## Contents

1 Introduction ...............................................................................................................................1

2 Background – Web GIS................................................................................................................1

  2.1 ArcGIS Online ................................................................................................................................ 2

  2.2 ArcGIS Enterprise .......................................................................................................................... 3

  2.3 Hybrid Deployments ..................................................................................................................... 4

  2.4 ArcGIS Mobile Apps ...................................................................................................................... 4

3 Enterprise Mobile App Management ...........................................................................................6

  3.1 Connecting ArcGIS Mobile Apps to the Enterprise ....................................................................... 6

  3.2 Enterprise Mobility Management (EMM) ..................................................................................... 7

    3.2.1 Mobile Device Management (MDM) .................................................................................... 8

    3.2.2 Mobile Application Management (MAM) ............................................................................. 8

    3.2.3 Mobile Content Management (MCM) .................................................................................. 8

  3.3 EMM and the ArcGIS Platform...................................................................................................... 9

4 Enterprise Security Mechanisms ...............................................................................................10

  4.1 Authentication ............................................................................................................................ 10

  4.2 Authorization .............................................................................................................................. 12

  4.3 Security Filters ............................................................................................................................. 13

  4.4 Encryption ................................................................................................................................... 14

  4.5 Certificates .................................................................................................................................. 15

  4.6 Logging and Auditing................................................................................................................... 16

5 ArcGIS Mobile Deployment Patterns .........................................................................................16

  5.1 ArcGIS Online .............................................................................................................................. 16

  5.2 Cloud-Based - Esri Managed Services .......................................................................................... 18

  5.3 Cloud-Based - Esri Cloud Images ................................................................................................. 19

  5.4 On-Premises - Reverse Proxy ...................................................................................................... 20

  5.5 On-Premises - Virtual Private Network (VPN) ............................................................................. 21

  5.6 On-Premises - Mobile Security Gateway .................................................................................... 22

  5.7 Hybrid Deployment ..................................................................................................................... 23

6 Conclusion ................................................................................................................................ 25

7 Acronyms ................................................................................................................................. 26
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 the ArcGIS Platform 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 whitepaper is a collection of strategies and deployment considerations; it is not a detailed step-by-step implementation guide. Background knowledge of the ArcGIS Platform, 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 – Web GIS

Web GIS is Esri’s recommended pattern for implementing GIS as a platform. One of the key concepts of Web GIS is 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 benefit from 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 Images**: 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](image-url)
Each of the four options support varying levels of risk and has different security options, which are discussed in more detail in section 5, while more detailed compliance information is available on Trust.ArcGIS.com. Although four separate Web GIS deployment models have been defined, hybrid deployments combining different models are also common. Selecting the appropriate Web GIS deployment model: ArcGIS Online, managed services, cloud images, on-premises, 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 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) Tailor Low 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 section 2.3. Organizations around the world utilize ArcGIS Online as the FedRAMP security controls map to ISO 27001 controls. Though ArcGIS Online’s cloud infrastructure is located within the United States, Esri is Privacy Shield certified which meets EU adequacy requirements and ArcGIS Online will be GDPR compliant when enforcement begins.

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 frequently 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 data collection 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 adverse to storing data in cloud-based services frequently supplement ArcGIS Online with one of the ArcGIS Enterprise deployment models addressed in this paper.

---

1 “Hybrid” implies using both ArcGIS Online and ArcGIS Enterprise together – see sections 2.3 and 5.7 for details.
2 See the Trust website and Cloud Security Alliance answers for ArcGIS Online for more details.
3 This is a US federal program for security validation and authorizations – see FedRAMP About Us.
4 The FedRAMP Tailored Low controls mapped to ISO 27001 controls is available on Trust.ArcGIS.com.
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 images, and on-premises solutions. It offers a flexible deployment model, allowing use that’s completely on-premises, connected or disconnected from the Internet, on physical hardware or in virtualized environments, in the cloud on Amazon Web Services or Microsoft Azure, or as an Esri managed service (see sections 5.2 and later).

ArcGIS Enterprise consists of four components:

- **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**: Back-end repository to store spatial content

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. For the purposes of this paper, the base deployment of ArcGIS Enterprise will be 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 the ArcGIS Platform, (see Figure 3). In a base deployment, ArcGIS Data Store is registered with ArcGIS Server. ArcGIS Server has been federated with Portal for ArcGIS and becomes its hosting server - 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. All four components can be installed on the same machine or in a multi-machine deployment; the latter option is recommended for production deployments.

---

5 For more product security details see [About configuring portal authentication](https://esri.com) and [How ArcGIS Server security works](https://esri.com).
6 To learn more, see [Base ArcGIS Enterprise deployment](https://esri.com).
7 Where ArcGIS Server has been configured to use Portal for ArcGIS’s security model, see [Federate an ArcGIS Server site](https://esri.com).
8 To learn more, see [Configure a hosting server](https://esri.com).
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 4).

- **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 Portal for ArcGIS are used, the former for public 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\(^9\) is leveraged to integrate GIS data across a network of participants, including those with membership in ArcGIS Online organizations, ArcGIS Enterprise, or both.

![Figure 4: Three Example Hybrid Deployments of ArcGIS Online with ArcGIS Enterprise](image)

There are many other possible hybrid deployment patterns\(^{10}\) and they will vary based on different business workflow requirements. Section 5.7 discusses the security considerations for hybrid deployments.

2.4 ArcGIS Mobile Apps

With the pervasive use of smart phones and tablets, many enterprise GIS deployments now include a mobile field component. GIS data and maps can now be easily taken outside the office and into the field to support mobile field workers for field data collection. Field personnel can work with the same authoritative datasets on their mobile devices, helping collect new data that can be easily shared with the office and monitored in real-time by dispatchers.

The ArcGIS Platform includes several mobile apps that allow users to sign into and work with ArcGIS Online and/or ArcGIS Enterprise\(^{11}\), (see Figure 5). These apps include the following:

---

\(^9\) To learn more about distributed collaboration, see the ArcGIS Online and ArcGIS Enterprise discussions for this topic.

\(^{10}\) Different Web GIS hybrid deployments are presented in Web GIS Patterns and Practices.

\(^{11}\) Apps sign into the Portal for ArcGIS component of ArcGIS Enterprise.
• **Workforce for ArcGIS**: Enables managing work assignments, and real-time field worker tracking
• **Collector for ArcGIS**: Provides map-centric data collection and editing, works offline
• **Survey123 for ArcGIS**: Supports form-centric data collection, works offline
• **Navigator for ArcGIS**: Enables routing, works offline
• **Explorer for ArcGIS**\(^\text{12}\)**: Supports viewing and markup of GIS maps, works offline

All these apps are available for both iOS and Android devices, and Collector for ArcGIS and Survey123 for ArcGIS are also available for the Windows platform. They can be used separately or collectively as part of a larger mobile workflow, depending on the organization’s business requirements.\(^\text{13}\)** 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

There are two additional mobile apps in the ArcGIS Platform that do not support field data collection workflows, but support other business use cases, (see Figure 5). These apps are mentioned in this document for completeness and are available for both iOS and Android devices. They will follow the same mobile implementation patterns described in later sections of this document. The apps are:

• **ArcGIS Business Analyst**\(^\text{14}\)**: Enables demographic and socio-economic data in the field
• **AppStudio Player for ArcGIS**: Displays custom apps built with *AppStudio for ArcGIS*\(^\text{15}\)

![Figure 5: ArcGIS Mobile Apps](image-url)

All these apps are designed to work with the ArcGIS Platform and support all Web GIS deployment models: SaaS, managed services, cloud images, on-premises, or a hybrid variation. Some apps offer support for more security options (see section 4.1) than others. Please check the online help

---

\(^\text{12}\)** Explorer for ArcGIS can open and view publicly shared maps without requiring a login for access.

\(^\text{13}\)** To learn more about the ArcGIS Mobile Field Apps, see *Apps for the Field*.

\(^\text{14}\)** Deploying this app with ArcGIS Enterprise has supplementary requirements, see *Business Analyst Server – Overview*.

\(^\text{15}\)** Enables you to create native mobile apps without programming, to learn more see *AppStudio for ArcGIS product page*. 
documentation for each app for details.\textsuperscript{16} While the ArcGIS mobile apps offered as part of the ArcGIS Platform meet the needs of most customers, Esri also offers mobile Runtime SDKs to facilitate custom application development.\textsuperscript{17} As ArcGIS Mobile apps are built with mobile Runtime SDKs, concepts regarding Enterprise Mobile App Management will directly apply to these custom solutions.

3  Enterprise Mobile App Management

Just like any other app found in public app stores, ArcGIS mobile apps are designed for ease of use, allowing general users to be up and running within minutes. In alignment with 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 will need to 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 the Enterprise

Before jumping into 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 all) of the ArcGIS mobile apps connecting to either ArcGIS Online and/or ArcGIS Enterprise, (see Figure 6). This is the Web GIS deployment pattern with the ArcGIS Platform, supporting GIS workflows in the field.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure6.png}
\caption{ArcGIS Mobile Apps Connecting to ArcGIS Online and/or ArcGIS Enterprise}
\end{figure}

\textsuperscript{16} Help documentation for the Apps: ArcGIS Help – Apps.
\textsuperscript{17} To learn more, see the ArcGIS Developers site.
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?
- Where will the GIS data and content reside? Can they be stored in the Esri cloud infrastructure, or must they reside only within the organization’s infrastructure? Can they be in a combination of the two?
- How will mobile app end users access the organization’s internal network/infrastructure? What is the organization’s current IT security model/infrastructure?
- When accessing the organization’s internal network, is a single sign-on (SSO)\(^\text{18}\) user experience a requirement?
- What hardware resources (e.g., machines and network infrastructure) are available, in terms of both mobile devices and infrastructure technology?
- What IT personnel resources are available to support this deployment (in terms of both setup and maintenance)?
- 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 5).

There are many potential security risks and mitigations with respect to using mobile technology as part of an organization’s business workflows; a comprehensive list can be found in the open web application security project (OWASP) Mobile Top 10 list. A key strategy to address these risks is to use an EMM solution in addition to ArcGIS Platform security settings.

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.\(^\text{19}\)

EMM can be separated into three different conceptual components:

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

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.

\(^{18}\) SSO means a user would only login once to access resources, see Understanding Enterprise Single Sign-On.

\(^{19}\) To learn more, see How to choose the right enterprise mobility management tool.
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 the Apple App Store and/or Google Play.

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) 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 blacklist/whitelist; email configurations; device encryption; location tracking; WiFi configurations; and app, services, and device feature restrictions. These options will vary between different MDM software vendors.

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 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.

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 that the ArcGIS mobile apps do not support MAM’s “app wrapping”, where a dynamic library is explicitly added to help control certain aspects of the application.

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.

---

20 To learn more, see [VPNs for Beginners](#).
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 Platform

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 component. The MDM aspect of the EMM solution is the main component that the ArcGIS mobile apps interact with.

An organization’s MDM software can connect directly to the Apple App Store and/or Google Play. The ArcGIS mobile apps in the stores are either registered or uploaded (depending on the MDM vendor) to 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 is 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 is focused on providing tools and best practices for native capabilities in mobile operating systems, (see Figure 7).

![How AppConfig works in the Enterprise](image)

*Figure 7: AppConfig Community – MDM*  

21 Source: AppConfig Community.
The guidelines provide a more consistent, open and simple way to configure and secure mobile apps that eases and advances mobile adoption in business. Below are resources on the capabilities that can be enabled:

- iOS Capabilities Summary
- Android Capabilities Summary

Support for the various app configuration and management properties defined by the AppConfig Community will differ among the ArcGIS mobile apps, but nearly all of them support the following capabilities:

- **App Tunnel**: Leverage “per app VPN” capability available in most commercial VPN solutions
- **App Security - Remotely Wipe App**: EMM can remotely wipe an app from a device

Esri updates the ArcGIS mobile apps frequently and is continually working to support additional capabilities in future releases. The ArcGIS Platform has 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. More details on EMM deployments with the ArcGIS Platform are discussed in section 5.4. A discussion of how AppConfig and MAM can be leveraged with the Explorer for ArcGIS App may be helpful to understand Esri’s roadmap regarding this guidance.

4  Enterprise Security Mechanisms

In this section, common security mechanisms utilized across an enterprise are discussed in the context of the ArcGIS Platform. 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

Authentication is the process of verifying the identity of users 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 6). 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) protocols. The HTTPS option is recommended to ensure secure communications. 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?
- Does the organization have specific methods for providing enterprise network credentials (e.g., VPN or mobile security gateway)?

---

22 Exception: ArcGIS Business Analyst does not currently support these properties.
23 To learn more, see Understanding HTTP Authentication and What is HTTPS?.
24 See details in section 5.3.
25 See details in section 5.4.
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\(^{26}\) 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 that unsecured GIS resources (i.e., content shared with the “public”) are typically set to \textit{Anonymous} access.

\textbf{ArcGIS Online has three authentication options:}

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in security</td>
<td>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.</td>
</tr>
<tr>
<td>Enterprise logins with security assertion markup language (SAML)(^{27}) authentication</td>
<td>In this option, the ArcGIS Online organization is registered with a third-party identity provider (IDP)(^{28}) 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.</td>
</tr>
<tr>
<td>Social Logins</td>
<td>Authentication via a social network like Google or Facebook.</td>
</tr>
</tbody>
</table>

\textbf{ArcGIS Enterprise (via the Portal for ArcGIS component\(^{29}\)) offers several authentication options:}

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-tier authentication(^{30})</td>
<td>This uses integrated Windows authentication (IWA) or Lightweight Directory Access Protocol (LDAP)(^{31}), which provides an 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 server for validation. When mobile devices access the internal enterprise network, they will automatically have access to the Portal for ArcGIS website.</td>
</tr>
<tr>
<td>Portal-tier authentication</td>
<td>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(^{32}), they need to provide a valid Portal named user account.</td>
</tr>
<tr>
<td>Enterprise logins with SAML authentication</td>
<td>In this option, Portal for ArcGIS is registered with a third-party Identity Provider 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.</td>
</tr>
</tbody>
</table>

\(^{26}\) See Esri SSA FAQ document \textit{ArcGIS Platform Enterprise Logins via SAML 2.0}.

\(^{27}\) To learn more, see \textit{SAML v2.0 specification}.

\(^{28}\) To learn more, see \textit{Creating SAML Identity providers}.

\(^{29}\) ArcGIS Server must be federated with Portal for ArcGIS to enable a hosting server deployment. See footnote 6 for more.

\(^{30}\) ArcGIS Enterprise supports PKI authentication, but is not supported by ArcGIS mobile apps and not discussed further here.

\(^{31}\) To learn more, see \textit{Integrated Windows Authentication} and \textit{What is LDAP}?

\(^{32}\) The logins are enterprise users (e.g., Windows Active Directory or LDAP) as the identity store.
User credential information is stored in an identity store\textsuperscript{33}: 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 and roles. A “user” is an end user of a client application accessing the network and is identified by a set of credentials. A “role” is a logical grouping of users; users in the same role typically have the same permissions assigned. In theory, a user can belong to more than 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.

4.2 Authorization

After a user has been authenticated, the authorization model will determine what resources the user can access within the ArcGIS Platform, 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 website is often called the portal website. Items in the portal website such as web apps, web maps, web scenes, and web layers can be logically aggregated into groups for organizational purposes. Groups\textsuperscript{34} in the portal website can be used to control user access to different types of GIS data and contents in the organization (see Figure 8).

![Figure 8: Configuring Authorization Settings](image)

Within the portal website, there are two levels and several portal role options. Levels determine capabilities that are licensed for a user and portal roles define specific functionality.

**Membership Levels in a Portal**

- **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 mobile field apps involve data collection; therefore, field users should be assigned level 2 membership.\textsuperscript{35})

\textsuperscript{33} This is also sometimes termed “identity provider”.

\textsuperscript{34} To learn more about Groups in a portal website, see What is a group?.

\textsuperscript{35} Explorer for ArcGIS is the exception, see footnote 9.
Portal Website Roles

- **Viewer**: Privileges to view items such as maps and apps that have been shared with the member. Join groups owned by the organization. Use network analysis and geocoding. Members assigned the Viewer role cannot create, own, share content, or perform analysis. The Viewer role can be assigned to level 1 or level 2 accounts.
- **User**: Viewer privileges plus the ability to see a customized view of the site, use the organization's maps, apps, layers, and tools, and join groups owned by the organization. Members assigned to the User role can create maps and apps, add items, share content, and create groups. The User role can be assigned to level 2 accounts.
- **Publisher**: User privileges plus the ability to publish features and map tiles as hosted web layers. Members assigned the Publisher role can perform standard feature analysis on layers in maps. The Publisher role can be assigned to level 2 accounts.
- **Administrator**: Publisher privileges plus privileges to manage the organization and other users. An ArcGIS organization subscription must have at least one administrator. However, there is no limit to the number of roles that can be assigned within an organization. For example, if an organization has five members, all five members can be administrators. The Administrator role can be assigned to level 2 accounts.36

The previous list of portal website roles are the default roles available in ArcGIS Online and ArcGIS Enterprise (Portal for ArcGIS component). However, portal website administrators can also create and define custom portal roles37 – which provides them with more granular control on permission settings for their users.

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. 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.38
- **Demilitarized zone (DMZ)** 39: 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 9, one strategy is to deploy the ArcGIS Web Adaptor on a third-party web server; both are located in the DMZ, while the remaining ArcGIS Enterprise components are located behind a firewall beyond the DMZ. This ensures that Portal for ArcGIS, ArcGIS Server, and the ArcGIS Data Store are protected behind multiple firewalls. More on this deployment will be covered in section 5.2.

---

36 To learn more about levels and roles in a portal website, see [Levels, roles, and privileges](#).
37 To learn more, see [Custom roles](#).
38 To learn more, see [What is a firewall?](#).
39 To learn more, see [DMZ (Computer Networking)](#).
Network ports: Communication access points for a server to the network. The ArcGIS Enterprise components use the standard ports 80 (unsecured) and 443 (secured) for communication. As a best practice, port 443 should be used to ensure HTTPS communication protocols. Using non-standard ports is not recommended.

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 of 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 Trust.ArcGIS.com. This includes security guidance for server-based products as well as online offerings. Some organizations go so far as to filter the domains they allow for communication, which can be disruptive if not configured based on our guidance.

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, there are two aspects of encryption to consider:

Encryption at rest: By default, ArcGIS mobile apps are not separately encrypting content when the data is at rest on the device. The apps will defer to the operating system of the mobile device to perform encryption. Data on an iOS device running an operating system later than iOS4 is always encrypted. Android’s data encryption feature is typically disabled by default, but can be enabled on-demand. This function could also be enforced by using MDM software options.

See Esri SSA briefing on ArcGIS Online Domain Requirements and recommendations.
Encryption in transit\textsuperscript{41}: Data can be encrypted in transit by requiring HTTPS across the enterprise GIS. Both ArcGIS Online and ArcGIS Enterprise have options to enforce HTTPS across all transactions beyond operations requiring user authentication. MDM software also enables leveraging the “per-app VPN” capability available in most commercial VPN solutions through configuration. This feature is available in iOS 9 and later, and in Android 5.0 and later.

4.5 Certificates
To ensure security between different components of an enterprise GIS, in HTTPS protocol communications, security certificates\textsuperscript{42} are used to verify and confirm that endpoints in a transaction are legitimate and valid. It is strongly recommended that domain and/or commercial Certificate Authority (CA) certificates be used.

Most 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 for importing a valid CA certificate into their mobile devices.

All secure connections to the organization’s internal network starts with authentication to verify the server's identity. 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, which are files that deliver settings to the devices. Each profile consists of 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 has the same format.
3. **Simple Certificate Enrollment Protocol (SCEP)\textsuperscript{43}**: 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. See the links below for examples showing how to import into and install a valid CA on a mobile device when not using EMM:

- [How to install a CA Certificate on your iOS Device](#)
- [How to install a CA Certificate on your Android Device](#)

\textsuperscript{41} See Esri SSA briefing on [ArcGIS Platform SSL/TLS Support and Configuration](http://www.arcgis.com).
\textsuperscript{42} To learn more, see [What are Certificates?](http://www.arcgis.com).
\textsuperscript{43} To learn more, see [Simple Certificate Enrollment Protocol Overview](http://www.arcgis.com).
4.6 Logging and Auditing

Logging involves recording events of interest collected from the enterprise 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 particular transaction that occurred. Logging and auditing can be facilitated at the following levels for mobile devices:

- At the device level, as facilitated by the 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 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 and 4.1, intended to help guide security considerations, should be discussed with senior management 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 is worth noting that the following mobile deployment patterns are not necessarily mutually exclusive. For example, an organization could deploy the ArcGIS Platform with a hybrid deployment as mentioned in section 2.3. In that case, there could potentially be a deployment of ArcGIS Online in combination with one of the other on-premises or cloud-based deployment options. Hybrid deployments are covered in section 5.7.

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

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Implementation Difficulty</th>
<th>Relative Risk-Level</th>
<th>Common Data Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcGIS Online</td>
<td>Low</td>
<td>Low - Moderate</td>
<td>Public / Hybrid-metadata</td>
</tr>
<tr>
<td>Cloud – EMCS</td>
<td>Low</td>
<td>Low - Moderate</td>
<td>Low - Moderate</td>
</tr>
<tr>
<td>Cloud – Images</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Low by default</td>
</tr>
<tr>
<td>On-Prem – Rev Proxy</td>
<td>Moderate</td>
<td>Moderate - High</td>
<td>Low - Moderate</td>
</tr>
<tr>
<td>On-Prem – VPN</td>
<td>Moderate - High</td>
<td>Low - Moderate</td>
<td>Moderate - High</td>
</tr>
<tr>
<td>On-Prem - Gateway</td>
<td>Moderate - High</td>
<td>Low</td>
<td>Moderate - High</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Moderate</td>
<td>Low - High</td>
<td>Low - High</td>
</tr>
</tbody>
</table>
5.1 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 10). Three authentication options are available: built-in security, social logins, or enterprise logins with SAML.

![ArcGIS Mobile Apps](image)

**Figure 10: ArcGIS Mobile Apps using ArcGIS Online pattern**

**Risk Level**: 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 currently not available. However, this level of isolation is frequently not desired.

**Data**: This offering is ideal for public 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 will higher sensitive data frequently implement a hybrid approach with ArcGIS Enterprise (using the on-premises or cloud option), see section 5.7.

**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:**
- All GIS data and content is stored in the cloud and not in the organization’s infrastructure (unless using a hybrid deployment)
- May need to export data from organization’s infrastructure to ArcGIS Online
- 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)
- 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.

| 44 Risk level is a general indicator of how “risky” a pattern is relative to others in this paper. |
5.2 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 11). This implementation is completely managed by Esri for the organization. The operational logistics are performed by Esri, but the organization owns and uses the ArcGIS Platform to support its business workflows.

Figure 11: ArcGIS Mobile Apps using Esri Managed Services

Esri Managed Cloud Services (EMCS) Advanced Plus\(^{45}\) is an offering that provides security benefits that meet strict Federal Risk and Authorization Management Program (FedRAMP) Moderate security requirements\(^{46}\). 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 Web Application Firewall (WAF) to mitigate against common web application attacks such as cross-site scripting (XSS)
- FIPS 140-2 compliant encryption\(^{47}\) 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
- Yearly 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 don’t provide the bulleted security benefits listed above.

**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.

---

\(^{45}\) To learn more, see [Esri Managed Cloud Services](#).

\(^{46}\) To learn more, see [FedRAMP](#) and [Trust.ArcGIS.com - Compliance](#).

\(^{47}\) To learn more, see [FIPS PUB 140-2 standard](#).
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 enterprise 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

5.3 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 12). This option is useful for customers that want to take on managing and maintaining an ArcGIS Enterprise deployment in the cloud.

Risk Level: Moderate (This risk can be mitigated by a customer deploying and managing extensive security infrastructure beyond the 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.48

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.

48 See Esri’s Security On Amazon Web Services for details.
**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

### 5.4 On-Premises - Reverse Proxy

In this pattern, the ArcGIS Web Adaptor serves as a reverse proxy, is deployed in the DMZ, and passes mobile app requests to Portal for ArcGIS and ArcGIS Server (see Figure 13). 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 enterprise 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 grant a more granular level of access control via ProxyPass directives or routing rules. This pattern is the lowest-cost ArcGIS Enterprise approach when compared to the other patterns that follow, but it presents significant risk to the enterprise internal infrastructure.

**Risk Level:** Moderate to High – This is the lowest cost ArcGIS Enterprise implementation, but it presents significant 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.

---

To learn more, see [Apache - Reverse Proxy Guide](#).
Advantages:
- Lower cost (compared to the other on-premises ArcGIS Enterprise deployment patterns) – Most organizations typically already have a web server
- More authentication options available
- All GIS data and content is stored within the organization’s infrastructure
- No or, if required to support specific workflows, minimal need to copy data to ArcGIS Online
- 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 Windows Active Directory/LDAP
- Technical expertise needed among the organization’s staff to manage hardware and software.

5.5 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 14). 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 14: ArcGIS Mobile App Traversing VPN**

Risk Level: Low to Moderate – This enables a dedicated tunnel for your enterprise communications reduces risk, however it can have a significant 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 being stored within the organization’s infrastructure
- No or, if required to support specific workflows, minimal need to copy data to ArcGIS Online
- 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
- All traffic from mobile devices being routed through the corporate network when using VPN
- Contractors or semi-trusted users being given more access to the internal enterprise network than required (which may be a security issue)
- Technical expertise needed among the organization’s staff to manage hardware and software

5.6 On-Premises - Mobile Security Gateway

In this pattern, mobile device clients are authenticated with a mobile security (or application) gateway (see Figure 15). 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.

**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 not being 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 or, if required to support specific workflows, minimal need to copy data to ArcGIS Online
- Resources only available for the organization (not shared)
Disadvantages:
- Medium to higher cost (compared to the other deployment patterns) – if 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
- Hardware and software is managed by staff with technical expertise

5.7 Hybrid Deployment
As mentioned in section 2.3, a common pattern is to use a hybrid of ArcGIS Online and an on-premises deployment option (sections 5.4 – 5.6). Figure 16 illustrates one common ArcGIS Platform hybrid deployment architecture.

![Figure 16: ArcGIS Mobile Using a Hybrid Deployment – Content Stored in Cloud and On-Premises](image)

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 the ArcGIS Platform 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 Platform hybrid deployment architecture is shown in Figure 17. 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 at ArcGIS Enterprise.  

![Diagram of ArcGIS Mobile Using a Hybrid Deployment – Registering services with ArcGIS Online]

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 ArcGIS 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.

Note that many hybrid deployment variations are possible and a comprehensive discussion is outside the scope of this document (see footnote 7).  

---

50 To learn more, see Add items from the web.
6 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 the ArcGIS Platform components, EMM offerings, IT/security mechanism options, and the various pros and cons of the deployment patterns. The intention of this whitepaper is to make the design process easier to deliver the level of security an enterprise demands for mobile applications today.

The Software Security & Privacy team would like to give a note of thanks for the broad input and reviews from fellow teams at Esri, customers, and even distributors. Esri intends to update this document in the future, so feel free to provide your comments and suggestions to SoftwareSecurity@Esri.com.
7  Acronyms
This section lists acronyms that are used in this whitepaper.

• 3PAO: Third-Party Assessment Organization
• CA: Certificate Authority
• DISA: Defense Information Systems Agency
• DMZ: Demilitarized Zone
• EMM: Enterprise Mobility Management
• EU: European Union
• FISMA: Federal Information Security Management Act
• FedRAMP: Federal Risk and Authorization Management Program (Based on FISMA law)
• GDPR: General Data Protection Regulation
• HTTP: Hypertext transfer protocol
• HTTPS: Hypertext transfer protocol secure
• IdP: Identity Provider
• IDS: Intrusion Detection System
• ISO: International Standards Organization
• 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
• 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
• SIEM: Security Information & Event Management
• SSA: Security Standards & Architecture team
• SSO: Single-Sign-On
• STIG: Security Technical Implementation Guide
• VPN: Virtual Private Network
• WAF: Web Application Firewall
• XML: Extensible Markup Language
• XSS: Cross-site Scripting
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