An Esri
Software Security & Privacy
Technical paper

August 2021

ArcGIS Secure Mobile Implementation Patterns

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

esri | THE SCIENCE OF WHERE™

Contents

1 Introduction

In recent years, enterprise geographic information system (GIS) deployments have increasingly moved from traditional office-based workflows to leveraging GIS apps in the field with mobile technology. This makes security considerations more complex and challenging for information technology (IT) architects and security specialists to deploy an effective enterprise GIS security strategy. However, industry-standard security principles and controls can be applied at all levels of ArcGIS architecture to ease this effort.

This document contains relevant information that helps guide IT managers and GIS administrators in deploying an enterprise GIS with a mobile field component. This paper discusses several different deployment scenarios along with some security considerations. The objective is to provide users with background, tips, and guidance as they implement a secure enterprise GIS solution. This technicalpaper is a collection of strategies and deployment considerations; it is not a detailed step-by-step implementation guide. Background knowledge of ArcGIS, IT, and security concepts is not a requirement, but is strongly recommended. Be advised that enterprise GIS solutions will vary from organization to organization, and security architects should use the concepts discussed in this document for planning secure solutions that meet the needs of their specific enterprise GIS implementation.

2 Background – The Esri Geospatial Cloud

The concept of a geospatial cloud combines cloud platform technology with GIS to enable businesses and organizations to analyze massive amounts of information. The resultant location intelligence often reveals deeper insights and innovative ways to increase efficiency. A geospatial cloud also allows location intelligence data to be easily combined with artificial intelligence and predictive analytics. The Esri Geospatial Cloud is the ArcGIS technology platform delivered at scale and can be leveraged by organizations of every size from local municipalities to federal agencies and global companies.

One of the key ideas of the Esri Geospatial Cloud is the Web GIS pattern: that all members of an organization can easily access and use geographic information within a collaborative environment. GIS analysts still provide technical expertise in the traditional sense, but other staff with little or no GIS knowledge can also leverage and contribute to their organization's GIS platform. Web GIS leverages existing GIS investments and makes them discoverable and more accessible. It provides a platform for integrating GIS with other business systems and promotes cross-organizational collaboration. Consequently, Web GIS extends the reach of GIS to everyone in an organization, enabling better decision-making.

From a technology perspective, the Web GIS pattern can be deployed in four ways (see Figure 1):

- **ArcGIS Online**: Multi-tenant, software-as-a-service (SaaS)
- **Managed Services:** Single-tenant, ArcGIS Enterprise SaaS or Platform-as-a-Service (PaaS)
- **Cloud Environment:** Ready-to-deploy ArcGIS Enterprise images for numerous cloud providers
- **On-Premises**: ArcGIS Enterprise software installed in an organization’s infrastructure

Figure 1: Web GIS Deployment Patterns

Each of the four options support varying levels of risk and offer different security options, which are discussed in more detail in section 6, and more detailed compliance information is available within the ArcGIS Trust Center. Although four separate Web GIS deployment models have been defined, hybrid deployments[1] combining different models are also common. Selecting the appropriate Web GIS deployment model: ArcGIS Online, managed services, cloud environment, on-premises[2], or a hybrid, will depend on an organization's business workflows, security requirements, and the available technology/skill sets within the organization.

2.1 ArcGIS Online

ArcGIS Online is a web-based GIS, hosted by Esri and delivered as a SaaS solution, (see Figure 2). With ArcGIS Online, organizations can get up and running quickly, and securely[3] create, organize, and manage geographic information within one system. It connects users in the organization with up-to-date content including ready-to-use apps, maps, 3D scenes, and layers so they can build useful information products and accomplish their work more efficiently. It facilitates collaboration and sharing of information with internal stakeholders, customers, contractors, and the public by providing access to maps, apps, and data from any device, anywhere, anytime. ArcGIS Online is built on open, scalable technology that automatically adjusts to meet peak demand periods. ArcGIS Online is Federal Risk and Authorization Management Program (FedRAMP)[4] Tailored Low SaaS authorized by the United States government for sharing information with the public. Many organizations with stringent security demands utilize ArcGIS Online as part of a hybrid deployment described in sections 2.3 and 6.7. Organizations around the world utilize ArcGIS Online as the FedRAMP security standards map to ISO 27001 Security Controls[5]. Though ArcGIS Online's cloud infrastructure is located within the United States, ArcGIS Online is General Data Protection Regulation (GDPR)[6] aligned with a Data Processing Addendum (DPA) available for customers to sign. For more information on compliance, see section 5.

[1] "Hybrid" implies using both ArcGIS Online and ArcGIS Enterprise together – see sections 2.3 and 6.7 for details.
[2] This deployment model is labeled "DISA STIG" – this refers to the "Defense Intelligence Systems Agency (DISA) - Security Technical Implementation Guide (STIG)" and only applies to the ArcGIS Server component of ArcGIS Enterprise, see section 2.2.
[3] See the ArcGIS Trust Center website and Cloud Security Alliance answers for ArcGIS Online for more details.
[4] This is a US federal program for security validation and authorizations – see FedRAMP About Us.
[5] The FedRAMP Tailored Low mapped to ISO 27001 Security Controls is available on Trust.ArcGIS.com.
[6] Learn more about EU GDPR on their site.

Figure 2: ArcGIS Online Conceptual Diagram (this will be used in later figures)

This option is the easiest in terms of implementation and security consideration perspective because the solution is hosted and maintained by Esri. An organization does not need to worry about infrastructure logistics and simply uses ArcGIS Online as a software service. GIS data and content (e.g., maps and apps) are hosted in Esri's cloud infrastructure. From a mobile deployment perspective, this is the easiest deployment option, because mobile devices do not need to connect to an organization's corporate data behind a firewall. This is a good solution for field operation workflows, such as capturing the location and status of assets, marking observations, and sharing information with the public. This may not be a good solution for multi-user feature update workflows, such as asset inspections, where conflicts may arise from multiple editors updating the same feature, or updates need to be merged with an existing production database. Customers risk averse to storing data in cloud-based services frequently supplement ArcGIS Online with one of the ArcGIS Enterprise deployment models addressed in this paper.

2.2 ArcGIS Enterprise

ArcGIS Enterprise is the software offering from Esri that enables an organization to use the Web GIS pattern as managed services, cloud environment, and on-premises solutions. It offers a flexible deployment model, allowing use that is completely on-premises, connected or disconnected from the Internet, on physical hardware or in virtualized environments, in the cloud on Amazon Web Services, Microsoft Azure, or any cloud platform that provides virtual machines that meet the system requirements and specifications, or as an Esri managed service (see sections 6.2 and 6.3).

ArcGIS Enterprise consists of four components (see Figure 3):

- **ArcGIS Web Adaptor**: Installs in a third-party web server, operates as a reverse proxy
- **Portal for ArcGIS**: Website serving as a central destination and focal point in the Web GIS
- **ArcGIS Server**: Spatial server that enables GIS data and content to be shared as web services
- **ArcGIS Data Store**[7]: Back-end repository to store spatial content

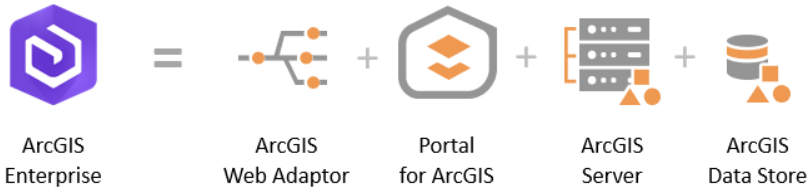

Figure 3: Components of ArcGIS Enterprise

[7] The ArcGIS Data Store can be deployed in 3 different ways: relational, tile cache, and spatiotemporal. In this document, we refer to the relational ArcGIS Data Store (see section 6 for further details). To learn more, see What is ArcGIS Data Store?

These four components can be deployed in diverse combinations and patterns to support many different business workflows. In terms of security, both the Portal for ArcGIS and ArcGIS Server components can support separate security models or share the same security model. A comprehensive discussion on the different security models that these products support is beyond the scope of this document.[8] Note: at the ArcGIS Enterprise 10.5 release, the concept of *ArcGIS Server licensing roles* was introduced – these "licensing roles" provide additional capabilities and may have some deployment implications beyond the four components.[9]

For the purposes of this paper, the *base deployment*[10] of ArcGIS Enterprise is referenced. An ArcGIS Enterprise base deployment implies that all 4 components are deployed together to enable the Web GIS pattern and leverage the full capabilities of ArcGIS, see Figure 4.

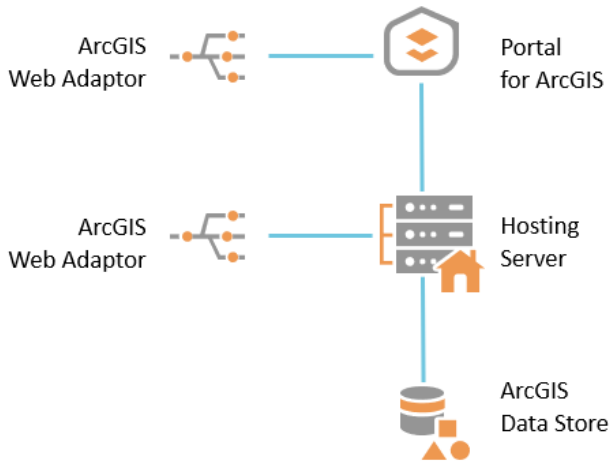

Figure 4: ArcGIS Enterprise Base Deployment

In a base deployment, the ArcGIS Data Store is registered with ArcGIS Server. ArcGIS Server is federated[11] with Portal for ArcGIS and becomes its hosting server[12] - a dedicated GIS server to support Portal capabilities such as the Map Viewer analysis tools. Lastly, the ArcGIS Web Adaptor is used by Portal for ArcGIS and ArcGIS Server, however customers can substitute their own load balancers in place of utilizing the ArcGIS Web Adaptor. All four components can be installed on the same machine or in a multi-machine deployment; the latter option is recommended for production deployments.

2.3 Hybrid Deployments

Some organizations choose a combination of deployment models, using a hybrid approach because of their business requirements. Many different deployment combinations are possible, and this section presents three examples in brief, see Figure 5.

[8] For more product security details see About configuring portal authentication and Control Access in ArcGIS Server.
[9] See ArcGIS Server licensing roles to learn more. Note the term "ArcGIS Server licensing role" is a separate and different concept than "Portal member roles" which are discussed later in section 4.2.2.
[10] To learn more, see Base ArcGIS Enterprise deployment.
[11] Where ArcGIS Server has been configured to use Portal for ArcGIS' security model, see Federate an ArcGIS Server site with your portal.
[12] To learn more, see Configure a hosting server.

- **Scenario A:** ArcGIS Online is used as a front-end website to access GIS assets, while ArcGIS Server is used to host web services. GIS data can be shared publicly, but are stored within the organization's infrastructure.
- **Scenario B:** Both ArcGIS Online and ArcGIS Enterprise are used, the former for public[13] content, and the latter for sharing content within the organization. Staff can create their own GIS content within Portal for ArcGIS. All GIS data are stored within the organization's infrastructure.
- **Scenario C:** Both ArcGIS Online and ArcGIS Enterprise are used, and distributed collaboration[14] is leveraged to integrate GIS data across a network of participants, including those with membership in the ArcGIS Online organization, ArcGIS Enterprise, or both.

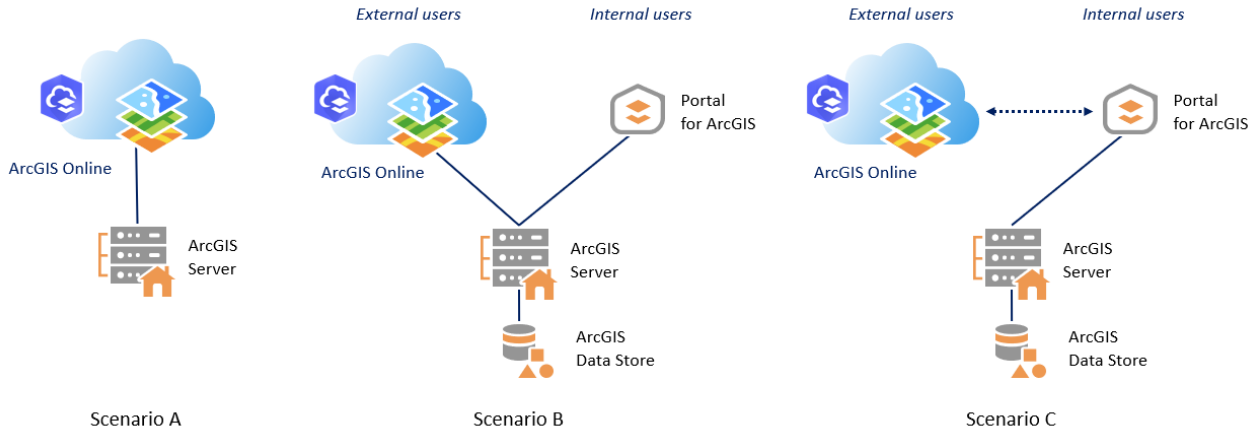

Figure 5: Three Example Hybrid Deployments of ArcGIS Online with ArcGIS Enterprise

There are many other possible hybrid deployment patterns[15] and they will vary based on different business workflow requirements. Section 6.7 discusses the security considerations for hybrid deployments.

2.4 ArcGIS Mobile Apps

Smart phones and tablets are pervasive and many enterprise GIS deployments include a mobile component. ArcGIS Mobile apps support all of the Web GIS deployment models: SaaS, managed services, cloud environments, on-premises, or a hybrid variation.

ArcGIS Mobile Apps can be grouped into two categories:

- **Field operations mobile apps**: Support field operations
- **Solution mobile apps:** Support specialized workflows

GIS data and maps can easily be taken into the field to support mobile field workers. Field personnel can work with the same authoritative datasets on their mobile devices, helping collect new data (or edit attributes of existing data) that can be easily shared with the office and monitored in real-time by dispatchers. Field operations tasks include: planning, coordination, navigation, data capture, and monitoring personnel and assets (see Figure 6).

[13] In this instance, "public" implies end users to are not part of the organization – typically external to the organization's IT network.

[14] To learn more about distributed collaboration, see the ArcGIS Online and ArcGIS Enterprise discussions on this topic.

[15] Different Web GIS hybrid deployments are presented in Web GIS Patterns and Practices.

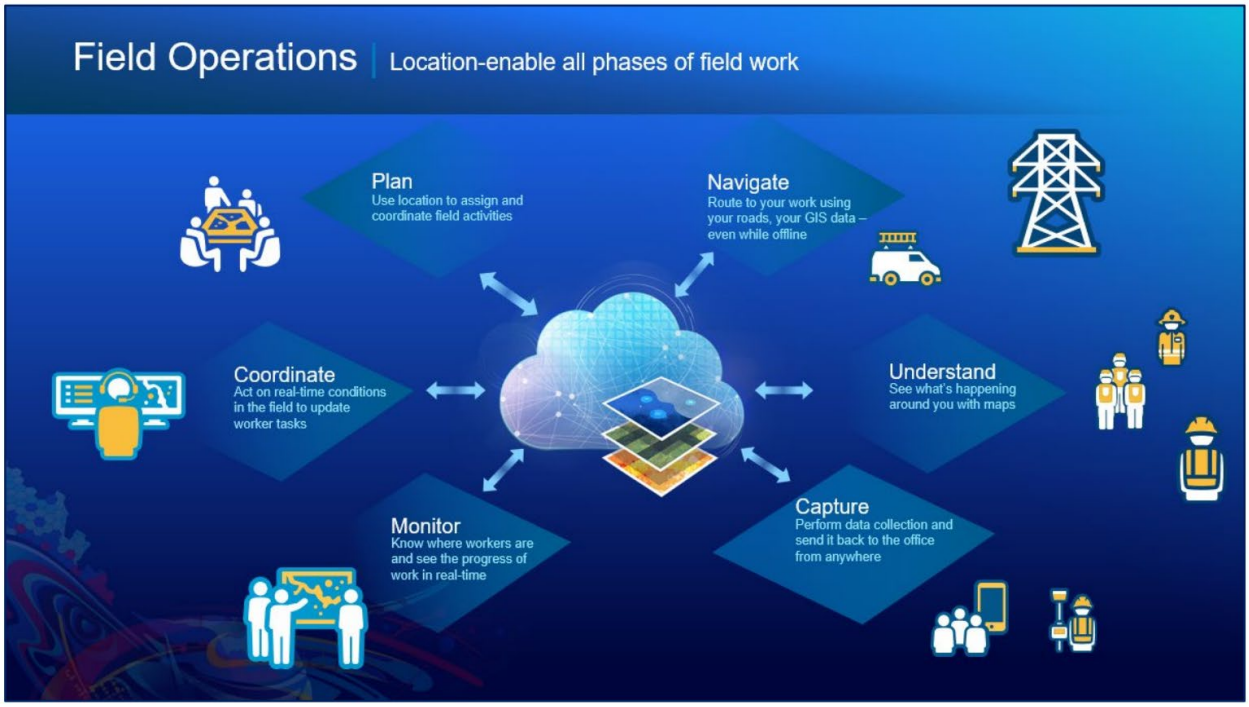

Figure 6: Field Operations in ArcGIS

The ArcGIS field operations mobile apps are available for iOS and Android devices, and some also support the Windows, macOS and Linux platforms. All ArcGIS Mobile apps sign into and work with ArcGIS Online and ArcGIS Enterprise[16], see Figure 7. They support connected and disconnected environments and they can use used separately or collectively as part of a larger mobile workflow, depending on the organization's business requirements[17]. Enabling a mobile GIS component as part of an enterprise GIS deployment provides many benefits including:

- Replacing redundant inefficient field processes
- Reducing costs and overhead
- Improving collection speed, accuracy, and currency of data
- Modernizing workflows and replacing paper-based workflows
- Helping management make timely and informed decisions

ArcGIS field operations mobile apps (see Figure 7a) consist of three main apps:

- **ArcGIS Field Maps:** Explore maps, collect and update GIS data in the field, and location tracking
- **ArcGIS Survey123**: Supports form-centric data collection and editing
- **ArcGIS QuickCapture:** Enables single-button, rapid data collection

Figure 7a: ArcGIS Field Operations Mobile Apps

[16] Apps sign into the Portal for ArcGIS component of ArcGIS Enterprise.
[17] To learn more about ArcGIS mobile Field Operations, see ArcGIS Apps for the Field: An Introduction.

ArcGIS field operations includes several apps which will be deprecated (see Figure 7b) longer term[18].

- **ArcGIS Collector**[19]: Provides map-centric data collection and editing
- **ArcGIS Explorer**[20]: Supports viewing and markup of GIS maps
- **ArcGIS Navigator**: Enables routing with turn by turn directions
- **ArcGIS Tracker**: Enables monitoring personnel and their movement in the field
- **ArcGIS Workforce**[21]: Enables planning and coordinating work assignments

Figure 7b: ArcGIS Field Operations Mobile Apps to Be Deprecated

ArcGIS solution mobile apps are designed to support different business use cases from field operations, see Figure 8. These apps range from 3D data visualization, to offering a building occupant mobile experience, to supporting situational awareness scenarios. Some of these are not stand-alone apps but offered a part of a Geo-Enabled system from Esri. Theare mentioned in this document for completeness. ArcGIS solution mobile apps include:

- **ArcGIS AppStudio Player**: Displays custom apps built with *ArcGIS AppStudio*[22]
- **ArcGIS Business Analyst Mobile**[23]: Enables demographic and socio-economic data in the field
- **ArcGIS Companion:** Enables the management of your ArcGIS organization from a mobile device
- **ArcGIS Earth**: Displays and provides interaction with 2D and 3D data
- **ArcGIS Indoors**[24]: Displays indoor maps and enables interactions such as searching and getting landmark based directions
- **ArcGIS Mission Responder:** Provides mobile workers with situational awareness on a map with messaging and location tracking among team members.

Figure 8: ArcGIS Solution Mobile Apps

Some apps offer support for more security options (see section 4.1) than others. Please check the online help documentation for each app for details.[25] While the ArcGIS field apps offered as part of ArcGIS

[18] Initial deprecation announcement of December 2021. Please refer to the product life cycle page of each app for status.
[19] Note: There are 2 currently offerings of this app: i) *Collector Classic* and a revised release ii) *Collector for ArcGIS*.
[20] Explorer for ArcGIS can open and view publicaly shared maps without requiring a login for access.
[21] Offline support is planned and should be available in 2020.
[22] Enables you to create native mobile apps without programming, to learn more see AppStudio for ArcGIS product page.
[23] Deploying this app with ArcGIS Enterprise has supplementary requirements, see An overview of Business Analyst Enterprise.
[24] ArcGIS Indoors currently only works with ArcGIS Enterprise, the app is part of a larger ArcGIS Indoors solution.
[25] Help documentation for the Apps: ArcGIS Help Documentation.

meet the needs of most customers, Esri also offers ArcGIS Runtime Software Developer Kits (SDKs) to facilitate custom application development.[26] When mobile apps are built with ArcGIS Runtime SDKs, the concepts regarding enterprise mobile apps discussed in this paper will apply to these custom solutions.

3 Enterprise Mobile App Management

Like other apps in public app stores, the ArcGIS mobile apps are designed for ease of use, allowing general users to be up and running within minutes. Following the Web GIS pattern, the default configuration of each ArcGIS mobile app supports the broad dissemination of GIS data and content across an organization and frequently with the public. If an organization wants to ensure that tighter enterprise security measures are in place for its mobile solutions, it can apply more stringent controls in its Web GIS architecture, and include more advanced security components such as enterprise mobility management (EMM).

3.1 Connecting ArcGIS Mobile Apps to ArcGIS Web Services

Before discussing the details on how an EMM can help, it is useful to define that an enterprise GIS deployment with a mobile field component is one or more (or all) of the ArcGIS mobile apps connecting to either ArcGIS Online and/or ArcGIS Enterprise (see Figure 9). This is the Web GIS deployment pattern with the ArcGIS Platform, supporting GIS workflows in the field.

Figure 9: ArcGIS Mobile Apps Connecting to ArcGIS Online and/or ArcGIS Enterprise

Some common security considerations to support this deployment include:

- Will the Web GIS pattern be enabled with ArcGIS Online, ArcGIS Enterprise, or a hybrid deployment? Refer to section 2.3.
- Where will the GIS data and content reside? Can they be stored in the Esri cloud infrastructure, or must they only reside within the organization's infrastructure? Can they be a combination of the two? The nature of the data collected, and the intent of the services used to distribute this data becomes a critical question.
- How will mobile app end users access the organization's internal network/infrastructure? What is the organization's current IT security model/infrastructure? Are there corporate security policies and/or procedures that must be adhered to?

[26] To learn more, see the ArcGIS Developers site.

- When accessing the organization's internal network, is a single sign-on (SSO)[27] user experience a requirement?
- What hardware resources (e.g., machines and network infrastructure) are available, in terms of both mobile devices and infrastructure technology?
- Does the organization support a bring your own device (BYOD) policy? What are the security requirements and policies with respect to these devices?
- What IT personnel resources are available to support this deployment (in terms of both setup and maintenance)?
- What is the risk tolerance for the organization in terms of the proposed services to be offered?
- What are the deployment costs?

The list of questions above is not comprehensive and many of the questions are high level, but they should be taken into consideration when planning and designing the security model for an enterprise GIS deployment with a mobile field component. How these questions are answered by senior management and stakeholders will likely impact which mobile deployment pattern is selected (see section 6).

There are many potential security risks and mitigations with respect to using mobile technology as part of an organization's business workflows. The open web application security project (OWASP) foundation is a non-profit organization that is "*an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted*". [28] In 2016, OWASP finalized their global study on mobile security and compiled a Top 10 list of Mobile Risks. A discussion on these items is beyond the scope of this document, but they are noted as a reference source when planning mobile security strategies. One approach to address these risks is to use an EMM solution in addition to ArcGIS security settings (discussed in section 4).

3.2 Enterprise Mobility Management (EMM)

When mobile devices are part of an enterprise deployment, the challenge is to ensure that the data and apps are secure with minimal (or no) impact to the user experience. EMM is a solution strategy for managing mobile devices, apps, and content in the organization. The main objective is to determine how mobile devices are integrated with business processes, support field workers, and ensure that IT security and compliance requirements are met.[29]

EMM can be separated into three different conceptual components:

1. Mobile Device Management
2. Mobile Application Management
3. Mobile Content Management

There are many different EMM technology vendors, some have functionality that covers all three components, while others specialize in one area. Selecting the appropriate one will depend on the specific security requirements, policies, and business workflows of your organization. Using EMM technology can provide additional security options at the mobile device level and helps the enterprise GIS with mobile field component deployment be more secure.

[27] SSO means a user would only login once to access resources, see Enterprise Single Sign-On.
[28] To learn more, see About The Open Web Application Security Project.
[29] To learn more, see How to choose the right enterprise mobility management tool.

Some key recommendations when deploying an EMM as part of your enterprise GIS mobile deployment:

- Develop and deploy a realistic device security policy
  - Support for different mobile device operating system (OS) platforms
  - Consider BYOD program implications
- Provide a backup and recovery service for devices
- Require anti-malware software on devices
- Perform regular security audits against the EMM solution
- Always remove all residual application data from devices when not being used
- Implement a staff education program to teach them about mobile device threats

As in section 3.1, the list provided is meant to be used as a starting point for security discussions and policy planning in your organization.

3.2.1 Mobile Device Management (MDM)

Mobile device management (MDM) is the administration of mobile devices within an organization. This is typically applied with software that enables the centralization and optimization of functionality and security management for mobile devices. The software commonly includes a server component that sends out management commands to mobile devices that have a client component to receive and execute the management commands. Another key aspect typical of MDM software is the concept of "containerization", which means corporate data is separated from a user's personal data on the mobile device. MDM software can be used by organizations to deploy apps on their devices by connecting and working with public app stores.

An MDM solution typically includes the following capabilities:

- Device monitoring, reboot, and encryption
- Enforcement of password policies, password reset
- Predefined WiFi settings/virtual private network (VPN)[30] configurations
- Remote lock and wipe capabilities
- Backup settings enforcement
- Jailbreak detection

An administrator can also use MDM software to define and deploy configuration templates for mobile devices. The templates can be used to customize the device's security settings such as: password requirements; personal identification number (PIN) length; app denylist/allowlist; email configurations; device encryption; location tracking; WiFi configurations; and app, services, and device feature restrictions. These options will vary between different MDM software vendors. Please refer to the ArcGIS Field Apps and Mobile Device Management Support paper for additional details.

3.2.2 Mobile Application Management (MAM)

Mobile application management (MAM) provides an additional level of security for mobile devices; it is the use of software and services that provision and control access of individual apps on devices. This enables administrators to have more granular control at the application level to manage and secure app data. An MDM software solution can include MAM capabilities as part of its functionality.

[30] To learn more, see VPNs for Beginners.

An MAM solution typically includes the following capabilities:

- Application-level authorization and provisioning
- App updating
- User authentication, access control
- App version and configuration management
- Push services
- Event management

Be advised, Esri has observed that MDM-centric MAM offerings that require rebuilding the app by embedding the MDM SDK typically do not work well. Esri does have some customers utilizing MAM offerings that do not require incorporating an MDM SDK. Esri will provide support for released, store versions, listed within the product's life cycle support only. In certain cases, Esri Professional Services can be engaged to help support customer-specific variances if desired."[31]

3.2.3 Mobile Content Management (MCM)

This third component, mobile content management (MCM), is a type of content management system that stores and delivers content and services to mobile devices.

An MCM solution can have the following capabilities:

- Multi-channel content delivery
- Content access control
- Specialized templating system
- Location-based content delivery

This aspect of EMM is not leveraged by the ArcGIS mobile apps.

3.3 EMM and the ArcGIS

It is important to coordinate security implementations of the enterprise GIS with the organization's IT department, as an EMM strategy works with more than just the organization's GIS technology group. The MDM aspect of the EMM solution is typically the main component that the ArcGIS mobile apps interact with.

An organization's MDM software can connect directly to public app stores like the Apple App Store and Google Play. The ArcGIS mobile apps in the stores can be registered or uploaded (depending on the MDM vendor) with the MDM. This enables the MDM software to access the apps as resources and can manage and deploy them to the organization's mobile workforce. In the MDM software, each app can be configured to meet the specific security requirements of the organization in which they are used.

When deploying the ArcGIS mobile apps with MDM software, it is recommended that the guidelines found within the AppConfig Community be followed. This community works with several EMM vendors and is focused on providing tools and best practices for native capabilities in mobile operating systems, see Figure 10.

[31] While binaries are available for Android OS apps on the Esri website, customers who want to deploy Apple iOS app binaries will need to agree to supplemental terms in alignment with the Apple Developer terms of use; please consult an Esri account manager or Distributor.

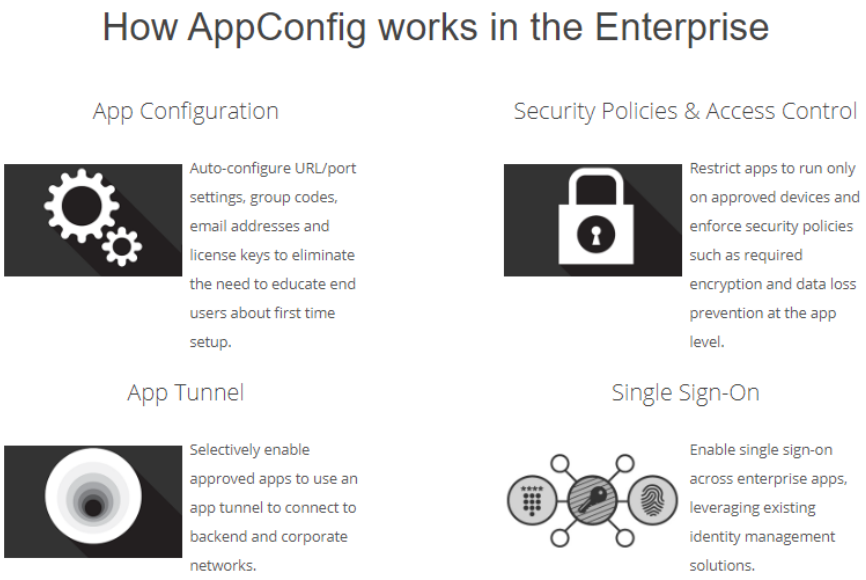

Figure 10: AppConfig Community –key concepts[32]

The objective of the guidelines are to help provide a more consistent, open and simple way to configure and secure mobile apps that eases and advances mobile adoption in business. The AppConfig Community has defined lists of recommended configuration parameters for iOS and Android devices:

- iOS Capabilities Summary
- Android Capabilities Summary

These parameters are meant to guide app developers and help them develop apps that work well in MDM environments.

The ArcGIS mobile apps development teams strive to follow the recommendations and patterns provided by the AppConfig Community. In general, ArcGIS mobile apps[33] support the following capabilities:

- **App Configuration:** Setting app properties such as URL, port, email address, etc
- **App Tunnel:** Leverage "per app VPN" capability (secure connection)
- **Security Policies & Access Control:** Restrict apps to approved devices and enforce policies
- **Single-Sign-On (SSO):** Provides a user-friendly corporate network sign-on experence

To elaborate on "per app VPN", this implies that the device will connect to an organization's VPN to access internal resources when the app opens. This reduces the inbound connection to the organization's internal network to a single app.

In terms of App Configuration settings, most of the ArcGIS mobile apps support the implementation of the `portalURL` key. For ArcGIS mobile apps that support this functionality, when the app is opened, it will bypass the portal URL sign-in screen and display the portal member login screen (see Figure 11).[34]

[32] Source: AppConfig Community.
[33] Exception: ArcGIS Business Analyst does not currently support the App Tunnel property.
[34] This workflow is discussed in section 4.1.

This means that the ArcGIS mobile apps can be deployed from an MDM with the portal URL address already configured; when a mobile user opens the app, all they need to input is their login credentials.[35] Responding to user requirements, Navigator for ArcGIS on iOS also supports `enableLocalAuthentication`, a setting that enables local authentication within Navigator that can tie into a device's FaceID, TouchID, and passcode security settings.[36]

The ArcGIS Mobile App Compliance and Security Capability Settings table below summarizes the FedRAMP compliance status of ArcGIS mobile application API connections to ArcGIS Online as well as MDM configuration settings. For additional details concerning the MDM settings available for each mobile app, please refer to the help documentation for each app and the ArcGIS MDM Support document referenced earlier.

ArcGIS Mobile App Compliance and MDM Settings

App	FedRAMP	portalURL	portalName	portalAuth	portalResource	requireSignIn	LocalAuth	Switch Accounts	PortalManagement	Ext Browser Auth	Webview Auth	Anonymous Access	LKL Upload Freq	Upload Track Freq	Diagnostics	Data recovery	Biometrics	Custom apps	Branding
ArcGIS Field Maps	*	■								■	■	■	■						
ArcGIS Survey123	■	■	■	■	■	■			■	■					■	■			
ArcGIS QuickCapture	■	■																	
ArcGIS Collector		■																	
ArcGIS Explorer		■								■	■								
ArcGIS Navigator		■					■										■		
ArcGIS Tracker		■										■	■						
ArcGIS Workforce		■																	
ArcGIS AppStudio Player		■	■							■								■	
ArcGIS Business Analyst Mobile		■																	
ArcGIS Companion		■						■											
ArcGIS Earth		P																	
ArcGIS Indoors	P	■																	■
ArcGIS Mission Responder		P																	

* = Limited to capabilities not utilizing Location Tracking
P = Planned

ArcGIS mobile apps have been successfully deployed with an EMM strategy by many customers. Examples of MDM vendor solutions used include: *AirWatch, F5 Big IP, InTune, MaaS360, Meraki, MobileIron,* and *XenMobile*. The ArcGIS mobile apps are frequently updated and are continually working to support additional capabilities in future releases.

Deploying an EMM solution as part of your enterprise GIS with a mobile field component is not required, and if not, security efforts should focus on topics discussed in the next section. Independent of having an EMM solution, customers should still implement the Enterprise Security Mechanisms in section 4.

[35] Implementation details are covered in the blog: MDM and Explorer for ArcGIS.

[36] Learn more in the blog: Navigator supports enhanced security – and it's configurable with your MDM!

4 Enterprise Security Mechanisms

In this section, common security mechanisms utilized across an enterprise are discussed in the context of the ArcGIS. Esri recognizes the challenges encountered when deploying an enterprise GIS with a mobile field component and is committed to help customers determine how to best apply these security practices to their GIS implementations.

4.1 Authentication

When using the ArcGIS mobile apps, a user specifies if they are connecting to ArcGIS Online or ArcGIS Enterprise.[37] In the latter case, they would input a portal URL address.[38] Next, the user provides login credentials to access the portal and its content.[39] An example of the login workflow is shown with Collector for ArcGIS in Figure 11.

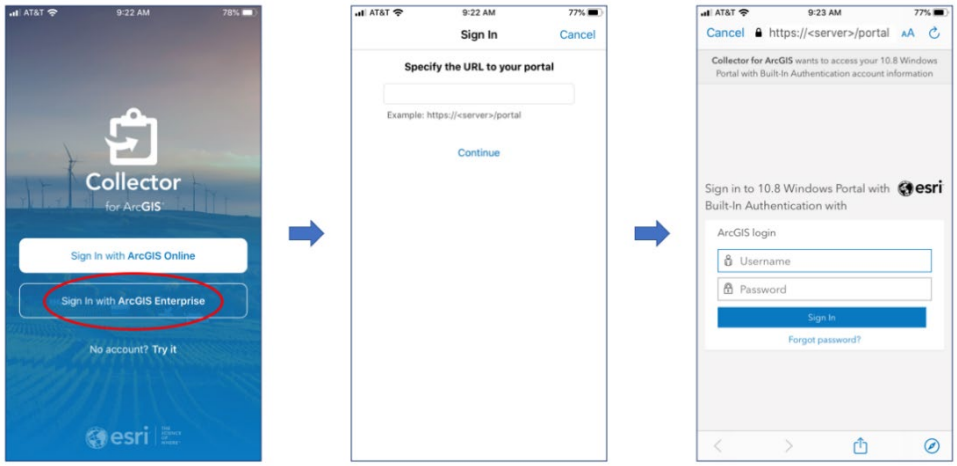

Figure 11: ArcGIS Collector – ArcGIS Enterprise login dialogs

Authentication is the process of verifying the identity of a user by checking their credentials. In the context of ArcGIS mobile apps, the user is authenticated by a customer's identity provider, ArcGIS Online, and/or ArcGIS Enterprise (see Figure 9). After a user is authenticated, ArcGIS Online or ArcGIS Enterprise then performs an authorization check to determine which actions the user can perform (see section 4.2).

Based on successful authentication, the applications generate an authorization token for future transactions. All requests, including authentication requests, are done in Hypertext Transfer Protocol Security (HTTPS)[40] protocols. The enterprise GIS with mobile field app solution should be considered with several factors in mind:

- What types of mobile devices will access the GIS data and content?
- What authentication mechanisms do the mobile devices support?
- Does the enterprise system have authentication mechanisms already in place?
- Does the IT enterprise system have specific HTTPS authentication requirements?

[37] Note that a login to ArcGIS Online is a different account than a login to ArcGIS Enterprise; they are two separate and distinct accounts.

[38] To learn more, see Portal for ArcGIS URLs help topic.

[39] Exception: Explorer for ArcGIS can access publicly shared content without a login.

[40] To learn more, see What is HTTPS?.

- Does the organization have specific methods for providing enterprise network credentials (e.g., VPN[41], SAML[42] or mobile security gateway[43])?

When a mobile device attempts to access a secured GIS resource, it needs to provide credentials to ensure it has the appropriate permissions. The mobile device's credentials could be the same as the user's enterprise network login[44] info (i.e., SSO authentication), or additional credentials could be required to access the secured GIS resource. Typically, an organization's security level requirements will determine which option is used – this relates back to the previous list of questions.

Note: Unsecured GIS resources (i.e., content shared with the "public") are typically set to *Anonymous* access (as these do not require a login to access). Configuring a publicly accessible application to protect data collected from users can be challenging. A separate paper addresses this scenario for Survey123 called "Discovering and Limiting Access to Public Survey123 Results".

Caution: Using webhooks with ArcGIS applications can accelerate the process to integrate capabilities from third-party providers, however, they bring up significant security and privacy challenges that require extensive efforts to mitigate associated risks. We strongly recommend that customers validate any third parties utilized as part of a webhook workflow are approved by their organizations for handling sensitive information such as credentials or datasets before incorporating them. Additionally, we suggest reviewing and incorporating the recommendations from OWASP's lastest draft of the "Webhook Security Guidelines Cheat Sheet".

ArcGIS Online has three authentication options:

Security Option	*Comments*
Built-in security	This is the default built-in security model where user and role information is stored within ArcGIS Online. Mobile devices connect to ArcGIS Online and provide credentials.
Organization-specific logins with security assertion markup language (SAML) authentication or OpenID Connect	In this option, the ArcGIS Online organization is registered with a third-party identity provider (IDP) to verify credentials. Users requesting to login are directed to the IDP. They log in to the IDP, which verifies their credentials and provides an authentication token to allow them to login to ArcGIS Online.
Social Logins	Authentication via a social network like Google or Facebook.

ArcGIS Enterprise (via the Portal for ArcGIS component[45]) offers several authentication options:

Security Option	*Comments*
Web-tier authentication[46]	This uses integrated Windows authentication (IWA) or Lightweight Directory Access Protocol (LDAP)[47], which provides a SSO user experience in Windows-based environments. In this option, a login is requested when the user connects to the ArcGIS Web Adaptor, which is connected to the Windows Active Directory or LDAP

[41] See details in section 6.5.
[42] SAML – Security Assertion Markup Language; to learn more, see SAML v2.0 specification.
[43] See details in section 6.6.
[44] See Esri Software Security & Privacy (SSP) FAQ document Organization-Specific Logins FAQ.
[45] ArcGIS Server must be federated with Portal for ArcGIS to enable a hosting server deployment. See footnote 13 for details.
[46] ArcGIS Enterprise supports public key infrastructure (PKI) authentication, but only Collector for ArcGIS on iOS supports this option – see Configure Collector help topic.
[47] To learn more, see Integrated Windows Authentication and What is LDAP?.

	server for validation. When mobile devices access the internal enterprise network, they will automatically have access to the Portal for ArcGIS website.
Portal-tier authentication	Default built-in security model where user and role information is stored within Portal for ArcGIS. This approach uses tokens that enables a client to access a secure GIS resource. Mobile devices access the internal enterprise network, then when they attempt to connect to Portal for ArcGIS[48], they need to provide a valid portal named user account.
Organization-specific logins with SAML authentication or OpenID Connect	In this option, Portal for ArcGIS is registered with a third-party IDP to verify credentials. Users requesting a login are directed to the IDP. They log into the IDP which verifies their credentials and provides an authentication token to allow them to login to portal and access resources that have been provisioned to them.

User credential information is stored in an identity store[49]: a list of valid users who can access the enterprise network. A user's identity is typically comprised of unique information (e.g., name, email, password, etc.) and their membership in roles. Enterprise systems typically have two "categories" of identity stores:

- **Users**: End user of a client application accessing network and identified by a set of credentials.
- **Role:** Set of privileges; users in the same role have the same permissions assigned.

A user can only belong to one role, and a role typically contains multiple users. Users and roles could be stored in the same or separate identity stores. Two frequently used identity store options in enterprise systems are Active Directory for Windows domains and LDAP for Linux-based domains. Note that ArcGIS Enterprise on Kubernetes supports Portal-tier authentication and Organization-specific login methods listed in the table above. For more information refer to the ArcGIS Enterprise on Kubernetes FAQ.

4.2 Authorization

After a user has been authenticated, the authorization model will determine what resources the user can access within the ArcGIS, and what operations or actions they can perform. Users should be assigned privileges based on roles and should follow the *principle of least privilege*: they should only be able to access the information and resources necessary for their legitimate purposes. For both ArcGIS Online and ArcGIS Enterprise (Portal for ArcGIS component), the central destination homepage is often called the *portal*. Items in the portal such as web apps, web maps, web scenes, and web layers can be logically aggregated into *groups* for organizational purposes (see section 4.2.3). Groups[50] in the portal can be leveraged to help control user access to different types of GIS data and contents in the organization, see Figure 12.

[48] The logins are typically enterprise users (e.g., Windows Active Directory or LDAP) as the identity store. Built-in named users (who are not enterprise users) could also be used, but will not have a SSO user experience.
[49] This is also sometimes termed "identity provider".
[50] To learn more about Groups in a portal, see What is a group?

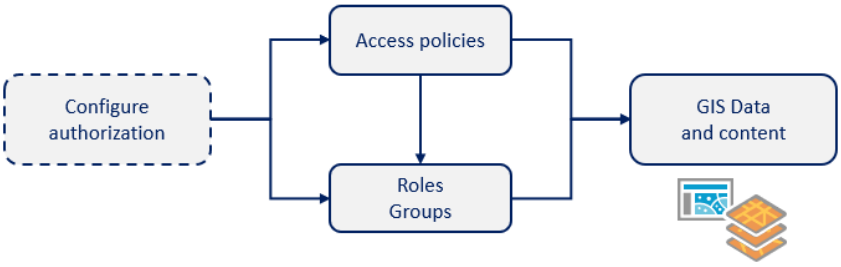

Figure 12: Configuring Authorization Settings

In this technical paper, a portal named user account in the portal will be called a "portal member", and they are assigned a *user type* and *role*. User types are assigned to portal members based on their work duties and portal roles define specific functionality.

4.2.1 Portal Membership and User Types (Licensing Levels)

In the December 2018 ArcGIS Online update and at the ArcGIS Enterprise 10.7 release, the concept of *user types* was introduced.[51] User types enable administrators to provide more granular control over the deployment of portal members and can help minimize the costs for user accounts. A user type is selected for a portal member based on an assessment of their role in an organization, work duties, and how they will use the portal (see Figure 13). A user type defines a portal member's capabilities in the portal and access to certain ArcGIS client apps. There are five core user types[52]:

- **Viewer** - Viewers can view items that are shared with them by other ArcGIS users. They can't create, edit, share, or perform analysis on items or data.
- **Editor** - Editors can view and edit data in ArcGIS maps and apps that are shared with them by other ArcGIS users. They can also be used with custom editing applications created by customers or by Esri business partners. Editors can't analyze, create, or share items or data.
- **Field Worker** - Field Workers can view and edit data that has been shared with them by other ArcGIS users. Ideal for portal members who primarily interact with ArcGIS content through ArcGIS field apps. They can't analyze, create, or share items or data.
- **Creator** - Creators have all the capabilities of the Viewer, Editor, and Field Worker user types, plus the ability to create content, administer the organization, and share content. This user type is designed for those who need to create web maps and apps, perform in-depth spatial analysis using the analysis tools in the portal, and work with data using ArcGIS field apps.
- **GIS Professional** - GIS Professionals have all the capabilities and app bundles of the Creator, plus access to ArcGIS Pro (Basic, Standard, or Advanced). This user type is designed for those who need the full suite of GIS apps to perform their work.

[51] To learn more about User Types, see 10.7 help topic User types, roles, and privileges.

[52] Additional user types exist for more specialized workflows and others may be introduced by Esri in the future.

Figure 13: Core ArcGIS User Types

For an enterprise GIS deployment with a mobile field component, the *Field Worker user type* is an important consideration and would be the most applicable to support field operation workflows (shown in Figure 6). This user type includes access to: Workforce for ArcGIS, Collector for ArcGIS, Survey123 for ArcGIS, and ArcGIS QuickCapture. This would be the user type typically assigned to personnel working in the field with the ArcGIS field apps. For example, field crew staff who perform data collection and asset management inspections.

Please review the help topic referenced in footnote 54 for a comprehensive description of the five core user types available in a portal. Ensuring portal members are assigned the appropriate user type before they interact with the portal is strongly recommended.

For pre-10.7 versions of ArcGIS Enterprise, portal membership is defined by two license levels[53]:

- **Level 1:** Members who only need privileges to view content, such as maps and apps, that have been shared with them through the organization, or to join groups within the organization.
- **Level 2:** Members who need to view, create, and share content and their own groups, and perform other tasks.

Most of the ArcGIS field apps involve data collection; therefore, field users should be assigned level 2 membership.

4.2.2 Portal Member Roles (Permission Levels)

A portal member's role defines the set of privileges assigned to the member. There are several default roles available in a portal:

- **Viewer**: View items such as maps, apps, scenes, and layers that have been shared with the public, the organization, or a group to which the member belongs. Join groups owned by the organization. Drag CSV, text, or GPX files into the Map Viewer to geocode addresses or place

[53] To learn more about portal levels, see 10.6 help topic Levels, roles, and privileges.

names. Get directions in Map Viewer and apps. Members assigned the Viewer role cannot create or share content or perform analysis. The Viewer role is compatible with all user types.

- **Data Editor:** Viewer privileges plus the ability to edit features shared by other portal users. The Data Editor role is compatible with all user types except Viewer.
- **User**: Data Editor privileges plus the ability to create groups and content; use the organization's maps, apps, layers, and tools, and join groups that allow members to update all items in the group. Members assigned the User role can also create maps and apps, edit features, add items to the portal, share content, and create groups. The User role is compatible with the Creator and GIS Professional user types.
- **Publisher**: User privileges plus the ability to publish hosted web layers, GIS Server layers, register data stores, publish from data store items, and perform feature and raster analysis. The Publisher role is compatible with the Creator and GIS Professional user types.
- ***Administrator***: Publisher privileges plus privileges to manage the organization and other portal users. An organization must have at least one administrator, though two is recommended. There is no limit to the number of members who can be assigned to the Administrator role within an organization. However, for security reasons, this role should only be assigned to those who require the additional privileges associated with it. The Administrator role is compatible with the Creator and GIS Professional user types.

This list of user roles are the default roles available in ArcGIS Online and ArcGIS Enterprise (Portal for ArcGIS component). [54] However, portal administrators can also create and define custom user roles[55] – which provides them with more granular control on permission settings for their users. Please review the help topic referenced in footnote 54 for a comprehensive description of the different user roles available in a portal.

4.2.3 Portal Groups

A portal group is a set of users that share access to the same collection of portal items. Groups can be used to help control access to items in the portal, because they help to organize portal content.[56] Groups and their contents are public by default and portal members are given access by the group owner. Groups can be configured to be seen in several ways:

- **Only group members** - Only members of the group can find and view the group. Portal members will need to be explicitly invited to join the group.
- **People in the organization** - Only members of the organization can find and view the group. Members can be invited to the group or apply to join.
- **Everyone (public)** - Anyone with access to the portal, even if they are not a member of the portal organization, can search for and view the group and access any content that is shared with both the group and the public. This is the default setting.

This portal feature helps implement and apply governance policies for portal members. Groups can be modeled in many ways and should be utilized based on the best implementation that meets an organization's business requirements. For example, groups could be based on different departments within an organization, different teams, or project stage.

[54] Pre-ArcGIS Enterprise 10.7 releases may not support all the roles listed in this section.
[55] To learn more, see Custom roles.
[56] See footnote 53 to learn more.

4.3 Security Filters

For ArcGIS Enterprise deployments, another aspect to consider is the enterprise network implementation. Specifically, organizations can apply standard server-side hardening recommendations that align with industry best practices. A comprehensive discussion on this topic is beyond the scope of this technical paper, but typical strategies include applying the following:

- **Firewalls**: A network security system that monitors the inbound and outbound network traffic based on a predefined set of security rules.[57] The ArcGIS Enterprise help documentation discusses using firewalls for both physical and cloud deployments. [58]
- **Web Application Firewalls (WAF)**[59]**:** A WAF filters, monitors, and blocks traffic to and from a web application. It is different from a regular firewall in that it can filter the content of specific web applications, while regular firewalls serve as a safety gate between servers.
- **Demilitarized zone (DMZ)** [60]**:** A physical or logical sub-network containing elements that are exposed to the Internet within the internal enterprise network. Typically, only a single endpoint on the DMZ is exposed to the external Internet. A DMZ helps provide an additional security layer to an organization's local area network (LAN).

For example, in Figure 14, one strategy is to deploy the ArcGIS Web Adaptor on a third-party web server; both are in the DMZ, while the remaining ArcGIS Enterprise components are located behind a firewall (or a WAF) beyond the DMZ. This ensures that Portal for ArcGIS, ArcGIS Server, and the ArcGIS Data Store are protected behind multiple firewalls. Note: this is a simplified example and not a comprehenisive discussion on deploying ArcGIS Enterprise components in the DMZ. Organizations should discuss their specific security and IT requirements with appropriate Esri personnel such as a solution architects and technical advisors. More on this deployment will be covered in section 6.4.

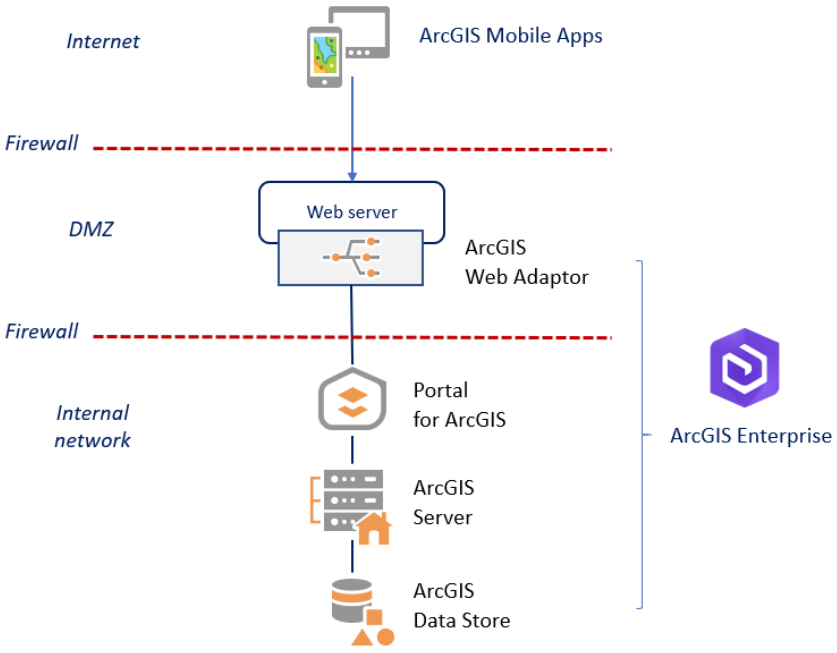

Figure 14: ArcGIS Enterprise firewall and DMZ deployment

[57] To learn more, see What is a firewall?.
[58] To learn more, see Firewalls and ArcGIS Server and Windows Firewall and the Esri AMIs.
[59] To learn more, see Web Application Firewall (WAF).
[60] To learn more, see DMZ (Computer Networking).

- **Network ports:** Communication access points for a server to the network. Public facing ArcGIS Enterprise components like the ArcGIS Web Adaptor, load balancer, or reverse proxy are typically configured to listen on the standard HTTP ports 80 (unencrypted) and 443 (encrypted) for communication. These technologies proxy traffic coming into the standard ports out to the ports used by the ArcGIS Enterprise components. The Portal for ArcGIS component uses port 7443 and the ArcGIS Server component uses port 6443 for secure communications. The ArcGIS Data Store component uses several different ports to communicate with each other and with other parts of ArcGIS Enterprise.[61] Using non-standard ports for public facing ArcGIS Enterprise components is not recommended.[62]
- **Anti-virus software**: Commonly deployed across workstations in an organization and increasingly becoming necessary for mobile devices not under the protection of an EMM.

To ensure a secure environment for the enterprise GIS with mobile field component using ArcGIS Enterprise, an organization may use some or all these options. Additional security best practice resources for an ArcGIS deployment as it is installed and maintained within an organization's infrastructure are available on ArcGIS Trust Center; this includes security guidance for ArcGIS Enterprise and ArcGIS Online. Some organizations also filter the domains they allow for communication, which can be disruptive if not configured properly based on Esri guidance.[63]

4.4 Encryption

Encryption is the process of transforming data so that it is unreadable without access to a decryption key. With respect to mobile apps in general, there are two aspects of encryption to consider:

Encryption at rest: By default, the ArcGIS mobile apps are not individually encrypting content when the data is at rest on the device. The apps will defer to the mobile device operating system to perform encryption. Data on an iOS device running iOS 4 or later is always encrypted.[64] Data on an Android device running Android 7 Nougat or later is also encrypted by default.[65] This function could also be enforced by using MDM software options (see section 3).

Encryption in transit: Data can be encrypted in transit by requiring HTTPS across the enterprise GIS – this is a best practice and strongly recommended. ArcGIS uses transport layer security (TLS)[66] as a key component of its communication protocol security. TLS is a protocol that provides privacy and data integrity between two communicating applications. It is the most widely deployed security protocol currently used by web browsers and other applications that require data to be securely exchanged over a network. TLS ensures that a connection to a remote endpoint is the intended endpoint through encryption and endpoint identity verification. HTTPS uses TLS as a key component of its security.

In April 2019, ArcGIS Online was set to enforce TLS 1.2 only for all inbound and outbound connections.[67] The communication protocols for ArcGIS Enterprise can be adjusted to meet the specific needs of an

[61] See Ports used by ArcGIS Data Store for more details.
[62] See Ports used by Portal for ArcGIS and Ports used by ArcGIS Server for more details.
[63] See Esri SSA briefing on ArcGIS Online Domain Requirements.
[64] To learn more about iOS encryption, see iOS 12.3 Security document.
[65] To learn more about Andriod encryption, see Android Encryption.
[66] To learn more, see What is Transport Layer Security (TLS)?
[67] See these blogs for details 2019 ArcGIS Transport Security Improvements and ArcGIS Online TLS 1.2 Only Enforcement In-Place Now.

organization, although enforcing HTTPS only (the default setting at the 10.7 release) and enforcing TLS 1.2 is strongly recommended.[68] TLS 1.3 is currently not available yet from most cloud infrastructure providers nor Esri's Online services, but support is planned in a future update.[69]

4.5 Certificates

Communication over HTTPS is established using digital security certificates. Security certificates[70] are used to verify and confirm that endpoints in a transaction are legitimate and valid. It is imperative and strongly recommended that domain and/or certificates obtained through a commercial certificate authority (CA) be used in an enterprise GIS deployment. Mobile devices can be very sensitive in terms of TLS communications and may not work properly if self-signed certificates are used.

Many enterprise mobile deployments are done through EMM technology. This enables an organization to push valid CA certificates to any mobile device that is involved in the organization's mobile deployment. Organizations should check with their respective IT departments on the procedure(s) for importing a valid CA certificate into their mobile devices.
All secure connections to the organization's network start with a TLS "handshake" to verify the server's identity and encryption algorithms it can support. Most mobile devices are configured to accept valid certificates issued by a trusted CA certificate, so the devices can tell which network servers are legitimate. IT needs to follow a few simple guidelines to configure CA certificates for mobile devices:

1. **Web distribution:** IT can point its mobile staff to a web page where a valid CA certificate is stored. Clicking the certificate file URL will launch a wizard that can be followed through to import the certificate into the device.
2. **Configuration profiles:** A more automated and robust method of adding CA certificates to mobile devices is to use configuration profiles (in an MDM solution), which are files that deliver settings to the devices. Each profile consists of extensible markup language (XML) formatted payloads, that include the certificates and the settings for applications that use those certificates. No matter how profiles are deployed, their XML payload content would have the same format.
3. **Simple Certificate Enrollment Protocol (SCEP)[71]:** This provides a scalable, robust method of adding CA certificates. Mobile devices can use SCEP to remotely request certificates from the organization's CA for subsequent device and user authentication, including enrollment with the company's MDM server.

Note: Once a CA certificate is added to a mobile device, it can be removed at any time, either through the MDM solution or by the users themselves.

4.6 Logging and Auditing

Logging involves recording events of interest collected from the enterprise GIS system. Auditing is the practice of inspecting those logs to ensure that the system is functioning as desired or to answer a specific question about a transaction that occurred. Logging and auditing can be facilitated at the following levels for mobile devices:

[68] See help topic Secure ArcGIS Server communication for more security recommendations. ArcGIS Enterprise can be configured to use older security protocols if needed.
[69] To learn more, see Esri SSP briefing on ArcGIS Platform SSL/TLS Support and Configuration.
[70] To learn more, see What are website certificates?
[71] To learn more, see Simple Certificate Enrollment Protocol Overview.

- At the device level, as facilitated by an EMM solution
- At the application level, by logging specific user transactions

These results should be fed into a centralized Security Information and Event Management (SIEM) solution to facilitate automatic correlation of the log data to aid in the detection of malicious activity.

5 Compliance and The Esri GeoSpatial Cloud

ArcGIS has been designed and is managed in alignment with regulations, standards, and best practices. This helps give confidence to the many government agencies at the federal, state, and local levels, both domestic and international, when using ArcGIS. Esri's compliance initiatives can be broadly categorized into four areas:

- Products and Services Security - Esri product and service-based security compliance
- Privacy Initiatives - Company and product privacy commitments
- Solution Based - Deployment patterns that align with compliance requirements
- Cloud Providers - ArcGIS Online cloud infrastructure provider compliance

Specific details and current status on the ArcGIS level of support in each of these areas is discussed in detail on the ArcGIS Trust center, Compliance section. Some notable compliance initiatives and guidance for ArcGIS are shown in Figure 15.

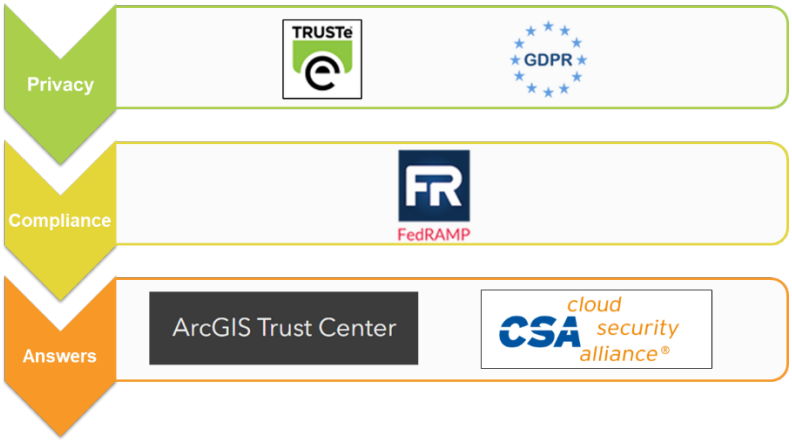

Figure 15: ArcGIS compliance

With respect to the ArcGIS field apps, there has been recent support for FirstNet[72] – a national agency in the United States that is working to develop and build a broadband network to support first responders. Esri's Public Safety team works in collaboration with FirstNet and Explorer for ArcGIS has met minimum requirements to support FirstNet.[73] There is also an app MyUSNG[74] – that reports device location in US National Grid (USNG) used to support search and rescue operations, that also meets FirstNet standards.

[72] To learn more, see FirstNet: First Responder Network Authority.
[73] To learn more, see FirstNet and Esri solutions.
[74] MyUSNG app, see its ArcGIS Marketplace listing.

Esri is continually striving to enable ArcGIS to meet more compliance standards and certifications. Additional security documentation related to ArcGIS can also be found on the ArcGIS Trust center, Documents section.

6 ArcGIS Mobile Deployment Patterns

In this section, several common implementation patterns for deploying an enterprise GIS with mobile field component are presented and discussed. The questions in sections 3.1 and 4.1, intended to help guide security considerations, should be discussed with senior management, the IT department, and stakeholders. Answers to these questions will likely determine which mobile deployment pattern would best meet the needs and business/security requirements of the organization.

It should be noted that the following mobile deployment patterns are not necessarily mutually exclusive. For example, an organization could deploy ArcGIS with a hybrid deployment as mentioned in section 2.3. In which case, there could potentially be a deployment of ArcGIS Online in combination with one of the other ArcGIS Enterprise on-premises or cloud-based deployment options. Hybrid deployments are discussed in section 6.7.

Summary of Mobile Deployment Patterns and Typical Difficulty, Risk, and Data Categories:

Pattern	*Implementation Difficulty*	*Relative Risk-Level*	*Common Data Categories*
ArcGIS Online	Low	Low - Moderate	Public / Hybrid-metadata
Cloud – EMCS[75]	Low	Low - Moderate	Low - Moderate
Cloud – Images	Moderate	Moderate	Low by default
On-Prem – Rev Proxy	Moderate	Moderate - High	Low - Moderate
On-Prem – VPN	Moderate - High	Low - Moderate	Moderate - High
On-Prem - Gateway	Moderate - High	Low	Moderate - High
Hybrid	Moderate	Low - High	Low - High

System Architecture Note: For ArcGIS Enterprise, the ArcGIS Data Store component enables data storage for the hosting server of the portal. (To review, see section 2.2) The ArcGIS Data Store can be deployed in 3 different ways: relational, tile cache, and spatiotemporal – where each type supports the storage of different content.[76] With respect to the ArcGIS field apps (Workforce, Collector, Survey123, and QuickCapture) and ArcGIS Enterprise, they use a relational data store. An exception is Tracker for ArcGIS which requires a spatiotemporal data store to support the storage of its content. These system requirements should be taken into consideration when planning a deployment to support these field apps.

[75] EMCS – Esri Managed Cloud Services

[76] To learn more, see footnote 8.

6.1 ArcGIS Online

As noted in section 2.1, frequently the easiest implementation option to use is ArcGIS Online. Esri hosts and maintains the infrastructure to support the enterprise GIS and mobile apps, so customers can simply connect to the ArcGIS Online organization via the Internet, (see Figure 16). Three authentication options are available: built-in security, social logins, or organization specific logins with SAML.

Figure 16: ArcGIS Mobile Apps using ArcGIS Online pattern

Risk Level[77]: Low to Moderate (depending on the sensitivity of the data and content) - A dedicated connection between an ArcGIS Online organization and a customer's enterprise is possible using distributed collaboration (see footnote 15).

Data: This offering is ideal for publicly accessible data and content, or where customer content is determined to be low security sensitive. ArcGIS Online is a FedRAMP Tailored Low authorized solution that is ideal for public dissemination use cases. Customers with higher sensitive data frequently implement a hybrid approach with ArcGIS Enterprise (using the on-premises or cloud option), see section 6.7.

Advantages:

- Easy implementation, no operational or management effort by the organization
- Allows segmenting less sensitive information in ArcGIS Online from more sensitive ArcGIS Enterprise deployments
- Software updates automatically applied by Esri
- Supports scalability if needed
- No need to connect mobile devices to the organization's internal network
- Great for asset inventory projects

Disadvantages:

- May need to export data from the organization's infrastructure to ArcGIS Online or use distributed collaboration methods
- For asset maintenance workflows, will need to export data from ArcGIS Online back to the organization's infrastructure
- Multi-tenant environment where customers share resources (i.e., where other organizations are also leveraging Esri's cloud infrastructure)

[77] Risk level is a general indicator of how "risky" a pattern is relative to others in this document.

- The process of updating is managed by Esri and updates are deployed system-wide. There is a possibility that workflow changes and software regressions may occur.

6.2 Cloud-Based - Esri Managed Services

In this pattern, an organization would have its own instance of ArcGIS Enterprise (with all components) deployed in the cloud, see Figure 17. This implementation is completely managed by Esri for the organization. The operational logistics are performed by Esri, but the organization owns and uses ArcGIS to support its business workflows.

Figure 17: ArcGIS Mobile Apps using Esri Managed Services

Esri Managed Cloud Services (EMCS) Advanced Plus[78] is an offering that provides security benefits that meet strict FedRAMP Moderate security requirements[79]. This includes the following:

- A 24/7 Security Operations Center for monitoring and threat detection
- An Intrusion Detection System (IDS) to detect malicious activity
- Continuous security monitoring of log data through a SIEM platform that is reviewed by security experts
- A WAF to mitigate against common web application attacks such as cross-site scripting (XSS)
- Federal Information Processing Standards (FIPS) 140-2 compliant encryption[80] for data-in-transit and data-at-rest
- A hardened network and virtual machine environment utilizing advanced inbound/outbound traffic rules
- Mandatory continuous application, system, and database scans
- Annual vulnerability assessment, penetration testing, and security control reviews by an accredited Third-Party Assessment Organization (3PAO)

Risk Level: Low to moderate (depending on the sensitivity of the data and content). EMCS Advanced Plus is a FedRAMP Moderate authorized solution. Other EMCS service levels such as Basic, Standard and Advanced do not provide the security benefits listed above.

[78] To learn more, see Esri Managed Cloud Services.
[79] To learn more, see FedRAMP and Trust.ArcGIS.com - Compliance.
[80] To learn more, see FIPS PUB 140-2 standard.

Data: This pattern can be used for data with low to moderate sensitivity levels. This offering is currently designed to process/store information within the United States, therefore organizations with government regulation data residency requirements need to confirm this aligns with their requirements.

Advantages:

- Minimal to no operational or management effort by the organization with Esri handling the logistical implementation (e.g., software optimization and maintenance)
- No need to copy data and content to ArcGIS Online – or minimal if required to support specific workflows
- Software updates are applied within months of release by Esri
- Segmentation of customer's datasets and systems
- Users are not accessing the organization's internal enterprise network
- Supports a web SSO user experience with organization specific logins
- Can leverage cloud benefits such as scalability

Disadvantages:

- Additional cost for cloud services
- The need for GIS data and content to be copied into the Esri cloud infrastructure
- GIS data and content may need to be copied to the organizational infrastructure, depending on need

6.3 Cloud-Based - Esri Cloud Images

In this pattern, Esri provides ArcGIS virtual machine images on two popular cloud platforms, Amazon Web Services and Microsoft Azure with more platforms likely to follow in the future, see Figure 18. This option is useful for customers that want to take on managing and maintaining an ArcGIS Enterprise deployment in the cloud themselves.

Figure 18: ArcGIS Mobile Apps using Esri Cloud Images

Risk Level: Moderate. This risk can be mitigated by a customer deploying and managing extensive security infrastructure beyond the machine image provided. These images are designed for ease of use and deployment. While the underlying cloud infrastructure providers have security certifications, they do not address the security management of the ArcGIS software at the application tier. A discussion on

securing a cloud-based deployment is beyond the scope of this document, but this pattern is mentioned for completeness.[81]

Data: Out-of-the-box these images can be used for data with low sensitivity levels. These images are useful to get a proof of concept up and running, but are not recommended for production datasets without ensuring that appropriate security infrastructure and processes are incorporated.

Advantages:
- No need to copy data and content to ArcGIS Online – or minimal if required to support specific workflows
- Resources only available for the organization (not shared)
- Can leverage cloud benefits such as scalability

Disadvantages:
- Additional cost for cloud services
- The need for GIS data and content to be copied to the cloud infrastructure
- Technical expertise needed among the organization's staff to manage systems, security, and software
- GIS data and content may need to be copied to the organizational infrastructure, depending on need

6.4 On-Premises - Reverse Proxy

In this pattern, the ArcGIS Web Adaptor serves as a reverse proxy, is deployed in the DMZ, and passes ArcGIS mobile app requests to Portal for ArcGIS and ArcGIS Server (see Figure 19). Authentication would occur at the Web Adaptor (web tier authentication), or it can be done at the Portal for ArcGIS tier (built-in security, token-based authentication, or organization specific logins with SAML) – see section 4.1. Alternatively, other third-party reverse proxy or load balancer solutions may be leveraged with or without the ArcGIS Web Adaptor, which can provide a more granular level of access control via ProxyPass directives[82] or routing rules. This pattern is the lowest-cost ArcGIS Enterprise approach when compared to the other patterns that follow, but it presents some risk to the enterprise internal infrastructure.

[81] See Esri's Security On Amazon Web Services for details.

[82] To learn more, see Apache - Reverse Proxy Guide.

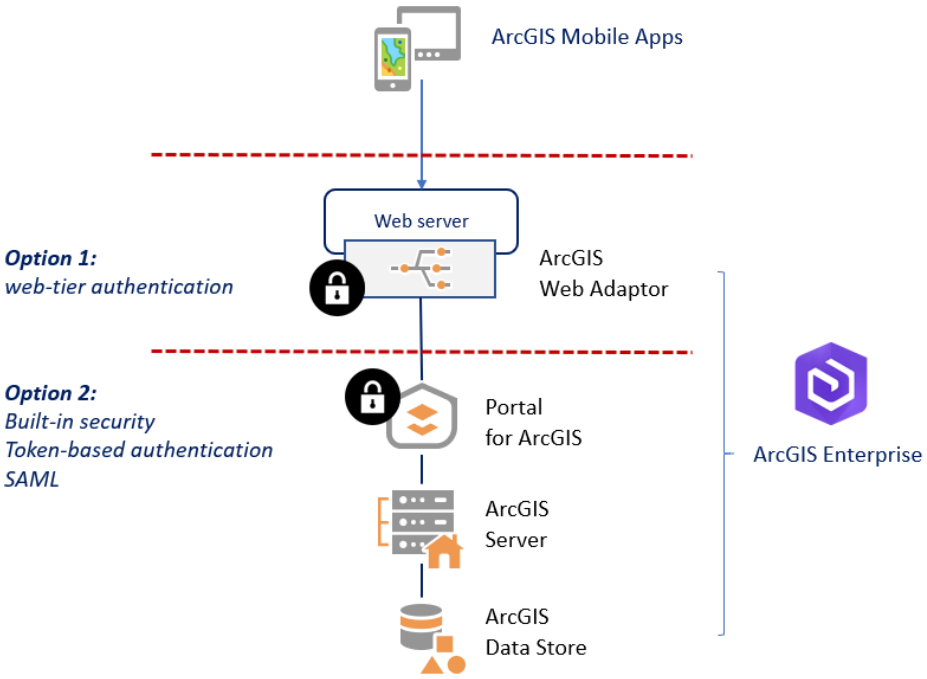

Figure 19: ArcGIS Mobile App Traversing Reverse Proxy

Risk Level: Moderate to High – This is the lowest cost ArcGIS Enterprise implementation, but it presents some risk to internal enterprise infrastructure. The security risk is higher with this option, but it is the organization's decision as to which data is externally accessible.

Data: This pattern can be used for data with low to moderate sensitivity levels. More sensitive data should be segmented from external access, even by reverse proxy.

Advantages:

- Lower cost (compared to the other on-premises ArcGIS Enterprise deployment patterns) – many organizations typically already have a web server
- More authentication options available
- All GIS data and content is stored within the organization's infrastructure
- No need to copy data to ArcGIS Online, or if required to support specific workflows, it is minimal; distributed collaboration can be used
- Resources only available for the organization (not shared)

Disadvantages:

- Higher risk due to web requests being proxied through the DMZ
- The need for contractors or semi-trusted users to be managed in the organization's Windows Active Directory/LDAP
- Technical expertise needed among the organization's staff to manage hardware and software

6.5 On-Premises - Virtual Private Network (VPN)

In this pattern, mobile devices connect to the internal enterprise network via a VPN connection – a secure, encrypted tunnel between the client and a server (see Figure 20). VPN access enables the mobile device to leverage the functionality and security of the internal network. The organization's IT

department configures and maintains a VPN service.

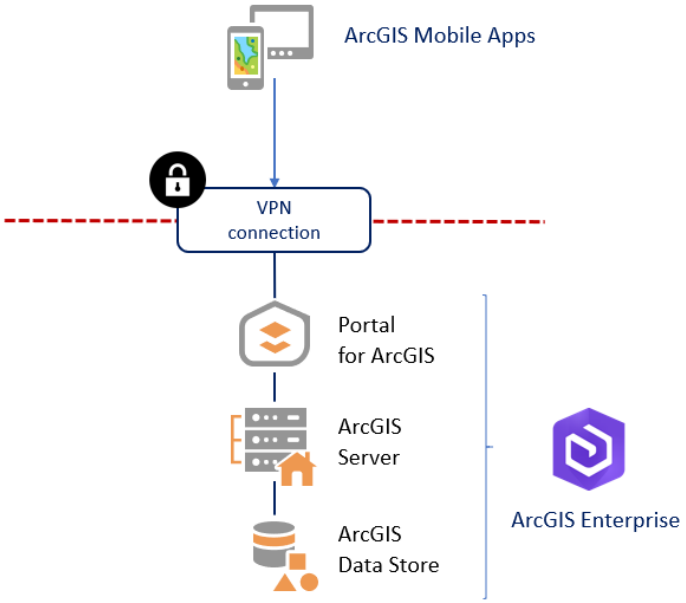

Figure 20: ArcGIS Mobile App Traversing VPN

Risk Level: Low to Moderate – This enables a dedicated tunnel for your enterprise communications and reduces risk, however it can have an impact on performance. Implementing strict authentication (e.g., 2-factor) as well as granular authorization (i.e., determining which assets can VPN users' access) can improve the security posture of this option.

Data: This pattern can be used for data with moderate to high sensitivity levels.

Advantages:

- Lower cost than requiring a separate security gateway for mobile components
- More authentication options available
- All GIS data and content are stored within the organization's infrastructure
- No need to copy data to ArcGIS Online, or if required to support specific workflows, it is minimal; distributed collaboration can be used
- Resources only available for the organization (not shared)

Disadvantages:

- The need for the IT department to enable and maintain a VPN service, if not already in place in the organization
- Users who access the enterprise GIS must use corporate VPN
- Most traffic from mobile devices being routed through the corporate network when using VPN (this will vary depending on the organization's network infrastructure)
- Contractors or semi-trusted users may need to be given more access to the internal enterprise network (which may be a security issue)
- Technical expertise needed among the organization's staff to manage hardware and software

6.6 On-Premises - Mobile Security Gateway

In this pattern, mobile device clients are authenticated with a mobile security (or application) gateway, see Figure 21. The security gateway is typically located in the DMZ and is usually part of a larger EMM solution in the organization. The EMM solution will likely include both MDM and MAM components. See section 3.2 for more details on EMM technology and its components.

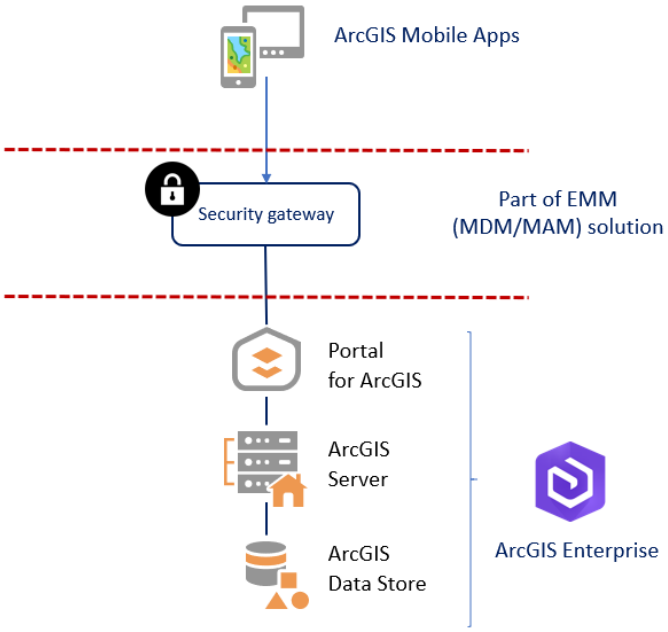

Figure 21: ArcGIS Mobile App Traversing Security Gateway (EMM)

Risk Level: Low – EMM technology provides more secure options on mobile devices, see section 3.2.

Data: This pattern can be used for data with moderate to high sensitivity levels.

Advantages:

- Users are not dependent on corporate VPN
- Potential SSO user experience if using IWA depending on security gateway capabilities
- More options to manage mobile devices and apps via EMM technology
- All GIS data and content stored within the organization's infrastructure
- No need to copy data to ArcGIS Online, or if required to support specific workflows, it is minimal; distributed collaboration can be used
- Resources only available for the organization (not shared)

Disadvantages:

- Medium to higher cost (compared to the other deployment patterns) – if an EMM solution and network infrastructure is not already present in the organization
- The need for the IT department to enable and maintain an EMM solution; if not already in place in the organization
- Minimal segmentation, where publicly accessible data are separated from private data; and separate servers are used to store each type
- EMM technical expertise needed within the organization's staff
- Technical expertise needed among the organization's staff to manage hardware and software

6.7 Hybrid Deployment

As mentioned in section 2.3, a common pattern is to use a hybrid of ArcGIS Online and an on-premises ArcGIS Enterprise deployment option (sections 6.4 – 6.6). Figure 22 illustrates one common ArcGIS hybrid deployment architecture.

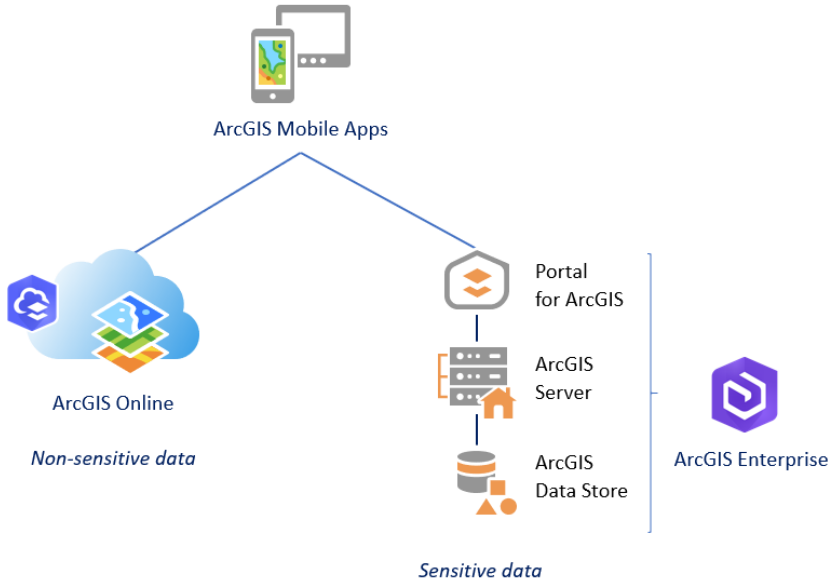

Figure 22: ArcGIS Mobile Using a Hybrid Deployment – Content Stored in Cloud and On-Premises

In this example, the ArcGIS mobile apps can connect and access content from both ArcGIS Online and ArcGIS Enterprise. Data could be stored in both locations. Using this hybrid approach, organizations have the flexibility to use ArcGIS to support multiple use cases. On-premises data and services could be used to provide sensitive information to mobile workers, and non-sensitive data and content stored in ArcGIS Online could be shared with a broader range of constituents. Increasingly, organizations are thinking about their data on a layer-by-layer basis to determine which data should be stored on-premises and which data is appropriate to store in a SaaS system.

Another common ArcGIS hybrid deployment architecture is shown in Figure 23. In this instance, the ArcGIS mobile apps connect to ArcGIS Online, but the data is stored in ArcGIS Enterprise in an organization's infrastructure. Data and services from ArcGIS Enterprise are *registered* with ArcGIS Online, but stored on-premises. ArcGIS Online can create proxies to access data secured at the organizational level, if desired. This type of deployment can support authentication in ArcGIS Online and in ArcGIS Enterprise.[83]

Figure 23: ArcGIS Mobile Using a Hybrid Deployment – Registering services with ArcGIS Online

[83] To learn more, see Add items from the web.

The advantage of a hybrid deployment is that sensitive data covered under a strict security mandate is stored and served by an in-house instance of ArcGIS Enterprise, while other data is managed via the robust and secure ArcGIS Online infrastructure, providing bandwidth, uptime, and scalability.

The following scenarios typically apply to this pattern:

- The organization wants to leverage the full capabilities of ArcGIS Enterprise by creating and sharing web maps with both on-premises and hosted services. This requires complete flexibility in how ArcGIS is deployed to everyone in the organization, to contractors, and to customers.
- This scenario may be combined with the fully hosted option, such that all internal users access the hybrid environment and external users access the fully hosted ArcGIS Online organization.
- This scenario also scales well with distributed collaboration, where users may connect and integrate the enterprise GIS across a network of participants including those with membership in ArcGIS Online organizations, ArcGIS Enterprise, or both (see footnote 15).

Note that many hybrid deployment variations are possible, but a comprehensive discussion is outside the scope of this document (see footnote 16).

7 Conclusion

There are many considerations to designing the optimal secure enterprise GIS with an ArcGIS mobile field component for an organization. It requires an understanding of ArcGIS components, EMM offerings, IT/security mechanism options, and the various pros and cons of the deployment patterns. The intention of this technical paper is to make the design process easier to deliver the level of security an enterprise demands for mobile applications today.

The Esri Software Security & Privacy team would like to give a note of thanks for the broad input and reviews from fellow teams at Esri, Distributors, and customers. Esri intends to update this document in the future, so feel free to provide your comments and suggestions to *SoftwareSecurity@Esri.com*.

8 Acronyms

This section lists acronyms that are used in this technical paper.

- 3PAO: Third-Party Assessment Organization
- BYOD: Bring Your Own Device
- CA: Certificate Authority
- DISA: Defense Information Systems Agency
- DMZ: Demilitarized Zone
- EMCS: Esri Managed Cloud Services
- EMM: Enterprise Mobility Management
- EU: European Union
- FIPS: Federal Information Processing Standards
- FISMA: Federal Information Security Management Act
- FedRAMP: Federal Risk and Authorization Management Program (Based on FISMA law)
- GDPR: General Data Protection Regulation
- GIS: Geographic Information Systems
- HTTP: Hypertext transfer protocol
- HTTPS: Hypertext transfer protocol secure
- IDP: Identity Provider
- IDS: Intrusion Detection System
- ISO: International Standards Organization
- IT: Informaton Technology
- IWA: Integrated Windows Authentication
- LAN: Local Area Network
- LDAP: Lightweight Directory Access Protocol
- MAM: Mobile Application Management
- MCM: Mobile Content Management
- MDM: Mobile Device Management
- OS: Operating System
- OWASP: Open Web Application Security Project
- PaaS: Platform-as-a-Service
- PKI: Public Key Infrastructure
- SaaS: Software-as-a-Service
- SAML: Security Assertion Markup Language
- SCEP: Simple Certificate Enrollment Protocol
- SDK: Software Developer Kit
- SIEM: Security Information & Event Management
- SSA: (Esri) Security Standards & Architecture team
- SSO: Single-Sign-On
- STIG: Security Technical Implementation Guide
- TLS: Transport Layer Security
- VPN: Virtual Private Network
- WAF: Web Application Firewall
- XML: Extensible Markup Language
- XSS: Cross-site Scripting

esri | THE SCIENCE OF WHERE™

Esri, the global market leader in geographic information system (GIS) software, offers the most powerful mapping and spatial analytics technology available.

Since 1969, Esri has helped customers unlock the full potential of data to improve operational and business results. Today, Esri software is deployed in more than 350,000 organizations including the world's largest cities, most national governments, 75 percent of Fortune 500 companies, and more than 7,000 colleges and universities. Esri engineers the most advanced solutions for digital transformation, the Internet of Things (IoT), and location analytics to inform the most authoritative maps in the world.

Visit us at esri.com.

For more information, visit:
Trust.ArcGIS.com

Contact Esri

380 New York Street
Redlands, California 92373-8100 USA

1 800 447 9778
T 909 793 2853
F 909 793 5953
info@esri.com
esri.com

Offices worldwide
esri.com/locations