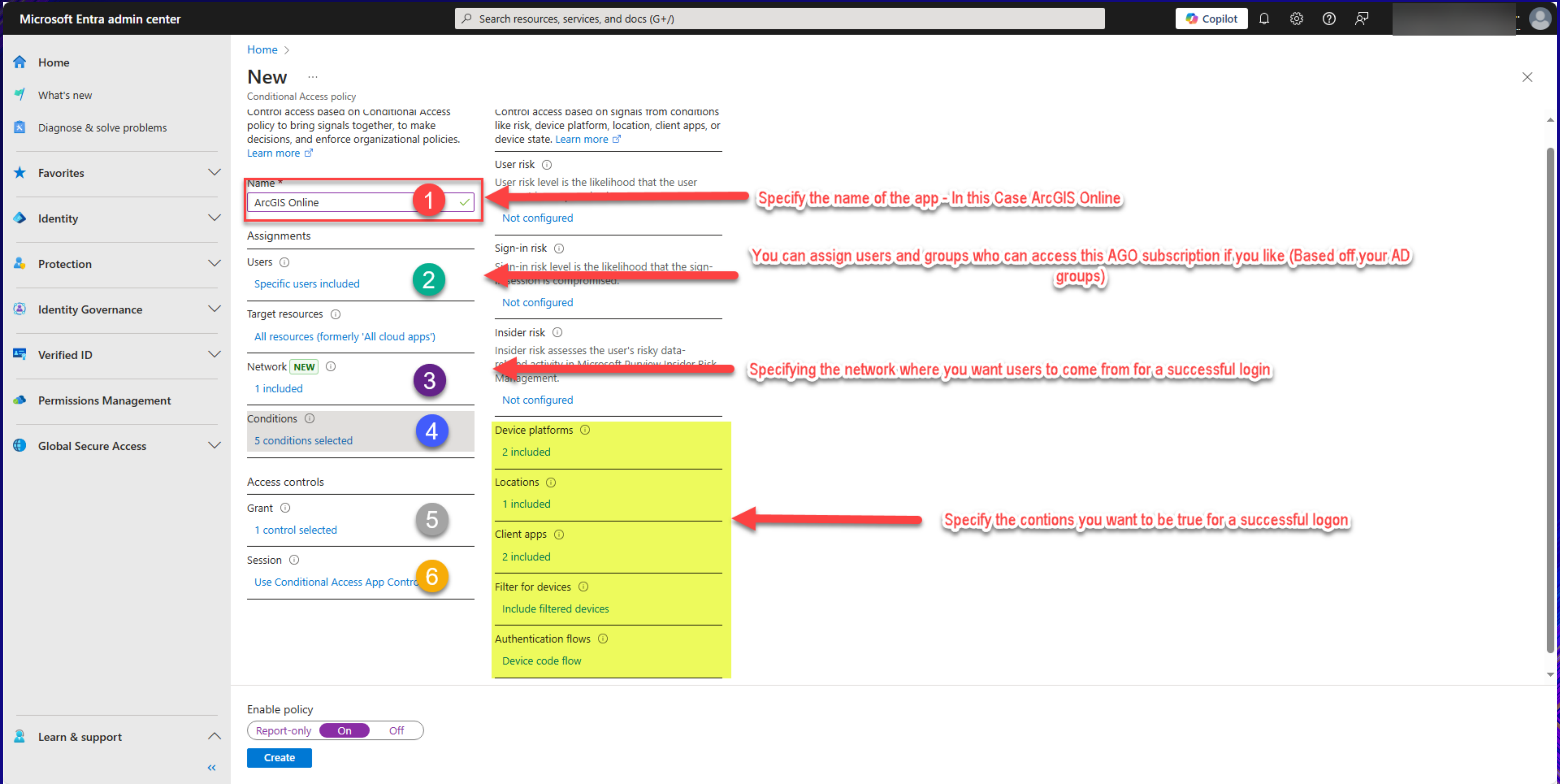
- Passwords are inadequate to secure user accounts
- Standard Multi Factor Authentication (MFA) is much better
  - However, when MFA relies on a human entering a code, they can be phished

- Therefore, ensure you are utilizing phishing resistant MFA options:

1. FIDO / Web Authn Authentication (requires authenticators)
   - Separate physical tokens (called “roaming” authenticators) connected to a device via USB or near-field comms (NFC), or
   - Embedded into laptops or mobile devices as “platform” authenticators – e.g. Windows Hello
2. PKI-based MFA
   - Less widely available / frequently supported with smart cards

Zero Trust Architecture

Guidance - Conditional Access with Entra ID



New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name * ArcGIS Online

Assignments

Users: Specific users included

Target resources: All resources (formerly 'All cloud apps')

Network NEW: 1 included

Conditions: 5 conditions selected

Access controls

Grant: 1 control selected

Session: Use Conditional Access App Contr

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk: User risk level is the likelihood that the user ... Not configured

Sign-in risk: Sign-in risk level is the likelihood that the sign-in session is compromised. Not configured

Insider risk: Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management. Not configured

Device platforms: 2 included

Locations: 1 included

Client apps: 2 included

Filter for devices: Include filtered devices

Authentication flows: Device code flow

Enable policy: Report-only [✓ On] Off

Create

Specify the name of the app - In this Case ArcGIS Online

You can assign users and groups who can access this AGO subscription if you like (Based off your AD groups)

Specifying the network where you want users to come from for a successful login

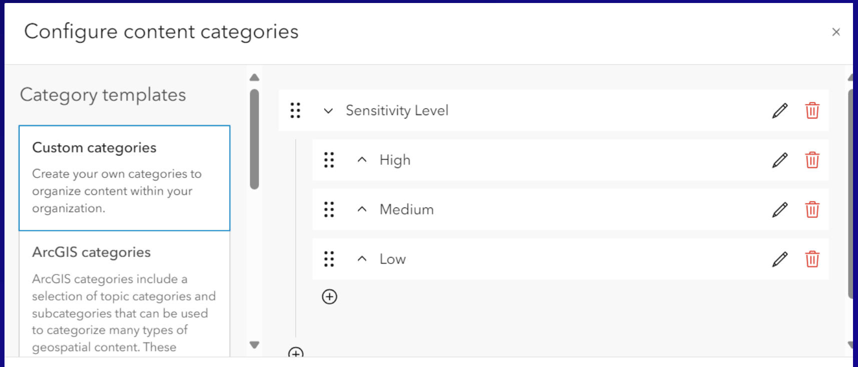
Specify the contions you want to be true for a successful logon

Zero Trust Architecture

Guidance - Categorize Sensitive Datasets

- To ensure your organization is on track for effective ZTA protections, you need to ensure your data are categorized NOW based on sensitivity level
  - Ensure your organization utilizes **categories** to identify data sensitivity level in a consistent manner

Setup Custom Category



Configure content categories

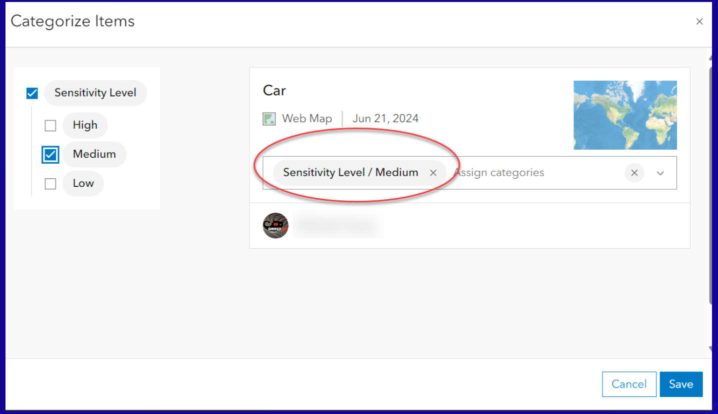
Category templates

Custom categories
Create your own categories to organize content within your organization.

ArcGIS categories
ArcGIS categories include a selection of topic categories and subcategories that can be used to categorize many types of geospatial content. These

- Sensitivity Level
  - High
  - Medium
  - Low

Select Category for Your Items



Categorize Items

☑ Sensitivity Level
- □ High
- ☑ Medium
- □ Low

Car

Web Map | Jun 21, 2024

Sensitivity Level / Medium × Assign categories

[redacted]

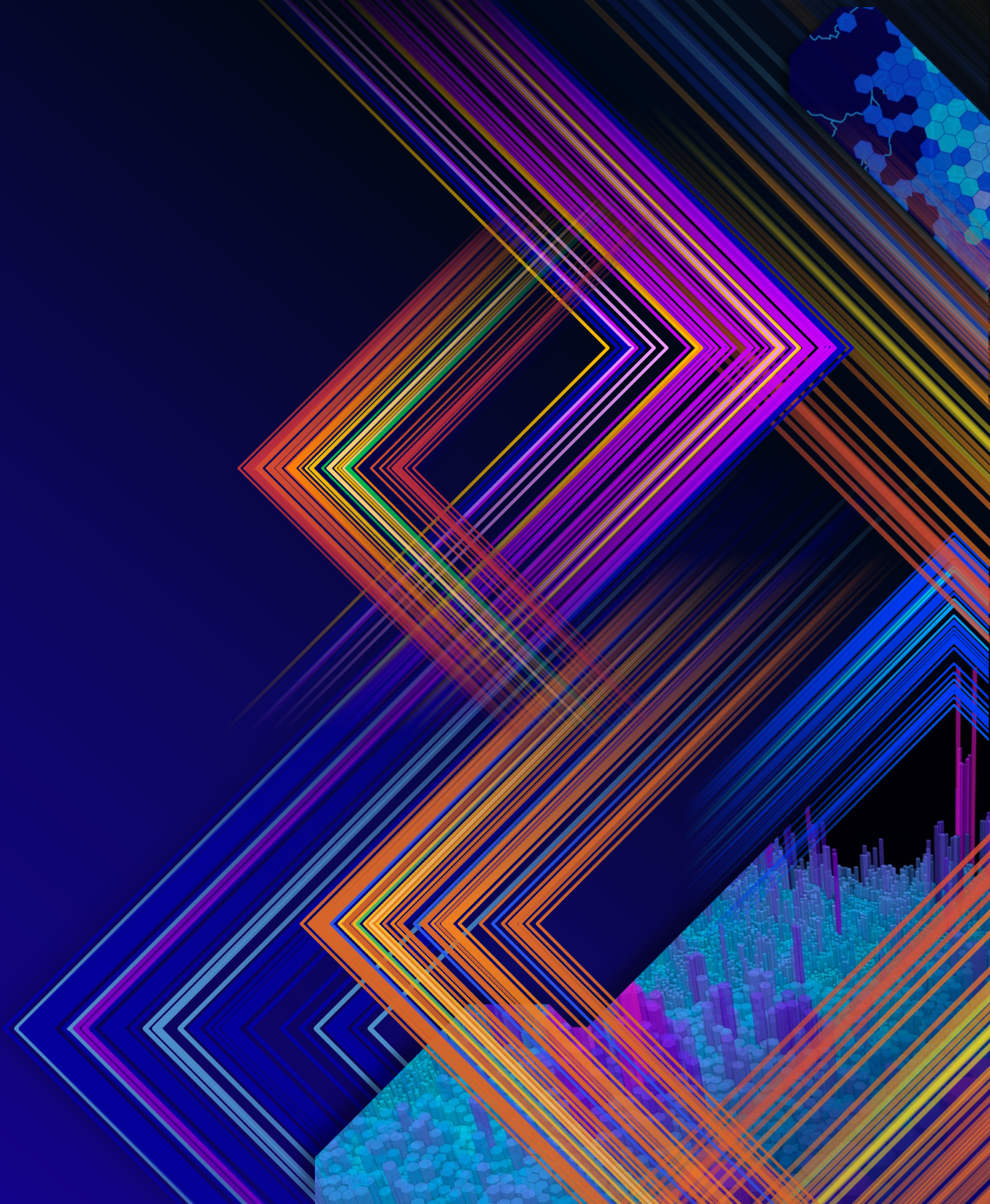
***Note**: Use ArcGIS Categories or Tags to identify sensitivity levels based on agency preference*

Summary

Summary

- FedRAMP Moderate
  - Opens new use case opportunities for agencies
- Esri compliance and certification commitments
  - Continue to expand including coverage of authorized services
- Security & privacy are shared responsibilities between Esri and agencies
  - Ensure alignment with Customer Responsibility Matrix
- Regularly check for best practice alignment
  - ArcGIS Security & Privacy Adviser tool
- Prepare for generative AI capabilities
  - Enforce generative AI standards and ensure alignment via Esri’s transparency cards
- Zero Trust Architecture is a journey
  - Ensure foundations now in place

Q & A



https://trust.arcgis.com/en/trusted-ai esri® | THE SCIENCE OF WHERE®