# Introduction

Apperian App Management is Arxan's mobile application management (MAM) platform that uses cloud-based software to support the complete mobile app lifecycle by interconnecting backend modules with a unified administrative portal.

To get up and running quickly, see Quick Start. For white papers, demo videos, and much more, see www.arxan.com/apperian.

How Apperian Works

Modules contain services and capabilities provided by Arxan and third-party partners; Apperian App Management is the "glue" that pulls it all together into a coherent management framework. Its modular architecture makes Apperian highly scalable and customizable, allowing organizations to use only those modules that make sense in their mobile environment.

The following diagram illustrates the primary components:
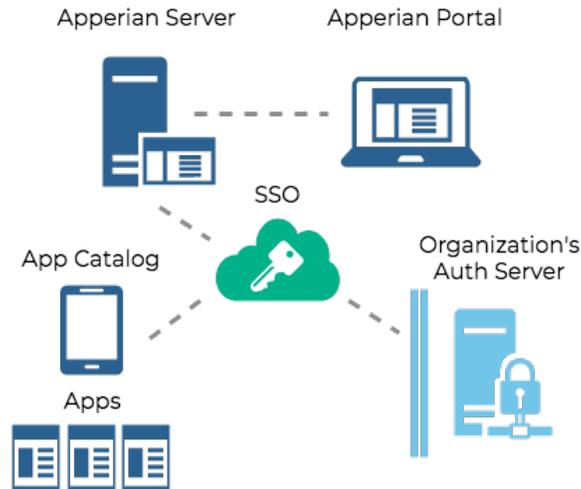
Apperian Server

The Apperian Server is a SaaS (Software as a Service) configuration hosted in the cloud. It manages each stage in the MAM lifecycle with a cohesive set of functions that support an enterprise's best practices to ensure a robust and secure deployment.

Apperian throughout the MAM Lifecycle		
On-board	During this stage, you define the content of your enterprise app store ("App Catalog"). An App Catalog can include many types of apps: native apps, links to public apps and web apps, device profiles and email configuration profiles, and "hybrid apps" (web apps packaged as native apps). In addition to the app, Apperian can manage associated content, such as screenshots and training videos, to enrich the mobile users' experience. You can upload native apps via the Admin Portal web interface or through the Apperian publishing API. Using plugins to Apperian's partner's platforms, developers can publish apps directly to Apperian from a development environment.	• Add an Application • Hybrid Apps (Delivering a Web App as a Native App) • Media File Types • Managing App Catalogs • Customize the App Catalog

Inspect	Before making apps available to your users, you want to know they are safe. Apperian's App Inspection is like a code x-ray that screens an app for risky behavior and vulnerabilities, such as malware and Trojans, and generates a detailed report along with remediation recommendations.	• Inspect an Application • Application Inspection Report
Protect	You can use policies to provide added layers of security, management, and measurement capabilities to support corporate requirements and enhance your users' mobile experience. Policies are applied *post-development*, so there is no change to the original source code, no need for an SDK, and no extra work for you. And because the protection is provided as a layer *around* the app, it does not alter the functionality or performance of the app, nor does it compromise the user experience in any way.	• Managing Application Policies • About Policies • Apply Policies to an App
Sign	Signing is a packaging process by which an app is sealed and identified as yours. Most apps need to be signed before they can be distributed to your mobile users. For more information, see About Signing.	• About Signing • Signing Prerequisites • Sign an App (Admin Portal) • Sign an App (Signing Package)
Deploy	Once an app has been inspected, protected, and packaged, it is ready for distribution. Using role-based user groups, you specify which apps users see in their App Catalog. You can also use a Direct Download URL to distribute a single app to someone who is not an Apperian user and does not have access to the App Catalog. Apperian also makes distributing updates easy; when you upload a new version of an app, Apperian sends a push notification to App Catalog users' devices so they know the update is available for download.	• Managing Users • Managing Groups • Edit or Update an Application • Managing Application Updates • Delivering Applications via a Direct Install URL • Push Notification for an App Catalog

The Apperian Server ensures that a large number of simultaneous users can download and update apps quickly. Commonly downloaded files are situated on a content delivery network to ensure fast delivery at peak demand times.

The Apperian Server supports a variety of authentication options. An account can authenticate its Apperian users with a built-in "white list" invitation system, or implement an SSO (Single Sign-On) solution to integrate with Apperian as well as other service providers. SSO—Apperian's preferred authentication method—leverages industry standards, such as SAML 2.0, and your enterprise's existing authentication method.

Back to Top

Apperian App Catalog (The Mobile User's View)

An App Catalog enables users to see all the apps that they are authorized to access. From an App Catalog, users can install an app and view detailed information for each app, including screenshots and related media such as PDF files and videos. Users can also search for apps, like, dislike, and review apps, and install updates. Apperian supports a native App Catalogs for a variety of devices, as well as a web App Catalog that can run in a browser on any device. For a list of specific devices, see Supported Platforms.

The following example shows the default, Apperian-branded iOS App Catalog, but both native and web App Catalogs can be customized to incorporate your corporate brand.
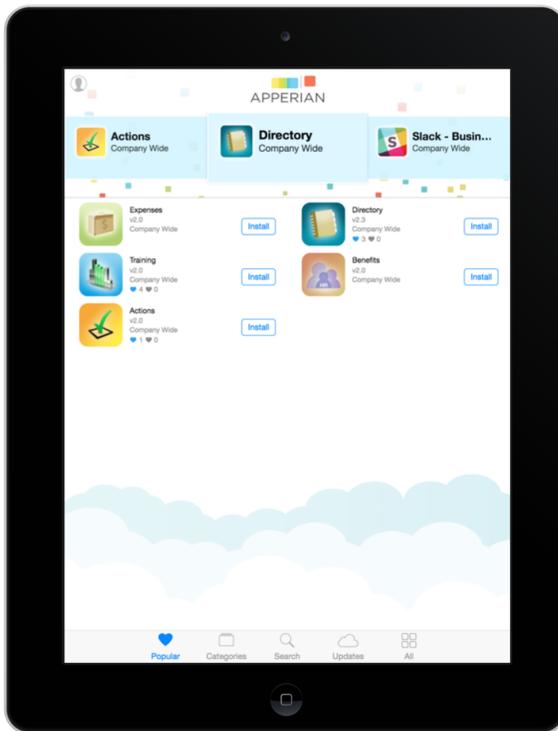
## Apperian Admin Portal (The Administrator's View)

The Apperian Admin Portal is a web-based console that makes it easy for IT administrators to manage their enterprise mobile environment. In the Admin Portal, administrators can:

- Manage the apps available in the App Catalog
    - Provide role-based access
    - Inspect apps
    - Apply policies
    - Remove apps from devices
- Add and manage users, groups, and app categories
- View app data in reports
- And much more
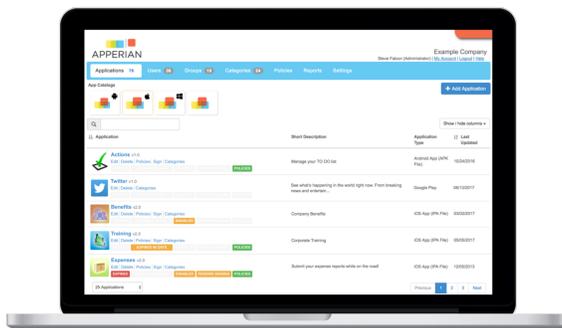
Apperian API

Through web services APIs, customers and partners have the ability to integrate Apperian with existing IT solutions, as well as extend new capabilities on top of the platform.

For a complete reference to Apperian's REST API, see Index of APIs.

To add and update applications in Apperian through the API, see Apperian Publishing API Guide.

Back to Top

Apperian Workflow

The following table lists activities in a typical Apperian platform implementation workflow. You may not choose or need to perform all of these activities.

Step	Activities	More Info
Brand App Catalogs	• Customize user interface components of your App Catalog to incorporate corporate branding and enhance your users' experience. Customization options depend on the type of App Catalog (Web, iOS, Android). • Work with Customer Support to customize the EULA displayed to App Catalog users.	Branding App Catalogs
Create Groups and Categories	• Create user groups to control access to apps in the App Catalog. When you add an app, you specify which groups of users can access the app. When you create a user, you place the user in groups. • Create categories to group and classify apps. Users can display apps by category.	Managing Groups Managing Categories
Add and Organize Applications	• Add the mobile apps that you want to make available to users in your enterprise App Catalog. Along with an app, you can upload associated files, such as screenshots and training videos. When you first add an app, you may wish to disable it in the App Catalog until you have inspected and applied usage and security policies to it. • Create a hybrid app to deliver a web app packaged as a native app. • Associate apps with one or more groups to control user access. • Associate apps with one or more categories to organize apps in a user's App Catalog. • Select applications to feature in the Featured Apps section of the iOS App Catalog.	Add an Application Hybrid Apps (Delivering a Web App as a Native App) Select Featured Apps for the App Catalog
Protect, Inspect, and Approve Applications	• Apply security and usage policies to individual apps in your Apperian account to apply multiple layers of protection around any app that needs more security. Depending on which policies you apply, you may need to re-sign the app after wrapping it. You can do this directly through the Admin Portal. • Inspect apps to screen for risky behavior and vulnerabilities, such as malware, trojans, and intellectual property exposure. When you request an inspection, Apperian returns an Inspection Report that serves as a powerful mobile app risk management tool. • Distribute a test version of an app to specific reviewers to ensure that the app meets quality and security standards. • After an app has been protected, inspected, and approved and you are ready to make it available to your end users, enable it in the App Catalog.	Apply Policies to an App Sign an Application Inspect an Application Application Versions Disable or Enable an Application
Add and Organize Users	• Choose the method that Apperian will use to authenticate users. You can use a built-in "white list" invitation system, or you can leverage your existing infrastructure with Single-Sign On. • Add users to the Apperian platform. You can add one user at a time or you can add multiple users at once by uploading a Comma-Separated Values (CSV) file. If you implement Single-Sign On (SSO) for authentication, Apperian automatically provisions users. • Place users in groups to control access to apps. • Delete users that should no longer have access to the App Catalog.	Specify the User Authentication Method Single Sign-On with Apperian Managing Users Managing Groups Delete a User

Secure and manage Applications and Application Data	• Update apps when new versions become available. • Enforce mandatory update compliance. • Delete an obsolete app from the Apperian platform so it no longer appears in the App Catalog. • Enable/disable a device.	Edit or Update an Application Managing Application Updates Delete an Application Delete Application Data from a Device
Monitor Apps and Send Messages to Users	• Check inventory of all apps installed on a device, as well as list apps that were installed from the App Catalog. • Track the number of downloads and usage of an app. • Run reports to track and monitor information about App Catalog users and access. • Send messages (notifications) to all members of a particular group or all users of a particular app.	View User Details Track Application Usage Running Reports Sending Notifications to Users
Manage User Reviews	• View app rating details and manage user reviews	App Ratings and Reviews

Back to Top