airwatch™
mobile security
mobile device management
mobile application management

Enabling Bring Your Own Device (BYOD) in the Enterprise

Leveraging AirWatch to Create a Secure and Convenient BYOD Program

Table of Contents

Disclaimer

While AirWatch strives to provide some level of direction for customers in terms of initially implementing a BYOD program, it is up to each organization's legal, human resources, and management teams to create a device management program that is right for your organization. The example scenarios and issues in this document are provided as a courtesy and are not meant to act as official guidance or recommendations regarding device management or liability.

References in this document to any specific service provider, manufacturer, company, product, service, setting, or software do not constitute an endorsement or recommendation by AirWatch. Under no circumstances shall AirWatch be liable to you or any other person for any damages, including without limitation, any direct, indirect, incidental, special or consequential damages, expenses, costs, profits, lost savings or earnings, lost or corrupted data, or other liability arising out of or related in any way to information, guidance, or suggestions provided in this document.

BYOD and Enterprise Mobility

With the consumerization of enterprise mobility, a growing percentage of workers are using their personal devices to access corporate resources. When these devices are not secured by Mobile Device Management (MDM), this introduces a wide range of security threats. Research suggests that this trend is only continuing to increase; a study conducted by an AirWatch partner found that 40% of workers are using their personal devices to access business applications and resources. Rather than trying to mitigate this trend by further locking down corporate resources, corporations are taking advantage of it by empowering and securing the personal device for business use through Bring Your Own Device (BYOD) programs.

40% OF WORKERS ARE USING
THEIR PERSONAL DEVICES
TO ACCESS BUSINESS
APPLICATIONS AND RESOURCES

Instead of insisting that employees maintain a separate, work-dedicated device, many organizations are implementing BYOD models that enable employees to use their own device for both personal and business purposes. Before asking employees to "Bring Your Own Device" and enabling those devices with corporate content, though, businesses need to understand a few things:

- What is BYOD and why should we enable it?
- How do we enable a successful BYOD program and what questions should we be asking?

AirWatch can help your corporation gain a deeper understanding of what BYOD entails and how to address any concerns with BYOD. While BYOD may not be the right solution for every corporation, it is a feasible solution for many businesses, and AirWatch has the tools you need to **enable** a successful BYOD program and **configure** BYOD-friendly settings in AirWatch.

BYOD: A Growing Business Strategy

An increasing number of corporations are implementing BYOD programs, and more and more employees are asking their employers to consider BYOD models. Any organization interested in hiring the best talent and in staying on top of the latest and most efficient enterprise trends cannot dismiss the idea of BYOD without careful consideration. One of the reasons that BYOD has become such a popular trend is the fact that each corporation can develop a model tailored to their unique business and employee needs. In general, BYOD programs may include the following components:

- **BYOD Deployment Options**: Corporations using a BYOD model may ask all employees to bring their own devices, or they may employ a hybrid mobile deployment where the devices are a combination of employee-owned and corporate-dedicated devices.
- **MDM Provider**: The MDM provider is a critical component of any BYOD program. AirWatch MDM enables corporations to achieve the right balance between providing enterprise security while maintaining employee convenience and privacy.
- **Plan management**: Employees handle all aspects of device management. They choose their provider, device type, and device plan. Employees are responsible for paying all costs to the provider.
- **Reimbursement Strategy:** Reimbursement models vary, but a popular model is for employers to simply issue a monthly stipend to employees who bring their own device.

Benefits of BYOD

By asking employees to bring their own device and enabling those devices with corporate content, companies can gain the following valuable resources:

- **Management flexibility**: BYOD eases the management burden by eliminating the need to select and manage a provider and plan.
    - There is no need to monitor employee telecom usage data for overages or other extras.
- **Cost savings**: In addition to the reduced overhead costs in managing a corporate phone plan, corporations also save money due to the lower costs associated with individually-managed call, data, and SMS plans.
- **Maximized employee performance:** Employees are more likely to be productive while traveling or working away from the office if they are comfortable with the device.
- **Greater employee contentment**: Employees are often partial to a certain device platform or service provider, and are much more content do not appreciate being forced to use a device with which they are not comfortable.
- **Simplified IT Infrastructure**: BYOD models eliminate or reduce the requirement for an IT administrator to administrate a mobile plan. Furthermore, BYOD reduces the strain on IT help desks since end-users will be primarily responsible for reaching out to their mobile provider if they need support.

Beyond these advantages to the corporation, BYOD programs have become increasingly popular among employees due to the higher level of **convenience** they provide:

- Employees want the **freedom of choosing the type of device** they use.
- Workers that already have their own device and want the **convenience of only having one device.**
- BYOD is an appealing **recruitment incentive** because the best employees want to be able to bring their own device into the workplace.

Successfully Enable and Configure BYOD with AirWatch

Organizations and their employees are eager to reap the benefits of BYOD programs, but despite their desire to embrace the BYOD model, both groups have lingering concerns about BYOD. While businesses are mainly concerned with maintaining **security**, employees are worried about preserving the **convenience** they need in order to work from their mobile device, and the **privacy** they expect regarding the personal information on the device.

AirWatch meets the BYOD challenges head on by helping your organization identify and address the considerations it needs to make before enabling BYOD, and providing a tool that helps you successfully configure employee-owned devices. By using AirWatch's multi-tenant MDM solution that is flexible, customizable, scalable, and secure, you can be sure to give your employees the privacy they need while maintaining the required level of corporate protection.

Bring Your Own Device (BYOD)

AirWatch provides a flexible solution for managing employee-owned devices for organizations supporting a Bring Your Own Device (BYOD) program. Manage devices, apps and content uniquely based on ownership model.

- Businesses want to know how to create and manage a reimbursement policy and how to balance corporate and employee liability regarding proprietary data on the device.
  - AirWatch contains integrated financial and legal tools for easier management.
- Enterprises are concerned with the types of devices their employees might have. For example, they want to prevent unapproved operating systems and device types from accessing corporate resources.
  - AirWatch contains robust enrollment controls to dictate and monitor device and user eligibility based on customizable settings
- Enterprises may have a hybrid of employee-owned, corporate-dedicated, and line of business devices. They need flexible management and restrictions policies for each device type.
  - AirWatch enables the end-user and administrator to define and leverage **device ownership type** when assigning restrictions and compliance profiles and internal applications.
  - Administrators can isolate personal and corporate data on the device to secure all devices while provisioning looser restrictions where necessary.
- Businesses want to ensure secure and convenient mobile access to corporate content, Email, and other resources.
  - AirWatch's content and profile management tools to ensure that BYOD employees have comprehensive, convenient and secure access to corporate resources.
- Enterprises need to protect corporate assets if an employee leaves the company or if a device is lost or stolen, while employees do not want the administrator to have the ability to wipe all data from their personal device.
  - AirWatch allows for removal of corporate access and data on devices while preserving all other device features, and AirWatch privacy settings enable the administrator to disable the full device wipe feature for employee-owned devices.
- Employees want to assure their employees privacy by not collecting personal data from employee-owned devices.
  - AirWatch contains robust privacy settings and an end-user self-service portal.

Management and Liability Considerations for BYOD

Your corporation probably has several concerns regarding the financial, legal, and management implications of BYOD. For example, how will you determine a reimbursement model and share liability in the case of a broken or lost device? AirWatch gives you the freedom to create your own policies but the tools to help you manage them in a way that is convenient for and unique to your organization.

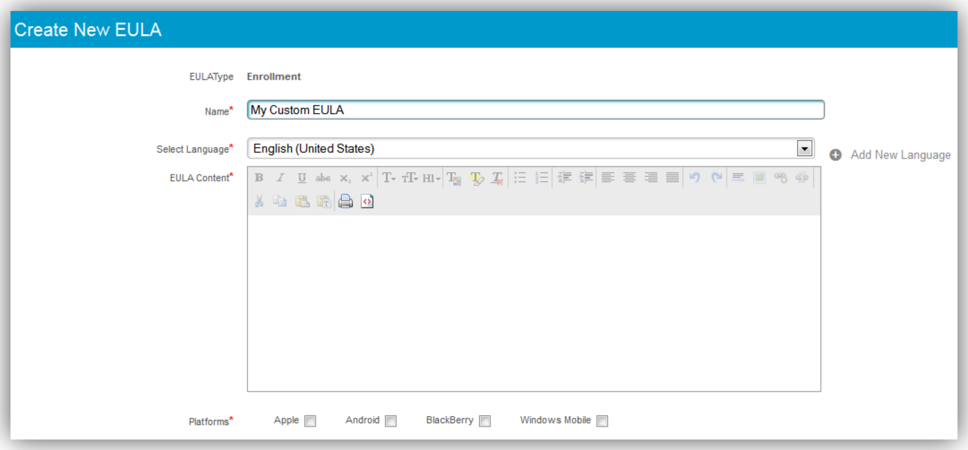
Financial Management tools

- Reporting capabilities to facilitate reimbursement logistics.
- Application Reimbursement indications
- Integration with Apple VPP for streamlined application purchase and distribution.

Legal Considerations

AirWatch offers the ability for each enterprise to create a custom End User License Agreement (EULA), which users will be prompted to read and accept before enabling MDM on their personal device. This is an important feature for legal and liability management regarding BYOD. Your legal team should carefully consider how to tailor your AirWatch EULA for personal devices. A common practice is to reference a more extensive document (hosted elsewhere) which details your legal agreements at length, but a few areas you may want to address in the EULA are:

- Highlight key MDM allowances (such as administrator permissions)
- Address user obligations in the event of a lost or stolen device
- Acknowledge that the device will be enabled with proprietary corporate data and is subject to enterprise security policies regarding sensitive data



Create New EULA

EULAType Enrollment

Name* My Custom EULA

Select Language* English (United States)

EULA Content*

Platforms* Apple □ Android □ BlackBerry □ Windows Mobile □

Customizing MDM for BYOD

Even while organizations implement BYOD programs as a means of providing greater freedom and flexibility to their employees, the IT administrator still needs a way to identify employee-owned devices as distinct from corporate –dedicated devices, and prevent compromised or other unauthorized devices from enrolling in MDM and accessing enterprise resources. AirWatch addresses and manages these issues from the very beginning of the MDM lifecycle during the enrollment process.

Enrollment

AirWatch recognizes that a fully customized enrollment process is a key support factor for BYOD. In addition to offering a custom EULA, AirWatch offers a variety of other options to help streamline and control enrollment for BYOD initiatives. Among the many challenges in managing personal devices are:

- Recognizing and distinguishing employee-owned devices
- Limiting enrollment to only approved devices

Furthermore, your corporation can leverage the following AirWatch features for flexible and customized management:

Defining Device Ownership Type

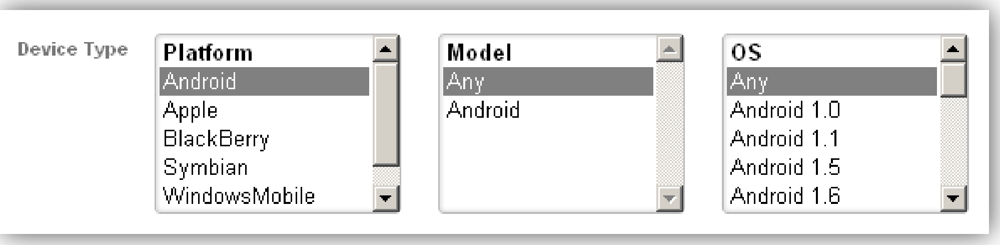
Management flexibility is a key advantage of MDM. AirWatch enables multi-platform, multi-OS, and multi-ownership type device management, all in one environment. AirWatch facilitates easier and more flexible management by leveraging device “ownership type” in the following ways:

- AirWatch enables **user-defined ownership type** upon MDM enrollment (the administrator can update the ownership type if necessary).
- AirWatch uses **ownership type as assignment criteria** for security policies, privacy levels, profiles, and content access.
  - Administrators can set different policies for employee-owned and corporate-dedicated devices.

Blocking Device Types

Not every personal device has a use in the workplace. After your corporation evaluates the kinds of devices your employees own and determines which ones make sense to use in your work environment, the AirWatch administrator can configure the following enrollment settings:

- **Whitelisting** policies to restrict enrollment to a list of specific devices and operating systems.
- **Blacklisting** policies allow all devices and operating systems to enroll except for those that are specifically prohibited by the Blacklist.



- Further device restrictions such as establishing the max devices allowed per user.

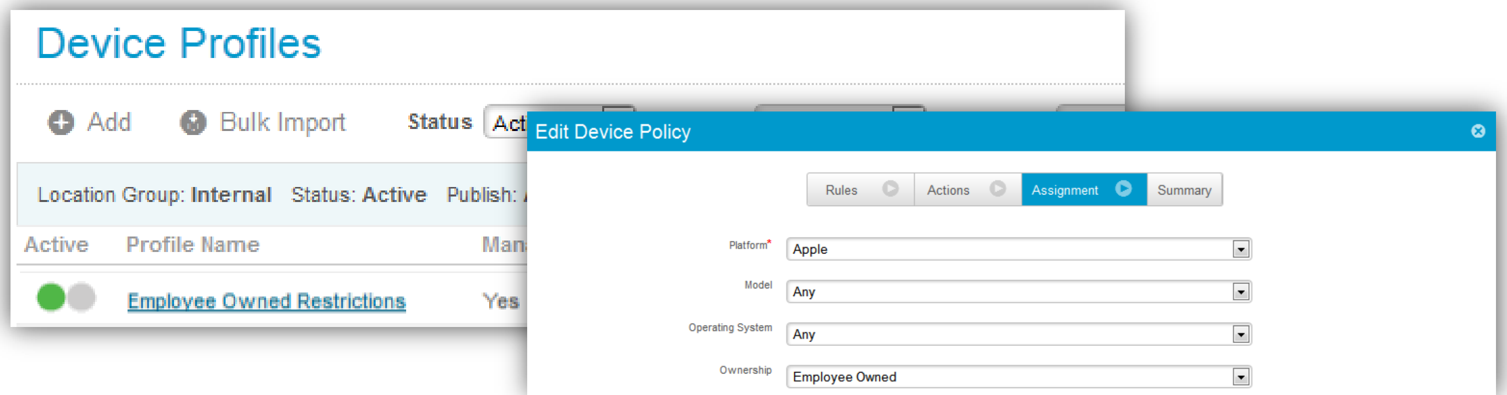
Securing Devices for Corporate Use

Regardless of whether devices are corporate-dedicated or employee-owned, AirWatch acknowledges the need for comprehensive security as a core component of MDM. There are no extra features or configuration required for administrators to maintain a high level of security for both employee-owned and corporate-dedicated devices. In addition to providing full administrative visibility over the security status of a device, AirWatch continuously works in the background and proactively alerts the administrator if any issues arise. This enables visibility and control over the smart device fleet without the need for an administrator to constantly monitor the devices.

AirWatch secures **all devices** by:

- Performing **continuous security checks for** unsecure applications, operating systems, and other threats
- Constantly **enforcing restrictions** through over-the-air provisioning
- Enforcing **data encryption** requirements
- **Isolating corporate and personal data** on devices to assure the highest level of security for corporate data

AirWatch is an all-in-one solution for maintaining the fullest and most flexible level of security on employee owned devices. Due to the flexible management options in AirWatch, administrators can deploy security policies and restrictions to employee-owned devices while simultaneously provisioning a greater level of restrictions to corporate-dedicated devices.



Location Group: Internal Status: Active Publish: /

Active	Profile Name	Man
●●	Employee Owned Restrictions	Yes

Platform* Apple

Model Any

Operating System Any

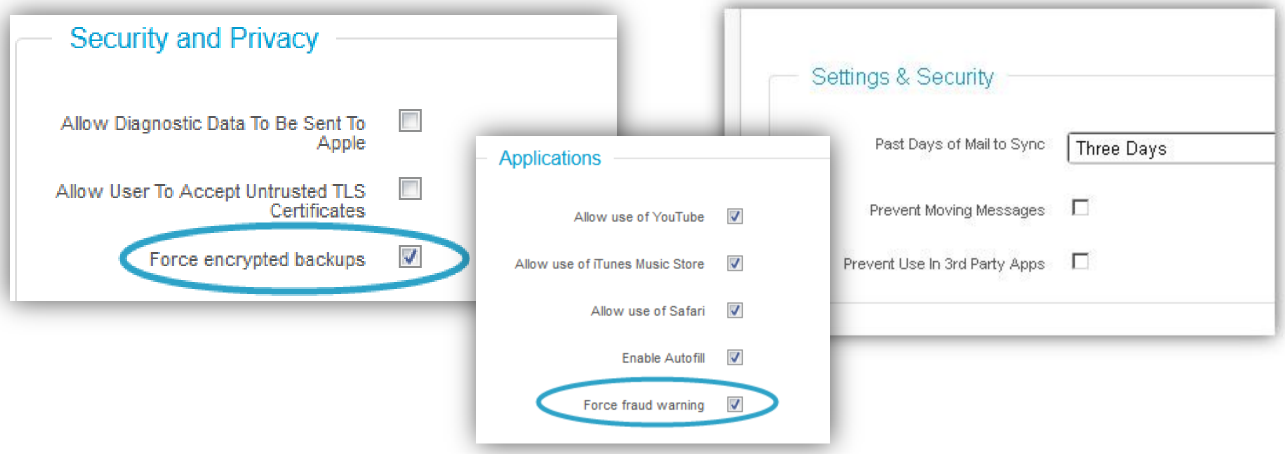
Ownership Employee Owned

The Right Restrictions for BYOD

AirWatch offers a number of restriction profiles through over-the-air profile provisioning. AirWatch offers a range of restrictions settings that enable administrators to set very tight restrictions for corporate-dedicated devices while applying looser restrictions to employee-owned devices.

They type of restrictions offered by AirWatch is also ideal for managing employee-owned and corporate-dedicated devices. While some restrictions do prohibit the use of certain features on the device, such as the iTunes store or YouTube (these restrictions are not typically deployed to employee-owned devices), many of the restrictions in AirWatch are actually security enforcements that increase the level of device security without having a negative impact on device functionality. AirWatch includes the following options, which are great examples of restrictions policies for BYOD devices:

- **Encrypted backups** – Now that BYOD devices will have access to corporate content, any backups should be protected with data encryption.
- **Force fraud warning in supported browsers:** –Force users to acknowledge all warnings issued by the browser when it detects a suspicious site.
- **Disable moving emails** –Prohibit the exposure of sensitive corporate data by disabling the ability to forward a corporate Email to a personal account or open it in third party applications.



Security and Privacy

Allow Diagnostic Data To Be Sent To Apple ☐
Allow User To Accept Untrusted TLS Certificates ☐
Force encrypted backups ☑

Applications

Allow use of YouTube ☑
Allow use of iTunes Music Store ☑
Allow use of Safari ☑
Enable Autofill ☑
Force fraud warning ☑

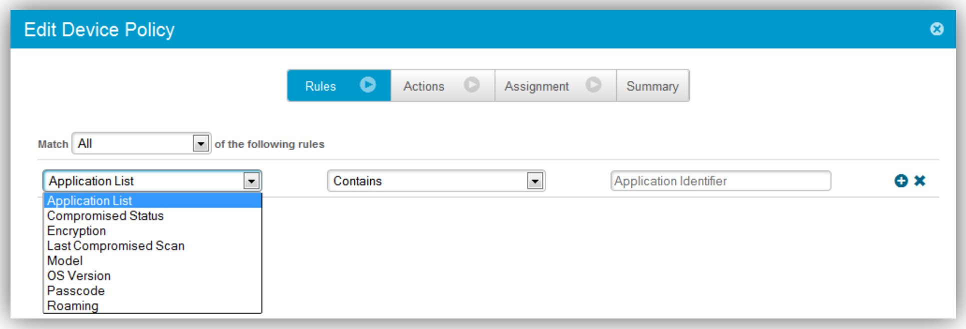
Settings & Security

Past Days of Mail to Sync: Three Days
Prevent Moving Messages ☐
Prevent Use In 3rd Party Apps ☐

Customized Compliance Policies and Actions

In addition to provisioning device restrictions, administrators of BYOD users need to have a way to monitor the security status of all devices across the smart device fleet, and respond to any policy violations. AirWatch contains a robust and highly customizable compliance policy engine to help administrators create and enforce custom policies in the following areas:

- Applications
- Last Compromised Scan
- Model
- Passcode
- Compromised Status
- Encryption
- Operating System Version
- Roaming Status

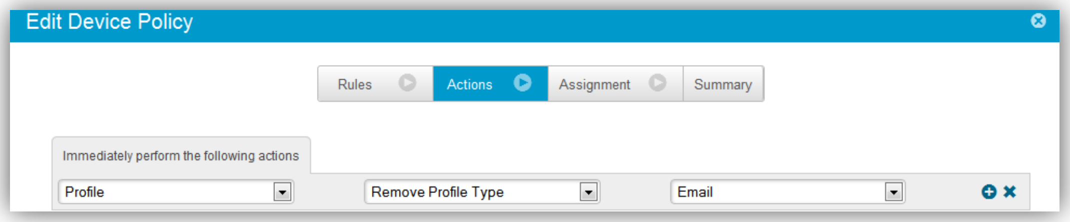


Edit Device Policy

Match All of the following rules

Application List | Contains | Application Identifier

After defining the compliance rule, administrators can determine what actions to take if the policy is violated. The response can range from sending a warning SMS or Email to removing corporate resources (such as applications and profiles) from the device.

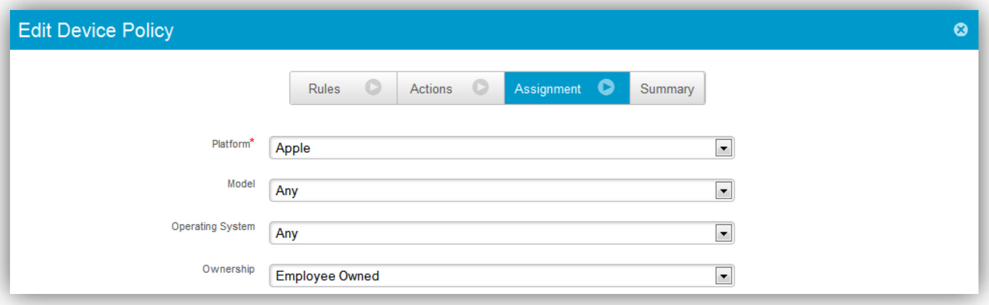


Edit Device Policy

Immediately perform the following actions

Profile | Remove Profile Type | Email

Finally, the policy can be deployed to devices according to a wide variety of criteria, including **device ownership type.**



Edit Device Policy

Platform* Apple

Model Any

Operating System Any

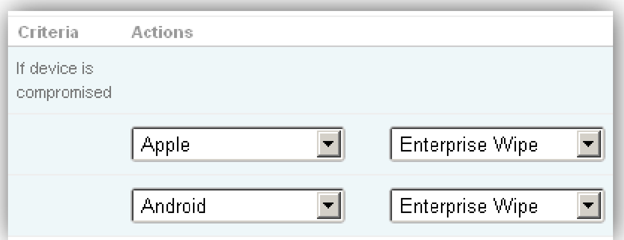
Ownership Employee Owned

The ability to leverage and enforce custom compliance policies is important for all smart device fleets, but it is especially crucial to maintaining a baseline security level when devices are employee-owned. The administrator must be able to define the mobile security standards for your organization, and tailor the response according to device ownership type.

Important Compliance Considerations

The following compliance policies, which can be created and enforced through AirWatch, will help your corporation meet the recommended levels of security for incorporating employee owned devices into the corporate workforce:

- **Encryption Enforcement**—Full device and SD card encryption (iOS 4+, Android 3.0+).
- **Passcode Policies**—A passcode should be present and enforced for any devices with access to corporate content. This provides hardware level encryption and protects information in the event of a lost or stolen device.
- **Compromised Detection**—Devices that have been modified to remove security limitations imposed by manufacturers are known as “jailbroken” or “rooted” devices and are deemed **compromised** by AirWatch. Because of the security vulnerabilities exposed on these devices they should not be granted access to corporate content. As soon as devices are detected as compromised, AirWatch can automatically remove access to all corporate content enabled through MDM.



Criteria	Actions	
If device is compromised		
	Apple	Enterprise Wipe
	Android	Enterprise Wipe

Convenient and Complete Corporate Access

Even after an organization recognizes that employee-owned devices can be fully secured to the desired extent, they often wonder whether or not this security will come at the cost of convenience to their employees. With AirWatch, you don't need to worry about your employees making this sacrifice. AirWatch recognizes that mobile access to enterprise resources needs to be both secure and convenient, and the flexible administrative tool set will help your organization determine and enforce a tailored policy for balancing mobile work and play.

Convenient Access to Email, VPN, and Wi-Fi

By integrating with corporate infrastructure and leveraging the employee accounts and hierarchy that already exists, AirWatch can **automatically configure** devices for authenticated access to:

- Email
- VPN
- Wi-Fi

To facilitate the process of integrating BYOD devices into the corporate workforce, AirWatch can automatically configure email, VPN, and Wi-Fi for your corporate network. As a "managed profile" on the device MDM administrators will have the ability to remove this access at any time.

Secure Access to Corporate Apps and Documents

AirWatch can **securely deploy** access to the following corporate resources simultaneously:

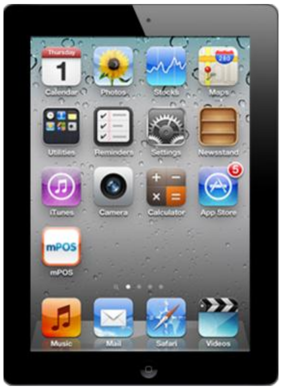
- Corporate apps
- Proprietary documents

These resources are sent directly to devices, with little to no end-user interaction.

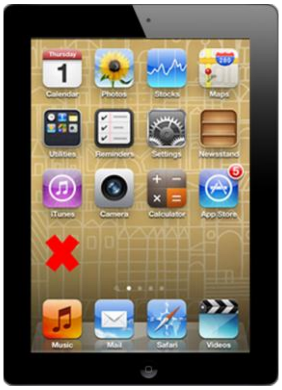
AirWatch Application Management

In addition to deploying corporate apps to your fleet of devices AirWatch can filter which device types receive certain apps. For many corporations there are proprietary apps that do not belong on personal devices. By leveraging device ownership types in AirWatch, enterprises can protect sensitive applications from employee owned devices.

Corporate Dedicated

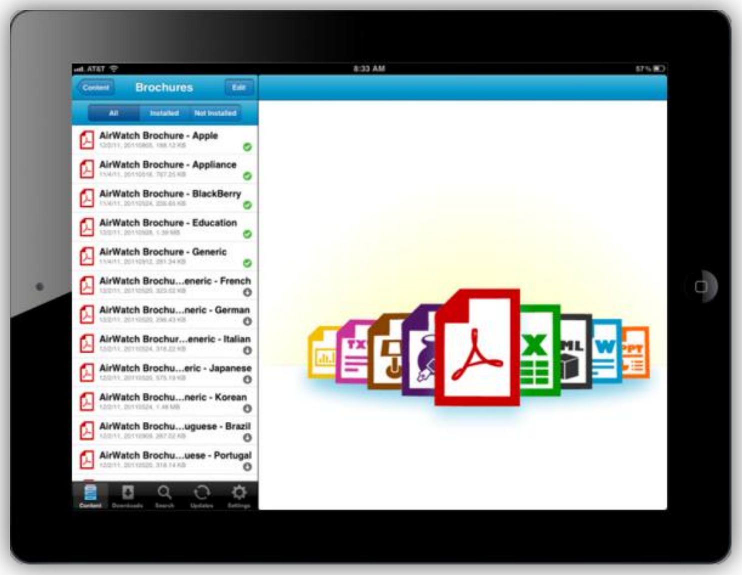


Employee Owned



Secure Content Management with the Secure Content Locker

The AirWatch Secure Content Locker enables employees to securely access corporate resources on-the-go from their mobile devices. Content can be configured to be accessed in online or offline modes and content data is encrypted on the device. Similar to managing the deployment of applications, administrators can decide through AirWatch which device ownership types have access to sensitive documents.



AirWatch Brochure - Apple

AirWatch Brochure - Appliance

AirWatch Brochure - BlackBerry

AirWatch Brochure - Education

AirWatch Brochure - Generic

AirWatch Brochu...eneric - French

AirWatch Brochu...neric - German

AirWatch Brochur...eneric - Italian

AirWatch Brochu...eric - Japanese

AirWatch Brochu...neric - Korean

AirWatch Brochu...uguese - Brazil

AirWatch Brochu...uese - Portugal

To maximize content security, AirWatch can enforce the following criteria for Secure Content Locker use:

- Require the device to be enrolled in MDM order to access content
- Prevent content access if the device is compromised
- Can only access content while online
- Prohibit opening content in another application

Providing End-User Privacy and Support

The primary concern for many BYOD users is preservation of the private and personal resources that they keep on their phone. Corporations must be able to assure employees that their personal data will not be threatened by any management actions, and that it will not be subject to corporate oversight.

For this reason, AirWatch has incorporated device ownership type into many facets of its MDM toolset, allowing corporations to customize privacy and administrative settings according to the device type.

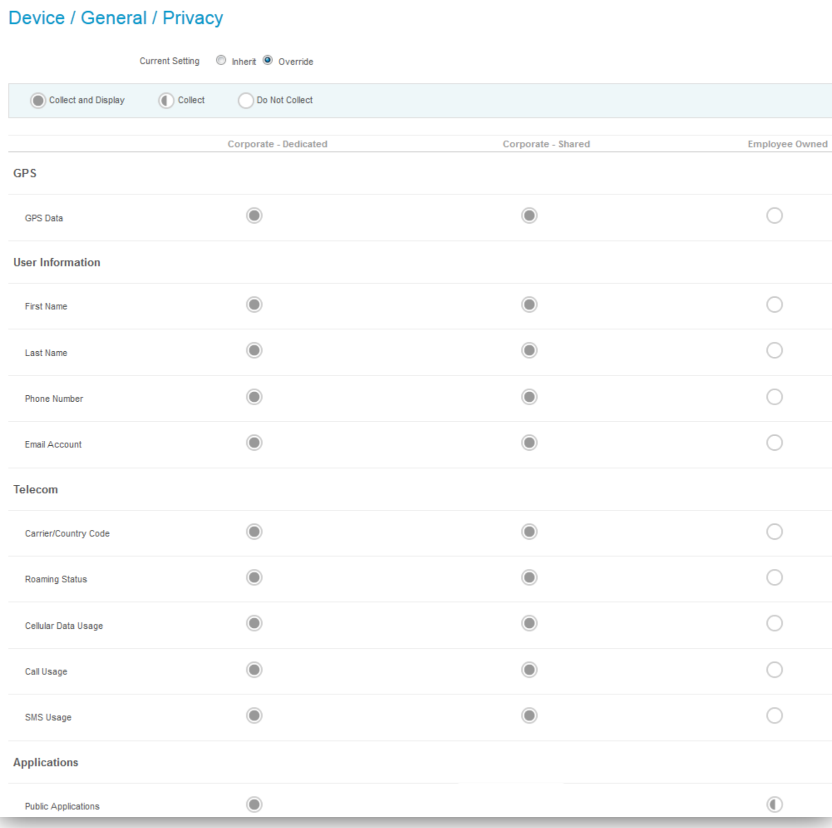
Privacy

With the influx of personal devices in BYOD deployments, AirWatch recognizes the need for preserving end-user privacy. Through AirWatch the collection of sensitive data can be turned off and customized for employee devices. Administrators have the option to disable the collection of the following data for employee-owned devices to ensure employee privacy:

- GPS coordinates
- Telecom data such as call logs, data usage, and messaging history
- Personal Information Management (PIM) data
- Application lists

Privacy Controls by Ownership Type

AirWatch can protect employee privacy by limiting the information it collects about devices. These settings are customizable by ownership type so you can maintain privacy for personal devices and still capture full administrative data for corporate dedicated ones.



Device / General / Privacy

Current Setting ○ Inherit ● Override

● Collect and Display ◐ Collect ○ Do Not Collect

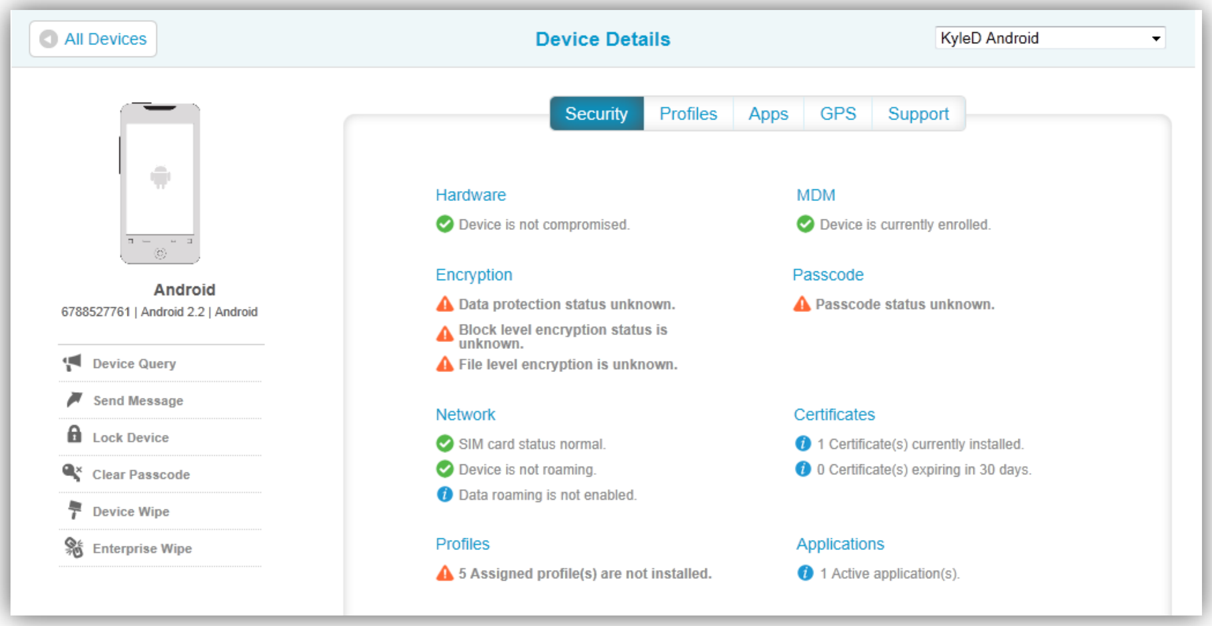
	Corporate - Dedicated	Corporate - Shared	Employee Owned
GPS			
GPS Data	●	●	○
User Information			
First Name	●	●	○
Last Name	●	●	○
Phone Number	●	●	○
Email Account	●	●	○
Telecom			
Carrier/Country Code	●	●	○
Roaming Status	●	●	○
Cellular Data Usage	●	●	○
Call Usage	●	●	○
SMS Usage	●	●	○
Applications			
Public Applications	●		◐

Customizable End-User Self-Service

MDM provides a greater level of management visibility and many remote actions options for administrators of managed smart devices, but when the devices are employee-owned, employees may wish to access equivalent management tools for their own use. The AirWatch Self-Service Portal provides a means for employees to utilize some of the key MDM tools without any IT involvement.

If enabled by the administrator, end-users can access the Self-Service Portal in a web browser to access key MDM support tools:

- View device information, such as installed apps and profiles, GPS location, and security status.
- Perform remote actions to their device from the Self-Service Portal:
  - Query the device (the device will play an alert sound)
  - Send a message to the device
  - Lock the device
  - Clear the passcode on the device
  - Enterprise Wipe: Wipes all corporate data from the selected device and removes the device from AirWatch MDM. All of the enterprise data contained on the device is removed, including MDM profiles, policies, and internal applications. The device will return to the state it was in prior to the installation of AirWatch MDM.
  - Device Wipe: Wipes all data from the device, including all data, Email, profiles, and MDM capabilities and returns the device to factory default settings.



Android
6788527761 | Android 2.2 | Android

Hardware
✓ Device is not compromised.

MDM
✓ Device is currently enrolled.

Encryption
⚠ Data protection status unknown.
⚠ Block level encryption status is unknown.
⚠ File level encryption is unknown.

Passcode
⚠ Passcode status unknown.

Network
✓ SIM card status normal.
✓ Device is not roaming.
ⓘ Data roaming is not enabled.

Certificates
ⓘ 1 Certificate(s) currently installed.
ⓘ 0 Certificate(s) expiring in 30 days.

Profiles
⚠ 5 Assigned profile(s) are not installed.

Applications
ⓘ 1 Active application(s).

The administrator can specifically enable or disable the display of information in the Self-Service portal in addition to enabling or disabling the ability to perform remote actions.

Reclaiming Corporate Data upon Employee Departure

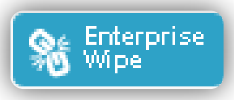
Perhaps the most worrisome aspect of enabling personal devices with corporate content is *removing* that content when employees leave, or if their devices are lost or stolen. AirWatch eliminates this concern by offering a full “**Enterprise Wipe**” for all corporate content enabled through MDM.

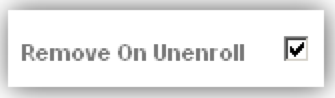
Enterprise Wipe

An enterprise wipe is designed to remove all corporate content and access while leaving personal files and settings untouched. This command essentially “un-enrolls” the device from AirWatch and strips it of all content enabled through MDM.

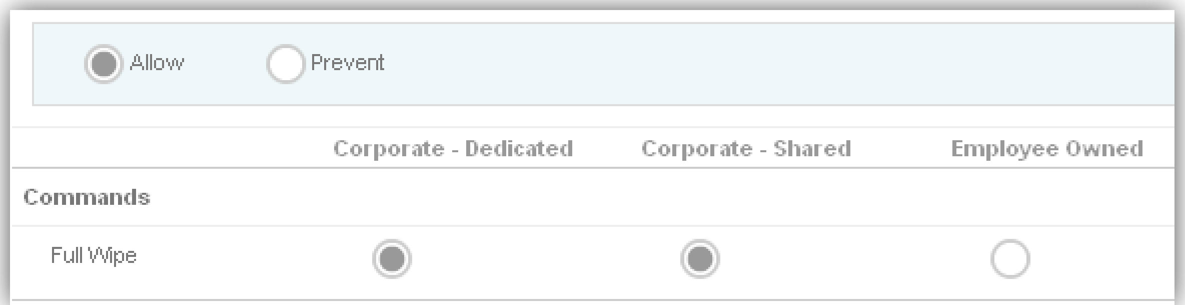
This includes:

- Email accounts
- VPN settings
- Wi-Fi profiles
- Secure content & files
- Enterprise Apps
    - For added convenience, AirWatch lets admins decide how this Wipe applies to public applications that sit in a gray area between corporate and employee owned. This functionality extends to purchased applications distributed through AirWatch using the Apple Volume Purchase Program (VPP).




Remove On Unenroll ☑

Finally, to eliminate any chance of issuing a full device wipe on personal devices, AirWatch can disable this command as an option for employee owned devices.


● Allow ○ Prevent

	Corporate - Dedicated	Corporate - Shared	Employee Owned
Commands			
Full Wipe	●	●	○

Develop a Successful BYOD Program with AirWatch

As your enterprise prepares to deploy their BYOD program, consider the following issues:

- The biggest challenge that BYOD represents in the enterprise is the question of **security vs. convenience**.
- It is important that the MDM provider acknowledges, alleviates, and supports these concerns throughout the entire device lifecycle.

AirWatch is committed to providing a functional and flexible MDM toolset that addresses the fundamental concerns about BYOD programs. We are committed to helping organizations stay on top of the latest IT trends as they securely manage devices. By integrating BYOD management tools into our core MDM offering, AirWatch makes it easy for you to incorporate BYOD into your device deployment model. AirWatch acknowledges that there are inherent concerns with BYOD, but with our secure, multi-tenant, and flexible MDM solution, administrators and end-users no longer need to worry about making the sacrifice between convenience and security in order to enjoy the flexible benefits of BYOD programs.

airwatch®

We simplify enterprise mobility