ESRI EXTERNAL

July 2025

ArcGIS Field Apps and Mobile Device Management (MDM) Support

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

Contents

1. Introduction

There has been extensive growth of mobile device usage as part of enterprise geographic information system (GIS) deployments in many organizations. Advancements in mobile technology has made it easy for organizations to bring their maps and data into the field, to support different types of field operations across many industries. Mobile GIS has moved into the late majority phase of the technology adoption life cycle[1]. Coinciding with this mobile growth trend, is the need for organizations to ensure that proper security protocols are in place to protect their data and business interests. A high-level discussion on strategic security planning and best practices is discussed in the ArcGIS Trust Center: Security Mobile implementation guidance website.

For medium to large organizations who may have 100s to 1000s of mobile workers, one of the significant deployment patterns for mobile device security is the adoption of mobile device management (MDM) technology. MDM technology enables information technology (IT) departments to centralize the security management of mobile devices. This document focuses on deploying ArcGIS mobile apps with MDM technology. It is meant to guide IT managers and GIS administrators to help them understand how ArcGIS mobile apps can work with MDM technology and which capabilities are possible.

This technical paper provides some background and deployment considerations; it is not a detailed step-by-step implementation guide. Knowledge of ArcGIS System, IT, and MDM concepts is not a requirement, but is strongly recommended. Be advised that enterprise GIS mobile deployments with MDM technology will vary from organization to organization, and solution architects should use the concepts discussed in this document for planning secure solutions that meet the needs of their specific enterprise GIS implementation.

2. ArcGIS Mobile Apps

ArcGIS offers distinct mobile apps that support many different business use cases. For the purposes of discussion in this document, these apps can be separated into two categories: i) field operations mobile apps and ii) solution mobile apps. Apps in the former group are designed to support field operations, while apps in the latter group support specialized workflows. All ArcGIS mobile apps work with ArcGIS Online and/or ArcGIS Enterprise[2]. These apps support all ArcGIS deployment models: software-as-a-service (SaaS), managed services, cloud environments, on-premises, or a hybrid variation.[3] Please review the online help documentation for each app for details.[4]

GIS data and maps can be easily taken into the field to support field workflows. Field personnel can work with the same authoritative datasets on their mobile devices, helping collect new data (or edit existing data) that can be shared immediately to the office. Core field operations capabilities include: planning and coordinating the work in the field, the ability to understand surroundings and assets more deeply with access to enterprise data

[1] To learn more, see Technology adoption life cycle.
[2] Apps sign into the ArcGIS enterprise portal component of ArcGIS Enterprise.
[3] Some of ArcGIS solution mobile apps may not support all of ArcGIS deployment options.
[4] Help documentation for the Apps: ArcGIS Help Documentation.

and highly accurate and efficient data capture, see Figure 1.

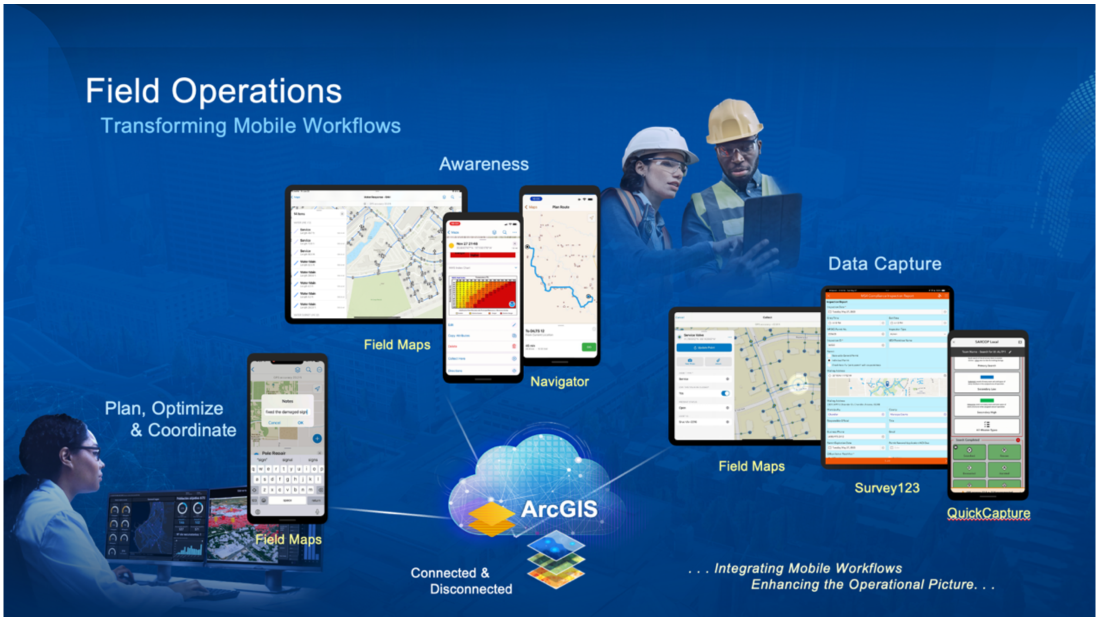

Figure 1: Field Operations in ArcGIS

ArcGIS field operations mobile apps are available for iOS and Android devices, and some also support the Windows platform.[5] They support connected and disconnected environments and they can be used separately or collectively as part of a larger mobile workflow, depending on the organization's business requirements.[6] 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 2) consist of five apps:

- **ArcGIS Field Maps**: Explore maps created in ArcGIS, collect and update GIS data in the field, and monitor movements with location sharing;
- **ArcGIS Survey123**: Focused on form-centric data collection and editing, includes analysis and reporting capabilities;
- **ArcGIS QuickCapture:** Enables rapid data collection with a single button or voice command;
- **ArcGIS Navigator**: Enables routing with turn-by-turn directions;

[5] Please review the System Requirements documentation for each individual app to learn which OS platforms they support.
[6] To learn more, see Field Operations: Overview

- **ArcGIS Workforce**: Enables planning and coordination of work assignments. This app will be deprecated in longer term as the functionality will be incorporated into ArcGIS Field Maps (Tasks capability).

Figure 2: ArcGIS field operations mobile apps

ArcGIS solution mobile apps are specialized apps, see Figure 3. These range from 3D data visualization, to offering a building occupant mobile experience and supporting drone workflows. Some of these are not stand-alone apps, but offered as part of a Geo-Enabled system from Esri. These apps are included in this document because some of them can also be managed with MDM technology. ArcGIS solution mobile apps include:

- **ArcGIS Business Analyst Mobile**[7]: Provides demographic and socio-economic data, infographics and reports in the field;
- **ArcGIS Earth**: Displays and provides interaction with 3D data on a globe;
- **ArcGIS Flight**: Provides tools to collect images to create accurate, high-resolution maps and 3D models using drones;
- **ArcGIS Indoors**[8]: Successor to ArcGIS Indoors Classic provides building occupants, employees, and visitors a native mobile mapping experience that supports indoor way-finding, workspace reservations, and building incident reporting;
- **ArcGIS Indoors Classic**[9]: Provides building occupants, employees, and visitors a native mobile mapping experience that supports indoor way-finding, workspace reservations, location sharing, and building incident reporting;
- **ArcGIS Mission Responder**[10]: Provides mobile workers with situational awareness on a map with messaging and location tracking among team members.

Figure 3: ArcGIS solution mobile apps

[7] This app is part for the ArcGIS Business Analyst solution.
[8] This app is part of a larger ArcGIS Indoors Geo-Enabled system.
[9] This app is part of a larger ArcGIS Indoors Geo-Enabled system.
[10] This app is part of a larger ArcGIS Mission Geo-Enabled system.

3. Mobile Device Management (MDM) solutions

Evolutions in security practices have led more organizations to seek tools that support their policies. This includes ensuring sensitive data is protected while maintaining compliance with regulatory standards, as well as streamlining device management and enabling efficient deployment of devices within the organization. In these cases, organizations typically use Mobile Device Management (MDM) technology to effectively manage their mobile devices and create a secure mobile environment. While MDM solutions are primarily targeted at medium to large organizations, small organizations can also benefit from implementing an MDM solution.

MDM technology is third party software that IT administrators use to control, secure, and enforce policies on mobile devices for an organization.[11] The software optimizes the functionality and security of mobile devices within the enterprise, while protecting the corporate network, see Figure 4. MDM solutions apply to all members of an organization accessing the corporate network via mobile devices, not just mobile workers supporting GIS workflows. Some examples of MDM solutions are: Citrix Endpoint Management (formerly XenMobile), IBM Security MaaS360, Microsoft Intune (formerly Microsoft Endpoint Manager), Ivanti Neurons (formerly MobileIron Unified Endpoint Management), and VMware Workspace ONE (formerly VMWare AirWatch).

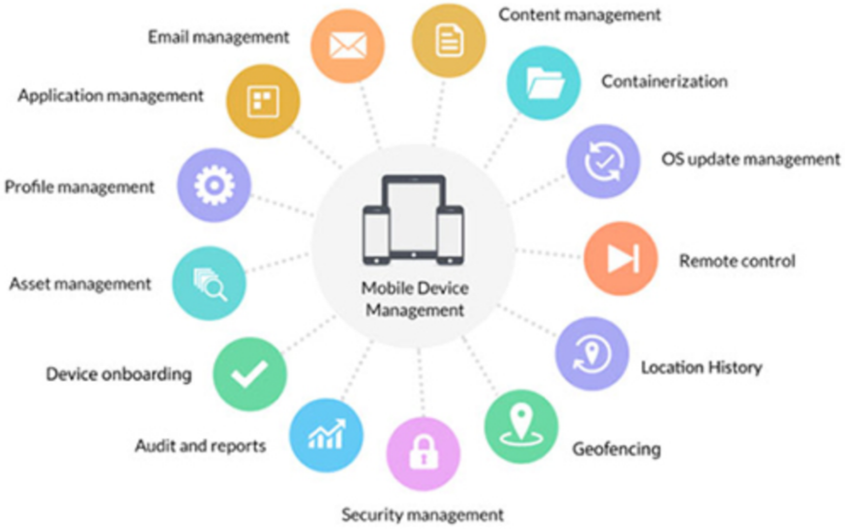

Figure 4: MDM technology conceptual diagram[12]

There are many advantages to using MDM technology such as:

- Streamlined device management
- Make app deployments more efficient and save time
- Help keep apps and data secure
- Help with bring your own device (BYOD) management and policies
- Active monitoring for malware and other threats
- Better security and more control of devices for the organization

[11] To learn more, see mobile device management (MDM).
[12] Source: Six MDM Features and Functions - Which One Do You Know?

Typically, using an MDM solution is part of an organization's broader enterprise mobility management (EMM) strategy. MDM technology helps IT managers integrate mobile devices with business processes, provide mobile workers with an easier user experience, and ensures that the organization's security and compliance requirements are met. Some of the administrative tasks that can be performed using an MDM solution include:

- *Configure devices* → Set up email, Wi-Fi, virtual private network (VPN) connections, security certificates, and other settings wirelessly;
- *Restrict devices* → Restrict specific device features like the camera, browser, app store, etc.;
- *Remotely manage devices* → Locate the device geographically and lock or wipe them remotely;
- *Manage mobile applications* → Install/uninstall apps, push in-house apps to the devices, allow list/block list apps, control app versions and update(s);
- *Ensure security* → Define policy requirements and identify devices that do not comply; generate reports to document compliance status, and initiate actions to restore compliance.

At a conceptual level, an MDM solution typically includes an MDM server component that sends out management commands to mobile devices that have a client component (MDM agent) installed, see Figure 5. An MDM administrator uses the MDM console to define policies, restrictions, and apps for various groups in the MDM; each group would represent a different business unit or role - each having their own configuration settings. The MDM also has an app catalog, which is a list of apps it can deploy. When a mobile device (corporate owned or BYOD) is registered with the organization's MDM software, it becomes a *managed device* and will have the MDM agent installed.

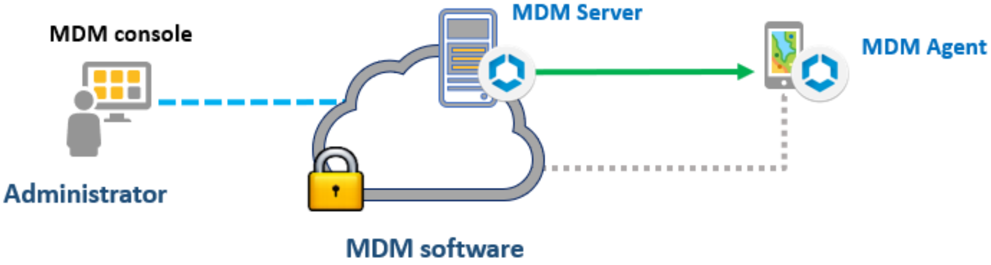

Figure 5: MDM architecture concept diagram

IT admins simply configure the policies, restrictions, and app configurations via the MDM console, and the MDM server will push them to the MDM agents on each managed device. This workflow makes the process of configuring large numbers of mobile devices much easier and more consistent. The MDM solution can connect directly to public app stores like the Apple App Store and Google Play, allowing access to the latest app releases. Another aspect typical of an MDM solution is the concept of "containerization", which means corporate data can be separated from a user's personal data on the mobile device. MDM configuration options will vary between different MDM solution vendors.

4. ArcGIS and MDM solutions

Esri designs its mobile apps to work and behave the same way across different third-party MDM vendors. Esri's ArcGIS mobile app development strategy follows the guidelines promoted by the AppConfig Community. This is a community that works with several EMM and MDM vendors focused on providing tools and best practices for native capabilities in mobile operating systems. Their objective is to help promote a more consistent, open, and simple way to configure and secure mobile apps that advances mobile adoption in business. There are four main focus areas:

- *App configuration* → Allows IT administrators to remotely configure settings of a managed app. Each app can be custom configured using key and value settings;
- *App tunnel* → This enables per-app VPN capabilities to an organization's network, enabling a secure connection between the mobile device and internal servers;
- *Security policies and access control* → Restrict apps to only run on approved devices and enforce security policies at the app level;
- *Single sign-on (SSO)* → Provide a user-friendly sign-on user experience to the corporate network.

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 mobile app developers and help them create apps that work well in MDM environments. ArcGIS mobile apps do not support any MDM vendor application programming interfaces (APIs) for customization. They also do not support the concept of app wrapping: the process of applying an additional security layer to a mobile app, without modifying the app itself.[13] This content is included as background, as ArcGIS mobile apps are discussed in the context of working with MDM solutions.

While ArcGIS mobile apps are designed to support specialized GIS workflows, from an MDM perspective they are managed like any other mobile app. Therefore, ArcGIS mobile apps can be registered with an MDM solution, then deployed to managed devices via the MDM server and agent(s), see Figure 6.

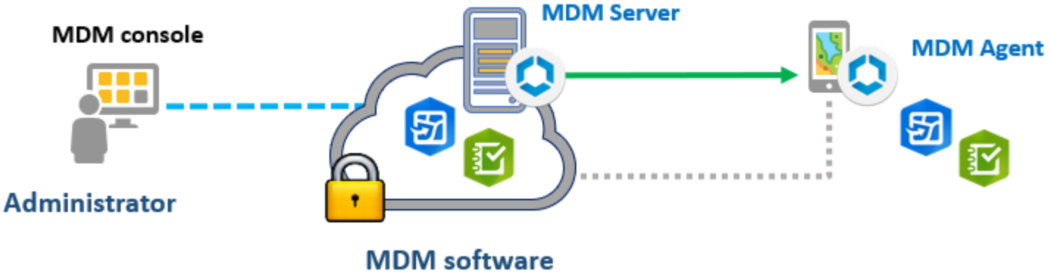

Figure 6: MDM deployment of ArcGIS mobile apps concept diagram

[13] To learn more, see What is app wrapping? One way to more secure mobile apps

The following is the general workflow to deploy ArcGIS mobile apps with an MDM solution:

1. Register the app with the MDM solution; the app is added to the MDM application catalog
2. Enroll the mobile device (corporate or BYOD) with the MDM solution; the device becomes a managed device
   - The MDM agent is installed on the device
3. Assign managed device to an MDM group – typically the groups are aligned with the organization's business units or security roles
   - The MDM admin defines specific policies, configurations, and restrictions on the various MDM groups
4. Deploy the app from the MDM application catalog to the managed device
   - The MDM agent applies the configuration to the device via built-in APIs.

This high-level workflow is generalized so it can be applied to any third-party MDM vendor. For specifics, please check the respective third-party MDM vendor help documentation.

In advance of discussing the specifics of which management and security capabilities are possible when deploying ArcGIS mobile apps with an MDM solution, it should be made clear:

ArcGIS mobile apps do work with third party MDM solutions, but their deployment within an MDM environment is not currently supported by Esri Technical Support.

To elaborate on this statement: ArcGIS mobile apps can be managed and deployed with MDM solutions, but if an organization encounters technical issues – they will not be able to contact Esri Technical Support services to get assistance.[14] It is incumbent on the organization to have internal expertise on MDM technology and resolve MDM-related issues. Alternatively, organizations can work with Esri Professional Services to request assistance with MDM deployments.

ArcGIS mobile apps have been successfully deployed with third party MDM solutions by many customers. Many organizations including US federal agencies, water and gas utilities, and natural resources companies use MDM software to help deploy ArcGIS mobile apps. Example MDM solutions used by Esri's user base include: Cisco Meraki, Citrix Endpoint Management, F5 Big IP, IBM Security MaaS360, Microsoft Intune, Ivanti Neurons, and VMware Workspace ONE.

4.1 App Configuration

ArcGIS mobile apps can be deployed, updated, and removed from managed devices with an MDM solution, like any other registered app. This is beneficial for IT and GIS administrators, because they can ensure that mobile workers are using the same and latest app release(s).

[14] If the issue can be reproduced with the latest app store version, outside of an MDM deployment, then Esri Technical Support can investigate further.

For the MDM managed app configuration capabilities, ArcGIS mobile apps are configured using key-value pairs (i.e., an app setting can be defined by a specific key and value). Esri's ArcGIS mobile app development teams have made several keys available which can be leveraged within the MDM solution. These keys were defined based on user requirements and some are only available for specific apps based on their workflow needs. The app configuration key list is continually evolving depending on requirements. Additional configuration parameters may be added in future app updates.

The most common key is `portalURL`, which enables an app to have a preset link to connect to an ArcGIS organization (ArcGIS Online or ArcGIS Enterprise portal).[15] Enabling this setting provides a convenient user experience for the mobile worker, as the app will be automatically configured to use the appropriate ArcGIS organization to sign into by default. Figure 7 shows the user interface where an end user selects the ArcGIS organization to connect the app to; this display may be bypassed when the `portalURL` setting is already configured in the MDM software (this will depend on the app). When the `portalURL` key is set, the end user will be automatically taken to the sign-in screen for your organization and prompted to sign in.

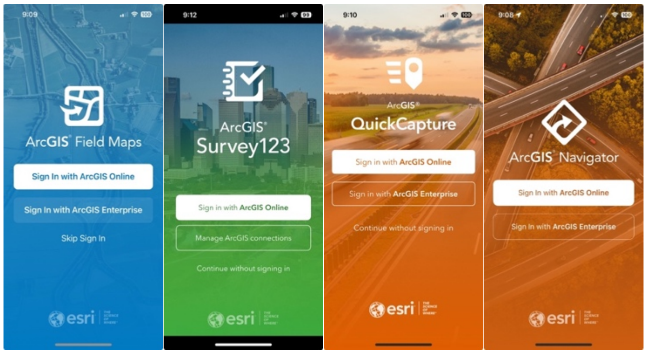
9:09
ArcGIS Field Maps
Sign In with ArcGIS Online
Sign In with ArcGIS Enterprise
Skip Sign In
esri
9:12
ArcGIS
Survey123
Sign in with ArcGIS Online
Manage ArcGIS connections
Continue without signing in
esri
9:10
ArcGIS
QuickCapture
Sign in with ArcGIS Online
Sign in with ArcGIS Enterprise
Continue without signing in
esri
9:08
ArcGIS Navigator
Sign In with ArcGIS Online
Sign In with ArcGIS Enterprise
esri

Figure 7: ArcGIS organization connection displays for ArcGIS Field Maps, Survey123, QuickCapture, and Navigator

All of ArcGIS mobile apps support the `portalURL` key (or have it on their development roadmap). Table 1 lists the available MDM configuration settings for the different ArcGIS mobile apps.

App	**portalURL**	**App specific settings**
ArcGIS Field Operations Apps		
ArcGIS Field Maps	✓	▪ Authentication settings ▪ Anonymous access to Enterprise ▪ Tracks and LKL[16] upload frequency ▪ Location profile and offset config
ArcGIS Survey123	✓	▪ Authentication settings ▪ Enterprise portal configuration ▪ Diagnostics ▪ Data recovery
ArcGIS QuickCapture	✓	
ArcGIS Navigator	✓	▪ Biometric authentication

[15] To learn more about the portalURL key, see Mobile device management.

[16] "LKL" is an acronym for the last known location (LKL) of a person or asset; this is a feature of location sharing.

ArcGIS Workforce	✓	
ArcGIS Solution Apps		
ArcGIS Business Analyst Mobile[17]	✓	
ArcGIS Earth	✓	
ArcGIS Indoors	planned	Note: Branding is done through portal config
ArcGIS Indoors Classic	✓	▪ Branding ▪ Authentication settings
ArcGIS Mission Responder	planned	

Table 1: ArcGIS mobile app MDM configuration settings

As noted in Table 1, several of ArcGIS mobile apps have additional keys to provide more app configuration settings in an MDM solution. The following series of tables 2-9 describe the various MDM keys available for these apps. To learn more about each MDM setting, please review the help documentation for each app (see footnote 4).

ArcGIS Field Maps[18]

Key	Description
`anonymousAccess`	Specifies whether to sign in anonymously or require credentials
`isAutoSyncEnabled`	Specifies whether auto-sync is enabled
`locationProfiles`	Defines the parameters of one or more location profiles
`offsetProvider`	Specifies the offset provider
`portalURL`	Specifies a preset link to connect to an ArcGIS organization
`locationSharingMode`	Specifies whether battery life is optimized or unoptimized while recording tracks
`locationSharingUploadLKLFrequency`	Specifies the last known location upload frequency
`locationSharingShareLKLOnly`	Specifies how location sharing history is stored
`locationSharingUploadTracksFrequency`	Specifies the track upload frequency
`maxRefreshTokenExpiration`	Specifies an expiration time for the token
`maxTraceResults`	Specifies the maximum number of elements that can be returned from a Utility Network selection trace.
`useInAppAuth`	Specifies whether a web view is used for sign-in and authentication in Field Maps

Table 2: ArcGIS Field Maps MDM settings

[17] To learn more, see the App Config using MDM for ArcGIS Business Analyst Mobile App blog.
[18] For more information see the ArcGIS Field Maps - Mobile device management help topic.

ArcGIS Survey123[19]	
Key	Description
`portalURL`	Specifies a preset link to connect to an ArcGIS organization
`portalName`	Specifies the portal display name
`portalAuthentication`	Specifies the portal authentication method
`useExternalBrowserAuth`	Specifies whether an external browser is used for sign-in and authentication
`portalResourceKey`	Specifies the resource name used for organization level properties
`requireSignIn`	Specifies if a sign-in is required to use the mobile app
`delaySignIn`	Specify the delay (in seconds) before the field app attempts to authenticate with the portal.
`enablePortalManagement`	Specifies if a user can manage ArcGIS connections
`enableDiagnostics`	Specifies if a user can log diagnostics information
`enableDataRecovery`	Specifies if a user can recover data using the Send Database option

Table 3: ArcGIS Survey123 MDM settings

ArcGIS Navigator	
Key	Description
`portalURL`	Specifies a preset link to connect to an ArcGIS organization
`enableLocalAuthentication`	iOS Only - Whenever the app is brought to the foreground, the app will prompt for authentication

Table 4: ArcGIS Navigator MDM settings

ArcGIS Indoors Classic[20]	
Key	Description
`portalURL`	Specifies a preset link to connect to an ArcGIS organization
`splashImageURL`	Specifies an image to use in a splash screen
`menuImageURL`	Specifies a menu image
`primaryColor`	Specifies the background color
`secondaryColor`	Specifies the foreground color

Table 5: ArcGIS Indoors Classic MDM settings

[19] More information available in the Configure Survey123 Properties in your MDM with AppConfig blog.
[20] More information available in the help topic: Configure Indoors for mobile device management.

4.2 App Tunnel

MDM solutions can enable native app tunneling features on supported mobile devices using a protocol called per-app VPN. The per-app VPN capability means that a secure connection can be made back to the corporate network only for the specific app (where this functionality is enabled). A VPN tunnel insulates network traffic, usually with some type of encryption, between the device and back end servers, see Figure 8.

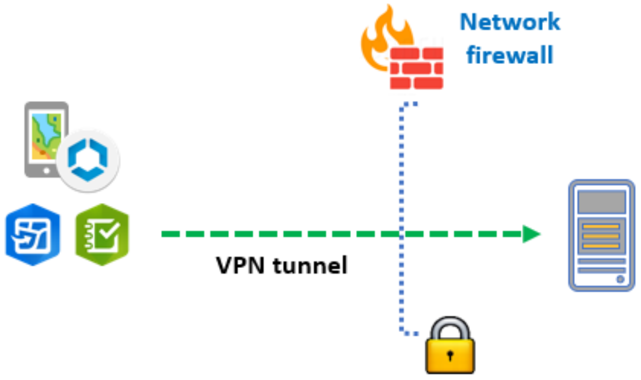

Figure 8: Per-app VPN conceptual diagram

ArcGIS mobile apps can be configured with MDM solutions to support this functionality. No additional configurations to the apps are needed.

4.3 Security Polices and Access Control

It is possible to restrict apps to only run on approved devices and enforce security policies at the app level. ArcGIS mobile apps can be configured with an MDM solution to support this functionality. As mentioned earlier, the MDM admin defines specific policies, configurations, and restrictions for different MDM groups. The MDM groups represent different business units or security roles within the organization. Managed devices are assigned to these groups based on business requirements and workflows. Then apps are deployed to the managed devices. No additional configurations to the apps are needed.

4.4 Single Sign-On (SSO)

This capability enables an end user to log into a mobile device once, then their credentials are passed to apps on the device. This provides a user-friendly authentication experience without requiring the end user to re-enter login credentials when trying to access resources on the device like apps. Support for this functionality will vary depending on the authentication method(s) enabled in an organization, the type of mobile device(s) used, and the mobile device operating system (i.e., iOS, Android, or Windows). It is possible to enable this functionality with some of ArcGIS mobile apps for specific authentication methods and operating systems.[21] Please review the online help documentation for each app to get the latest status on support for this capability (see footnote 4).

[21] A comprehensive discussion on this topic is beyond the scope of this technical paper.

5. Troubleshooting

As mentioned in section 3, organizations should have internal expertise on MDM technology to help resolve any MDM-related challenges. This section is included to provide some general guidance for IT and GIS managers when encountering MDM issues with ArcGIS mobile apps:

- Check MDM logs
- Check app logs on device (where possible)
- Check and review web traffic from the device (where possible)
- Check device status page in MDM for errors or warnings for that device
- Verify MDM groups are configured correctly
- Verify managed device profiles and resources are configured and assigned correctly
- Verify app assignments and app config settings are configured correctly
- Unenroll device (i.e., remove from MDM management) and enrol again in MDM
- Reformat device and start with fresh OS install and MDM configuration
- Check if issue can be replicated outside of the MDM deployment

The above is not a complete list and is meant to give some high-level suggestions to investigate and resolve issues. It is not possible to be more specific, because it will depend on what the problem is. Troubleshooting help documentation for the respective third-party MDM vendor may also provide some insight to resolve issues.

6. Summary

For medium to large organizations who may have 100s to 1000s of mobile workers, using an MDM solution to configure apps for their mobile workers can streamline deployment workflows. IT and GIS managers can be more efficient and ensure app deployments are more secure and consistent. ArcGIS mobile apps can be deployed with MDM solutions and support some app configuration options. ArcGIS mobile apps are frequently updated and are continually enhanced to support additional capabilities in future releases.

7. Appendix

Deprecated Apps:

- ArcGIS field operations apps: ArcGIS Explorer, ArcGIS Collector, and ArcGIS Tracker have all been deprecated on iOS and Android.
- ArcGIS solution mobile apps: AppStudio Player, ArcGIS Companion

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.

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

For more information, visit esri.com/URL.