VMware AirWatch Bring Your Own Device (BYOD) and Privacy Guide

Supporting Bring Your Own Device deployments

AirWatch v9.3

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Overview

Introduction to BYOD Deployments

According to Gartner, Inc., 70% of mobile professionals will conduct business on personal smart devices by 2018 (http://www.gartner.com/newsroom/id/2466615). AirWatch has identified three operational challenges of a predominantly Bring Your Own Device (BYOD) model:

- Governance and Compliance
- Mobile Device Management
- Security

To meet these challenges in a stable enterprise-mobility sphere, AirWatch has provided its customers a ready-made BYOD environment.

> AirWatch has created a BYOD Adoption Campaign Kit to help you inform your employees about the AirWatch BYOD solution. To download the BYOD Adoption Campaign Kit, visit https://support.air-watch.com/articles/115001681528.

Supported Platforms for BYOD Deployments

AirWatch supports all major platforms as part of a BYOD deployment, including the most common platforms below:

- Android (versions 4.0+)
- iOS (versions 7.0+)
- macOS (10.9+)
- Windows Phone (Windows Phone 8/ 8.1, Windows 10 Mobile)
- Windows Desktop (8/8.1/RT/10)

BYOD Documentation Disclaimer

AirWatch strives to provide general direction for customers implementing a BYOD deployment. However, it is up to your legal, human resources, and management teams to create a specific device management plan that is right for your organization. The scenarios in this document are provided as examples, 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 VMware. VMware cannot be held liable 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.

Chapter 2:
BYOD Privacy Settings

Privacy for BYOD Deployments

One of the biggest concerns for BYOD end users is the privacy of the personal content on their devices. Your organization must assure employees that their personal data is not subject to corporate oversight.

With AirWatch MDM, you can ensure the privacy of personal data by creating customized privacy policies that do not collect personal data based on the device ownership type. In addition, you can define granular privacy settings to disable the collection of the personally identifiable information and disallow certain remote actions to employee-owned devices to ensure employee privacy.

You must inform your end users about how their data is collected and stored when they enroll into AirWatch.

> **Important:** Countries and jurisdictions have differing regulations governing the data that can be collected from end users. Your organization must thoroughly research the applicable laws before you configure your BYOD and privacy policies.

> AirWatch has created a BYOD Adoption Campaign Kit to help you inform your employees about the AirWatch BYOD solution. The kit includes material about privacy and data collection. To download the BYOD Adoption Campaign Kit, visit https://support.air-watch.com/articles/115001681508.

Configure Privacy Settings

End-user privacy is a major concern for you and your users. AirWatch provides granular control over what data is collected from users and what collected data is viewable by admins.

Configure the privacy settings to serve both your users and your business needs.

1. Navigate to **Devices** > **Device Settings** > **Devices & Users** > **General** > **Privacy**.
2. Select the appropriate setting for **GPS**, **Telecom**, **Applications**, **Profiles**, and **Network** data collection.

   ● **Collect and Display** – User data is collected and displayed in the AirWatch Console.

   ◐ **Collect Do Not Display** – User data is collected for use in reports but is not displayed it in the AirWatch Console.

   ○ **Do Not Collect** – User data is not collected and therefore it is not displayed.

3. Select the appropriate setting for the **Commands** that can be performed on devices.

   ● **Allow** – The command is made on devices without permission from the user.

   ◐ **Allow With User Permission** – The command is made on devices but only with the permission of the user.

   ○ **Prevent** – The command does not run on devices.

   Consider disabling all remote commands for employee-owned devices, especially full wipe. This disablement prevents inadvertent deletion or wiping of an end user's personal content.

Note: If you disable the wipe function for select iOS ownership types, users do not see the "Erase all content and settings" permission during enrollment.

If you are going to allow remote control, file manager, or registry manager access for Android/Windows Rugged devices, consider using the **Allow With User Permission** option. This option requires the end user to consent to admin access on their device through a message prompt before the action is performed. If you opt to allow use of any commands, explicitly mention these commands in your terms of use agreement.

4. For **User Information**, select **Display** or **Do Not Display** in the Console for the **First Name**, **Last Name**, **Phone Number**, **Email Accounts**, and **user name** data.

   If an option other than **user name** is set to **Do Not Display**, that data displays as "Private" wherever it appears in the AirWatch Console. Options you set to **Do Not Display** are not searchable in the console. When a user name is set to **Do Not Display**, the user name displays as "Private" only on the Device List View and Device Details pages. All other pages in the AirWatch Console show the user name of the enrolled user.

   You can encrypt personally identifiable information, including first name, last name, email address, and telephone number. Navigate to **Groups & Settings > All Settings > System > Security > Data Security** from the Global or Customer-level organization group you want to configure encryption for. Enabling encryption, selecting which user data to encrypt, and selecting **Save** encrypts user data. Doing so limits some features in the AirWatch Console, such as search, sort, and filter.

5. Select whether to **Enable** or **Disable** the **Do Not Disturb Mode** on the device. This setting lets user devices ignore MDM commands for a specified period. When Enabled, you can select a grace period or activation time in minutes, hours, or days, after which the **Do Not Disturb Mode** expires.

   For more information about using Do Not Disturb Mode, see the following VMware AirWatch Knowledge Base article: https://support.air-watch.com/articles/115001662448.

6. Select to **Enable** or **Disable** the **User-Friendly Privacy Notice** on the device.

   - When **Enabled**, you may choose **Yes** (display a privacy notice) or **No** (do not display a privacy notice) for each ownership level: **Employee Owned**, **Corporate - Dedicated**, **Corporate - Shared**, and **Unknown**.

7. Click **Save**. You must enter your PIN to save the changes. Click **Save**.

Privacy Notices for BYOD End Users

A privacy notice informs your end users about what data you collect from their devices based on their device type, deployment type, and ownership type.

Privacy Notice Configuration

Privacy notices are automatically delivered based on the organization group and device ownership of the device connecting. You may choose to display a privacy notice for each ownership type: **Employee Owned**, **Corporate - Dedicated**, **Corporate - Shared**, and **Unknown**.

You must create a privacy notice before you assign ownership types to receive the notice. For more information, see Create a Privacy Notice for BYOD Users on page 9. See Create a Privacy Notice in the **VMware AirWatch BYOD & Privacy Guide**, available through AirWatch Resources.

Privacy Notice Deployment

When you assign an ownership type to receive privacy notices, all users in the selected ownership type receive the privacy notification immediately as a Web clip. If you inserted the privacy notice lookup value `PrivacyNotificationUrl` in your message template, then the message includes a URL where the user can read the privacy notice.

Users receive the privacy notice automatically if:

- They enroll a new device and they are of an ownership type for which the privacy notice is enabled.
- They currently use an enrolled device and their ownership is changed post-enrollment to a type that is assigned the Web clip.

To learn how to deploy a privacy notice as part of a device activation, see **Register an Individual Device** in the **VMware AirWatch Mobile Device Management Guide**, available through AirWatch Resources.

Create a Privacy Notice for BYOD Users

Inform your users about what data your company collects from their enrolled devices with a customized privacy notification. Work with your legal department to determine what message about data collection you communicate to your end users.

1. Navigate to **Groups and Settings > All Settings > Devices and Users > General > Message Templates**.
2. Select **Add** to create a template. If you have already created a privacy notification template, select it from the list of available templates to use or edit it.
3. Complete the **Add/Edit Message Template** settings.

Setting	Description
Name	Enter a name for the notification template.
Description	Enter a description of the template you are creating.
Category	Select **Enrollment**.
Type	Select **MDM Device Activation**.
Select Language	Select the default language for your template. Use the **Add** button to add more default languages for a multi-language delivery.
Default	Select this check box to make this template the default message template.
Message Type	Select one or more message types: **Email**, **SMS**, or **Push** message.

4. Create the notification content. The message types that you selected in the **Message Type** selection determine which

messages appear for you to configure.

Element	Description
	Email
Email Content Formatting	Choose whether your email notification is delivered as **Plain Text** or **HTML**.
Subject	Enter the subject line for your email notification.
Message Body	Compose the email message to send to your users. The editing and formatting tools that appear in this text box depend on which format you chose in the **Email Content Formatting** selection. If you have enabled the Visual Privacy Notice, include the lookup value `PrivacyNotificationUrl` in the message body.
	SMS
Message Body	Compose the SMS message to send to your users. If you have enabled the Visual Privacy Notice, include the lookup value `PrivacyNotificationUrl` in your message body.
	Push
Message Body	Compose the Push notification to send to your users. If you have enabled the Visual Privacy Notice, include the lookup value `PrivacyNotificationUrl` in your message body.

5. Select **Save**.

User Data Collection from BYOD End Users

The AirWatch infrastructure collects and stores many types of user-generated data. The following matrix matches each data type to the platforms and operating systems from which the data can be collected.

Use this matrix to determine which data collection is necessary for your deployment. AirWatch also defines optional data that you can collect, such as Bluetooth MAC. You can configure these options and assign privacy settings by ownership type: dedicated corporate, shared corporate and employee owned.

	Android	Apple iOS	macOS	Windows Rugged	Windows Phone	Windows 7	Windows Desktop
Application Tracking							
View installed internal apps	✓	✓	✓	X	✓	✓	✓
View app versions	✓	✓	✓	X	✓	✓	✓
Capture app status	✓	X	✓	X	✓	X	✓
Certificates							
View list of installed certificates	✓	✓	✓	X	✓	X	✓ *
Asset Tracking							
Device Name	✓	✓	✓	✓	✓	✓	✓
Device UDID	✓	✓	✓	✓	✓	✓	✓
Phone Number	✓	✓	X	✓	✓	X	✓
IMEI/MEID Number	✓	✓	X	✓	✓	X	✓
Device serial number	✓	✓	✓	✓	✓	✓	✓
IMSI number	✓	X	X	✓	✓	X	✓
Device model	✓	✓	✓	✓	✓	X	X
Device model name (Friendly)	X	✓	✓	✓	✓	X	X
Manufacturer	✓	✓	✓	✓	X	X	✓
OS Version	✓	✓	✓	✓	✓	✓	✓
OS Build	✓	X	✓	✓	✓	✓	✓
Firmware/kernel version	X	X	✓	X	X	X	X
Track device errors	X	X	✓	✓	✓	✓	✓
Device Status							
Battery available	✓	✓	✓	✓	✓	✓	✓
Battery capacity	✓	✓	✓	✓	✓	X	X
Memory available	✓	✓	✓	✓	X	✓	X
Memory capacity	✓	✓	✓	✓	X	✓	X

	Android	Apple iOS	macOS	Windows Rugged	Windows Phone	Windows 7	Windows Desktop
Location							
GPS tracking	✓	✓ **	✓	✓	✓	X	✓
Network							
Wi-fi IP Address	✓	✓	✓	✓	✓	✓	✓
Wi-fi MAC	✓	✓	✓	✓	✓	✓	✓
Wi-fi signal strength	X	X	✓	✓	X	✓	✓
Carrier Settings version	✓	✓	X	X	X	X	X
Cell signal strength	✓	X	X	X	X	X	X
Cell technology (none, GSM, CDMA)	✓	✓	X	X	X	X	X
Current MCC	✓	✓	X	X	X	X	X
Current MNC	✓	✓	X	X	X	X	X
SIM card number	✓	✓	X	X	✓	X	✓
SIM carrier network	✓	✓	X	X	X	X	X
Subscriber MNC	✓	✓	X	X	X	X	X
Bluetooth MAC	✓	✓	✓	X	✓	✓	X
Show IP addresses	✓	✓	✓	X	✓	✓	X
Show LAN adapters	X	X	✓	X	X	✓	X
Show MAC address	✓	✓	✓	X	✓	✓	X
Roaming							
Detect roaming status	✓	✓	X	X	✓	X	X
Disable Push notifications when roaming	X	✓	X	X	X	X	X
Voice roaming enabled (allowed)	X	✓	X	X	X	X	X
Data Usage							
Track data usage through cell network	✓	✓	X	X	X	X	X
Track data usage through Wi-fi network	X	X	X	X	X	X	X
Calls							
Track call history	✓	X	X	X	X	X	X

	Android	Apple iOS	macOS	Windows Rugged	Windows Phone	Windows 7	Windows Desktop
Messages							
Track SMS history	✓	X	X	X	X	X	X
Cellular Status							
Current Carrier network	✓	✓	X	X	✓	X	X
Current network status	✓	✓	X	X	X	X	X
Remote View							
Remotely control device	✓	X	✓	✓	X	✓	✓
Screen capture (save, email, print, etc.)	✓	X	✓	✓	X	✓	✓
Screen sharing (remote view within apps)	✓	✓	X	✓	X	✓	✓
File Manager							
Access device file manager	✓	X	✓	✓	X	✓	✓
Access device registry manager	X	X	X	✓	X	✓	✓
Copy files	✓	X	✓	✓	X	✓	✓
Create folders	✓	X	✓	✓	X	✓	✓
Download files from device	✓	X	✓	✓	X	✓	✓
Move files	✓	X	✓	✓	X	✓	✓
Rename folders and files	✓	X	✓	✓	X	✓	✓
Upload files to device	✓	X	✓	✓	X	✓	✓

✓ - Can be collected

X - Cannot be collected

✓ * - Can be collected on AirWatch Agent deployments

✓ ** - Can be collected on AirWatch Agent or iOS 9.3+Supervised Mode deployments

Chapter 3:
BYOD Terms of Use

Terms of Use for BYOD End Users

For liability reasons, you must inform employees about the data that is captured and the actions that are allowed on devices enrolled in AirWatch. To help communicate your strategy, create Terms of Use agreements in the AirWatch Console.

Users are prompted to read and accept the terms of use you configure before they can enable MDM on their personal devices. By assigning Terms of Use agreements based on the ownership type, you can create and distribute different agreements for corporate and BYOD users.

After your organization has written its Terms of Use agreement, consider giving it to end users in a one to two-page white paper that omits unnecessary legal language. This white paper is not the official Terms of Use to which end users agree, but instead serves to communicate your corporate policies. Ideally, end users do not see the terms of use for employee-owned devices for the first time when they enroll their device. Be upfront about what end-user information you collect and how your BYOD policies affect them.

Create Enrollment Terms of Use

You can create an agreement about terms of use (TOU) specific to enrollment purposes. You can also limit devices allowed for enrollment by device platform, ownership type, and enrollment type.

1. Ensure that your current active organization group is correct for the TOU you are creating.
2. Navigate to **Devices** > **Device Settings** > **Devices & Users** > **General** > **Enrollment** and select the **Terms of Use** tab.
3. Select the **Add New Enrollment Terms of Use** button and complete the following options.

Setting	Description
Name	Enter a unique name for the new TOU.
Type	This option is pre-populated as **Enrollment**.
Version	This option is automatically tracked and populated accordingly.
Platforms, **Device Ownership**, and **Enrollment Type**	If you do not want to make your TOU for any specific category of device, then keep the default selection of **Any** for these options. If you prefer to specify a platform, ownership, and enrollment, you can select one or more of these categories and define the limitations specific to your TOU. • If you select **Selected Platform** option, then choose your desired platforms from the list that appears. Your TOU applies to the device platforms you select, excluding all others. • If you select **Selected Ownership Types** option, then you must choose your desired ownership from the list that appears. Your TOU applies to the ownership types you select, excluding all others. • If you select **Selected Enrollment Types** option, then you must choose your desired enrollment from the list that appears. Your TOU applies to the types of enrollment you select, excluding all others.

Setting	Description
Notification	Send an email to users whenever the TOU is updated by selecting this check box. The notification email is sent when you select **Save** in step 5.
Select Language	Optionally, for localization purposes, you may enter a TOU agreement for each language applicable to your needs by making a choice in the **Select Language** drop-down.

4. In the text box provided, enter your customized TOU.

   The editor provides a basic text entry tool to create a TOU or paste in an existing TOU. To paste text from an external source, right-click the text box and choose **Paste as plain text** to prevent any HTML or formatting errors.

5. Select **Save**.

You can enforce MDM terms of use acceptance by creating a compliance policy for **MDM Terms of Use Acceptance**. This enforcement does not apply to devices using AirWatch Container.

BYOD Terms of Use Recommendations

Your legal team must carefully consider how to tailor your terms of use for personal devices. Reference a more extensive document, hosted elsewhere, which details your legal agreements at length.

A few items to highlight in the Terms of Use agreement are:

- Key MDM allowances (such as administrator permissions).
- User obligations if a device is lost or stolen.
- Devices (platforms, operating systems, versions) granted access to corporate resources.
- Corporate resources (email and calendars, for example) that users can access through their personal devices.
- Security policies about sensitive information. Acknowledge that the device is enabled with proprietary corporate data and is subject to enterprise security policies. For example, include details about a passcode profile that sets a maximum number of failed passcode attempts before a device is wiped.
- Inappropriate behaviors that are not tolerated according to your normal business standards, such as using the device to harass others.
- Reimbursement policies for telecom and other costs. For example, whether you have a stipend plan for telecom charges, the cost of apps (personal vs. work-related), and roaming charges.

One option is to modify an existing document that employees sign for computer use and access. Customize this document to BYOD by including the information that is collected from employee-owned devices.

Chapter 4:
BYOD Enrollment

BYOD Enrollment

A major challenge in managing employee-owned devices is balancing the need for end-user privacy and enterprise security. AirWatch helps address these concerns by providing two types of enrollment for BYOD users.

AirWatch helps you customize how the end user enrolls a personal device. Before you begin, consider how you plan to manage employee-owned devices. For example, you can:

- Require employee-owned devices to enroll using the AirWatch Container application.
- Require employee-owned devices to enroll using the AirWatch Agent.
- Permit employees who enroll their own devices to select their Group ID or ownership type.
- Add corporate-owned whitelisted devices, then set all other devices that enroll to "employee-owned" by default.
- Allow or block certain platforms or operating systems based on your enterprise security requirements.

The following sections detail these considerations and help you determine the best enrollment configuration for your environment.

Device Ownership Types

Every device enrolled into AirWatch has an assigned device ownership type: corporate dedicated, corporate shared, or employee-owned. Personal devices fall under the employee-owned type and are subject to the specific privacy settings and restrictions you configure for that type.

For both AirWatch Container-based and Agent-based enrollment, you have the following options:

Upload a List of Corporate Devices - Best Practice

You can identify a set list of corporate devices, which is useful if you have a mix of corporate-owned and employee-owned devices. As devices are enrolled, items on a pre-approved list automatically have their ownership type configured based on the ownership type you selected (either Corporate Owned or Corporate Shared). Then you can configure all other devices (end-user personal devices) to set their ownership type as Employee Owned automatically.

Configure AirWatch to Apply a Default Ownership Type During Enrollment - Best Practice

You can set the **Default Device Ownership** type to Employee Owned, or you can create a restriction that only allows Employee Owned as the ownership type during open enrollment. These restrictions ensure that any device that enrolls into this applicable organization group lists as Employee Owned by default. Corporate devices do not default to Employee Owned, since those devices are updated post-enrollment to reflect their Corporate Owned status.

Allow Users to Choose the Appropriate Ownership Type

While simpler for the admin, this approach assumes that every user selects the appropriate ownership type for their device during enrollment. If a BYOD user chooses the Corporate-Owned ownership type, their device is subject to policies and profiles that normally do not affect an employee-owned device. Misapplied policies can have serious legal implications regarding user privacy. While you can always update the ownership type later, it is better to identify a list of corporate devices and then set the default ownership type to Employee Owned.

Prompt BYOD Users to Identify Ownership Type

If you have organization groups with multiple ownership types, you can prompt users to identify their ownership type during enrollment.

1. Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment**. Click the **Optional Prompt** tab.
2. Select **Prompt for Device Ownership Type**. During enrollment, users are prompted to select their ownership type.
3. Click **Save**.

Specify Default Device Ownership for BYOD Devices

Create a restriction that lists all devices as Employee Owned during enrollment. These restrictions ensure that any device enrolling into the selected organization group defaults to Employee Owned.

1. Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment**. Click the **Grouping** tab.
2. Select **Employee Owned** as the **Default Device Ownership**.
3. Select the **Default Role** assigned to enrolled users. Roles determine the levels of access users have to the Self-Service Portal.
4. Select the **Default Action** for **Inactive Users**, which determines what the Console does if the user is flagged as inactive.
5. Click **Save**.

Configure Enrollment Restriction Settings

When integrating AirWatch with directory services, you can determine which users can enroll devices into your corporate deployment.

You can restrict enrollment to only known users or to configured groups. Known users are users that already exist in the AirWatch Console. Configured groups are users associated to directory service groups if you choose to integrate with user groups. You can also limit the number of devices enrolled per organization group and save restrictions as a reusable policy.

These options are available by navigating to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and choosing the **Restrictions** tab. The Restrictions tab allows you to customize enrollment restriction policies by organization group and user group roles.

- Create and assign existing enrollment Restrictions policies using the Policy Settings.
- Assign the policy to a user group under the Group Assignment Settings area.
- Blacklist or whitelist devices by platform, operating system, UDID, IMEI, and so on.

For information about integrating your directory services groups with AirWatch, refer to the **VMware AirWatch Directory Services Guide** document, available on AirWatch Resources.

Setting	Description
User Access Control	All user access control options are supported by Workspace ONE Direct Enrollment. **Restrict Enrollment to Known Users** – Enable to restrict enrollment only to users that already exist in the AirWatch Console. This applies to directory users you manually added to the AirWatch Console one by one or through batch import. It can also be used to lock down enrollment after an initial deployment that allowed anyone to enroll. This enables you to selectively allow users to enroll. Disable this option to allow all directory users who do not already exist in the Admin Console to enroll into AirWatch. AirWatch user accounts are automatically created during enrollment. **Restrict Enrollment to Configured Groups** – Enable to restrict enrollment and only allow users belonging to All Groups or Selected Groups (if you have integrated with user groups) to enroll devices. You should not select this option if you have not integrated with your directory services user groups. Disable this option to allow all directory users to create new AirWatch user accounts during enrollment. In addition, you can select the **Enterprise Wipe devices of users that are removed from configured groups** option to automatically enterprise wipe any devices **not** belonging to any user group (if **All Groups** is selected) or a particular user group (if **Selected Groups** is selected). One option for integrating with user groups is to create an "MDM Approved" directory service group, import it to AirWatch, then add existing directory service user groups to the "MDM Approved" group as they become eligible for AirWatch MDM.
Set limit for maximum enrolled devices at this OG and below	Enable and **Enter Device Limit** to limit the number of devices allowed to enroll in the current organization group (OG). Setting a maximum enrolled devices is supported by Workspace ONE Direct Enrollment.

Note: Restrictions do not apply for iOS devices enrolled through Apple's Device Enrollment Program (DEP), because the required device information is only received after the device has been enrolled.

Upload a List of Corporate Devices for BYOD Enrollment

Because corporate devices enterprise-owned, they can be preapproved for AirWatch enrollment.

Before your non-BYOD users enroll, add their assigned corporate devices to a preapproved list. These devices automatically have their ownership type configured based on the ownership type you selected (either Corporate Owned or Corporate Shared).

1. Navigate to **Devices > Lifecycle > Enrollment Status** and select **Add**, then **Batch Import**.

   Alternatively, you can select **Whitelisted Devices** to enter up to 30 whitelisted devices at a time by IMEI, UDID, or Serial Number. Also, select either **Corporate Owned** or **Corporate Shared** as the Ownership Type.

2. Enter a **Batch Name** and **Batch Description**, then select **Add Whitelisted Device** as the **Batch Type**.

3. Select **Choose File** to upload a file or select the **Information** icon to download a sample template.

   If you are saving a template, fill out the required information.

4. Select **Save**.

Chapter 5:
BYOD Device Management

Restrictions for BYOD Devices

AirWatch permits you to deploy different security policies and restrictions to employee-owned and corporate-dedicated devices.

Using restriction profiles, you can set tight restrictions for corporate-dedicated devices, and looser restrictions for employee-owned devices. For example, restrictions to apps like YouTube or native App Stores are not typically deployed to employee-owned devices. Instead, you can create security profiles and restrictions that increase the level of device security without having a negative impact on functionality.

Device-Agnostic Restrictions

AirWatch makes the following restrictions available for every device and platform:

- **Encrypted backups** - Protect all backups with data encryption for BYOD devices with access to corporate content.
- **Force fraud warning in supported browsers** - Require 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.

Platform-Specific Restrictions

Each platform has its own set of enforceable restrictions. Evaluate these restrictions individually to determine their value to your deployment. Some, like iOS restrictions limited to supervised devices, do not apply, because employee-owned devices must not be enrolled with Apple Configurator.

- You can create security profiles and restrictions by navigating to **Devices > Profiles > List View** and selecting **Add**, then selecting the appropriate platform.
- If you create profiles specifically for employee-owned devices, only assign them to Smart Groups based on Ownership Type: Employee-Owned.

Compliance Policies for BYOD Devices

AirWatch provides a robust and highly customizable compliance policy engine that can help you create and enforce policies for employee-owned devices.

The compliance engine is a tool which ensures that all your enrolled devices abide by your policies, such as requiring a passcode and having a minimum device lock period.

When a device is determined to be out of compliance, the compliance engine warns users to address detected compliance errors. If the errors are not corrected in the specified time, the device loses access to content and functions according to the policies you define. Compliance policies and actions vary by platform.

Compliance policies appropriate for employee-owned devices include:

- **Encryption Enforcement**: Require full device and SD card encryption.
- **Passcode Policies**: Require a device or app passcode. Passcode policies provide hardware-level encryption and protect information in case a device is lost or stolen.

Explicitly inform end users of any passcode policies, such as maximum failed attempts before device lock, in your Terms of Use agreement.

- **Compromised Detection**: Because of the security risks to which jailbroken or rooted devices are exposed, they must not be granted access to corporate content. When devices are detected as compromised, AirWatch can automatically remove access to all corporate content enabled through MDM.
- **MDM Terms of Use Acceptance**: Ensure that users accept your Terms of Use agreement by performing escalating actions that increasingly restrict access to corporate content the longer users go without accepting.

You can create compliance policies in the AirWatch Console by navigating to **Devices > Compliance Policies > List View** and selecting **Add**. Select the correct **Ownership** type on the **Assignment** tab for the devices you are configuring.

Compliance Policy Rules by Platform

Not all compliance policy rules apply to all platforms. The **Add a Compliance Policy** page is platform-based so you see only the compliance policy rules and actions that apply to your device.

Use the following table to determine which rules are available to deploy to your devices.

Compliance Policy	Android	Apple iOS	Apple macOS	Chrome OS	QNX	Windows Rugged	Windows 7	Windows Phone	Windows Desktop
Application List	✓	✓	✓						
Antivirus Status									✓
Cell Data Usage	✓	✓							
Cell Message Usage	✓								
Cell Voice Usage	✓								
Compliance Attribute									✓
Compromised Status	✓	✓							✓
Device Last Seen	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Manufacturer	✓								
Encryption	✓	✓	✓				✓	✓	✓
Firewall Status			✓						✓
Free Disk Space		✓							
iBeacon Area		✓							
Interactive Certificate Profile Expiry	✓	✓							
Last Compromised Scan	✓	✓							
MDM Terms of Use Acceptance	✓	✓	✓			✓	✓	✓	✓
Model	✓	✓	✓					✓	
OS Version	✓	✓	✓	✓			✓	✓	✓
Passcode	✓	✓					✓	✓	✓
Roaming *	✓	✓							✓
Roaming Cell Data Usage *	✓	✓							
Security Patch Version	✓								
SIM Card Change *	✓	✓						✓	
Windows Automatic Update Status									✓
Windows Copy Genuine Validation							✓		

* **Note:** Only available for Telecom Advanced Users.

Enterprise Content Management for BYOD Devices

The VMware Content Locker enables your employees to access corporate resources securely from their mobile devices.

Admins can configure which device ownership types have access to sensitive documents. To maximize content security as part of your BYOD deployment, you can manage the following security features:

- Require the device to be enrolled to access content. This policy ensures that employee-owned devices are subject to security profiles and compliance policies before they have access to sensitive content.
- Prevent content access if the device is compromised. This policy maximizes security by preventing potentially vulnerable devices from accessing content.
- Allow access to content only while online. This policy ensures that the device is compliant with your AirWatch policies. Compliance cannot be verified if the device is offline and cannot report in.
- Edit the **Assignment** criteria for specific content. For example, determine if certain sensitive content is not accessible by employee-owned devices.

For more information about securing access to sensitive content, see the **VMware AirWatch Content Locker Guide**, available on AirWatch Resources.s

Corporate Email, VPN, and Wi-Fi on BYOD Devices

Configuration profiles permit employee-owned devices to access and authenticate email, VPN, and Wi-Fi settings. Because these profiles are managed, you can remove access to these resources at any time.

For instructions about creating configuration profiles, refer to the specific platform guides and the **Mobile Device Management Guide**, available on AirWatch Resources.

Email Containerization

Employee-owned devices can use **Boxer** for secure access to corporate email. This containerized solution requires a passcode to access email, but does not force end users to enter a passcode to access their devices. It also provides separation between personal and work content.

VPN Access

AirWatch manages device VPN settings so end users can remotely and securely access your organizations internal network. The VPN profile provides detailed VPN setting control, including specific VPN provider settings and Per-App VPN access.

Wi-Fi Profiles

A Wi-Fi profile permits devices to connect to corporate networks, even if they are hidden, encrypted, or password-protected. This profile is useful for end users who travel to office locations that have their own wireless networks. Wi-Fi profiles configure devices to connect to the appropriate wireless network.

Internal Applications on BYOD Devices

AirWatch can filter which device types in your fleet receive certain applications. By using device ownership types in AirWatch, you can protect sensitive applications from employee-owned devices.

For example, your organization might have certain proprietary applications that must not be deployed to personal devices. When you create or edit smart groups, you can modify the **Ownership** type to include or exclude Employee Owned devices.

Enterprise Wipe for BYOD Devices

An essential aspect of your BYOD deployment is removing corporate content when an employee leaves, or when a device is lost or stolen. AirWatch allows you to perform an Enterprise Wipe on devices to remove all corporate content and access, but leave personal files and settings untouched.

AirWatch lets you decide how an Enterprise Wipe applies to public and purchased VPP applications that sit in a gray area between corporate and employee-owned devices. An Enterprise Wipe also unenrolls the device from AirWatch and strips it of all content enabled through MDM. This content includes email accounts, VPN settings, Wi-Fi profiles, secure content, and enterprise applications.

If you used Apple Volume Purchase Plan redemption codes for devices running iOS 6 and earlier, you cannot reclaim any redeemed licenses for that application. When installed, the application is associated to the user App Store account. This association cannot be undone. However, you can redeem license codes used for iOS 7 and later.

Perform an Enterprise Wipe for a BYOD Device

An enterprise wipe unenrolls the device from AirWatch and strips it of all enterprise content, including email accounts, VPN settings, profiles, and applications.

To unenroll a device and remove all access to enterprise content and settings:

1. In the Admin Console, select the appropriate organization group.
2. Navigate to **Devices > List View** and select a device or multiple devices from the list.
3. The Device Details view displays a list of actions you can perform under the **More** drop-down in the top right. Select **Enterprise Wipe**.
4. In the confirmation dialog box, select **Prevent Re-Enrollment** to prevent this device from enrolling again.
5. Enter a Security PIN if applicable, and then select **Enterprise Wipe** to finish the action.

Remove BYOD User Access to Apps

AirWatch lets you decide how Enterprise Wipes apply to public and purchased VPP applications in the gray area between corporate and employee-owned devices.

To require an application to uninstall:

1. Navigate to **Apps & Books > Applications > Native**.
2. Select whether to view Public, Internal, or Purchased applications, and select the application name from the list.

3. The application screen displays. Click **Edit**.

4. To remove an application, select the **Deployment** tab, if it displays. Check **Remove on Unenroll**.

Disable Full Wipe for BYOD Devices

For security and privacy reasons, you can disable the ability to perform a full wipe on a BYOD Device.

To disable full wipes for employee-owned devices:

1. Navigate to **Devices > Device Settings > Devices & Users > General > Privacy**.

2. Scroll down to the **Commands** section and find the **Employee Owned** column.

3. Set the **Full Wipe** option to **Prevent** and select **Save**.

If you disable full wipe for select iOS ownership types, then users enrolling under that ownership type do not see "Erase all content and settings" permissions during profile installation.

Chapter 6:
AirWatch Self-Service Portal

AirWatch Self-Service Portal

AirWatch gives administrators several remote actions and options for managed devices. The AirWatch Self-Service Portal (SSP) allows employees to access similar management tools for their own use.

The AirWatch SSP provides a means for employees to use some key MDM tools without any IT involvement. If you enable it, end users can run the SSP in a Web browser and access key MDM support tools. You can also enable or disable the displays of information and the ability to perform remote actions from the SSP.

By empowering and educating device users on how to perform basic device management, and investigate and fix problems, you may reduce end user help desk tickets and support issues.

The Self-Service Portal automatically matches the browser default language. However, you can override this default setting by choosing from the **Select Language** drop-down on the login screen.

Self-Service Portal Tabs

The Self-Service Portal is organized into tabs that let the user easily navigate to the function or setting they need.

When a user logs in to the SSP, their primary device appears in the main viewer. The main view page displays basic information such as **Enrollment Date**, the **Last Seen** date, and the device **Status**.

The **Go to Details** button displays tabs containing information about the selected device under the selected user account.

Tab	Description
Security	Shows general security information about a particular device enrolled under your user account.
Compliance	Shows the compliance status of the device, including the name and level of all compliance policies that apply to the device. It is important for end users to take note of these policies to ensure that devices remain compliant and operate as intended.
Profiles	Shows all the MDM profiles that have been sent to the devices enrolled under your user account and the status of each profile.
Apps	Lists all applications that have been installed on the selected device and provides basic application information.
Location	Reports the coordinates of the selected device.
Event Log	Contains a comprehensive log of all interactions between the AirWatch Console and the device.
Support	Contains detailed device information and contact information for your support representatives.

Remote Actions on the Self-Service Portal

The **Remote Actions** menu, if enabled, allows users to perform remote actions over the air to their selected devices. Registration and Enrollment actions only display in the SSP when the enrollment of a selected device is still pending.

Portal access rights affect which remote actions are available to users. The table shows all SSP actions that are available to end users.

Action	Description
Change Passcode	Set a new passcode for the selected device.
Clear Passcode	Clear the passcode on the selected device and will prompt for a new passcode. This is useful if users forget their device passcode and are locked out of their device.
Delete Device	Remove the device from the Self Service Portal.
Delete Registration	Delete any pending enrollment record from the Self Service Portal.
Device Query	Request the device to send a comprehensive set of MDM information to the AirWatch Server.
Device Wipe	Wipe all data from the selected device, including all data, email, profiles and MDM capabilities and returns the device to factory default settings.
Download Agent	Download and install the AirWatch Agent to the device from which you are viewing the SSP.
Enterprise Wipe	Wipe 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.
Locate Device	Activate the GPS feature to locate a lost or stolen device. This action is hidden when privacy settings are restrictive.
Lock Device/Screen	Locks the selected device so that an unauthorized user cannot access it, which is useful if the device is lost or stolen. End-users may also want to use the GPS feature to locate the device.
Lock SSO	Lock the single sign on passcode for apps on this device. The next SSO app opened will prompt for a passcode.
Make Noise	Rind a device by remotely causing it to ring.
Resend Enrollment Message	Send another copy of the initial enrollment email, SMS or QR code to the device intended to register.
Send Message	Send a message using email, phone notification or SMS to the device.
Set Roaming	Set whether roaming is enabled for this device.
Sync Device	Outfit devices with the latest company policies, content, and apps.
View Enrollment Message	See the actual email, SMS, or QR code that comprised the initial enrollment message.

Self-Service Portal Actions by Device Platform

From the **Remote Actions** menu, end users can perform remote actions over the air to their devices. Registration and Enrollment actions only display in the Self-Service Portal (SSP) when the enrollment of a selected device is still pending.

The mobile device platform determines which remote actions are available to the user.

The table below shows the basic and advanced SSP actions that are supported by the various major platforms.

Action	Android	iOS	Win Phone	macOS	Win Mobile	Win 7	Win Desktop
Basic Actions							
Change Passcode	✓						

Action	Android	iOS	Win Phone	macOS	Win Mobile	Win 7	Win Desktop
Clear (SSO) Passcode	✓	✓	✓				✓
Delete Device	✓	✓	✓	✓	✓	✓	✓
Delete Registration	✓	✓			✓	✓	✓
Device Query	✓	✓		✓		✓	✓
Device Wipe	✓	✓	✓	✓	✓		
Download Agent				✓		✓	
Enterprise Wipe	✓	✓	✓	✓	✓	✓	✓
Locate Device	✓	✓	✓		✓		
Lock Device/Screen	✓	✓		✓	✓	✓	
Lock SSO		✓	✓				
Make Noise	✓						
Resend Enrollment Message	✓	✓			✓	✓	✓
Send Message	✓	✓	✓	✓	✓	✓	✓
Set Roaming		✓					
Sync Device	✓	✓					
View Enrollment Message	✓	✓			✓	✓	✓
Advanced Actions							
Generate App Token	✓	✓	✓	✓	✓	✓	✓
Manage Email					✓	✓	✓
Review Terms of Use	✓	✓	✓	✓	✓	✓	✓
Revoke Token	✓	✓	✓	✓	✓	✓	✓
Upload S/MIME Certificate	✓	✓	✓	✓	✓	✓	✓

Create a New User Role

In addition to the preset Basic Access and Full Access roles, you can create customized roles. Having multiple user roles available fosters flexibility and can potentially save time when assigning roles to new users.

To create a user role:

1. Navigate to **Accounts > Users > Roles** and select **Add**. The **Add/Edit Role** page displays.
2. Enter a **Name** and **Description**, and select the **Initial Landing Page** of the SSP for users with this new role.

   For existing user roles, the default **Initial Landing Page** is the **My Devices** page.

3. Select from a list of options the level of access and control end users of this assigned role have in the SSP.
   - Click **Select None** to clear all check boxes on the page.
   - Select all the check boxes on the page by selecting **Select All**.
4. **Save** the changes to the role. The added user role now appears in the list on the Roles page.

From the Roles page, you can view, edit, or delete roles.

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.