

**Air watch (VMware)**

**A high-level guide of AirWatch**

5/9/2017

MagikMinds Software Services Pvt. Ltd.

**Contents**

[What is AirWatch? 3](#_Toc482198624)

[Products & Solutions: 3](#_Toc482198625)

[Why AirWatch? 3](#_Toc482198626)

[6 Reasons Why Businesses Use AirWatch: 3](#_Toc482198627)

[Solutions: 4](#_Toc482198628)

[Mobility Management: 5](#_Toc482198629)

[a) Bring Your Own Device (BYOD): 5](#_Toc482198630)

[b) Enterprise Mobility Management (EMM): 6](#_Toc482198631)

[c) Mobile Device Management (MDM): 6](#_Toc482198632)

[d) Unified Endpoint Management (UEM): 8](#_Toc482198633)

[Mobile Productivity 9](#_Toc482198634)

[e) Mobile Application Development 9](#_Toc482198635)

[f) Mobile Application Management 9](#_Toc482198636)

[Enterprise Security 10](#_Toc482198637)

[g) Identity Management 10](#_Toc482198638)

[h) Mobile Security 11](#_Toc482198639)

[i) VMWare Mobile Security Alliance (MSA) 12](#_Toc482198640)

[Products 13](#_Toc482198641)

[Airwatch: 13](#_Toc482198642)

[AirWatch Express: 13](#_Toc482198643)

[Workspace ONE: 13](#_Toc482198644)

# **What is AirWatch?**

**VMware AirWatch** is an enterprise mobility software provider based in Atlanta. AirWatch, a division of virtualization vendor VMware, provides technologies that help IT administrators deploy, secure and manage mobile devices, applications and data, as well as Windows 10 and Apple Mac computers. These products work thanks to a combination of an app installed directly on the endpoint device -- called the AirWatch Agent -- and back-end software that allows IT to set and enforce policies.

VMware AirWatch's flagship product is its enterprise mobility management software, which aims to protect corporate applications and data accessed from any device on any network.

As of 2016, AirWatch became fully integrated into VMware and completely re-branded itself as VMware AirWatch.

# **Products & Solutions**:

AirWatch has over 16,000 customers in 150 countries, and supports Android, Apple iOS, Apple TV, BlackBerry, Chrome OS, Mac OS X, Symbian, Tizen, and Windows platforms. Its product and solutions offerings include:

Enterprise mobility management:

* Bring your own device
* Container management
* Mobile security
* Mobile device management
* Mobile email management
* Mobile application management
* Mobile browsing management
* Telecom management
* Laptop management
* Rugged device management
* Multiuser management
* Identity management

# **Why AirWatch?**

AirWatch is widely recognized as the leading platform for enterprise mobility. Customers trust in products to advance their mobility strategies and transform their businesses.

## ****6 Reasons**** Why Businesses Use AirWatch:

* ***Comprehensive Portfolio:***

AirWatch is a solution for all end-user computing needs like apps& identity, Desktop & Mobile, Management & Security to drive digital transformation for your organization.

* ***Innovate Faster:***

**AirWatch is always a step ahead with the latest mobile innovations. It** pushes the boundaries with what's possible in enterprise mobility - keeping you ahead of the competition. Be agile with automatic upgrades and same-day support for the latest operating systems to keep your employees at maximum productivity.

* ***Market Leader*:**

Industry analysts consistently rank AirWatch as the clear choice for EMM (*Enterprise Mobility Management*) year after year. This platform is perfectly positioned to help your business prepare for the next generation of digital transformation.

* ***Built to Scale:***

Your mobility initiatives continue to evolve. AirWatch is built from the ground up to seamlessly scale as your deployment grows in numbers and complexity.

* ***Open Eco System:***

AirWatch platform is flexible and plays well with others. It built the most comprehensive mobility ecosystem in the industry so that AirWatch platform easily integrates with your existing infrastructure. Simply plug-and-play to make the most of your current investments.

* ***Security:***

It enables Security beyond to the endpoint. Its multi-layered approach to security encrypts sensitive company data and secures access from the user all the way to the network.

# **Solutions:**

**Embrace Mobility + Enhance Productivity + Improve Security**

Unify management of all end points into one comprehensive platform,

Provide users with a set of secure Productivity apps to increase efficiency,

Enable end-to-end Security from the user all the way to the network.

**Mobile technology** is making its presence felt around the world and is revolutionizing the way business is done by improving business processes, increasing productivity and enhancing the customer experience.

As mobility becomes critical to overall business strategy, you need a **solution** to officially secure, configure and manage all your mobile devices deployed across your organization.

AirWatch provides the most comprehensive solutions for securing and managing complex mobile deployments. It enables you to officially manage multiple business units and locations in a single console with the ability to dedicate access and management across your organization, and no matter what devices your organization is supporting today AirWatch provides the most extensive multi OS management solution across all the leading mobile operating systems. With AirWatch’s [MDM](http://www.air-watch.com/solutions/mobile-device-management) (Mobile Device Management) solution you can enable mobility to drive value for your business.

AirWatch has consequently turned out to be a success in the management of mobile devices, owing to its manifold features and impeccable functionality ranging from configuration to support.

The following points account for AirWatch becoming one of the leaders in **MDM**:

## Mobility Management:

Support every endpoint and every user from a single management console. Explore solutions for mobility management are as follows:

### **Bring Your Own Device (BYOD):**

Separate and protect Corporate data on employee-owned devices with BYOD.

* ***In-the-moment* *productivity-*** Increases the productivity with BYOD program that allows employees to complete work tasks from the personal device that never leaves their side.
* Enable employees to access any app from the convenience of their own mobile device with VMware Workspace ONE.
* Give users access to critical business apps through a single catalog across any device.
* Automatically authenticate users for all apps at once with mobile single sign-on.
* Provide frictionless access to company email, calendar, contacts, content repositories, intranet sites, social network and chat with our suite of consumer-simple mobile **productivity apps.**
* ***Data Security & Privacy-*** Secure your corporate data while providing IT teams with the tools for privacy controls.
* Leverage native OS platform features without managing the device.
* The AirWatch Privacy First framework provides controls to IT to enforce company-specific privacy policies.
* Encrypt and remotely wipe corporate data leaving personal info untouched.
* Built-in privacy app educates users about work data separation to increase **BYOD** program adoption.
* ***Adoption & Self Service-*** Once your BYOD strategy is in place, make your users comfortable enough to participate and empower them to troubleshoot simple issues on their own.
* Push relevant and contextual messages, offers and alerts to employee-owned devices from the console.
* Suggest useful apps based on user role and remind users to update existing apps.
* Use AirWatch custom messaging framework to tailor system messages to meet your specific needs.
* Notify users when their device is out of compliance and tell them how to fix it through a self-service process.

### **Enterprise Mobility Management (EMM):**

Transform Business with Comprehensive Enterprise Mobility Management. EMM typically involves some combination of mobile device management ([**MDM**](http://searchmobilecomputing.techtarget.com/definition/mobile-device-management)), mobile application management ([**MAM**](http://searchconsumerization.techtarget.com/definition/mobile-application-management)) and mobile information management ([**MIM**](http://searchconsumerization.techtarget.com/definition/mobile-information-management-MIM)). MDM focuses on locking down mobile devices, while MAM focuses on controlling which users can access which applications and MIM focuses on allowing only approved applications to access corporate data or transmit it.

* ***Unified Endpoint Management-*** Stop managing multiple tools and simplify your mobility program with EMM.
* Gain visibility into all smartphones, tablets, laptops, rugged, peripheral and IoT endpoints across Android, iOS, macOS, QNX, Tizen, Windows CE and Windows 10 platforms.
* Manage the device from initial on-boarding, configure apps and settings, apply security policies and remotely troubleshoot issues.
* Support all use cases across your organization including corporate-owned, BYO and line of business such as kiosks or shared devices.
* Protect users’ personal data and comply with global regulations with our privacy first framework.
* ***Mobile Productivity-*** Engage users with mobile-optimized apps that provide a consumer-simple experience with enterprise-grad security.
* Give users seamless access to all apps – native, web, remote – through a unified app catalog with built-in single sign-on (**SSO**).
* Provide a better-than-native email experience with turbo-charged productivity features and integrated mail, calendar and contacts with VMware Boxer.
* Deliver seamless access to intranet apps without requiring a VPN with VMware Browser.
* Secure and protect content and integrate with internal and cloud content management systems with AirWatch Content Locker.
* Bring people, information and ideas together with VMware Social cast for enterprise chat and social collaboration.
* ***Enterprise Security-*** Protect corporate data at every layer.
* Trust the user with identity management for advanced user authentication and conditional access controls.
* Secure the endpoint with policies for encryption, passcode and compromised device detection with remote lock or wipe.
* Containerize the app with separation of work and personal data, and enable secure data flow between enterprise apps.
* Safeguard company data and prevent data loss across work and personal applications.
* Protect data over the network by ensuring app traffic between the device and backend corporate network is managed, encrypted and secure.
* Integrate with your existing security products for even more advanced security with the VMware Mobile Security Alliance (**MSA**).

### **Mobile Device Management (MDM):**

Manage the complete Device life cycle.

* ***Easy Onboarding and Configuration-*** Add new devices quickly and easily provision with apps and policies without IT involvement.
* Configure devices during initial power on with bulk provisioning programs such as the Apple Device Enrollment Program (**DEP**) and Windows Out-of-Box Enrollment (**OOBE**).
* Enable users to self-activate devices by entering their corporate credentials in a simple MDM onboarding workflow.
* Configure MDM policies for device restrictions, layout, settings access, notifications and more and assign based on OS or ownership type (BYO or corporate-owned).
* Deploy public, internal or bulk-purchased apps to devices automatically or to an enterprise app catalog for on-demand install.
* Connect to enterprise email, VPN, Wi-Fi, content, intranet sites and other backend resources.
* ***Device and Data Security-*** Protect corporate information through devices security and data loss prevention (**DLP**)policies.
* Enable device-level encryption, data encryption and hardware security policies (TPM, biometrics, etc).
* Enforce a device- and/or app-level passcode with complexity and history requirements.
* Configure polices including: app blacklists, device pairing, Wi-Fi security, TLS enforcement and others.
* Prevent data loss with app sharing permissions, copy/paste restrictions, geo-fencing policies, and more.
* Monitor for malware threats or jailbroken devices and automatically remediate with a remote lock, device wipe or customizable device quarantine controls.
* ***Asset Inventory & Management-***  Gain full visibility and management of all endpoints from a single admin console.
* Gain visibility into all endpoints across BYO, corporate-owned and line of business use cases in a single admin console.
* Delegate management across divisions, regions and departments with multitenant architecture and role-based access controls.
* Get real-time MDM deployment analytics from modular and role-based dashboards by devices, apps, email, security, telecom and more.
* Capture detailed analytics with report templates and granular device, app and console event logging.
* Export deployment analytics to third-party business intelligence (**BI**) solutions with data mart integration.
* ***Remote Support & Trouble Shooting-*** Enable remote commands and controls to easily troubleshoot devices.
* Request device information and perform remote commands such as clear passcode, send message, lock device, or perform an enterprise or device wipe.
* Troubleshoot devices using remote control to view the device screen and gain access to the file manager, command prompts and more.
* Enable users with self-service access to basic management capabilities, such as resetting a passcode, to alleviate IT ticket requests.

### **Unified Endpoint Management (UEM):**

Unify Mobile and Desktop management into a single solution.

* ***Manage Users across all endpoints-*** Enable a user-centric management approach for all your endpoints in a single solution.
* Support major mobile operating systems including Android, iOS, QNX, Tizen, Windows CE, Windows 10, and frameworks like Android for Work and Samsung Knox.
* Manage the full lifecycle of macOS and Windows desktop and laptop devices with a modern EMM approach.
* Manage line of business rugged devices, easily provision apps and files, and remotely support and troubleshoot.
* Monitor and manage peripherals and IoT devices like wearables, printers and endpoints running the QNX platform.
* Support varying use cases across your business including: corporate-owned, BYO and line of business.
* Leverage our platform-agnostic solution and close relationships with major OEMs for same-day support for new releases and the latest features.
* ***Full Lifecycle management & Security-*** Manage the full life cycle for all end points from on-boarding to retirement.
* Register devices during initial power up or through a user self-service workflow using corporate credentials.
* Configure device restrictions and layout along with enterprise email, VPN, Wi-Fi, apps, content, intranet sites and other backend resources.
* Protect corporate data through encryption, passcodes, DLP policies, and remote lock and wipe if a device is compromised.
* Gain visibility into asset inventory with real-time modular dashboards, pre-configured reports and granular event logs.
* Request device information and troubleshoot common issues with commands and remote management.
* ***Consistent User Experience-*** Deliver a common experience for users to access applications on all their devices.
* Unify management of corporate-owned, BYO and line of business use cases across your organization.
* Support BYO devices with separation of work and personal apps and data.
* Manage corporate-owned assets with advanced management capabilities for additional device control.
* Configure a single device to be used by multiple users through **multiuser mode** with check-in and check-out functionality.
* ***Unified Solution-*** Scale your deployment as initiatives grow with a complete unified endpoint management solution.
* Gain visibility into device deployment with role-based contextual dashboards and access controls.
* Manage devices across divisions, regions, departments and more with our **multitenant** architecture.
* Automate processes through dynamic and intelligent policy engines to alleviate manual tasks for IT.
* Integrate with enterprise systems to make the most of your existing infrastructure investments.
* Enable users with self-service access to common requests, reducing helpdesk tickets and increasing employee satisfaction.

## Mobile Productivity

Keep employees connected and able to work anytime, anywhere, on any device. Find out how to increase productivity for your organization.

### **e) Mobile Application Development**

Choose a Framework to build Enterprise ready Apps.

The VMware AirWatch Developer Enablement Program provides app developers with the tools to easily secure and configure apps for the enterprise using the frameworks as developers already know. Whether you’re looking for enterprise-level security, data loss prevention (DLP), network connectivity, single sign-on, or something else, the capabilities available in Developer Enablement Program are flexible to meet your needs.

**The Developer Enablement Program consists of three frameworks:**

The VMware AirWatch Software Development Kit (SDK),

VMware AirWatch Mobile Device Management following App Config Community documentation, VMware AirWatch App Wrapping.

### **f) Mobile Application Management**

Distribute, Secure and Manage any App.

* ***Distribute-*** Get the right apps to the right users with a custom app catalog.
* Distribute publicly available or internally developed native, hybrid, web/SaaS or virtual Windows apps.
* Target apps specific to user role based on Active Directory organization groups and AirWatch smart groups.
* Distribute bulk-purchased apps from Apple, Google and Microsoft app stores.
* Provide a consistent app catalog across mobile phones, tablets, laptops and desktops.
* ***Secure-*** Enable apps with enterprise-grade security and configurations while separating corporate data.
* Achieve end-to-end security for data at rest and in transit with AES 256-bit encryption.
* Create rules to flag non-compliant devices and configure automated remediation actions.
* Limit content sharing between work apps only with advanced data loss prevention (**DLP**) policies.
* Secure access to business systems behind the corporate firewall with the AirWatch Tunnel.
* ***Manage-*** Protect apps and their data with our flexible management options.
* Use standalone **MAM** to add security and DLP to apps with the AirWatch SDK or app wrapping.
* Take advantage of native security and DLP controls built in to the operating system with OS MAM.
* Unlock a vast ecosystem of ISV apps with the AirWatch Workspace Services profile and adaptive management capability.
* Easily configure apps that conform to the best practices of the App Config Community.
* ***Productivity Apps-*** Deliver Consumer Simple, Enterprise Secure Productivity Apps.
* With the right productivity apps at their fingertips, your employees can get more done, faster. Productivity apps are engaging and intuitive with a consumer-simple experience and enterprise grade security.
* Harness the power of mobile micro-moments by enabling employees with productivity apps they

want to use.

## Enterprise Security

Security at every layer for complete protection of your corporate data.

### **g) Identity Management**

Establish trust between the User and the Device.

* ***Single Sign On-***  Remove the friction of access security with one-touch convenience.
* Eliminate the need for users to remember multiple usernames and passwords.
* Enable two-factor authentication (**2FA**) for an additional layer of security.
* Integrate with existing identity providers or use the included identity provider or token generator (**IDP**).
* Support web apps, virtual desktops, published apps, packaged apps and native mobile apps.
* ***Self Service App Catalog-*** Deliver the right apps to the right people with an identity-defined app catalog.
* Provide a single app catalog with a consistent user experience across any device, including Android, iOS, macOS and Windows.
* Deliver the widest variety of legacy and modern Windows apps, web-based, SaaS and native mobile apps, and virtualized desktops and apps to any device.
* Enable self-service by allowing employees to subscribe to the apps they need across all their devices.
* Brand the app catalog experience with personalization options including company logo, colors, backgrounds, textures and design elements.
* ***Security & Control-***  Secure and protect corporate data with advanced administrative controls.
* Enforce conditional access policies based on authentication strength, data sensitivity, user location, device compliance and more.
* Enable advanced data loss prevention (DLP) policies to protect against rooted or jailbroken devices, whitelist and blacklist apps, set open-in and cut/copy/paste restrictions and more.
* Leverage easy-to-use analytics to understand usage trends and assist with capacity planning, licensing management and new service development.

### **h) Mobile Security**

Protect corporate data from the Device to the Datacenter.

* ***Trust the User-*** Enable one-touch single sign on (SSO) or multifactor authentication across web, cloud and native apps.
* Enforce conditional access based on authentication strength, data sensitivity, user location, device compliance and more.
* Revoke access automatically if compliance policies are violated or an employee leaves the company.
* Deliver the right apps to the right people with an identity-defined app catalog.
* Enable self-service by allowing employees to subscribe to apps across devices with automated or manual provisioning.
* ***Manage the Endpoint-*** Protect corporate information through device security and data loss prevention(**DLP**) policies.
* Enable device-level encryption, data encryption and hardware security policies.
* Enforce a device-level passcode with complexity and history requirements.
* Configure policies including app blacklists, device pairing, Wi-Fi security, TLS enforcement and more.
* Monitor for malware threats or jailbroken devices and automatically remediate with a remote lock, device wipe or customizable device quarantine controls.
* Mitigate mobile and cloud threats with security solutions that have been integrated with the AirWatch platform through the VMware Mobile Security Alliance.
* ***Secure the App-*** Add enterprise grade security and configurations to apps while separating corporate data.
* Secure app data at rest and in transit with AES 256-bit encryption.
* Detect threats and automate remediation for apps and cloud services with VMware Trust Point.
* Use standalone MAM to add security and DLP to apps with the AirWatch SDK or app wrapping.
* Take advantage of native security and DLP controls built in to the operating system with OS MAM.
* Add advanced security and management capabilities during app development.
* ***Safeguard the Data-*** Secure access to data from any device, any app and any network.
* Secure corporate data with FIPS 140-2 compliant 256-bit SSL encryption.
* Enforce containerization of apps and data using native OS controls.
* Configure policies to tag work data based on the source and enable access to only authorized users and apps.
* Protect proprietary data with dynamic watermarking and open-in and copy/paste restrictions.
* View detailed system reporting and logs to analyze enterprise data.
* ***Protect the Network-***  Prevent unknown devices from connecting to corporate networks and configure certificate-based access to corporate VPN and Wi-Fi networks.
* Allow both internal and public apps to access corporate resources residing in your secure enterprise network on a per-app basis with AirWatch Tunnel.
* Combine per-app VPN through AirWatch Tunnel with VMware NSX (Network virtualization platform) to deliver user-level micro-segmentation into the datacenter.

### **i) VMWare Mobile Security Alliance (MSA)**

Mitigate mobile threats with Best-of-Breed Security solutions.

* **MSA**- App scanning and validation, malware and virus detection, network access control and cloud security.
* **AirWatch**- Identity management, conditional access, device compliance and DLP policies.
* **MSA + AirWatch**- Simple and comprehensive security against weak passcodes and PINs, malware and ransomware, phishing and spoofing websites, email and data viruses, malicious networks and more.
* ***Protect the Device-*** Detect modifications to device access privileges.
* Identify jailbroken or rooted devices.
* Block and un-enroll a device when a threat is detected.
* Enforce continuous device compliance.
* ***Secure the App-*** Assess app risk with fast and automated app behavioral analysis.
* Block malware and ransomware from infecting corporate apps***.***
* Scan applications and determine access based on threats.
* Remove and block applications that display risky behavior.
* ***Defend the Network-*** Limit mobile app users to specific internal networks.
* Scan the network for man-in-the-middle (MiTM) attacks.
* Block external targeted attacks on networks.
* Limit cyber-attack footprint if a network is breached.
* ***Guard Cloud Resources-*** Enforce cloud data loss prevention (DLP) policies.
* Detect and prioritize cloud usage anomalies.
* Perform forensic analysis on cloud breaches.
* Enable adaptive cloud access based on device posture and user profile.

# **Products**

Empower IT with a Platform to change the way users work.

1. AirWatch
2. AirWatch Express
3. Workspace ONE

## Airwatch:

* Unify management of all endpoints across BYO, corporate-owned and line of business use cases.
* Configure devices with emails, apps, Wi-Fi, VPN, Content intranet sites and more all over the air.
* Automate the process with dynamic and intelligent policy engines to alleviate manual tasks.
* Protect company information through device security and data loss prevention(DLP) polices.
* Integrate with your backend systems so that you can make the most of your existing infrastructure investments.
* Separate work and personal apps and data on employee-owned devices to protect employee privacy.
* Give employee seamless access to any app- native, web or remote through a unified app **catalog** with simple SSO.
* Engage users with mobile-optimized apps for email, content browsing and social, so that they can get work done in the moment, where they are.

## AirWatch Express:

AirWatch Express is Mobile Device Management (MDM) made easily configure your devices with apps, email and Wi-Fi. Protect your data with restrictions and remote lock wipe.

* ***Zero-Touch Configuration-*** Easily set up devices with apps, email and Wi-Fi from a single console. And you can access it from anywhere so you can always monitor your device inventory.
* ***Worry-Free Security-***  There’s important data on your devices. Protect them from unauthorized use with security policies and remotely wipe lost or stolen devices to keep your data out of the wrong hands.
* ***No Software-*** Get up and running minutes with simple, cloud-based MDM solution.

## Workspace ONE:

VMWare Workspace ONE combines identity and mobility management to provide frictionless and secure access to all the apps and data employees need to work, wherever, whenever and from whatever device they choose.

* ***Identity defined self-service app Catalog-*** Workspace ONE combines VMware Identity Manager and AirWatch Enterprise Mobility Management to deliver the widest variety of mobile, cloud and Windows apps to any device.
* ***One-touch Single Sign-On-***  Workspace ONE leverages device trust, PIN/biometric timeout settings and built-in two-factor authentication (2FA) to remove the friction of access security with one-touch convenience.
* ***Self-service On-boarding for BYO-*** The Workspace ONE app authenticates new employees and gives them instant access to a personalized app catalog where they can subscribe to virtually any app from their own smartphone, tablet or laptop.
* ***Contextual Access Management-*** Workspace ONE offers identity and device-based policies to enforce access decisions based on authentication strength, data sensitivity, user location, device compliance and more.

# **Mobile Application Development:**

**The Developer Enablement Program consists of three frameworks:** The VMware AirWatch Software Development Kit (SDK), VMware AirWatch Mobile Device Management following AppConfig Community documentation and VMware AirWatch App Wrapping.

1. AirWatch SDK:

* Add advanced security and management capabilities during initial app development.
* More development efforts required.3
* Flexible, granular solution providing advanced security and configurations.
* Available for internal and external apps.

1. AppConfig Community:

* Standard for enterprise apps to interpret configurations and policies. Standard for enterprise apps to interpret configurations and policies.
* Leverages native iOS and Android APIs to configure and secure apps.
* Quick implementation with low development effort.
* Available for internal and external apps.

1. AirWatch App Wrapping:

* Add security and management capabilities to already developed applications.
* Provides a sub-set of SDK functionality for internally-built apps.
* Quick implementation with low development effort.
* Available for internal apps.

A Developer’s guide to securely integrating apps with VMware AirWatch. It explains,

What Can I do?

How Can I do?

## What can I do?

### **AppConfig:**

Create seamless setup flows by provisioning app config values such as server, port and domain, down to your app. Improve user experience by eliminating first time setup steps and dynamically change settings in your app with over the air updates.

An app may require seed information for initial configuration or updated configurations throughout the course of its lifecycle.

For example, the backend server URL of an application can be seeded to the application during install so the app can auto-configure with minimal user input.

We can config the application for iOS and Android separately:

**Android Capabilities Summary:**

|  |  |
| --- | --- |
| **Capability** | **Capability summary of the AppConfig Community best practices** |
| App Configuration | Develop Android for Work / Android 5.0+ App Restrictions into the application. |
| App Tunnel / Per-App VPN | Leverage the “Per-App VPN” capability available in most commercial VPN solutions. Available in Android 5.0+. No development required. |
| Single Sign-On Login Hint | Provide a standardized login hint needed to implement tenant discovery for any standard single sign-on protocol, such as OAuth or OpenID Connect, and invoke the identity provider login page for that identity. Also, can be used to suggest an account (or domain) login restriction for the app. |
| App Security – Passcode | Application specific passcodes will require a custom implementation. For app specific passcodes, use app restrictions to enable admin configuration of the passcode settings and requirements.  For Android N devices, supported EMM vendors can enforce a passcode to apply only for Work Profile managed applications. Therefore, it’s recommended to enable the configuration capability to exempt Android N devices from the custom app specific passcode to avoid duplicate passcode prompts. |
| App Security – Document Sharing | Use an Android for Work / Android 5.0+ managed profile to enforce files to open only in managed applications. Developers should ensure apps are using Content URIs and not File URIs for both functional and security reasons. Use an Android for Work / Android 5.0+ managed profile to enforce files to open only in applications under the managed profile. Developers should ensure apps are using Content URIs and not File URIs for both functional and security reasons. |
| App Security – Prevent App Backup | Any app deployed under Android for Work / Android 5.0+ managed profiles will not participate in any backup infrastructure. No development required. Any app deployed under Android for Work / Android 5.0+ managed profiles will not participate in any backup and restore infrastructure. |
| App Security – Disable Screen Capture | Use an Android for Work / Android 5.0+ managed profile to prevent screenshots. No development required. |
| App Security – Enforce App Encryption | Enroll your device using Android for Work and the device will be encrypted as part of the enrollment process. No development required. |
| App Security – Remotely Wipe App | Distribute the app to the device as a managed application using the EMM tool to have the ability to remotely wipe the app from the device. No development required. |
| App Security – Disable Copy-Paste | Use an Android for Work / Android 5.0+ managed profile to containerize copy and pasting to only managed applications. No development required. |

**How to Configuration Android App:**

**Use Case:**

Many applications require users to enter URL, port, email address, and various configurations as part of a onetime setup of an application. These manual configurations can impact the adoption and success of an organization’s mobile app initiatives, increase the burden on a help desk fielding calls from users, and adds the burden of maintaining documentation that needs to be updated frequently as latest updates to the application are made available.

By leveraging native APIs, these configurations can be set remotely by the EMM server to simplify the setup process for end users, and alleviate the help desk and documentation burden caused by manual setup. An app developer can define a set of configuration keys it accepts from an EMM server and An IT administrator can simply set the keys and values in the EMM provider’s management console and they will be pushed into the app.

Apps commonly implement the following types of configurations – these are suggestions only:

Backend Service Configuration: server URL, port, use SSL, group/tenant code

User Configuration: username, email, domain (NOTE: for apps that support SSO, login hint using user domain format should be used instead of proprietary user configuration settings whenever it’s supportable).

**How it Works:**

Requirements:

* Android 5.0+ with Android for Work enrolled device
* App is developed with Android App Restrictions capabilities using Restrictions Manager
* Distribute app via an EMM vendor that supports Android for Work App Restrictions

Process Flow:

* App developer adds App Restrictions capability into the app
* App developer declares the app restrictions honored by the app in an xml file referenced in the Android Manifest xml.
* App developer makes the app available to the organization. The application can be a public app in the Google Play store, or may be an internally developed app available on a private channel
* Configurations are specified in the EMM admin console (contact your EMM vendor for documentation)
* App is distributed to devices, along with the configurations specified, via the EMM

Developer Requirements:

Apps installed on enrolled Android for Work devices running Android 5.0+ can leverage the App Restrictions to retrieve configuration values sent over the air by an EMM vendor. The enterprise app developer will need to implement Restrictions Manager to read and honor these configuration values and invoke the appropriate action based on the configuration.

The following 3 steps outline instructions for a developer to implement this capability:

Step 1:

Add the list of supported app restrictions in a restrictions file and defining the restrictions file in your app manifest.

You can choose to support any custom restrictions you’d like by defining them in a restrictions file and your manifest. Create an XML file named app\_restrictions.xml in the res/xml directory to house your defined app restrictions, the format for the XML can be found here: http://developer.android.com/reference/android/content/RestrictionsManager.html

After you create the XML file and have defined your restrictions within the file, declare the restrictions file in your app manifest XML.

<meta-data android:name=“android.content.APP\_RESTRICTIONS” android:resource=“@xml/app\_restrictions” />

Refer to the documentation link below for the full details: http://developer.android.com/training/enterprise/app-restrictions.html#define\_restrictions

Step 2:

Implement RestrictionsManager and use it to read the App Restrictions.

Use RestrictionsManager and call getSystemService with RESTRICTIONS\_SERVICE to get the appropriate RestrictionsManager instance. Follow with a getApplicationRestrictions call on the retrieved RestrictionsManager instance to get the app restrictions.

RestrictionsManager myRestrictionsMgr = (RestrictionsManager)getActivity().getSystemService(Context.RESTRICTIONS\_SERVICE);

Bundle appRestrictions = myRestrictionsMgr.getApplicationRestrictions();

Note: You can listen to the ACTION\_APPLICATION\_RESTRICTIONS\_CHANGED intent to be alerted when a configuration has changed so you can perform a re-query via Restrictions Manager.

Reference: https://developer.android.com/reference/android/content/RestrictionsManager.html#

Step 3:

Make your app available:

Deploy your app on the Play Store or Google Private Channel. An enterprise organization’s admin can configure their EMM to define the configuration values and deploy your app to devices.

Note: Only Android 5.0+ devices enrolled using Android for Work can make use of this capability. The application must be provisioned and installed through EMM for the configuration values to take effect.

**SDK (Supported):**

Integrate the AirWatch SDK into your app and configure an SDK profile with a custom payload containing your configuration values and assign it to your app.

Initialize the SDK and use the appropriate method calls to retrieve the custom settings containing your configuration values

Requires coding and device entry in AirWatch system, no MDM required.

### **App Passcode:**

For security reasons, enterprises may want to prevent continuous access to an app without periodic authentication.

Prevent unauthorized access by securing your app UI with an app passcode (separate from the passcode already set at the device level). Facilitate a great user experience by using easy biometric login alternatives like Touch ID.

Implementation Summary:

It can implement in three ways as explained below:

1. The recommended approach for implementing a passcode is to embed the AirWatch SDK into your app and set the SDK profile configuration to enable authentication.
2. Second Approach: App Config community - Security Policies

* Reference the sample code and documentation available at AppConfig.org
* Use the sample code as a starting point for the PIN code UI, and customize as needed
* Implement an app configuration in order to have the MDM server set the PIN code policy
* Requires device enrollment on iOS, and Android for Work on Android

**Use case:**

An organization requires granular security and data loss protection within enterprise applications to prevent sensitive data and documents from leaking outside company control. An app may also contain a capability that an enterprise wants to disable for security reasons, such as the ability to synchronize data with a public cloud file storage service. Some security capabilities are natively provided by the operating system and the EMM vendor without any code changes needed to the app, other capabilities require the implementation of an app configuration to enable a security capability. A summary of some of the capabilities are listed below, and an app developer can choose to implement a custom security policy as well.

Developer Requirements:

|  |  |
| --- | --- |
| **App Security – Passcode** | Application specific passcodes will require a custom implementation. For app specific passcodes, use app restrictions to enable admin configuration of the passcode settings and requirements.  For Android N devices, supported EMM vendors can enforce a passcode to apply only for Work Profile managed applications. Therefore, it’s recommended to enable the configuration capability to exempt Android N devices from the custom app specific passcode to avoid duplicate passcode prompts. |
| **App Security – Document Sharing** | Use an Android for Work / Android 5.0+ managed profile to enforce files to open only in managed applications. Developers should ensure apps are using Content URIs and not File URIs for both functional and security reasons. |
| **App Security – Prevent App Backup** | Any app deployed under Android for Work / Android 5.0+ managed profiles will not participate in any backup infrastructure. No development required. |
| **App Security – Disable Screen Capture** | Use an Android for Work / Android 5.0+ managed profile to prevent screenshots. No development required. |
| **App Security – Enforce App Encryption** | Enroll your device using Android for Work and the device will be encrypted as part of the enrollment process. No development required. |
| **App Security – Remotely Wipe App** | Distribute the app to the device as a managed application using the EMM tool to have the ability to remotely wipe the app from the device. No development required. |
| **App Security – Disable Copy-Paste** | Use an Android for Work / Android 5.0+ restrictions profile to containerize copy and pasting to only managed applications. No development required. |

1. The third approach is to leverage **AirWatch App Wrapping**. The app developer must validate that only approved MADP platforms and coding techniques as documented by the AirWatch App Wrapping Guide are used in the app in order to use this feature.

**Wrapping** (Supported):

* Develop and compile your application.
* Verify that the app is only using an approved MADP platform and coding techniques
* Run the compiled binary through the AirWatch application wrapping cloud engine.
* Assign a wrapping profile to your application with a passcode policy.
* Requires neither coding nor MDM, only device entry in AirWatch system.

**SDK (Recommended):**

* Integrate the AirWatch SDK for iOS and Android into your application.
* Configure the SDK profile policy for your application to enforce a passcode.
* The SDK will automatically display the “View Controllers & Activities” to secure your app with a passcode.
* Requires coding and device entry in AirWatch system, no MDM required.

### **App Tunneling:**

Enable select applications to access corporate intranet resources and ensure data security in transit.

An application may require access to web services residing behind a corporate firewall.

A traditional full device VPN solution is not adequate due to manual steps required to enable the VPN on the device, and the security exposure by allowing personal apps the same access to the VPN as corporate apps. A more secure, seamless, targeted solution is required to allow only certain applications restricted access to certain intranet endpoints.

Implementation Summary:

* The recommended approach for app tunneling is to configure a **Per-App VPN** profile through MDM to leverage native tunneling functionality provided by the operating system.
* Alternative approaches are to integrate either the AirWatch SDK or use AirWatch App Wrapping.

Per-App VPN:

**Use case:**

An application may require access to web services residing behind a corporate firewall, which requires a secure app tunnel connection between the app on the device and the backend services. A common use case for cloud based public apps is the ability to federate authentication to an organization’s identity provider (IDP) via SAML or similar standard. Since some organizations deploy the SAML identity providers (IDP) on premise in a way that is not publicly accessible, a secure app tunnel is required to authenticate and login to the app.

Mobile operating systems have addressed this use case by enabling a capability commonly referred to as “Per-App VPN”. Several common commercial VPN providers support the Per-App VPN capabilities. Many EMM vendors offer their own Per-App VPN capability as well. Whichever your preferred Per-App VPN vendor is, the EMM provider typically will have the ability to automatically distribute and enable the Per-App VPN on devices.

How it works:

Requirements:

* Android 5.0+
* VPN infrastructure deployed that supports the per-app VPN capability
* No code changes are needed in the app to support this capability

Process Flow:

* Organization deploys any needed VPN infrastructure (contact your VPN provider for details)
* EMM vendor distributes the VPN app along with a per-App VPN configuration profile
* The end user opens an app that requires a backend connection, and the VPN will automatically turn on

Developer Requirements:

No code change is needed to your application to take advantage of this capability. The Android operating system will automatically tunnel any network calls based on the configuration profile sent from EMM.

**SDK**(Support):

* Integrate the AirWatch SDK into your application and configure a SDK profile with Tunneling enabled and assign it to your application.
* Ensure the networking classes and methods used by your applications are supported in the AirWatch SDK guide.
* The SDK will redirect your app network traffic through a supported proxy to reach your targeted backend.
* Requires coding and device entry in AirWatch system, no MDM required.

**Wrapping**(Supported):

* Develop and compile your application.
* Verify that the app is only using an approved MADP platform and coding techniques
* Run the compiled binary through the AirWatch application wrapping engine.
* Assign a wrapping profile to your application with a Tunnel policy.
* Ensure the networking classes and methods used by your applications are supported in the AirWatch Wrapping guide.
* The wrapped app will then redirect its app network traffic through a supported proxy to reach your targeted backend.
* Requires neither coding nor MDM, only device entry in AirWatch system.
* Applications often have to connect to backend server-side resources that are protected using either NTLM, Basic, Certificates, or Kerberos.
* There is a best practice approach to accommodating each of the different authentication types.
* For an optimal user experience, the user should only have to login once and access should be persisted thereafter for an extended period of time.

### **SSO NTLM/ Basic: (NT Lan Manager)**

The recommended approach for implementing NTLM or basic SSO is through the AirWatch SDK.

**SDK**(Recommended):

* Integrate the AirWatch SDK into your application and configure a SDK profile with Integrated Authentication configured.
* Use the SDK provided interfaces to handle the networking authentication challenges.
* Requires coding and device entry in AirWatch system, no MDM required.

**Wrapping**(Supported):

* Develop and compile your application.
* Verify that the app is only using an approved MADP platform and coding techniques.
* Run the compiled binary through the AirWatch App Wrapping engine.
* Assign a wrapping profile to your application Integrated Authentication.
* Requires neither coding nor MDM, only device entry in AirWatch system.

### **SSO Certifications:**

* The recommended approach for implementing certificate authentication is through the AirWatch SDK.
* The alternative is to use App Wrapping.

**Use Case**

Organizations want to allow users to log into an application using their existing work credentials, as well as customize the security around the login experience to require various factors of authentication. Once a user has logged into one application successfully, that login process should automatically translate to other applications so users do not have to enter their credentials multiple times.

Many organizations use federated authentication to an identity provider (IdP) to accomplish this. The IdP typically supports standardized protocols (such as OAuth or OpenID Connect) that are implemented by many app developers. The single sign-on capability documented by the AppConfig community specifies the best practice for how an app developer should perform tenant discovery to invoke the IDP from the app in order to facilitate a single sign-on experience.

How it works:

Requirements:

* Fallback to system browser works on all versions of Android. Best user experience is on Android 4.3+ with Chrome 45+ (when using Chrome Custom Tabs specifically – all Google-certified Android devices since Android 4.0 ship with Chrome)
* App’s backend SaaS authorization service must support identity federation to an organization’s identity provider (IDP) via a standard such as SAML or OpenID Connect
* App developer must invoke the identity provider’s login page via a Custom Tab in order to share SSO state across apps.

Process flow:

* Customer organization deploys any needed identity provider (IdP) infrastructure
* App developers build in support for standard web SSO pattern (using OAuth or OpenID Connect) into their mobile app and the SaaS backend authorization service, using Custom Tabs during user auth flows
* (Strongly recommended, but not required) App developer user configuration settings include a specially-named string: “login hint” that can be set via managed configuration as described above in “App Configuration”
* When the app is launched, the user will see the identity provider’s login screen in a Chrome Custom Tab window
* If login hint has been supplied and it resolves to a valid user account on that IdP that is not logged in, that account will be shown by the IdP above the login password request. Depending on your SSO solution implementation, EMM and/or Identity vendor may support automatically authenticating to this page without the user needing to enter his/her credentials manually, contact your EMM vendor or Identity vendor for details
* Once the user is authenticated, any additional apps within the Android user or managed profile that leverage the same account and identity provider using a Custom Tab will be able to repeat the pattern without further user intervention and will not need to prompt the user to login again as long as the auth state remains valid.

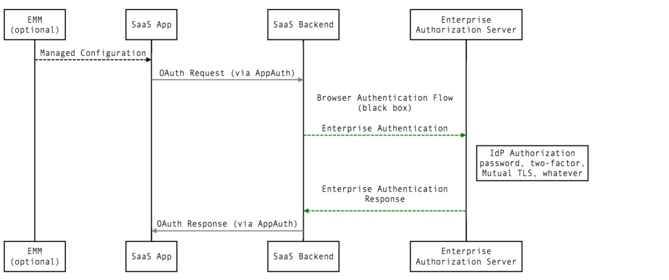
Developer Requirements:

The following steps outline instructions for a developer to implement this capability.

**Step 1**: Support a web SSO pattern with OAuth or equivalent standard protocol within your app’s backend SaaS authorization service

Sample code and documentation for this step in its entirety is outside the scope of the AppConfig Community. Contact your identity provider (IdP) of choice for recommendations on how to accomplish this step – some IdP suppliers offer specific solutions for SaaS provider authorization server integration using standardized protocols. Relevant standards documents for OAuth in the Internet Engineering Task Force (IETF) are published at

[https://tools.ietf.org/wg/oauth/](https://tools.ietf.org/wg/oauth/%20) and for OpenID Connect in the OpenID Foundation (OIDF) at <http://openid.net/wg/connect/>



**Step 2**: Invoke a Custom Tab window to display the IdP authentication page.

IMPORTANT: Always use a custom tab for login, do not render the login screen within your native app UI, which can compromise security and expose SSO credentials; the intended web SSO security pattern with independent IdP flow should be maintained within the custom tab. When a login hint is not available to your app via managed configuration (which will enable your SaaS authorization server to redirect immediately to the correct IdP), your SaaS authorization server or associated SaaS service should be prepared to render a generic login screen in the custom tab that requests the user to supply the account.

**SDK**(Recommended):

* Integrate the AirWatch SDK into your application and configure an SDK profile with Integrated Authentication configured for certificate authentication.
* Use the SDK provided interfaces to handle the networking authentication challenges.
* Requires some coding.

**Apply Config** (Android Only):

* Configure a credentials payload in an Android for Work profile. This will send the certificate to the device’s managed key store.
* Code your app to read the value stored at the “ManagedAppCertAlias” key from RestrictionsManager. This value is your certificate alias.
* Query the keychain using the alias you obtained for the ManagedAppCertAlias key from RestrictionsManager as the argument and retrieve the certificate to be used for authentication challenge.
* Requires Android 5.0+ and Android for Work device.
* Use this certificate to respond to any client certificate authentication challenges.

**Wrapping**(iOS only):

* Requires neither coding nor MDM, only device entry in the AirWatch system.
* Develop and compile your app.
* Verify that the app is only using an approved MADP platform and coding techniques.
* Run the compiled binary through the AirWatch App Wrapping engine.
* Assign a wrapping profile to your app with Integrated Authentication configured for certificates.

### **Data Loss Prevention:**

Protect your enterprise app data from being shared with unauthorized entities. Enforce controls around app data sharing interfaces such as ‘**copy & paste’**, ‘**open-in**’, ‘**cloud backup**’, and ‘**screen capture**’.

**Copy – paste**: For apps used in more regulated industries, it may be important for IT to prevent applications from openly sharing data with each other.

Copy / Paste restrictions can prevent data in a corporate app from being easily transferred to unmanaged or personal applications to protect against data leakage.

**AppConfig Community** (Recommended for Android):

* Configure an Android for Work restriction profile to restrict copy and paste to only occur within managed applications.
* Requires enrollment into MDM.
* Requires no coding.
* Requires Android 5.0+ with Android for Work device.
* On iOS, the AppConfig Community documents sample code that can be used to enable this capability in the app.

**SDK** (Recommended for iOS):

* Integrate the AirWatch SDK into your application and configure a SDK profile with a copy / paste DLP restriction and assign it to your application.
* Ensure any custom application copy / paste logic is done through native interfaces (UI Pasteboard).
* Requires coding and device entry in AirWatch system, no MDM required.

**Wrapping** (Supported):

* Requires neither coding nor MDM, only device entry in AirWatch system.
* Develop and compile your application.
* Verify that the app is only using an approved MADP platform and coding techniques.
* Run the compiled binary through the AirWatch App Wrapping engine.
* Assign a wrapping profile to your application with a copy / paste DLP restriction.

Managed Open-In / File Sharing: For apps used in more regulated industries, it may be important for IT to prevent applications from openly sharing data with each other.

Apps containing sensitive files can be controlled to only share files across managed corporate applications to prevent private information from leaking into unmanaged apps.

**Implementation Summary:**

* The recommended approach is to use the AppConfig Community practices to configure restrictions profiles for the device to protect sharing of files with unmanaged apps.
* An alternative is to use the AirWatch SDK or App Wrapping to prevent files from being shared with unmanaged apps.

**SDK** (Supported):

* Integrate the AirWatch SDK into your application and configure a SDK profile with a copy / paste DLP restriction and assign it to your application.
* Write your open-in logic to read the SDK profile settings first to ensure the sharing is permitted before executing the open-in.
* Requires coding.
* Supports non-MDM enrollment modes.

Prevent App Backup: Device users may want to back up their device data to later restore the data on a different or new device for various reasons.

IT may need to protect the data in the corporate set of apps from being backed up so company data cannot be transferred to a new unmanaged device or backup service.

Implementation Summary:

* The recommended approach is to use the AppConfig Community best practices to configure a restriction profile to prevent backup to cloud services.
* Alternative approaches include the use of keychain flags, file attributes, or AndroidManifest.xml flags during app development to prevent backup.

Prevent Screenshot: For app usage in highly regulated industries, it may be important for IT to prevent applications from openly sharing data with each other.

Apps and devices containing sensitive content can be restricted from taking screenshots in order to discourage easy transfer of app content.

Implementation Summary:

* The recommended approach is to use the AppConfig Community practices to configure restrictions profiles for the device to disable screen capture.
* Alternative approach for Android is to use the AirWatch SDK or Application Wrapping to prevent files from being shared with unmanaged applications.

**AppConfig Community** (Recommended):

* Configure an iOS MDM Restriction Profile or Android for Work restriction profile to disable screenshots.
* Requires enrollment into MDM.
* Requires iOS 9+.
* Requires no coding.

### **Encryption:**

Protect app data at rest by encrypting file and data storage using platform best practices and offerings.

For apps with sensitive data or files, you may want to encrypt the persisted contents of the app in case the file system is compromised.

Extraction of the persistent storage will only expose encryption ciphertext as opposed to the readable data.

Implementation Summary:

* The recommended approach is to use the AppConfig Community best practices to enforce device passcodes on iOS devices to ensure DAR encryption. Similarly, on Android, apply an MDM policy to enforce encryption on the device.
* One alternative approach for Android is to use the AirWatch SDK’s encryption read / write methods to encrypt your app data.

**AppConfig** (Recommended):

* For iOS, ensure a device passcode is set on the device through a MDM passcode policy. By setting a device-level passcode, the OS will encrypt all data on the device using the device PIN entry.
* For Android, configure an MDM policy to enforce device encryption.
* Requires no coding.

**SDK** (Android Only):

* The SDK provides data IO methods that can take in a data argument and return an encrypted cipher text and vice versa.
* Requires coding and device entry in AirWatch system, no MDM required.

**Wrapping** (Android Only):

* Enable the encryption capability and wrap the app.
* Verify that the app is only using an approved MADP platform and coding techniques.

## How can I Do?

### **Technical Approaches:**

There are three technical approaches you can use to securely integrate apps with AirWatch. Most commonly, developers use a combination of the **AppConfig Community** best practices along with the **VMware AirWatch SDK** to meet the desired outcome.

**AppConfig Community:**

The AppConfig Community is a collection of industry-leading EMM solution providers and app developers that are making it simpler for developers to use native platform APIs to configure and secure apps in the enterprise. Native capabilities documented by the AppConfig Community include sending key/value configurations into an app, enabling app tunneling (per-app VPN), SAML-based single sign on, data-at-rest encryption, and various security policies. VMware AirWatch is a founding member of and active contributor to the AppConfig Community and supports all capabilities described at AppConfig.org.

**VMware AirWatch SDK:**

The SDK code library from AirWatch can be used to enable additional app config and security capabilities that may not yet be available natively as part of the AppConfig Community. Certain use cases such as granular analytics can be provided through a deeper integration with the SDK. The SDK is also a good choice in deployment scenarios where a MDM profile installation on the device is not possible.

**AirWatch App Wrapping:**

App Wrapping starts with AirWatch automatically de-compiling an app that has already been written. The App Wrapping engine running in the AirWatch Cloud will then identify specific functionality in the app to replace with calls to the AirWatch SDK and recompile the app. This allows for a subset of AirWatch SDK capabilities to be added to an app without requiring any developer involvement. App Wrapping is only compatible with internal apps using approved app development platforms, coding practices and libraries.

Note: Support is only provided for App Wrapping once the app developer has confirmed the app is using a supported development platform and coding techniques documented by AirWatch. App Wrapping is not supported for third party apps found in the iOS App Store or Google Play store. App Wrapping is not available to be installed on premise. However, an on premise AirWatch deployment may leverage the app wrapping engine in the AirWatch Cloud.