Introduction to Mobile Application Management (MAM)

Overview

This guide details how your organization can manage mobile applications using AirWatch's Mobile Application Management (MAM) functionality. MAM entails distributing, securing, and tracking the organization's mobile applications. Organizations use mobile applications in ever increasing ways such as deploying mobile points of sale, configuring sales kiosks, creating business intelligence, and helping with everyday work related tasks.

Distribute, secure, and track mobile applications across your mobile fleet with the AirWatch’s MAM capabilities directly from the AirWatch Admin Console.

Distribute Applications

- Install, update, and remove managed applications remotely.
- Install required applications automatically during enrollment.
- Allow users to install applications on-demand from the Enterprise App Catalog.
- Configure application access based on assignment rules.

Secure Applications

- Restrict application usage by creating blacklists, whitelists, and application compliance policies.
- Restrict access to pre-installed applications on a device.
- Disable iTunes, Google, or other public application stores.
- Prevent data backup and automatically remove applications on un-enrollment from the AirWatch Agent.

Track Applications

- Track and view installed, approved, and blacklisted applications at the device and user level.
- Receive alerts when an end user has installed an unapproved application.
- Generate application inventory, version history, and compliance reports.

In This Guide

This document discusses the process of deploying applications to your end users using the AirWatch Admin Console from beginning to end. It is divided into the following sections where you learn about the following processes:

- **Before You Begin** – Evaluate actions and considerations prior to beginning your application management deployment. These actions are not prerequisites, but they can help the process of uploading and deploying applications smoothly.
- **Getting Started** – View how to create application categories, custom notifications, smart groups, and integrate with Google Play.
• **Internal Applications** – View how to upload your own enterprise applications to the AirWatch Admin Console and provide them to your end users.

• **Public Applications** – Review how to recommend public applications to your end users for work and related use.

• **Purchased Applications (Apple VPP)** – Explore how to manage your purchased iOS applications for Apple VPP to disseminate them to end users from the AirWatch Admin Console.

• **Managing Applications** – Review how to manage all your applications with actions for feedback, notifications, version control, retirement, and other management functions.

• **Application Groups** – See how to group applications into blacklisted, whitelisted, and required applications to help manage access to your applications.

• **Compliance** – View how to configure compliance policies for your applications.

• **Deploying an Application Catalog** – See how to deploy an Enterprise App Catalog so your end users can easily access all of your deployed applications.

• **Appendix A – Settings and Policies Compatibility Matrices** – See which advanced application management settings apply to which AirWatch applications, SDK applications, and wrapped applications.

• **Appendix B – Using the App Catalog without MDM** – Review details about the App Catalog without MDM feature that enables you to distribute applications without deploying and managing an MDM environment.

• **Appendix C – Enforcing Application Control for Android and Windows Phone 8** – See how to allow or prevent installation of applications on certain platforms.
Before You Begin

Overview

Before configuring MAM, you should consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the AirWatch team. Familiarizing yourself with the information available in this section helps prepare you for configuring MAM.

In This Section

- **Managed and Unmanaged Applications** – Read about the actions AirWatch can perform on managed applications and what it cannot do for unmanaged applications.
- **Supported Browsers** – View a list of supported browsers.
- **Supported Devices** – View a list of supported devices.
- **Recommended Reading** – Review helpful background and supporting information available from other AirWatch guides.

Managed and Unmanaged Applications

AirWatch categorizes applications as managed and unmanaged. The AirWatch Admin Console can perform particular tasks for managed applications that it cannot perform for unmanaged applications.

- **Distributing applications**
  - Managed – AirWatch pushes managed applications using the App Catalog to devices. The App Catalog automatically installs apps or makes apps available for download depending upon the configured push mode.
  - Unmanaged – AirWatch must direct end users through the App Catalog to an app store in order to download applications.
- **Removing applications**
  - Managed – AirWatch can remove managed applications off of devices.
  - Unmanaged – AirWatch cannot remove unmanaged applications from devices.

Supported Browsers

The AirWatch Admin Console supports the following web browsers:

- Internet Explorer 8+*
- Google Chrome 11+
- Firefox 3.x+
- Safari 5.x
*Some of the newer elements and features of the AirWatch Admin Console are not supported by IE8. Comprehensive platform testing has been performed to ensure functionality while using these web browsers. The AirWatch Admin Console may still function in non-certified browsers with minor performance issues.

**Supported Devices**

AirWatch supports the following devices for these listed features:

<table>
<thead>
<tr>
<th>Features</th>
<th>Android v2.3+</th>
<th>Apple iOS v5.0+</th>
<th>Windows Phone</th>
<th>Windows Phone 8</th>
<th>Windows 8/RT</th>
<th>Symbian 3rd Edition FP2</th>
<th>Anna Belle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy Public Applications</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Deploy Internal Applications</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Deploy Purchased Applications</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Enforce Application Compliance</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Use the AirWatch SDK</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Use AirWatch App Wrapping</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Reputation Analysis</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>App Catalog without MDM</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

✓ – AirWatch supports only unmanaged public applications for Windows 8/RT.

**Recommended Reading**

- Mobile Device Management (MDM) Guide – Review how to manage devices using the AirWatch Admin Console. This content is helpful for aligning your application management strategy with your device management strategy.
Getting Started

Overview

This section explains some of the application settings you can configure prior to uploading applications. Note that you can configure these settings at any time and change them as necessary, but doing so before you begin may help you to start thinking about how you intend to manage your application deployments. For example, how will your applications be categorized if using an Enterprise App Catalog? How will you configure your smart groups, which are the sets of users that receive applications? These topics and more are covered in detail below.

In This Section

- Creating Application Categories – Review how to categorize your applications and books for better management and so that users can find them in the App or Book Catalog.
- Creating Custom Notifications – View how to create notifications using templates to send to end users with information about applications and books.
- Smart Groups – Learn how to configure smart groups which help group users into units making it quicker to assign applications and books.
- Google Play Integration (On-Premise) – Read how to connect AirWatch to the Google Play Store so users can search and download Android applications.
- Distributing Windows 8/RT Apps – Review how to get a side-loading key to distribute Windows 8/RT applications using AirWatch and how to enable that distribution in the AirWatch Admin Console.
- Distributing Windows Phone 8 Apps – Read how to register Windows Phone 8 applications with the Windows Phone Dev Center so Windows approves them to for distribution using the AirWatch Admin Console.

Creating Application Categories

You can define your own application categories to filter applications and books by type or function. Although they are entitled application categories, they apply to AirWatch books, as well. You can create, view, edit, delete, and assign one or more categories for both public and internal applications and books in a selected organization group. The App and Book Catalogs display these categories, allowing end users to browse and filter.

Application Category Examples

Categories help you organize your repositories and offer the flexibility to manipulate repository organizations to meet your business needs. Some ways to create categories include the following ideas:

- Organization units – Make categories that match business units like IT, Accounting, Sales, Professional Services, and Human Resources. For example, you can apply categories to apps and books and filter them so that only Sales content displays on the app or book page.
• Organization needs – Make categories that match business needs like Security, Communication, Travel, Medical, and Education. You can filter apps and books to display security content and ensure that the latest version is deployed. If not, add a new version and push to devices. You do not have to create your own categories. You can use the seeded category your apps and books have pre-coded. AirWatch uses these seeded categories so that you can still filter and organize your content.

**Configuring Application Categories**

To create an application category, perform the following steps:

1. Navigate to **Apps & Books ➤ Applications ➤ Settings ➤ App Categories**.
2. Select **Add Category**.
3. Provide the **Category Name** and **Category Description** and save the settings.

**Note:** While adding a new internal or public application or book, the system automatically looks into all the existing seeded system categories and selects the one that matches the application or book as received from the app store.

**Creating Custom Notifications**

AirWatch enables you to notify end users about new and updated applications through custom or template messages. You can customize book notifications by distinguishing book notifications from application notifications using the **Name** and **Description** fields.

Send messages using email, SMS, or push notification and customize a message template to include application or book names, descriptions, images, and version information. Templates can include links to your App and Book Catalog and they can prompt end users to download content from the notification. This function ensures your mobile fleet gets the latest versions of your organization's applications and books.

**Configuring Notifications**

AirWatch sends this message when you use the **Notify Devices** option on the actions menu or from the **Manage Devices** feature.

To create a notification message, follow these steps:

1. Navigate to **Groups & Settings ➤ All Settings ➤ Devices & Users ➤ General ➤ Message Templates**.
2. Select **Add** and complete the required information:
• **Name** – Enter the name of the new template. If this is a book notification, use "book" in this field to distinguish it from an application notification.

• **Description** – Enter a description of the message that is used internally by AirWatch to describe this template.

• **Category** – Select the message template category, usually set as **Application**.

• **Type** – Select **Application Notification**.

• **Select Language** – Enter a parameter to limit the message delivery to only devices that belong to end users who understand the specified languages.

• **Default** – Select whether the AirWatch Admin Console uses this message template by default for the **Category** – **Application** and the **Type** – **Application Notification**. You can use the **Application Notification** template as a basic notification message on which to add your information.

• **Message Type** – Select the message types (email, SMS, or push) that AirWatch uses for this template.

• **Message Body** – Enter the message AirWatch displays on end user devices for each message type. Use the {ApplicationName} look-up value to automatically populate the application name in each message.

3. Select **Save**.

**Smart Groups**

Smart groups are customizable groups you define that determine which end users receive an application or book. With smart groups, you can deploy an application or book to additional organization groups, or refine parameters to deploy only to specific platforms, devices, or users.

The main benefit of smart groups is that you define these parameters once and apply them when needed rather than redefining the criteria every time you add an application or book.

While you can create smart groups when you upload applications and books, you can also create them at any time so they are available for use later.

**Creating a Smart Group**

Before you can assign a smart group to an application or book, you must first create it. Configure the smart group at the applicable organization group level.
1. Navigate to Apps & Books ►Applications ►Settings ►Smart Groups and then select Add Smart Group.

2. Enter a Name for the smart group.

3. Configure the smart group using Select Criteria or using Select Users and Devices.

   **Note:** Switching between Select Criteria and Select Users and Devices erases entries.

   - In the Select Criteria section, select the users and devices or select parameters to add in the smart group. Parameters include Organization Group, User Group, Ownership, Tags, Platform, Model, and Operating System.

     o Add Tags to help organize devices in your smart groups based on properties specific to your network. For example, if you wanted to group damaged devices, you could assign a damaged tag to these devices and then use the damaged tag to apply a smart group to your damaged devices group.

     Create and assign tags to devices in the Device Details page using the Notes option. You can also add and manage tags in Groups & Settings ►All Settings ►Devices & Users ►Advanced ►Tags.

     o You can add and exclude devices and users in the Additions and Exclusions sections.

     o Choose Select Criteria to specify details for the smart group that reflect and affect large numbers in your mobile deployment. This option works best for large groups that receive general updates.

   - In the Select Users and Devices section, search for the device or user. You must add one device or user or you cannot save the smart group.

     o Choose Select Users and Devices to assign this application to special cases outside of the general enterprise mobility criteria.

     o The Select Users and Devices option works best for groups with smaller numbers that receive sporadic, although important, updates because of the granular level at which you can select group members.

4. Select Save when finished.

**Assigning a Smart Group to a New Application or Book**

When uploading a new application or book, you select the smart group on the Assignment tab. From this tab, you can also view the current device assignments for a particular smart group.

**Assigning a Smart Group to an Existing Application or Book**

Once you upload an application or book, you can reassign or add devices to the assignment directly from the Applications List View page or the Books List View page.

1. Navigate to Apps & Books ►Applications ►List View or Apps & Books ►Books ►List View and select the appropriate tab, either Internal, Public, or Purchased.

2. Locate the application or book and perform one of the following actions:

   - Internal and Public – Select the Edit icon from the actions menu and select the Assignment tab.

   - Purchased – Select the Edit Assignment icon from the actions menu.

3. Select a smart group or create a new one. You can select more than one.

4. Select the following save option:

   - **Save & Publish** for internal and public applications and books, which makes the content available immediately.
Save for purchased applications and books. You must publish the application or book using the actions menu from the Purchased tab.

Note: You cannot delete a smart group if it is assigned to an application or book.

Google Play (Android Market) Integration (On-Premise)

To search for and deploy public Android application, you must first configure a connection between the AirWatch MDM and the Google Play Store. Enabling this feature is necessary for on-premise customers only.

Use the following steps to add a Google Account:

1. Navigate to Groups & Settings ►All Settings ►Device & Users ►Android ►Google Play Integration.

2. Complete the form for a Phone or a Tablet with the following information:
   - Username – Google Account username.
   - Password – Google Account password.
   - Android Device ID – Enter in a valid Android Device ID to provide the system with access to all applications in the Google Play Store.

   Note: To find the Device ID of your Android device, download the Device ID application from the Google Play Store.

3. Select Test Connection after filling out the form to see if the system can connect to the Google Play Store using the supplied credentials.

Distributing Windows 8/RT Apps

Before you can deploy internal and public applications to Windows 8.1/RT devices, you must obtain a side-loading key and obtain a code signing certificate by performing the following steps:

1. Contact either your system administrator or Microsoft for instructions on how to obtain a side-loading key.
2. Follow instructions until you obtain the key. The key is in this format: ADQ2Z-6TP3W-4QGHK-PSDAW-8WKYR
Note: The key provided by a Volume Licensing portal such as, https://www.Microsoft.com/licensing/servicecenter/default.aspx might be limited to a set number of device activations. Verify there is a key available for your use. For more information about a Microsoft account, visit the Microsoft Developer Network site.

Enabling AirWatch for Application Distribution

To set the AirWatch Admin Console to distribute approved enterprise applications automatically, perform the following steps.


2. Select the Enable Enterprise Applications Manager check box.

3. Enter in the Side Loading Key field the key that was provided to you. For example: ADQ2Z-6TP3W-4QGHK-PSDAW-8WKYR

4. Select Save. This uploads the Side Loading Key into the AirWatch Admin Console and automatically enables corporate devices to install the enterprise internal application.

Note: These settings affect devices enrolled after preparing the AirWatch Admin Console for application distribution. All devices enrolled before this process must re-enroll to access enterprise internal applications. Additionally, if you change the Side Loading key after devices enroll, all devices must re-enroll to access enterprise internal applications.
Distributing Windows Phone 8 Apps

Registering Applications with the Windows Phone Dev Center

Before you can deploy internal and public applications to Windows Phone 8 devices, you must create, register, and gain approval for the applications from the Windows Phone Dev Center. Use the following steps to register an application with the Windows Phone Dev Center:

1. Register with the Windows Phone Dev Center.
2. Obtain a Symantec authentication certificate.
3. Build and sign the enterprise application.
4. Generate an Application Enrollment Token (AET).
5. Register a Microsoft account for your company with the Windows Phone Dev Center.
   It costs a fee to join and the subscription enables your company to add applications to the Windows Phone Store. Registration creates a Windows account ID that you must use to obtain a Symantec authentication certificate. For more information about a Microsoft account, visit the Microsoft Developer Network site.
   Obtain an Enterprise Mobile Code Signing Certificate from Symantec with the Windows account ID. Use the certificate to digitally sign and verify that your company built the application. Also, use the certificate to generate the AET used by each device to obtain a copy of the application.
7. Build and digitally sign the enterprise application.
   Develop and test the corporate application. When the application is ready for distribution, digitally sign the application by following the precompile and signature steps outlined in the Windows Phone Dev Center.
8. Generate an AET for the enterprise application.
   Generate an AET that devices use to authenticate before installing the enterprise application. You can upload the AET to the AirWatch Admin Console. This action automatically enables corporate devices to install the enterprise application. Generate an AET by following the AET generation walkthrough outlined by the Windows Phone Dev Center.

Enabling AirWatch for Application Distribution

The AirWatch App Catalog is not supported for Windows Phone 8 devices at this time. However, you can distribute applications to devices using the AirWatch Agent. To set the AirWatch Admin Console to distribute approved enterprise applications automatically, upload AET you received when registering with the Windows Phone Dev Center.

1. Navigate to Groups & Settings ▶ All Settings ▶ Devices & Users ▶ Windows ▶ Windows Phone 8 ▶ Agent Settings.
3. Select Upload in the Upload Enterprise Token field to browse for the AET .aetx file and save your settings.
Uploading the AET and Device Re-Enrollment

Uploading the token to unenrolled devices
Uploading the token to unenrolled devices does not require re-enrollment because the device is not yet enrolled with AirWatch and gets the token after enrolling and syncing with AirWatch.

Uploading the token to enrolled devices
Uploading the token to enrolled devices requires re-enrollment because the device cannot get the token unless you upload the token before device enrollment.

Changing the token in AirWatch
Changing the token requires device re-enrollment to access internal applications.

Renewing the token before expiration
Renewing the token before it expires does not require re-enrollment.
Typically, an enterprise token expires in one year. If you upload a renewed token before it expires, devices automatically renew their token the next time they sync with the AirWatch Admin Console.

Renewing the token after expiration
Renewing the token after it expires does not require re-enrollment. However, end users cannot access internal Windows Phone 8 applications on their devices until you renew the token.

**Note:** At this time, no notifications are sent concerning the expiration date of tokens. Consider tracking the expiration date of tokens so that you can renew them and prevent a lapse in application accessibility.

<table>
<thead>
<tr>
<th>Using AET with Windows Phone 8</th>
<th>Require Device Re-Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uploading the token to unenrolled devices</td>
<td>No</td>
</tr>
<tr>
<td>Uploading the token to enrolled devices</td>
<td>Yes</td>
</tr>
<tr>
<td>Changing the token</td>
<td>Yes</td>
</tr>
<tr>
<td>Renewing the token before expiration</td>
<td>No</td>
</tr>
<tr>
<td>Renewing the token after expiration</td>
<td>No – Users cannot access internal applications until token is renewed</td>
</tr>
</tbody>
</table>
Internal Applications

Overview

Internal applications are those applications developed by your organization that you may not necessarily want to be in a public app store. Since internal applications are company-specific applications, you can obtain the application file from your developers and upload it to the AirWatch Admin Console. Once the internal application is uploaded, you can manage the application’s settings and deployment over-the-air from the AirWatch Admin Console alongside publicly-available applications or applications purchased in bulk. Install, remove and update the application wirelessly and with minimal end user interaction. Additionally, take advantage of available AirWatch SDK and App Wrapping features to maximize your internal application’s potential.

Note: Depending on which platform you build your internal applications, consider going to that platform’s site and reviewing their best practices for developing and packaging applications.

In This Section

- **Uploading Internal Applications** – Read about uploading an internal application into the AirWatch Admin Console.
- **Provisioning Profile (Apple iOS)** – Learn about the integration of iOS provisioning profiles and AirWatch for your internal iOS applications.
- **Using the Application Workflow** – Read how to use the application work flow feature to track the development of your internal applications.

Uploading Internal Applications

Use the AirWatch Admin Console as your central tool for deploying, managing and surveying internal applications developed by and for your team.

Note: For internal iOS applications, you have to provide a provisioning profile so that the internal application works when managed in your AirWatch application repository. Obtain this file from your Apple iOS application developers.

Using an External Application Repository Link

You can provide an external application repository link hosting the application file instead of uploading an actual file. Ensure that AirWatch and the repository can communicate. You can set the credentials used to authenticate with the repository by navigating to **Groups & Settings ➤ All Settings ➤ Apps ➤ Catalog ➤ External App Repository** and entering the credentials. Your AirWatch environment must integrate with the Mobile Access Gateway (MAG).

Configuring Internal Applications

1. Navigate to **Apps & Books ➤ Applications ➤ List View ➤ Internal** and select **Add Application**.
2. Upload the application file or enter the external application repository link. Upload an Application File in the following formats:

- .ipa for iOS
- .apk for Android
- .sis and .sisx for Symbian
- .xap for WP8
- .appx for Windows 8/RT

**Note:** Files for Windows 8/RT must work for all three processors, x64, x86, and ARM. You must upload all application files.

3. Select Continue and configure options for the internal application.

From the Add or Edit Application page, configure assignment and deployment options for the internal application. Most of the application information automatically populates for Apple iOS, Android, Windows Phone 8 and Windows 8/RT devices. Fill in the remaining fields in all the tabs.

4. Complete the following Info options:

- **Name** – Enter the name for the application.
- **Managed by** – View the organization group from which the file uploads when the information automatically populates.
- **Application ID** – View the name space for the application, often in a domain name format when the information automatically populates.
- **Actual File Version** – Review the development version of the file when the information automatically populates.
- **Version** – Enter version information you want to record in AirWatch to help organize versions so the mobile fleet uses the applicable one to perform tasks.
- **Is Beta** – Select to mark the application as still under testing and development.
- **Change Log** – Add comments to the field to keep notes on changes between versions.
- **Categories** – Provide a category type in the field to help identify how the application can help users. For more information, see Categories.
- **Minimum OS** – Select the oldest OS that you want to run this application.
- **Supported Models** – Select all the models that you want to run this application.
- **Default Scheme (iOS)** – Indicate the URL scheme for iOS applications.

Other iOS applications and web applications can integrate with this application using this scheme. The application also uses this scheme to receive messages from other applications and to initiate specific request. The AirWatch Workspace uses this scheme to launch the application in the Workspace.

5. Enter text in the Description field on the Description tab and set the following options to record information about your application. Completion of this tab is optional and exists to record information specific to your organization.

- **Keywords** – Enter words that might describe features or uses for the application. These entries are like tags and are specific to your organization.
- **URL** – Enter the URL from where you can download the application and get information about it.
- **Support Email** – Enter an email to receive suggestions, comments, or issues concerning the application.

- **Support Phone** – Enter a number to receive suggestions, comments, or issues concerning the application.

- **Internal ID** – Enter an identification string, if one exists, that the organization uses to catalog or manage the application.

- **Copyright** – Enter the publication date for the application.

- **Developer** – Enter the developer's name.

- **Developer Email** – Enter the developer's email so that you have a contact to whom to send suggestions and comments.

- **Developer Phone** – Enter a number so that you can contact the developer.

- **Send Logs to Developer Email (iOS)** – Enable sending logs to developers for troubleshooting and forensics to improve their applications created using a software development kit.

- **Logging Email Template (iOS)** – Select an email template AirWatch uses to send logs to developers.

- **Cost Center** – Enter the business unit charged for the development of the application.

- **Cost** – Enter cost information for the application to help report metrics concerning your internal application development systems to the organization.

- **Currency** – Select the type of currency that paid for the development, or the currency that buys the application, or whatever you want to record about the application.

6. Upload images of the application on the **Images** tab that end users view in the App Catalog before installing the application to their device.

7. Select a **Required Terms of Use** for the application, if desired.

   Create them if you have not already. Find the Terms of Use configuration options in **Groups & Settings ▶ All Settings ▶ System ▶ Terms of Use**.

   Terms of Use specifically state how to use the application. This option makes the organization’s expectations clear to end users. When the application pushes to devices, users view a Terms of Use page that they must accept in order to use the application. If users do not accept, they cannot access the application.

8. Upload auxiliary files needed to distribute internal applications through AirWatch on the **Files** tab:

   **Note:** You can use the default developer certificate for Windows 8/RT applications or you can override this option and upload a custom developer certificate.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Auxiliary File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Application File</td>
<td>Contains the application software to install and run the application and is the application you uploaded at the beginning of the procedure.</td>
</tr>
<tr>
<td>Apple iOS</td>
<td>Provisioning Profile</td>
<td>Authorizes developers and devices to create and run iOS applications. See Apple iOS Provisioning Profiles for information about AirWatch integration with this auxiliary file. Ensure this file covers enterprise distribution and not app store distribution.</td>
</tr>
<tr>
<td>Apple iOS</td>
<td>APNs files for development or production</td>
<td>Required for messaging functionality, if the application supports Apple Push Notifications Services (APNs), so you must upload either the development or production APNs certificate.</td>
</tr>
<tr>
<td>Windows 8/RT</td>
<td>X64, X86, and ARM Architecture</td>
<td>Contains the application software to install and run the application for the specific Windows 8/RT architecture.</td>
</tr>
</tbody>
</table>
9. Enable App Wrapping on the **Wrapping** tab to associate extra security and management features to an existing application and then to re-deploy it.

Complete the following options:

- **App Wrapping Profile** – Assign an app wrapping profile so the wrapped app uses the features.
- **Mobile Provisioning File (iOS)** – Upload a provisioning profile for iOS that authorizes developers and devices to create and run applications built for iOS devices.
- **Code Signing Certificate (iOS)** – Upload the code signing certificate to re-sign the wrapped application.
- **Require encryption (Android)** – Enable this option to use Data At Rest (DAR) encryption on Android devices.

### Re-Wrapping Applications

AirWatch does not push a wrapped app to devices until the wrapping engine reports wrapping success. Find the success status in the Admin Console at **Apps & Books ▶ Applications ▶ List View ▶ Internal** and view the **App Wrapping Status** column.

If wrapping fails, use the **Queue app for wrapping** check box on the **Wrapping** tab, which only displays upon failure. The wrapping engine re-wraps the application after you select **Save & Publish**. When the wrapping engine reports success, AirWatch pushes the application to devices. This workflow prevents pushing failed wrapped applications to devices.

10. Assign the application to smart groups on the **Assignment** tab and complete the following options:

- **Assigned Smart Groups** – Select an existing one or create a new smart group.

  **Note:** When you assign a smart group to an application that is already deployed, AirWatch pushes the application to devices in the smart group selected at the instance of re-assignment. It does not push to devices in the original smart group. This becomes important when you update applications, because you must ensure to re-assign an updated application to all applicable smart groups.

- **Restrict to Devices Supporting Silent Activity (Android)** – Assign this application to those Android devices that support the Android silent uninstallation feature. The end user does not have to confirm an uninstallation when you enable silent activity for a device. This feature makes it easier to uninstall many applications simultaneously.

  Only Android devices in the smart group that support silent uninstallation get this application.

- **View Device Assignment** – View the list of devices available by assigned smart groups.

11. Configure the deployment details of the application on the **Deployment** tab to control availability and SDK features.

- **Push Mode** – Set the application to install automatically (auto) or manually (on demand) when needed.

  - Automatically deploying an application immediately prompts users to install the application on their devices. **Auto** is the best choice for applications critical to your organization and its mobile users.
Manually deploying an application allows access and downloads this application, if selected, from an enterprise application catalog. On Demand is the best choice for applications that are not critical to the organization. Allowing users to download these applications when they want helps conserve bandwidth and limits unnecessary traffic.

- **Effective Date** – Set when the App Catalog pushes the application to devices (auto push mode) or makes it available for download (on demand push mode).

  When you change this date to the future for an existing application set to the auto push mode, the App Catalog removes the application from devices.

- **Expiration Date** – Set when the App Catalog removes the availability of this application.

- **Application uses AirWatch SDK** – Identify if the application was created using the AirWatch SDK and needs a profile to integrate with AirWatch.
  
  - Select the default or custom settings profile from the SDK Profile drop-down menu.
  
  - Select the certificate profile from the Application Profile drop-down menu so that the application and AirWatch communicate securely.

- **Remove On Unenroll (iOS)** – Set the removal of the application from a device when the device unenrolls from AirWatch.

- **Prevent Application Backup (iOS)** – Disallow backing up the application to iCloud. This option stops end users from saving different versions of a public application in the iCloud.

- **Use VPN (iOS 7+)** – Configure a VPN at the application level. This option sets end users to access the application using a VPN, which helps ensure application access and use is trusted and secure.

- **Send Application Configuration (iOS 7+)** – Send application configurations to iOS devices. This feature allows you to automatically configure managed applications. Users do not have to manually configure these specified values in the application.

  Enter the configuration values as unique keys into the appropriate fields. Supported entries for key/value pairs are String, Number, Boolean, and Date. You can also use Lookup Values when entering the application configurations.

  **Note:** If you make any changes to application configurations, you must re-publish the application to apply the changes.

- **Add Exceptions** – Deploy applications to those special use cases that can develop within an organization.
  
  - Apply User Groups and Device Ownership types to your exceptions in the Criteria area.
  
  - Select an Override Value to create specific exceptions to the options. Override Value options vary depending on the platform.

12. Enable Run Reputation Analysis on the Reputation tab to send the application to the AirWatch App Reputation Cloud Service. Use this tab to view scan results.

  Use the Notify Developer option to send a message to developers to notify them of potential risks with their applications. Send the message using email notifications and the applicable template to which the system attaches and sends a Reputation Analysis report.

  For information on enabling the engine, how the system works, and what platforms are supported, see Application Reputation.

13. Select Save & Publish to push the internal application to devices.
Provisioning Profiles (Apple iOS)

A provisioning profile for iOS authorizes developers and devices to create and run applications built for iOS devices. For an internal iOS application to work, every device that runs the application must also have the provisioning profile installed on it. When using provisioning profiles, ensure you upload the profile that was generated for that particular application.

Provisioning Profiles for Enterprise Distribution

For internal applications, use files and processes from the iOS Developer Enterprise Program.

- **iOS Developer Enterprise Program** – This program facilitates the development of applications for internal use.
- **iOS Developer Program** – This program facilitates the development of applications for the app store.

These are different programs, so when you get a mobile provisioning profile for your internal applications, ensure it is for enterprise (internal) distribution.

Apple's Enterprise App Signing Model

Apple generates development certificates that expire within three years. However, the provisioning profiles for the applications made with the development certificates still expire in one year. This model creates the following possible issues:

- Developers who build and deploy multiple versions of an application need a way to remove expired provisioning profiles that are associated with active applications.
- Device users receive busy warnings concerning the status of an application 30 days prior to a provisioning profile expiring.

AirWatch helps manage these issues with the following offerings:

- AirWatch notifies admins of expiring provisioning profiles 60 days before the expiration date.
- You can update provisioning profiles and apply them to all associated applications managed in AirWatch.
- You can remove or replace older provisioning profiles off of devices from a central location in AirWatch, as long as the files are not associated to other applications on devices.

Renewing Apple iOS Provisioning Profiles

AirWatch allows you to renew your iOS provisioning profiles without requiring device users to reinstall the application. The AirWatch Admin Console notifies you, in the Console, 60 days before the provisioning profile expires using expiration links in the **Renewal Date** column on the **Internal** tab. AirWatch also enables you to renew the file for all applications associated with it.

**Note:** Access expiration links for iOS provisioning profiles in the applicable Organization Group (OG). The AirWatch Admin Console does not allow access unless you are in the correct OG.

1. Navigate to **Apps & Books ▶ Applications ▶ List View ▶ Internal**.
2. Select the expiration link (**Expires in XX days**) for the application for which you want to update the provisioning profile in the **Renewal Date** column.
3. Use the **Renew** option on the **Files** tab to upload the replacement file.
4. Select the **Update Provisioning Profile For All Applications** setting to apply the renewed file to all associated applications.

**Note:** AirWatch displays this option only if multiple applications share the provisioning profile.

AirWatch lists the applications that share this provisioning profile for you on the Files tab. AirWatch silently pushes the updated provisioning profile to all devices that have the application installed.

### Expired Apple iOS Provisioning Profiles

When an iOS provisioning profile expires, device users cannot access the associated application, and new device users cannot install the application.

### Using the Application Workflow

Application workflow simplifies the internal application deployment process for organizations developing their own applications. It allows organizations to delegate key steps in the process to administrators who are responsible for individual stages. Some of the key benefits of this feature include:

- Separating responsibilities clearly.
- Notifying participants about completed steps automatically.

### Implementing Application Workflow

To bring the application workflow into effect, four different administrator user accounts have to be created. Each of the created user accounts must have different administrator workflow permissions assigned under a specific Organization Group.

### Roles involved in Application Lifecycle Workflow

There are four major administrator roles participating in the application lifecycle at various stages. The responsibilities of each of the roles are listed below.

<table>
<thead>
<tr>
<th>Admin Role</th>
<th>Description of Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developer</td>
<td>Is responsible for developing internal applications and revising them based on the analysis of performance and feedback provided by reviewer, publisher or sponsor. Once the application is ready to go out to end users, an administrator uploads the application to the AirWatch Admin Console.</td>
</tr>
<tr>
<td>Reviewer</td>
<td>Is responsible for reviewing a new application created by developer, and assigning it an appropriate description, screen shots, and Terms of Use. Reviewer also looks at the change log provided by the developer for the application to determine if the application is eligible for promoting to assignment or needs rework. From the Edit Application area of the Application page, the Reviewer can review the application’s description and change log, reject the application back to the developer and submit the application for assignment. Submitting the application pushes the status to <strong>To Be Assigned</strong> status.</td>
</tr>
<tr>
<td>Assigner</td>
<td>Is responsible for assigning the application to Smart Groups and promoting it to a full rollout based on whether the application meets the required criteria. The assigner makes recommendations to the publisher</td>
</tr>
</tbody>
</table>
## Admin Role | Description of Responsibility
---|---
Assigner | Accordingly. From the **Edit Application** area of the **Application** page, the Assigner can review application settings and descriptions, configure Smart Group and device assignment settings and submit the application for publishing. Submitting the application pushes the status to **Ready for Publishing** status.

Publisher | Is responsible for reviewing the assignment criteria for application configured by the assigner and determines whether the right set of devices is receiving the application. The publisher can also republish the application to devices that were assigned but have not installed the application. From the **Publish** area of the **Application** page, the Publisher can review application settings and descriptions, review or alter assignment configuration and publish the application to all assigned users.

### Enabling Application Workflow

Use the following steps to configure an application workflow in the AirWatch Admin Console:

1. **Navigate to** Groups & Settings ▶️ All Settings ▶️ Apps ▶️ Catalog ▶️ Application Workflow.

2. **Select the Enable Work Flow for Applications check box.**

3. **Select the Role** to define the admin role to perform the workflow action.

4. **Select a message template to notify users within the role when an application becomes available for performing the workflow action.**
Public Applications

Overview

AirWatch can deploy and manage your public applications as it leverages the benefits of app ratings and easy updating. Application stores and the App Catalog display user ratings for applications they offer. You can use the ratings to best gauge the usefulness of applications before adding them to your mobile fleet and to decide to keep unpopular applications. Public apps are often updated with a click of an agreement button or silently. AirWatch can help you manage these updates, pushing the update version you want and blocking the update version you do not.

Many of the applications available within public app stores can be used to enhance the business interactions that take place on your managed devices. Deploy and manage some of these applications from the AirWatch Admin Console for the specific groups and users within your organization.

In This Section

- **Uploading a Public Application** – Learn how to search, add, and configure public applications in the AirWatch Admin Console.
- **Enabling Restricted Mode for Public iOS Applications** – Review how to restrict end users from installing public applications from iTunes by enabling restricted mode for iOS devices.

Uploading a Public Application

Search for public applications in an application store when adding them to the AirWatch Admin Console. Retrieving the application from a store ensures you pull the latest version and also ensures the AirWatch Admin Console properly manages the public application for your mobile deployment.

1. Navigate to **Apps & Books ►Applications ►List View ►Public**.
2. Select **Add Application**.
3. View the organization group from which the application uploads in **Managed By**.
4. Select the a **Platform**.
5. Enter a descriptive name in the **Name** field to help search for the application in an app store.
6. Select **Search App Store** to search for the application in Apple App Store, Google Play Store (Android Market) or Microsoft Windows Phone Store.

Use the AirWatch search feature to add public applications rather than add them manually. Addition by searching lets you use management functions whereas manual addition does not. With addition by searching you can perform the following management functions for your public applications:

- Push the application to devices using the AirWatch Admin Console.
- Publish the application to devices on-demand or automatically.
• Install the application using the AirWatch Agent without users having to retrieve the application from the App Catalog manually.

**Note:** In order to search the Google Play Store in an on-premise deployment, you must integrate a Google Account with the AirWatch MDM environment. See Google Play Integration.

### 7. Enter the URL (Android only) – Enter the Google Play Store URL for the application. This option displays for only Android applications.

Google Play Stores are localized and they offer applications based on regions. If your AirWatch server is in a different region than the region from which an application is available, this option allows you to still use and deploy the application.

**Valid URLs**

You can enter the Google Play Store URL or a URL that you know to be valid but that is not from the Google Play Store. AirWatch can manage applications it finds in the app store, but it cannot manage applications uploaded from another source other than the Google Play Store. Also, AirWatch cannot return the application in its results because it cannot validate the URL with the store.

Entering a valid URL, enables you to deploy the application to devices, even when AirWatch cannot validate it with the Google Play Store. Your App Catalog makes the application available using the URL as a link. You must enter the exact URL for the application.

**Note:** Although AirWatch can manage applications with a valid Google Play Store URL, it cannot get screenshots or icons for the application from the Google Play Store.

### 8. Click Next and Select the desired application from app store result page.

### 9. Complete the following options on the Info tab:

a. **Name** – Enter a name for the application.

b. **Application ID** – View the name space for the application, often in a domain name format when the information automatically populates.

c. **URL** – Enter the URL for the application. Enter the URL from where you can download the application and get information about it.

d. **Managed By** – View the organization group from which the file uploads when the information automatically populates.

e. **Comments** – Enter text to appear in the Additional Comments tab in the App Catalog.

f. **Reimbursable** – Designate whether your organization reimburses end users for the application, if purchased. A small icon in the AirWatch App Catalog indicates if an application is reimbursable.

g. **Rating** – Select a rating from 1 to 5.

h. **Categories** – Identify the areas the application can help device-users. For more information, see Categories.

i. **Supported Models** – Select all the models that you want to run this application.

j. **Default Scheme (iOS)** – Indicate the URL scheme for iOS applications.

   Other iOS applications and web applications can integrate with this application using this scheme. The application also uses this scheme to receive messages from other applications and to initiate specific request. The AirWatch Workspace uses this scheme to launch the application in the Workspace.

### 10. Assign the application to smart groups on the Assignment tab and complete the following options:
a. **Assigned Smart Groups** – Select an existing one or create a new smart group.

b. **Restrict to Devices Supporting Silent Activity (Android)** – Assign this application to those Android devices that support the Android silent uninstallation feature. The end user does not have to confirm an uninstallation when you enable silent activity for a device. This feature makes it easier to uninstall many applications simultaneously.

Only Android devices in the smart group that support silent uninstallation get this application.

c. **View Device Assignment** – View the list of devices available by assigned smart groups.

You do encounter some instances where you cannot use Smart Groups for your public applications and you must use your legacy assignment settings. This feature ensures that your public applications do not loose their override settings. For example, a public application has legacy assignments that are configured at a child Organization Group (OG) and are set to override the parent OG settings. You cannot assign these applications to Smart Groups unless you change these override settings at the child level. To change the override settings, click the Edit Legacy Assignment link and change Override to Inherit.

**Important:** Before you change override settings, ensure other groups are not affected by these configuration changes.

11. Configure the deployment details of the application on the Deployment tab to control availability and SDK features.

**Note:** AirWatch supports only unmanaged public applications for Windows 8/RT. The AirWatch Admin Console cannot push unmanaged applications to devices and it directs end users to the Windows Store, using the App Catalog, to download these applications. AirWatch cannot remove unmanaged applications from devices.

a. **Push Mode** – Set the application to install automatically (auto) or manually (on demand) when needed.

   - Automatically deploying an application immediately prompts users to install the application on their devices. Auto is the best choice for applications critical to your organization and its mobile users.
   
   - Manually deploying an application allows access and downloads this application, if selected, from an enterprise application catalog. On Demand is the best choice for applications that are not critical to the organization. Allowing users to download these applications when they want helps conserve bandwidth and limits unnecessary traffic.

b. **Remove On Unenroll (iOS)** – Set the removal of the application from a device when the device unenrolls from AirWatch.

c. **Prevent Application Backup (iOS)** – Disallow backing up the application to iCloud. This option stops end users from saving different versions of a public application in the iCloud.

d. **Use VPN (iOS 7+)** – Configure a VPN at the application level. This option sets end users to access the application using a VPN, which helps ensure application access and use is trusted and secure.

e. **Send Application Configuration (iOS 7+)** – Send application configurations to iOS devices. This feature allows you to automatically configure managed applications. Users do not have to manually configure these specified values in the application.

Enter the configuration values as unique keys into the appropriate fields. Supported entries for key/value pairs are String, Number, Boolean, and Date. You can also use Lookup Values when entering the application configurations.

**Note:** If you make any changes to application configurations, you must re-publish the application to apply the changes.
f. **Application uses AirWatch SDK** – Identify if the application was created using the AirWatch SDK and needs a profile to integrate with AirWatch.
   - Select the [default or custom settings profile](#) from the [SDK Profile](#) drop-down menu.
   - Select the certificate profile from the [Application Profile](#) drop-down menu so that the application and AirWatch communicate securely.

g. **Add Exceptions** – Deploy applications to those special use cases that can develop within an organization.
   - Apply [User Groups](#) and [Device Ownership](#) types to your exceptions in the [Criteria](#) area.
   - Select an [Override Value](#) to create specific exceptions to the options. [Override Value](#) options vary depending on the platform.

12. **Select a Required Terms of Use** for the application, if desired.
    Create them if you have not already. Find the Terms of Use configuration options in [Groups & Settings ►All Settings ►System ►Terms of Use](#).
    Terms of Use specifically state how to use the application. This option makes the organization’s expectations clear to end users. When the application pushes to devices, users view a Terms of Use page that they must accept in order to use the application. If users do not accept, they cannot access the application.

13. **Select Save & Publish** to make the application available to end users depending on the [Push Mode](#) setting on the [Deployment](#) tab.

### Enabling Restricted Mode for Public iOS Applications

You can restrict end users from installing public applications from iTunes by enabling [Restricted Mode](#) for iOS devices. Once a device is enrolled into AirWatch, Restricted Mode end users are able to manage public applications deployed down to them, but are unable to download any other applications from iTunes. For example, end users are able to install and uninstall business-related applications made available in the App Catalog, but won’t be able to install games, social media applications or previous versions of applications from the App Store.

To enable Restricted Mode for iOS Applications:

1. Navigate to [Groups & Settings ►All Settings ►Apps ►Catalog ►App Restrictions](#).
2. Enable [Restricted Mode for Public iOS Applications](#).

**Note:** This option restricts the device by allowing you to install only the assigned applications from the iTunes App Store. Enabling the above setting automatically sends a restricted profile to the iOS devices. The presence of this restricted profile does not require configuring any additional restriction profiles to block the App Store.
Purchased Applications (Apple VPP)

Overview

If you want to distribute a public or B2B application to hundreds or thousands of iOS devices or users, you may consider using the Apple Volume Purchase Program (VPP). The Apple VPP enables organizations to purchase publicly available applications or specifically developed third-party applications in bulk for distribution. Any paid application from the App Store is available for volume purchase at the existing App Store price. Custom B2B applications can be free or purchased at a price set by the developer.

**Note:** The Apple VPP is currently available in Australia, Canada, France, Germany, Italy, Japan, New Zealand, Spain, the United Kingdom and the United States. See the article Volume Purchase Program for Business on the Apple website for detailed information.

Custom B2B Applications

Third parties make custom business-to-business (B2B) applications exclusively for organizations, so they are not available to everyone in an app store. You can upload custom B2B applications into your AirWatch app repositories using redemption codes:

- Redemption codes – AirWatch can install custom B2B applications bought using redemption codes on to devices using the App Catalog. End users can install these applications on-demand, but you cannot push these applications automatically. Also, AirWatch cannot manage these applications.

Managed Distribution or Redemption Codes

AirWatch has methods to let you centrally control the management and distribution of VPP applications. Use the order based method which includes VPP redemption codes or use the licensed based method which includes managed distributions.

The orders based method that uses redemption codes does not support the revoking of the code off an iOS device. Once the redemption code is redeemed, you cannot recycle it. If you use VPP applications, then you are familiar with redemption codes and you can continue to use them to purchase applications for iOS 7+, if desired. With the release of iOS 7+, Apple offers a new method for purchasing VPP applications.

The licensed based method that uses managed distribution does allow you to revoke a managed distribution code and recycle it. This is new for iOS 7+ but you cannot use it for Apple operating systems older than iOS 7+.

Deploying VPP Applications Process

Perform a three-part process to deploy applications in bulk through the Apple VPP:

1. **VPP Enrollment** – Enroll in the program and verify with Apple that you are a valid organization. See [Enrolling in the Apple VPP](#) for information.

2. **Application Purchasing** – Purchase applications in bulk through the VPP website. See [Purchasing Applications with VPP](#) for information.

3. **Application Deployment** – Distribute the applications throughout your device fleet using redemption codes or managed distribution tokens.
In This Section

- **Enrolling in Apple's VPP** – Read how to enroll with Apple's Volume Purchase Program.
- **Purchasing Applications and Books with VPP** – Review how to purchase applications from VPP.
- **Deploying VPP Content Using Redemption Codes** – View how to upload, assign, and publish applications using the redemption code model.
- **Deploying Public VPP Content Using Managed Distribution** – View how to upload, sync, assign, and publish content using the license-based model, also known as managed distribution.
- **Revoking Managed Distribution** – Review how AirWatch revokes managed distribution codes.
- **AirWatch Events for Managed Distribution** – Read the events AirWatch logs to report data about your VPP deployments.
- **Managed Distribution and AirWatch** – Read about using multiple sTokens and about AirWatch managed distribution installation behavior.
- **Managing and Tracking VPP Orders** – Use the Orders views to gather information about your VPP purchases.

### Enrolling in Apple's VPP

To register for the Apple VPP, navigate to [http://www.apple.com/business/vpp](http://www.apple.com/business/vpp) for businesses or [http://www.apple.com/itunes/education](http://www.apple.com/itunes/education) for educational institutions. You will need to provide the following information:

- Basic contact information, such as your business phone number and email address, to verify your business.
- A Dun & Bradstreet (D-U-N-S) number for your company.
- A corporate credit card or PCard to purchase applications.

**Note:** Once your enrollment information has been verified, you will create a new Apple ID specifically for the VPP. This Apple ID should not be used for other Apple services, such as the iTunes Store.

### Purchasing Applications and Books with VPP

2. Log in with the **VPP Apple ID** created during the enrollment process.
3. Search for applications and books by entering the name or copying and pasting a link from the app store in the search field. Enter the quantity you want to purchase and complete the purchases with a corporate credit card.
4. Check your email for an order processing confirmation from Apple. When you receive this email, you can log in to the VPP website and download a spreadsheet of redemption codes or an authentication token (sToken) for the applications or books you purchased.
Deploying VPP Content Using Redemption Codes

AirWatch enhances management and distribution of applications and books purchased through the VPP to your iOS devices.

Using iTunes Adam IDs

If your spreadsheet contains an Adam ID, then you do not have to locate applications and books in the app store. For custom B2B applications, the Adam ID enables AirWatch to automatically update application IDs in the AirWatch Admin Console.

Distributing Process

Use the following instructions to set up the distribution process.

1. The first step to manage and deploy VPP application orders through AirWatch is to upload the Apple VPP Redemption Code Spreadsheet to the AirWatch Admin Console:
   b. Select Add to add an order for Public or Custom B2B content. Select Purchased Public App or Purchased Custom App (Custom B2B) for applications (not for books).
   c. Click Choose File to upload the CSV or XLS file that you downloaded from the Apple Portal. This action creates the order.
   d. Select Save to continue to the Product Selection Form.
   e. Locate the appropriate product and choose Select to finish uploading the spreadsheet. This step is unnecessary if your spreadsheet contains an Adam ID.

   **Note:** You do not have to locate the product if your spreadsheet contains an Adam ID. AirWatch automatically adds applications and books from the app store if the spreadsheet contains the Adam ID. Adam IDs are specific to iTunes and are components of the Apple Search API.

   If the Apple VPP redemption code spreadsheet contains codes for multiple applications or books, AirWatch lists several products on this form. You can select only one per order.

2. Enable the AirWatch Admin Console to assign redemption codes to users and devices. Select the applicable organization groups and smart groups to which to assign redemption codes.
   b. Locate the specific order to enable and allocate redemption codes.
   c. Select Edit Assignment ✖ from the actions menu and then select the Assignment tab.
   d. Enter the number of redemption codes that you want to place on hold in the Redemption Codes On Hold field. Use this field to save the redemption codes for later use.
   e. Select Add Assignment By to assign redemption codes to organization groups or smart groups:
• **Organization Group** – Allocate redemption codes to an organization group and either select **All Users** to include all users in that organization group or select **Selected Users** to display a list of users in the organization group. Use the **Add** and **Remove** buttons to choose the specific users to receive the application.

• **Smart Group** – Allocate redemption codes to a smart group. You can create a new smart group, if necessary.

  **Note:** You can apply redemption codes to organization groups and to smart groups simultaneously. However, you can only specify the users for organization groups of the **Customer** type. You cannot specify users for smart groups. However, you can edit the smart group so that it contains the necessary users.

• Verify the information in the following columns for each organization group or smart group row:
  - **Users** – View the number of users for the order.
  - **Allocated** – Enter the number of licenses to allocate to the selected users. This entry should not exceed the total number in the order.
  - **Redeemed** – View the number of licenses that have already been redeemed, if any.

f. Select the **Assignment Type**. Set it as **Auto** to push the purchased application to the end user device automatically or select **On-Demand** to let the end user install the application or book on the device.

  **Note:** When **Assignment Type** is **Auto**, only eligible iOS 5+ devices receive the application or book automatically.

g. **Remove On Unenroll (Apps only)** – Set the removal of the application from a device when the device unenrolls from AirWatch.

  **Note:** Removing an application when a device is unenrolled does not recover the redeemed code. When installed, the application is associated to the user’s App Store account.

h. **Prevent Application Backup (Apps only)** – Disallow backing up the application to iCloud. This option stops end users from saving different versions of an application in the iCloud.

i. **Use VPN (iOS 7+, Apps only)** – Configure a VPN at the application level. This option sets end users to access the application using a VPN, which helps ensure application access and use is trusted and secure.

j. Select **Save** when you finish allocating codes.

3. Publish applications and books and push them to devices using the following steps:

a. Navigate to **Apps & Books ➤ Applications ➤ List View ➤ Purchased** or **Apps & Books ➤ Books ➤ List View ➤ Purchased**.

b. Select **Publish (/png)** from the actions menu for the purchased application or book.

### Deploying Public VPP Content Using Managed Distribution (iOS 7+)

Use the licensed based method to distribute your public VPP applications and books to iOS 7+ devices. The license based model uses authentication tokens (also called sTokens) to retrieve your VPP contents and distribute them to iOS 7+ devices using the AirWatch Admin Console.

**Note:** You cannot deploy managed distribution to iOS 6 and older.
Uploading the sToken

Upload the authentication token so that the AirWatch Admin Console can use it to access Apple web services. Apple uses web services to manage license codes. The highest level that you can upload an sToken is the Customer level and then you can add one per organization group (OG) after this Customer level.

Note: You can apply an authentication token to only one OG level. You cannot apply the same authentication token to another OG level or assign two authentication tokens to the same OG level.

1. Navigate to Groups & Settings ➤ All Settings ➤ Apps ➤ Catalog ➤ License Based VPP.
2. Enter a description for the token for your managed distribution in the Description field.
3. Select Upload to navigate to the sToken on your network.
4. Select the Country in which AirWatch should validate the sToken. This value reflects the region from where you bought content and ensures AirWatch uploads the correct versions of your purchases.

   When you sync your licenses on the purchased page, AirWatch pulls the correct regional version of the content.

   If AirWatch cannot find the content in the app store from the region entered in the Country setting, AirWatch automatically searches the iTunes App Store for the United States.
5. Enable Automatically Send Invite to send invitations to users immediately after you save the token.

   AirWatch sends an email invitation to users of iOS v7.0.0 through v7.0.2 based on the template option on this page.

   AirWatch automatically sends users of iOS v7.0.3+ an invite command to devices when you enable the Automatically Send Invite option. It does not send them an email message.

   You do not have to enable this immediately. You can leave it disabled and still upload your token and then return when you are ready to send invitations.
6. Select an email template from the Message Template drop-down to send an email message invitation for iOS devices on iOS v7.0.0 through v7.0.2.
7. Save the sToken and confirm the addition of the token.
8. Select Reinvite Users to resend invites to all iOS 7+ users who did not accept the initial invitation.

   Users of v7.0.3+ receive an invitation command AirWatch sends using a scheduler task. This scheduler task periodically checks for registered iOS v7.0.3+ users and sends them another invitation command if they have not joined the program.
9. Select Delete SToken to remove the token from the AirWatch Admin Console.

   Note (Apps only): You can view a list of devices that have accepted the invitation using the View Devices option. Send individual invitations to those who have not accepted an enrollment invite from this page. Find this option at Apps & Books ➤ Applications ➤ List View ➤ Purchased and select View Devices from the actions menu.

Syncing Licenses

Sync licenses for managed distribution using the following procedure. This procedure makes the VPP content available to your iOS 7+ devices.

Note: Sync licenses in the same organization group (OG) you uploaded the sToken. Also, you cannot access this option unless you are in an OG with an sToken uploaded to it.

2. Select Sync Licenses and choose one of the following options to make content available to devices:
   - **Sync Recent Purchases Only** – Reconciles codes added or modified after you initially uploaded the sToken to AirWatch. This sync option takes less time to process because it does not reconcile all codes on an sToken.
   - **Resync All Apps** – Reconciles all codes from an sToken with purchased content.

3. Refresh the screen to see when the sync completes. AirWatch makes the sync feature inaccessible until it reconciles codes with content. It replaces Sync Licenses with Sync In Progress upon completion and makes the Sync Licenses option accessible.

### Assigning Managed Distribution to Smart Groups

Assign content to smart groups. You cannot assign managed distribution codes to organization groups.

**Note:** Books do not include all options.


2. Locate the specific content you want to allocate managed distribution codes to.

3. Select Edit Assignment from the actions menu and then choose the Assignment tab.

4. Enter the number of managed distribution codes that you want to place on hold in the Licenses on hold field. Use this field to save the managed distribution codes for later use.

5. Hover over Add Assignment By and select License Codes By Smart Group to assign managed distribution codes. You can create a new smart group, if necessary.
   - **Users** – View the number of users for the order.
   - **Allocated** – Enter the number of licenses to allocate to the selected users.
   - **Redeemed** – View the number of licenses that have already been redeemed, if any.

6. Select the Assignment Type. Set it as Auto to push the purchased content to the end user device automatically or select On-Demand to let the end user install the content on the device.
   
   When set to Auto, AirWatch sends an invite command to devices so that they register with Apple's VPP if they have not. AirWatch does this for iOS 7.0.3+.

7. **Remove On Unenroll (Apps only)** – Set the removal of the content from a device when the device unenrolls from AirWatch.

8. **Prevent Application Backup (Apps only)** – Disallow backing up the content to iCloud. This option stops end users from saving different versions of content in the iCloud.

9. **Use VPN (Apps only)** – Configure a VPN at the application level. This option sets end users to access the content using a VPN, which helps ensure users can access the content and can use it on a trusted and secure network.

10. Select Save when you finish allocating licenses.
Publishing Managed Distribution

Publish managed distribution content to devices using these steps:


2. Select Publish (✓) from the actions menu for the purchased content.
   - VPP registered device-users of iOS 7.0.3+ automatically receive the content when the Assignment Type is Auto.
   - VPP device-users of iOS 7.0.3+ who have not accepted the VPP invitation receive an invite command to register with the program when the Assignment Type is Auto.

Revoking Managed Distribution

You can reuse managed distribution codes by revoking them. AirWatch makes codes available immediately after revoking or at a scheduled interval depending on the interval you set for the scheduler task.

You can revoke managed distribution codes using several methods:

- **Organization Group** – Delete an OG and AirWatch makes the licenses available for reuse.
- **User** – Unenroll all devices from a user. If another device does not use the unassigned managed distribution code, then the AirWatch Admin Console revokes it so that it is available for reuse.
- **Manual** – Revoke the code manually off the device.

**Note:** You can use the manual method only for those codes that are redeemed from an external system and you want to use them within AirWatch.

- **VPP Application or Book** – Delete VPP application or book from the AirWatch Admin Console and the code is available for reuse after the scheduler task runs.
- **SToken** – Delete the sToken, and AirWatch makes all associated codes available for reuse.
- **Unassign** – Unassign an application or book from a user and if that license is not used by anyone else, AirWatch revokes the license.
- **Smart Group** – Delete a managed distribution device user from a smart group and if that license is not used by anyone else, AirWatch revokes the license.

AirWatch Logged Events for Managed Distribution

AirWatch logs the following event data for managed distribution functionality.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Description</th>
<th>Event Triggers</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Revoked</td>
<td>This event logs information about revoked managed distribution codes for content due to a manual revocation.</td>
<td>Remove a managed distribution code manually that was originally redeemed when assigned by an external system (not AirWatch) off of a device.</td>
</tr>
</tbody>
</table>
Send VPP Invite

- This event logs information about sending VPP invitations using information from the sToken you upload at an organization group.

- Upload an sToken and configure the **Automatically Send Invite** check box.
- Use the **Reinvite Users** option to reach users who have not registered.
- Send invitations to those who have not registered from the **View Devices** page.
- Publish VPP content.
- AirWatch sends an invitation automatically to those who have not registered.

**Managed Distribution (iOS 7+) and AirWatch**

AirWatch integrates with Apple's Managed Distribution (MD) system using the following frameworks and behaviors.

**AirWatch and Multiple sTokens**

AirWatch supports the use of multiple sTokens. For the successful use of multiple sTokens, you can upload one sToken per organization group (OG). The highest level that you can upload an sToken is the **Customer** level and then you can add one per OG after this **Customer** level. AirWatch assigns a managed distribution code to a device using the sToken closest to the OG level of the device traveling up the OG hierarchy.

**Example of SToken Assignment Behavior**

- The AirWatch OG hierarchy looks like this:
  - Customer OG ➔ OG 2 (a child of Customer OG) ➔ OG 3 (a child of OG 2).
- You upload an sToken at Customer OG and at OG 2.
- You publish a VPP app or book at OG 3 and a device enrolls at OG 3. However, you have not uploaded an sToken at the OG 3 level.
- AirWatch checks OG 2 for an sToken.
  - If one is available, AirWatch assigns the device a license code from the sToken at OG 2.
  - If a license is not available at OG 2, AirWatch checks the Customer OG level for an available license code.

If you add an sToken to OG 3 later, AirWatch does not issue another license from that sToken at OG 3. The device at OG 3, keeps the license from the sToken at OG 2.

**Note:** AirWatch uses redemption codes before using managed distribution. If an OG has an available redemption code and an available managed distribution code, AirWatch assigns the redemption code to a device first.
Delay Behavior for Initial Install

AirWatch installs managed distribution (MD) applications and books immediately to devices when a device user already has a license associated to it for an MD application or book. However, when a device first installs MD content, Apple and AirWatch associate licenses and refresh purchase histories. Reconciling this data takes a moment, and if these processes are not reconciled when AirWatch installs the application or book, then the installation fails.

To reduce installation failures for the initial installation of an MD application or book, AirWatch delays the installation, and the device user might notice this delay. If the MD application or book should fail to install on a device on the first attempt, AirWatch tries to install it again. The system tries in increments of two minutes for the next hour.

Managing and Tracking VPP Orders

Once you allocate VPP orders to the device fleet, the VPP deployment is in effect. During this period, you can use the Available Views pages in the AirWatch Admin Console to manage and monitor the status of the order deployment.

You can perform management functions from these pages like deleting redemption code orders or managed distribution orders, editing assignments for applications and books, and deleting redemption codes.

You can view application and book orders from these pages.

Navigate to Apps & Books ▶ Orders ▶ List View. From the List View page you can:

- View the order status.
- View the order redemption status.
- Edit an assignment.
- Delete an order.

Navigate to Apps & Books ▶ Orders ▶ Products. From the Products page you can:

- View the status of the installation.
- Edit an assignment.
- Publish an application or book.
- Delete an application or book.

Navigate to Apps & Books ▶ Orders ▶ Redemption Codes. From the Redemption Codes page of the AirWatch Admin Console you can access the following order based method information:

Note: To perform these actions for managed distribution codes, go to the Purchased tab and select the link from the Managed Distribution column.

- View the availability status of the code.
- View each redemption code and the order number.
- View the date the redemption code was redeemed.
- View to whom the code is assigned.
- Delete a redemption code.
Managing Applications

Overview

From the Applications List View page, you can view all the applications that you manage in the AirWatch Admin Console and push applications to devices over-the-air. This page provides you with a detailed list of all the internal, public, and purchased applications options.

In This Section

- Sorting and Viewing Application and Book Information – See how to sort and view all your applications and books in the AirWatch Admin Console.
- Using the Application Actions Menu – View the different options for managing all your applications.
- Managing Devices – View options for controlling devices assigned to public and internal applications and to public books, and view how you can install, remove and notify end users about content.
- Managing Application Versions – Review how to updated the application version of your internal applications to incorporate new features and fixes.
- Managing Feedback (iOS 7+) – View how AirWatch integrates with iOS feedback options for iOS 7+ devices using request, clear, and view options for public or internal iOS applications.
- Managing Ratings – View how to control user ratings and comments for individual applications and books from users published to their devices.
- Deleting Applications and Books – Learn about deleting applications and books from the AirWatch Admin Console and the differences between deactivating, retiring, and deleting.
- Notifying End Users – Review how to notify users about applications and books using custom notifications.
- View Devices – Review how to see a list of devices that installed a purchased application or book. Also, review how to see a list of device-users who have accepted an invite to the enroll in the Apple's VPP.
- Tracking Applications – Review the different options for tracking applications.

Sorting and Viewing Application and Book Information

There are three separate pages for managing your public, internal and purchased applications. Navigating to Apps & Books ➤Applications ➤List View displays the three tabs, which you can select to view a list of those types of applications. You can use a number of filters to sort and view information for your public, internal and purchased applications. Once you have found an application you would like to manage, you can perform actions using the actions menu.

Note: Books do not include all options.
Sorting and Viewing Internal Applications and Books

The following columns/filters are available to sort public and internal applications and books:

- **Platform** – Filter based on platform type.
- **Status** – Filter based on whether an application or book is active or inactive.
- **Reputation Analysis (Apps only)** – Filter based on the status of a reputation analysis scan.
- **Categories (Apps only)** – Filter based on the application categories.
- **Requires Renewal (Apps only)** – Filter based on whether the iOS application need to have auxiliary files renewed like the provisioning profile file.

Sorting and Viewing Public Applications and Books

The following columns/filters are available to sort public applications and books:

- **Platform** – Filter based on platform type.
- **Status** – Filter based on whether an application or book is active or inactive.
- **Reputation Analysis (Apps only)** – Filter based on the status of a reputation analysis scan.
- **Categories** – Filter based on the application or book categories.

Sorting and Viewing Purchased Applications and Books

The following columns/filters are available to sort purchased applications:

- **Platform** – Filter based on platform type.
- **Status** – Filter based on whether an application or book is active or inactive.
- **App Type (Apps only)** – Filter based on whether a purchased app is a public or custom B2B app.

Using the Application Actions Menu

Each application is listed in a row, and each row has an actions menu on the right side that you can use to perform various actions. The availability of the action differs based on whether you are viewing public, internal, or purchased apps and based on the platform.

**Actions Menu** – Displays the main action areas; View, Edit, Edit Assignment, and actions.

- **Add Version** – (Jump to) Updates your internal application with a new version.
- **Deactivate** – Removes a public or internal application and all versions of it from all managed devices. See Deleting Applications and Books for an explanation of options for managing unneeded applications.
- **Delete** – (Jump to) Removes the application from devices and from the AirWatch Admin Console.
Edit Assignment – (Jump to) Edits settings of an application to exclude or include specific devices using smart groups. For purchased applications, this action’s icon is which lets you allocate available redemption codes and managed distribution codes.

Manage Devices – (Jump to) Offers options for installing, removing, or notifying users about a public or internal application.

Manage Feedback – (Jump to) Displays, requests and clears application feedback from iOS devices for public and internal applications.

Notify Devices – Sends a notification to devices with information about a purchased application.

Retire – Removes an internal application from all managed devices. If an older version of the application exists in the AirWatch solution, then this older version is pushed to devices. See Deleting Applications and Books for an explanation of options for managing unneeded applications.

User Ratings – (Jump to) Shows the application rating and feedback.

View – Provides detailed information about a public or internal application.

View Analytics – Exports the analytics for internal applications that use the AirWatch Software Developers Kit (SDK).

View Devices – (Jump to) Displays the devices to which you assigned purchased applications. You must assign the purchased application to a device in order to gain access to this option.

View Events – Shows device and console events for applications and allows you to export these events as a .csv file.

View Logs – (Jump to) Downloads or deletes log files for an internal SDK and wrapped applications.

View Other Versions – Shows previous versions of an internal application that were added to the AirWatch Admin Console.

Managing Devices

Use the Manage Devices option to control devices assigned to public and internal applications and for public books, either assigned individually or as members of a Smart Group. From this screen, you can install, remove and notify end users about applications.

1. Navigate to one of the following pages:
   - Navigate to Apps & Books Applications List View and select either the Public or Internal tab.
   - Navigate to Apps & Books Books List View and select the Public tab.

2. Select the Manage Devices icon ( ) from the actions menu for the row you want to manage devices for.

   Alternatively, you can select one of the links (represented as #/#/#) for the row in the Not Installed / Installed / Assigned column.

   The Manage Devices page displays. From here, you can perform actions depending on whether it is an application or book:
• **Install (Apps only)** – Installs the application to devices.

• **Remove (Apps only)** – Removes the application from devices.

• **Notify** – Notifies devices about the application or book. Settings include email, SMS, push and message template options for sending messages to devices.

3. Perform actions using one of these two options, selected or listed:

   *Note: You cannot install or remove public books from the Manage Devices feature.*

• Select the check boxes for the devices you want to manage and then select either **Install On Selected**, **Remove From Selected**, or **Notify Selected**.

   *Note: If the list is long and continues to another page, ensure to perform the action for the current page. Settings are not saved when you move to another page.*

• Select **Install On Listed**, **Remove From Listed**, or **Notify Listed** to perform the action for every device listed. You can filter the list of devices using the **Status** drop-down menu. Enabled check boxes have no affect with this method.

### Managing Application Versions

Update the application version of your internal applications to incorporate new features and fixes. Use the AirWatch Admin Console to:

• Deploy multiple versions of the same application.

• Assign different versions to different device groups.

• Push beta versions for testing purposes.

• Allow devices to ‘roll back’ to a previous version.

• Ensure employees are compliant with the latest version.

You can leverage the application management tools in AirWatch to manage different versions of the same internal application.

This feature is especially useful for application testing as you may wish to upload a beta version of an application update to deploy to specific users for testing purposes while still deploying the current version of the application to all other users. Once the testing is complete, you can replace the existing version of all devices with the newest version of the application.

### Adding Versions

1. Select **Add Version** for the application from the actions menu.

2. Upload the updated application file.

3. Retire the older version if you want to at this time using the actions menu. See information on the retire feature in the [Deleting Applications and Books](#) topic.

   *Note: If you do not want to immediately retire the previous version of the application you have the option to do so at a later time.*
4. Review version information and specify application settings, if they differ.

5. Click **Save** to save the application.

Managing Feedback for iOS 7+

Use the **Manage Feedback** option from the actions menu to request, clear, and view feedback for public or internal iOS applications. Feedback for iOS 7+ applications is stored on the device. The AirWatch Admin Console retrieves the feedback from the device and displays and stores it in the AirWatch Admin Console. This action offers a central location for you to view and manage the feedback.

In order to use Manage Feedback for iOS 7+ devices, the AirWatch Admin Console requires two criteria:

1. You must assign at least one iOS 7+ device to the application.

2. An iOS 7+ device must transmit to the AirWatch Admin Console that it contains feedback and data.

When these two criteria are met, you can see and use the Manage Feedback option in the AirWatch Admin Console.

From the **Manage Feedback** page, use the check boxes to select devices and apply the following functions:

- **Request Feedback** – Initiate a command to the device to retrieve the feedback from its location in the application on the device.

- **Clear Feedback** – Initiate a command to clear data in the directory where the feedback is stored in the application on the device.

- **View Feedback** – Display the **View Feedback** page. Use the View Feedback page to download and delete feedback. Download the file as a .zip file. Deleting the feedback from this page, deletes it from the AirWatch Admin Console.

Managing Ratings

AirWatch lets you view feedback in the form of user ratings and comments from users of applications and books. Use ratings to establish the effectiveness and popularity of applications and books in your repositories. For example, you can choose applications with better capabilities and push them to more users. You could also choose to delete specific applications and books because users do not find any value in them.

**Viewing User Ratings and Comments**

1. Navigate to one of the following pages:

   - Navigate to **Apps & Books ➤Applications ➤List View ➤Public, Internal, or Purchased**.
   - Navigate to **Apps & Books ➤Books ➤List View ➤Public, Internal, or Purchased**.

2. Select **User Ratings** from the actions menu to access the rating comments.

   - **Average Rating** – View the average of the total number of user ratings.
   - **User Group** – Filter the comments based on a specific User Group.
   - **Individual Entries** – Review entries for the individual rating, any comments, when the rating was created, and the user who created the entry.
Note: You can edit Ratings for public applications and books. To edit, select Edit from the actions menu on the Public application or book page and enter the number of stars (zero through five) in the Rating field.

Deleting User Comments

On the User Ratings page, select a rating entry, then select Delete Rating. Once deleted from the AirWatch Admin Console, the change gets reflected in the App Catalog and Book Catalog.

Deleting Applications and Books

Deleting applications and books is often necessary to free up storage space and to clean your application and book repositories. However, deleting applications and books permanently removes them and all versions from AirWatch.

As an alternative, AirWatch offers the options to deactivate applications and books and to retire applications. You cannot retire books because AirWatch does not store multiple versions of books at this time.

Review the differences between deactivating, retiring, and deleting before you perform any deleting actions to decide if the deactivate or retire options can meet your needs. Access these options from the actions menu.

Deactivate

Deactivating an application or book removes it and all versions of it from the devices it is assigned to. Deactivate does not delete it from your repository in the AirWatch Admin Console. You can still view deactivated applications and books in the AirWatch Admin Console so that you can track devices that remove applications and books.

Deactivate offers the advantage of reversing the inactive status in the future.

When to Use

Your organization is changing strategies and no longer needs applications and their versions that reflect the old focus. You can deactivate unnecessary applications so that they no longer clutter your device-user’s application repositories; however, you can still access them in the AirWatch Admin Console.

Retire (Apps only)

Retiring an application removes the selected application version from devices; however, if there is an alternate version of the application, then that alternate version pushes to devices.

When to Use

A new version of an application has several bugs and is causing end users productivity. The previous version worked fine for your organization. You can retire the current version of the application and the AirWatch Admin Console pushes the previous version to devices.

Important Setting – Push Mode

Configuring Push Mode as Auto or On-Demand impacts how the AirWatch Admin Console behaves when you use the Retire option.

- **Auto** – Set the application deployment option to Auto to push previous versions of an application to devices when you retire the current version.
Note: The previous version must be active. If you deactivated the previous version, then AirWatch does not automatically push it to devices.

- **On-Demand** – Set the application deployment to **On-Demand** to manually push older versions to devices. End users must initiate a search and installation of the application version.

**Uploading New Application Versions**

When you upload a new version of an application using the actions menu and the **Add Version** option, AirWatch enables the **Retire Previous Version** check box by default. This option sets the Console to remove alternate application versions from devices.

**Note:** Although, this option removes updates, this behavior also helps to manage security issues or bugs that might exist in the current version.

Disabling the **Retire Previous Version** check box upon upload, replaces the current version of the application depending on the Push Mode (automatically or on-demand). It does not mark the alternate application version as retired.

Select **View Other Versions** from the actions menu to see the alternate versions of the application that are available in your internal application repository.

**Delete**

Deleting an inactive application or book erases it from devices and from the AirWatch Admin Console.

**When to Use**

You know your organization has no future use for any version of the application or book. You want space in your AirWatch environment so you perform a clean up of retired applications and books.

**Important Behavior for Active and Inactive Applications**

When you use the **Delete** action, AirWatch checks to see if the application is active or inactive.

- An **active** application, when deleted, behaves as a retired application. You also lose the ability to audit the application.
  
  If AirWatch has a previous version of this application, depending on the **Push Mode**, a previous version is automatically or manually pushed to devices.

- An **inactive** application gets deleted completely from the AirWatch application repository.

**Note:** AirWatch does not apply this behavior to books because AirWatch does not version books at this time.

**Notifying End Users**

Push notifications to end users about applications and books using AirWatch message templates. You can use these notifications for internal, public, and purchased applications and books.

**Notify Public Books**

Notify public applications using the **Manage Devices** option from the actions menu.
**Notify Internal and Public Apps**

Notify internal and public applications using the **Manage Devices** option from the actions menu.

**Notify Purchased Apps and Books**

1. Create a Message Template. For instructions on how to do this, see Creating Custom Notifications.
2. Navigate to one of the following pages and locate the specific app or book for notification:
   - Apps & Books ➤ Applications ➤ List View ➤ Purchased
   - Apps & Books ➤ Books ➤ List View ➤ Purchased
3. Use the actions menu and select **Notify Devices**.
4. Select the **Message Type**, **Email**, **SMS**, or **Push**.
5. Use your custom message template from the **Message Template** menu and then select **Send**.

**View Devices**

Use the **View Devices** option to see the devices assigned to the purchased content.

For your managed distribution users, you can view the ones who accepted the invitation to join Apple's Volume Purchase Program (VPP). You can also send individual invitations to enroll in the program from this page.

**Note:** You can view devices for documents bought using redemption codes but you can only send invitations to join VPP for managed distribution users.

1. Ensure the purchased application is assigned to at least one smart group. If the content is not assigned, you cannot view applicable devices.
2. Navigate to Apps & Books ➤ Applications ➤ List View and select the **Purchased** tab.
3. Ensure you are in the same organization group that houses the sToken with the managed distribution codes you want to use. AirWatch does not apply managed distribution codes from the **View Devices** page to other organization groups.
4. Select the **View Devices** icon (__) from the actions menu.
   The **View Devices** page displays. You can perform the following actions
   - Install (publish) applications.
   - Delete applications.
   - Invite users to Apple's VPP. You can only access this option if the device-user has not accepted an invitation to join Apple's VPP for managed distribution. Use the following procedure to send individual invitations.
     - Filter using the **User Invite** option and select **Not Accepted**.
       This filter displays **Accepted**, **Not Accepted**, and **N/A**. **N/A** identifies a device as older than iOS 7+ or content bought using redemption codes.
     - Select the **Invite** action from the action menu for the applicable device.
AirWatch sends an email invitation to users of iOS v7.0.0 through v7.0.2 based on the template option set in Groups & Settings ►All Settings ►Apps ►Catalog ►License Based VPP.

AirWatch automatically sends users of iOS v7.0.3+ an invite command to the device. It does not send an email invitation.

Tracking Applications

Tracking applications helps you to monitor all applications for compliance, installation status, and ratings. There are many ways to track the applications on devices using the AirWatch Admin Console:

- **The AirWatch Hub** – Use the Compliance and Apps sections for tracking. The Hub is found at the top of the Main Menu.
  - Compliance section – The Compliance section provides a condensed summary of devices with blacklisted apps and devices without required apps.
  - Apps section – The Apps section provides a condensed summary of devices without the latest application version. It also provides a list of most generally installed applications. In addition, the App view also provides information on compliant applications, top installed/least installed, top rated/bottom rated and their installation percentage, health (the most crashed and those with the most errors), and size.

- **Devices Details View** – Shows the list of installed applications along with the status, name, type, version, identifier and size. To find the Devices Details View, select Devices from the Main Menu, choose the List View, select the device for which you want the details and finally select the Apps tab for that device.

- **Reports And Analytics** – The All Reports tab provides you with actionable, result-driven statistics. The Application Compliance report provides a way for tracking the devices that do not have the latest version of applications. To find Reports and Analytics, navigate to Hub ►Reports And Analytics ►Reports ►List View ►All Reports.
Application Groups

Overview

The AirWatch Admin Console provides the ability to group applications into blacklisted, whitelisted, and required applications. These groups are called Application Groups and each application group is tied to an Organization Group (OG). Use application groups to give access to desired users and to restrict access to unnecessary users.

Examples of application groups include the following suggestions:

- Blacklisted applications such as common games and other bandwidth intensive applications.
- Whitelisted applications such as the AirWatch Agent and Enterprise applications.
- Required applications such as the AirWatch Agent or Secure Browser.

In This Section

- Configuring an Application Group – View how to set application groups using the AirWatch Admin Console.
- Adding Custom MDM Applications to Application Groups – See how to add custom MDM apps for extra security and apply them to application groups.
Configuring an Application Group

The AirWatch Admin Console provides the ability to group applications into blacklisted, whitelisted, and required applications. These groups are called **Application Groups** and each application group is tied to an Organization Group. Use application groups to assign whitelists and blacklists to users.

**Note:** For more information about creating an **Application Control** profile, see Appendix C – Enforcing Application Control for Android and Windows Phone 8.

1. Navigate to **Apps & Books ► Applications ► Settings ► App Groups.**

2. Select **Add Group.**

- **List tab:**
  - Select **Type** as **Whitelist**, **Blacklist**, **Required** or **MDM Application**. On selecting the **Type**, the **Name** field is automatically populated.

  **Note:** Select **MDM Application** for custom MDM applications.

  - Select **Platform** as either **Apple**, **Android** or **Windows Phone 8**.

  - Enter the **Application Name** and the **Application ID**. The **Application ID** automatically completes when you use the search function to search for the app from an app store.

  - Select **Add Application** to add multiple applications and then select **Next** to navigate to the **Assignment** tab. Add exceptions to your application group to create detailed whitelists and blacklists.

  - Select **Add Publisher** for Windows Phone 8 to add multiple publishers to application groups. Publishers are organizations that create applications. Combine this option with **Add Application** entries to create exceptions for the publisher entries for detailed whitelists and blacklists on Windows Phone 8.

  Select **Next** to navigate to an application control profile. You must complete and apply an application control profile for Windows Phone 8.

- **Assignment tab:**
  - Enter a **Description** for the application group.
Define the **Device Ownership** as Corporate-Dedicated, Corporate-Shared, Employee Owned, or Undefined.

Assign the device **Model** and the **Operating System**.

Select the **Organization Group** and **User Group** for the application group to be assigned to and then select **Finish** to complete the process.

### Adding Custom MDM Applications to Application Groups

You can add custom MDM applications that track device location, device information and jailbreak status. Apply these custom MDM applications to desired application groups for information gathering, troubleshooting, and asset tracking.

*Note:* AirWatch does not remove custom MDM applications when the Compliance Engine detects a non-compliance status on the device.

To enable this feature, perform the following steps at the applicable Organization Group (OG):

1. Navigate to **Groups & Settings** ➤ **All Settings** ➤ **Devices & Users** ➤ **General** ➤ **Enrollment**.
2. Select **Customization**.
3. Enable **Use Custom MDM Applications**.
Compliance

Overview

You can create compliance policies that detect when users install forbidden applications and configure these policies to take actions to fix the non-compliance status.

To begin, group your applications into Application Groups, which gives you the ability to manage the various applications in your App Catalog. After you define your Application Groups, you can use these groups to initiate protective actions through the AirWatch Compliance Engine.

For example, if you detect a user with game-type application, which is one of the blacklisted application in a Blacklisted Application Group list, the Compliance Engine can be used to:

- Send a push notification to the user prompting them to remove the application.
- Remove certain features such as Wi-Fi, VPN or Email profiles from a device.
- Remove specific managed applications and profiles.
- Send a final email notification to the user copying IT Security and HR.

In This Section

Building an Application Compliance Policy – Review how to configure an application compliance policy in the AirWatch Admin Console.

Building an Application Compliance Policy

Build an application compliance policy to perform an action on devices with non-compliant applications:

1. Navigate to Devices ►Compliance Policies ►List View. Select Add.

2. Select Application List on the Rules tab. In the Contains drop-down, select whether this rule detects a whitelisted or blacklisted application, or the absence of a required application or app version. Define the other conditions to complete the rule:
• **Actions** – Set escalating actions to perform if a user is not in compliance with an application-based rule. For example, you could send a message to users with blacklisted applications informing them to uninstall the application or else risk losing access to corporate applications.

• **Assignment** – Set the assignment criteria for this rule. For example, you can specify particular platforms and models, or you can apply the rule to certain Organization Groups.

• **Summary** – Name the rule and give it a brief description.

3. Select **Finish and Activate** to enforce the newly created rule.

More information about compliance policies can be found in the **Mobile Device Management Guide**.
Deploying an Application Catalog

Overview

After you configure your public applications, internal applications, and purchased applications in the AirWatch Admin Console, you can deploy an Enterprise App Catalog to your end users, which will let them access those applications. While the AirWatch Admin Console allows you to manage applications over-the-air in a centralized location, the App Catalog serves as a one-stop shop for your end users to access applications based on the settings you established in the AirWatch Admin Console.

The AirWatch App Catalog is where users can do the following tasks:

- View and install recommended public, internal, purchased or web applications.
- Browse and filter applications by type and category.
- Receive notifications on application updates for both managed and unmanaged applications.
- Install application updates for managed applications.
- Add ratings and comments for public, internal, or purchased applications.
- View overall rating for the applications based on ratings provided by other users and view specific comments provided by other users.
- View application status whether an application is Not Installed, Installed, Needs Update, or Blocked.

In This Section

- Deploying the Enterprise App Catalog — Read how to push an app catalog automatically and manually.
- Adding Featured Applications — Read how to place applications in the featured area for easy recognition and access.
- Using the App Catalog — View how to use an app catalog on devices and read an explanation of its different features.

Deploying the Enterprise App Catalog

The first step to deploying applications through AirWatch is publishing the Enterprise App Catalog. You can do this in one of two ways. You can automatically push the App Catalog to devices upon enrollment, or you can create and deploy a device profile with a web clip or bookmark payload. The advantages of pushing the App Catalog automatically are ease of set up and maintenance. Advantages for manually pushing a device profile are control over updating and having different app catalogs for different platforms. However, you must maintain these different device profiles and you have to remember to republish or push the profile when you have updates.

Pushing the App Catalog Automatically

1. Set the active Organization Group to receive the App Catalog, navigate to Groups & Settings ➤ All Settings ➤ Apps ➤ Catalog ➤ General.
2. Configure the following settings on the General tab:

- **Require Encrypted Uid** – Require the encryption of communications with the App Catalog through the URL when using a devices profile to configure and push your App Catalog. If devices do not use an encrypted URL link to access your App Catalog when this is enabled, then devices cannot access your App Catalog.

  **Note:** This option only affects App Catalogs that you push using a separate devices profile. If you are pushing your App Catalog automatically using the Publish App Catalog option on the Publishing tab, then the App Catalog UID is always encrypted and you do not need to set this option.

- **Require Authentication for App Catalog** – Require users to log in with their username and password before they can access the App Catalog.

- **Keep User Signed In** – Keep users signed in and does not require them to log in each time.

- **Reauthenticate After (Days)** – Require users to authenticate (log in) after a set number of days.

- **Default Tab** – Set the default tab that displays when the App Catalog launches.

3. Configure the following settings on the Publishing tab:

- **Publish App Catalog** – Publish the App Catalog for iOS, Android, and Windows 8/RT devices in the currently selected Organization Group.

  **Note:** This option automatically pushes the App Catalog to devices upon enrollment.

- **App Catalog Title** – Enter a name for your App Catalog.

- **Platform** – Select the supported platforms for your App Catalog. Supported platforms include Android, Apple iOS and Windows 8/RT.

- **Full Screen (iOS only)** – Enable always having the App Catalog web clip open in full screen mode. Use this setting for iOS systems that, by default, do not open web clips in full screen mode.

- **Icon** – Upload an icon for your App Catalog.

### Pushing the App Catalog with a Device Profile

You can deploy the App Catalog using this method for iOS, Android and Windows 8/RT devices.

1. Navigate to Devices ►Profiles ►List View and select Add. Select Android, iOS or Windows 8/RT as the platform.

2. Enter General information as necessary.

3. Select the Web Clips (iOS and Windows 8/RT) or Bookmarks (Android) payload.

4. Enter one of the following App Catalog URLs:
   - Unencrypted – `https://<Environment>/Catalog/AppCatalog?uid={DeviceUid}`
   - Encrypted – `https://<Environment>/Catalog/AppCatalog?uid={SecureDeviceUdid}`
Adding Featured Applications

Once you've uploaded and configured all of your applications for the App Catalog, you often need a way to set a few select applications apart from all other applications. Use AirWatch's Featured Applications option to highlight specific applications within the App Catalog for your end users.

The App Catalog hosts Featured Applications on their own page and also lists them in the main list of applications. You can add internal or public applications as Featured Applications.

1. Navigate to **Apps & Books ➤Applications ➤Settings ➤Featured Apps**.

2. Select **Add Application** depending on platform type, either Apple or Android. Choose whether the application is an Internal or Public application and select the application from the list of applications in the AirWatch Admin Console.

3. Select **Add Category** depending on platform type, either Apple or Android. Choose the types of categories to make available in the App Catalog on a device.

4. Optionally, set an application type to highlight the most popular applications in the **Most Downloaded Applications** section.

Unmanaged devices enrolled using this method still create a device record in the AirWatch Admin Console for audit purposes. The status of these devices will be **App Catalog Only**. You cannot track the download status of applications on this device, but you can see a list of all assigned applications. If a user removes the unmanaged profile, the applications remain but the Web Clip is removed.

**Note:** In order for public and internal applications created using the AirWatch SDK to communicate and work with the AirWatch solution in a deployment that uses the App Catalog without MDM, the device user must activate the application within the App Catalog.

To activate the public or internal application, access the SDK-created application in the App Catalog. Before the application opens, it prompts you to activate it. By clicking the activation button, the application opens on the device and begins communication with AirWatch.

Using the App Catalog

Once deployed, the AirWatch App Catalog is accessible through the AirWatch Agent on a device. Additionally available for iOS devices, you can make the App Catalog accessible as a web clip directly from the device home screen.

Default and Other Tabs

The App Catalog opens to the page you configured as the Default Tab. Choose the default tab that best meets the needs of end users.

- **Featured** – Displays applications and categories you set as featured. This tab, with the help of your application categories, gives special applications up front real estate and helps draw your mobile fleet's attention to these applications.

- **Public** – Displays the public applications available for download to the device. Users can also update their public applications from this tab. Prices display on this tab for those public applications that are not free.

- **Purchased** – Displays the purchased applications your organization buys through the Apple VPP. Users can download these applications and they can also update their existing versions. If you do not use the Apple VPP, then this tab does not display.
- **Web** – Displays those applications you pushed to devices using a device profile, either a Bookmark (Android) payload or a Web Clip (iOS) payload.
  - Bookmarks – Enable the **Show in App Catalog / Workspace** check box in an Android Bookmarks device profile.
  - Web Clips – Enable the **Show in App Catalog / Workspace** check box in an iOS Web Clips device profile.
- **Internal** – Displays internal applications your organization created for use. Applications you created using the AirWatch SDK or that you have wrapped with the AirWatch App Wrapping feature can display on this tab.

**Application Detail Tabs**

When a user opens an application in the App Catalog, they can view descriptive and ratings information.

- **Description** – Displays a brief explanation concerning the application and can link the user to more information about the application. It displays new versioning details, contains screenshots and can list prices, if applicable. All this information you can configure in the AirWatch Admin Console when you upload and push applications.
- **Ratings** – Displays reviews for the application from other users and lets users write and add their own views about the application. You can manage ratings in the AirWatch Admin Console for all three types of applications, public, purchased and internal.

**Available Actions**

Use the action icons in the App Catalog to view the following information:

- Takes you to the homepage to view the default tab and other available application tabs.
- Displays the blacklisted applications detected on the device.
- Displays available updates for installed applications.

Displays featured and available categories and lets you filter applications to display applications in a specific category.

Other actions you can perform from the App Catalog include installing and uninstalling applications from devices using the applicable buttons. You can also search for applications in the App Catalog using the Search field.
Application Reputation

Overview

The AirWatch App Reputation Cloud Service and its Reputation Analysis Engine scan internal and public Android applications and internal iOS applications for security risks and identifies them in scan results. AirWatch offers this feature through the AirWatch MAM space so that you can control the influx of insecure applications to your mobile environment. The Reputation Analysis engine uses proprietary technologies to search applications for unwanted behaviors such as:

- Making insecure network connections
- Accessing privacy settings
- Deploying malicious code

How App Reputation Works

Enable a scan on an application recently uploaded into the AirWatch environment, or run the feature on an previously deployed application. The App Reputation system processes an application using the following steps:

1. The AirWatch Admin Console sends the application data to the AirWatch App Reputation Cloud Service.
2. The Reputation Analysis Engine scans the application, identifies risks and compiles scan results.
3. The AirWatch App Reputation cloud service sends results to the AirWatch Admin Console.
4. The AirWatch Admin Console displays the scan results as part of the application's AirWatch record. View the results on the internal or public application page by selecting the application and viewing the **Reputation** tab.

In This Section

- **Supported Platforms** – Review which platforms and application types AirWatch scans for security.
- **Leveraging App Reputation Analysis** – Review how to enable and scan applications with the Reputation Analysis Engine.
- **Gathering Results** – Read an overview of the available options to gather scan results.
- **Viewing Scan Results** – View a brief explanation of the scan results.

Supported Platforms

The AirWatch App Reputation Cloud Service scans the following platforms and application types:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Internal Apps</th>
<th>Public Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iOS</td>
<td>✓</td>
<td>X</td>
</tr>
</tbody>
</table>
Leveraging App Reputation Analysis

**Enabling the Engine**

Enable the App Reputation Cloud service at any time. You can analyze new applications when you upload them and you can analyze applications previously deployed in your environment.

1. Navigate to Groups & Settings ➤ All Settings ➤ Apps ➤ Catalog ➤ App Reputation.
3. Select **Require Analysis Before Publish** to prevent the publication of the application without an App Reputation scan.

**Scanning Applications**

Use the App Reputation feature to scan applications for possible security risks. You can scan when adding a new application, or you scan an application already stored in your AirWatch application repository.

**Scanning a new application**

Run a scan on the Reputation tab when adding new public or internal applications.

**Scanning an existing application**

Use the **Run Reputation Analysis** menu from the Applications List View page to scan public and internal applications already in the AirWatch Admin Console.

**Rescanning applications with updates**

Rescan applications when the App Reputation Cloud Service has new scan definitions. The AirWatch Admin Console displays when the engine has updates on the internal or public page, in the Reputation Analysis column.

**Gathering Results**

Use the **Run Reputation Analysis** option to request the AirWatch App Reputation cloud service to run a Reputation Analysis scan. It scans applications on Android devices to identify security risks. You can scan one application or multiple applications using this feature. This feature is useful for scanning those applications already deployed before the App Scanning feature was implemented in the AirWatch solution.

The available commands, **Scan Listed**, **Scan Selected**, and **Rescan for Updates** behave in the following ways:

- **Scan Listed** – Submit applications for Reputation Analysis to the AirWatch App Reputation Cloud Service. Use filtering options to focus the list to desired applications. Enabled check boxes have no affect on this function.
- **Scan Selected** – Submit applications for Reputation Analysis to the AirWatch App Reputation Cloud Service that are selected using individual check boxes or the main check box.
- **Rescan for Updates** – Resubmit selected or listed applications for Reputation Analysis to the AirWatch App Reputation Cloud Service.
Viewing Scan Results

Navigate to Apps & Books ▶ Applications ▶ List View ▶ Internal or Public and select the application to view scan results. Results display on the Reputation tab. Use the Console as a central repository of scan results for your most commonly used applications. The scan results qualify risks as high, medium, and low and are divided into three types; design and programming, privacy, and risky behavior. View the number of risks in each category.

- **Design and Programming** – Examples include insecure network communications.
- **Privacy** – Examples include reading calendars and accessing locations.
- **Risky Behavior** – Examples include inter-application communication and installing packages.
Advanced Application Management

Apps Settings and Policies

Settings and Policies control how users access and interact with AirWatch applications and how these applications behave and look on devices. Settings apply to all AirWatch applications.

Default Settings for Profiles

You can apply to AirWatch applications. You can choose to apply default settings for profiles at an Organization Group (OG) level so they are shared across applications located in the OG.

Default Settings for Profiles

Find the default settings for profiles in Groups & Settings ►All Settings ►Apps ►Settings and Policies and then select Security Policies or Settings. You can apply these options across all the AirWatch applications in an OG. Shared options offer ease of use and a single point of configuration.

The default settings profiles are titled iOS Default Settings @ [Organization Group] and Android Default Settings @ [Organization Group] in the AirWatch Admin Console. However, you do not have to use the default settings profiles. You can still use and apply your legacy profiles.

View the compatibility matrices for information on which default settings apply to specific AirWatch applications.

Applying the Default Profile

You must apply the applicable default or custom profile to an application.

- Default Settings Profile
  - For Android applications, select the Android Default Settings @ [Organization Group].
  - For iOS applications, select the iOS Default Settings @ [Organization Group].

In This Section

Read how to configure the following default options for Settings and Policies:

Security Policies

- **Passcode Mode** – View how to set a passcode requirement for AirWatch applications, wrapped applications, and applications created with the SDK.
- **Single Sign On (SSO)** – Review how to allow access to applications with a single authentication session.
- **Integrated Authentication** – See how to integrate authentication requirements for external resources using the Workspace or the AirWatch Agent.
- **Offline Access** – Read how to allow access to resources when devices are offline.
- **Compromised Protection** – View how to enable protecting the network from compromised devices.
- **Data Loss Prevention** – See the available options to configure to prevent data losses.
• **Network Access Control** – View how to control access to mobile networks including the control of cellular and wi-fi connections.

**Settings**

• **Branding** – Read how to reflect your organization's image in your AirWatch applications.

• **Logging** – View how to enable logging for your AirWatch applications, wrapped applications, and applications created with the SDK.

• **Custom Settings** – Review how to add XML code to customize your application deployment.

**Passcode Mode**

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications. For more information about default versus custom profiles, refer to the "Default or Custom Settings for Profiles" section of the AirWatch Mobile Application Management Guide.

**Configuring Passcode Mode**

Choose an option to control access to applications.

• **Passcode Mode, Numeric or Alphanumeric** – Designates a local passcode requirement for AirWatch applications or wrapped applications that have the default settings profile applied to them. Device users set their passcode on the device at the application level when they first access the application. This option is set in the Passcode settings.

• **Disabled** – Requires no authentication to access the application.

1. Navigate to **Groups & Settings ➤All Settings ➤Apps ➤Settings and Policies ➤Security Policies**.

2. Complete the following **Passcode Mode** options:

   • **Passcode Mode** – Set as **Numeric, Alphanumeric or Disabled**.

     o **Authentication Timeout** – Set the allowable time for access to applications before disallowing access due to inactivity. If SSO is enabled and the passcode times out, the SSO identity logs out of all AirWatch and configured corporate applications and resources.

     o **Allow Simple Value** – Set the passcode to allow simple strings. For example, allow strings like 1234 and 1111.

     o **Minimum Passcode Length** – Set the minimum number of characters for the passcode.

     o **Minimum Number Complex Characters** – (Alphanumeric) Set the minimum number of complex characters for the passcode. For example, allow characters like [], @, and #.

     o **Maximum Passcode Age (days)** – Set the number of days the passcode remains valid before you must change it.

     o **Passcode History** – Set the number of passcodes the AirWatch Admin Console stores so that users cannot use recent passcodes.

     o **Maximum Number Of Failed Attempts** – Set the maximum times a user can login with an incorrect passcode before having to authenticate and set a new passcode.

3. **Save** your settings.
Single Sign On (SSO)

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications. For more information about default versus custom profiles, refer to the "Default or Custom Settings for Profiles" section of the AirWatch Mobile Application Management Guide.

**Note:** For information about Single Sign On for iOS 7 using Kerberos authentication, refer to the AirWatch iOS Platform Guide.

AirWatch's single sign on (SSO) feature allows end users to access all AirWatch apps with a single SSO Passcode without having to enter login credentials for each application. Using either the AirWatch MDM Agent or the AirWatch Workspace as a "broker application", end users can authenticate once using either their normal credentials or an SSO Passcode and then gain access to other applications so long as the SSO session is active.

**Enabling Single Sign On**

Enable SSO as part of the Security Policies that you configure to apply to all AirWatch apps, wrapped apps, and SDK-enabled apps using a Default SDK Profile. To enable SSO:

2. Set Single Sign On to Enabled to allow end users to access all AirWatch applications and maintain a persistent login.
3. Optionally set Passcode Mode to either Numeric or Alphanumeric to require an SSO Passcode on the device. If you enable SSO but do not enable a Passcode Mode, end users will use their normal credentials (either directory service or AirWatch account) to authenticate, and an SSO Passcode will not exist.

**Note:** Wrapped apps must have a passcode, either numeric or alphanumeric. Without this passcode, wrapped apps do not display true SSO functionality.

**Apps / Settings And Policies / Security Policies**

![Settings and Policies](image)

**SSO Session**

Once an end user authenticates with either the Workspace or the Agent, an SSO session is opened. It lasts so long as the Workspace is running in the background or until the Passcode Timeout value defined in the Passcode Mode settings is exceeded. With an active session, end users can access managed applications without having to enter their SSO Passcode.
Integrated Authentication

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications.

Configuring Integrated Authentication

Enable Integrated Authentication to allow access to corporate resources, such as content repositories, through the AirWatch Workspace or the AirWatch Agent using AirWatch SSO credentials.

**Note:** Integrated Authentication works in the AirWatch Browser.

2. Select Enabled and set the following options:
   - Enable Use Enrollment Credentials to access corporate resources listed in the Allowed Sites field with the SSO credentials.
   - Enter systems in the Allowed Sites field to control access to a specific set of sites and domains. You must complete this setting for Integrated Authentication to work. This setting ensures that AirWatch does not expose credentials to non-trusted resources.
3. Save your settings.

SSO and Integrated Authentication

On the Security Policies page, you can set Integrated Authentication to Enabled to allow the credentials used for applications to be passed on and used for authenticating into websites, such as wikis. Currently this setting only applies to the AirWatch Browser. Once enabled, you must define a list of allowed sites, which are the only sites that will support Integrated Authentication.

Additional requirements for SSO:

- SSO must be enabled and the user must successfully authenticate within an SSO session.
- The URL of the requested website must match an entry in your list of allowed sites.
- The website must use NTLM or basic authentication and return a 401 status code requesting authentication.
- The AirWatch Workspace can only use the enrollment credentials of the user when attempting to authenticate with a website. If a website requires a domain, for example, ACME\jdoe, to log in, and your end user's enrolled with only a basic username, for example, jdoe, then the authentication will fail.

Offline Access

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications.

Configuring Offline Access

Select Offline Access to allow access using the SSO identity to applications when the device is offline.

2. Select Enabled and then choose an acceptable time frame for offline access before the device requires re-authentication to the network and applications in the Maximum Period Allowed Offline field.

   Devices should return online periodically so the system can check device compliance and security status.

3. Save your settings.

Compromised Protection

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications.

Configuring Compromised Protection

Enable Compromised Protection so that the AirWatch Admin Console blocks access if the device is compromised.


2. Select Enabled to block an compromised device from accessing your mobile network.

3. Save your settings.

Data Loss Prevention

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications.

Configuring Data Loss Prevention

Enable Data Loss Prevention (DLP) to protect sensitive data in applications. This setting controls copying and pasting, printing, taking pictures and screen captures, using Bluetooth, and other areas where data transmits back and forth.


2. Select Enabled for the specific DLP option:

   - Enable Copy And Paste – Allows an application to copy and paste on devices when set to Yes.

   - Enable Printing – Allows an application to print from devices when set to Yes.

   - Enable Camera – Allows applications to access the device camera when set to Yes.

   - Enable Composing Email – Allows an application to use the native email client to send emails when set to Yes.

     **Note:** When you disable this option, iOS device users receive a system message that states they do not have an email account. This message is an artifact of the disabled functionality and does not reflect a true issue.

   - Enable Data Backup – Allows wrapped applications to sync data with a storage service like iCloud when set to Yes.
• **Enable Location Services** – Allows wrapped applications to receive the latitude and longitude of the device when set to **Yes**.

• **Enable Bluetooth** – Allows applications to access Bluetooth functionality on devices when set to **Yes**.

• **Enable Watermark** – Displays text in a watermark in documents in the Secure Content Locker when set to **Yes**. Enter the text to display in the **Overlay Text** field. You cannot change the design of a watermark from the AirWatch Admin Console.

• **Limit Documents to Open Only in Approved Apps** – Enter options to control the applications used to open resources on devices.
  
  • Enter the applications that you allow to open documents in the **Allowed Applications List** field.

3. **Save** your settings.

### Network Access Control

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications

**Configuring Network Access Control**

Enable **Network Access** to allow applications to access the mobile network.

1. Navigate to **Groups & Settings ► All Settings ► Apps ► Settings and Policies ► Security Policies**.

2. Select **Enabled** and then complete the following options:

  • **Allow Cellular Connection** – Controls cellular connections by allowing them all the time, allowing connections when the device is not roaming, or never allowing cellular connections.

  • **Allow Wi-Fi Connection** – Allows connections using wi-fi networks always or limits connections by Service Set Identifier (SSID). Enter the SSIDs devices can use to access the wi-fi network in the **Allowed SSIDs** field.

3. **Save** your settings.

### Branding

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications

**Configuring Branding**

Change the look and feel of applications to reflect your company’s unique brand by configuring images and colors through the use of **Branding** settings.

1. Navigate to **Groups & Settings ► All Settings ► Apps ► Settings and Policies ► Settings**.

2. Select **Enabled** for **Branding** and then complete the following options:
• Reflect your company colors by choosing the Toolbar, Toolbar Text, Primary, Primary Text, Secondary, and Secondary Text colors from a color palette.

• Enter in your Organization Name.

• Upload a custom Background Image.

• Rebrand the following iOS devices: iPhone, iPhone (Retina), iPhone 5 (Retina), iPad, and iPad (Retina).

• Rebrand Android devices by uploading the following sizes: Small, Medium, Large, and Extra Large.

• Upload a Company Logo for your Phone, or Tablet in regular or High Resolution.

3. **Save** your settings.

### Logging

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications.

#### Configuring Logging

View event records of errors or other actions in the AirWatch Admin Console with **Logging**.

1. Navigate to Groups & Settings ► All Settings ► Apps ► Settings and Policies ► Settings.

2. Select **Enabled** for Logging.

3. Choose your **Logging Level** from a spectrum of recording frequency options:

   - **Error** – Records only errors. An error displays failures in processes such as a failure to look up UIDs or an unsupported URL.
   
   - **Warning** – Records errors and warnings. A warning displays a possible issue with processes such as bad response codes and invalid token authentications

   - **Info** – Records a significant amount of data for informational purposes. An info displays general processes.

   - **Debug** – Record all data to help with troubleshooting.

      The AirWatch Admin Console reports the messages that match the configured logging level plus any logs with a higher critical status. For example, if you set the logging level to Warning, messages with a Warning and Error level display in the AirWatch Admin Console.

4. Select **Send logs over Wi-Fi only** to prevent the transfer of data while roaming and to limit data charges.

5. **Save** your settings.

### Custom Settings

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications.
Configuring Custom Settings

Use Custom Settings to enter XML code to manually enable or disable certain settings.

1. Navigate to Groups & Settings ► All Settings ► Apps ► Settings and Policies ► Settings.
2. Select Enabled for Custom Settings.
3. Enter the code in the Custom Settings field.
4. Save your settings.
AirWatch offers the ability to apply AirWatch SDK functionality to AirWatch applications. Use the default settings profile to apply an AirWatch SDK feature to an application by setting the configurations in Policies and Settings and then applying the profile. The default settings profiles are entitled:

- iOS Default Settings @ [Organization Group]
- Android Default Settings @ [Organization Group]

**Note:** You can continue to use legacy profiles to control the behaviors of your AirWatch applications. You are not restricted to using default settings at this time.

### Settings and Policies, AirWatch Applications Compatibility Matrix

<table>
<thead>
<tr>
<th>Settings and Policies Option</th>
<th>UI Label</th>
<th>Workspace</th>
<th>AirWatch Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>iOS</td>
<td>Android</td>
</tr>
<tr>
<td><strong>Passcode Mode</strong></td>
<td>Passcode Mode</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Allow Simple Value</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Minimum Passcode Length</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Minimum Number Complex Characters</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Maximum Passcode Age</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Passcode History</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Maximum Failed Attempts</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Passcode Timeout</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Single Sign On</strong></td>
<td>Enable</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Integrated Authentication</strong></td>
<td>Enable</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Use Enrollment Credentials</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Offline Access</strong></td>
<td>Enable</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Maximum Period Allowed Offline</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Compromised Protection</strong></td>
<td>Enable</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Data Loss Prevention</strong></td>
<td>Enable</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Copy and Paste</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Printing</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Watermark</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Open Documents in Approved Applications</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Allowed Applications</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Network Access Control</strong></td>
<td>Enable</td>
<td>Cellular Connection</td>
<td>Wi-Fi Connection</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------</td>
<td>---------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Branding</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>✓ ✓ ✓ ✓</td>
<td>x x x x</td>
<td></td>
</tr>
<tr>
<td>Toolbar Color</td>
<td>✓ ✓ x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toolbar Text Color</td>
<td>✓ ✓ x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Color</td>
<td>x x ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Text Color</td>
<td>✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary Color</td>
<td>✓ x x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary Text Color</td>
<td>x x ✓ x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Image (iPhone)</td>
<td>✓ x x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Image (iPhone – High Res)</td>
<td>✓ x x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Image (iPad)</td>
<td>✓ x x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Image (iPad – High Res)</td>
<td>✓ x x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Image (iPhone 5 – High Res)</td>
<td>✓ x x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Small</td>
<td>x ✓ x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Medium</td>
<td>x ✓ x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Large</td>
<td>x ✓ x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background XLarge</td>
<td>x ✓ x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company Logo Phone</td>
<td>✓ x ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company Logo Phone – High Res</td>
<td>✓ x ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company Logo Tablet</td>
<td>✓ x ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company Logo Tablet – High Res</td>
<td>✓ x ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization Name</td>
<td>✓ x ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>x x x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging Level</td>
<td>x x x x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Logs Over Wi-Fi</td>
<td>x x x x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* ✓ This option is supported but is not configured using Settings and Policies.
Appendix B – Using the App Catalog without MDM

Overview

Many organizations do not need to manage devices for their mobile fleets for various reasons, including possible privacy or legal issues. However, they may need to distribute mobile applications, so AirWatch offers the flexibility of using a deployment that uses the App Catalog without MDM.

Users do not have to enroll with AirWatch using an Agent, but rather enroll with the AirWatch App Catalog without MDM. This App Catalog distributes all application types, public, purchased, and internal.

Although end user devices are not enrolled in MDM, you can access a device record in the AirWatch Admin Console. The device record is for auditing purposes and the status of these devices in the AirWatch Admin Console displays as **App Catalog Only**.

Supported Platforms

AirWatch supports the Apple iOS and Android platforms for this feature.

Considerations

Review these considerations to see if an App Catalog without MDM benefits for your AirWatch deployment.

Configuring Considerations

- You configure applications with the Deployment Push Mode setting of **On-Demand** because you cannot push applications automatically with this deployment.

End User Considerations

- End users enroll with AirWatch using the App Catalog and not with an Agent.
- End users must re-enroll with the App Catalog without MDM when you make updates. Even if they do not re-enroll, they still have access to applications. However, they cannot receive an updated title or an updated icon for the catalog.

Deployment Considerations

- Devices in your App Catalog without MDM deployment, sometimes called a standalone MAM deployment, are unmanaged. An unmanaged device does not have the security controls offered by the AirWatch MDM feature.
- Applications distributed using this deployment remain on devices after an end user unenrolls with the App Catalog without MDM.
- You cannot track application downloads but you can see a list of assigned applications for the device in the device record in the AirWatch Admin Console.
Creating a Deployment for the App Catalog without MDM

Creating the AirWatch standalone MAM deployment has the following parts.

1. Configure an App Catalog without MDM.
2. Send end users their enrollment credentials and the AirWatch environment URL so that they can enroll with the App Catalog without MDM. Enrolling pushes the App Catalog profile to their devices.

   Enrollment credentials include an email address and a Group ID. You configure the Group ID when you create the OG and you add email domains when you configure the App Catalog without MDM.

Enabling the App Catalog without MDM

AirWatch provides a solution for deploying the App Catalog without requiring users to enroll in full MDM using the AirWatch Agent. Not using the AirWatch Agent prevents users from enrolling into MDM, but they can still have access to applications assigned to an App-Catalog-Only-Organization-Group through the App Catalog.

1. Navigate to Groups & Settings ►All Settings ►Apps ►Catalog ►App Catalog without MDM.
2. Enable the App Catalog without MDM to prevent users that enroll into the selected App-Catalog-Only-Organization-Group from enrolling into MDM. Users that this setting should apply to should be created in this OG or in a parent above it.
3. Enable the Allow New User Registration check box to allow new users to register for access to the App Catalog.
4. Select the Enable Email Domain Validation option to use specified email domains to validate users when they register to access to the App Catalog without MDM.

   Enter email domains in the Allowed Email Domains field for the standalone MAM users. End users enter their email addresses and a Group ID to enroll with this App Catalog. AirWatch matches the domains in this field to the domains of MAM only users.
5. Enter a title for the App Catalog Web Clip.
6. Upload an image for the App Catalog.
7. Select Save.

End users can enroll and select or enter the Group ID of the App-Catalog-Only-Organization-Group you set up. After completing enrollment, the App Catalog profile prompts for install. When finished, it displays on the launch screen.

Unmanaged devices enrolled using this method still create a device record in the AirWatch Admin Console for audit purposes. The status of these devices is App Catalog Only. You cannot track the download status of applications on this device, but you can see a list of all assigned applications. If a user removes the unmanaged profile, AirWatch does not remove the applications remain but it does remove the Web Clip.
Appendix C – Enforcing Application Control for Android and Windows Phone 8

Use application control profiles in conjunction with your application groups to whitelist and blacklist content on devices.

- **Configuring Application Control for Android** – View how to configure an application control profile for Android.
- **Configuring Application Control for Windows Phone 8** – View how to configure an application control profile for Windows Phone 8.

**Configuring Application Control for Android**

To allow or prevent installation of applications on devices, you enable Application Control to whitelist and blacklist specific applications. While the Compliance Engine sends alerts and takes administrative actions when a user installs or uninstalls certain applications, Application Control prevents users from even attempting to make those changes. For example, prevent a certain game application from ever installing on a device, or force the AirWatch Agent to remain on a device.

**Note:** Application Control is available only for specific device models. See the OEM Specific Key Features Matrix for more information.

2. Select Device to deploy your profile to a device.
   Alternatively, select Container to deploy your profile to a container within a Samsung KNOX device.
   **Note:** For more information on Samsung KNOX containerization, please see the Configuring Containerization with Samsung KNOX section.
3. Configure General profile settings as appropriate.
4. Select the Application Control payload.
5. Enable or disable the following settings to set the level of control for your application deployments:
   - Enable **Prevent Installation of Blacklisted Apps** to enforce the automatic removal and/or prevent the installation of blacklisted apps defined in Application Groups.
   - Enable **Prevent Un-Installation of Required Apps** to prevent the un-installation of required apps defined in Application Groups.
   - Enable **Only Allow installation of Whitelisted Apps** to prevent the installation of any application that is not a whitelisted app defined in Applications Groups.
6. Select Save & Publish.

**Note:** For instructions on creating application groups, see Configuring an Application Group.
Configuring Application Control for Windows Phone 8.1

**Note:** This payload is only available to devices using Windows Phone 8.1. If you wish to use this payload, you must download and install the free update.

To allow or prevent installation of applications on devices, you can enable Application Control to whitelist and blacklist specific applications. While the Compliance Engine sends alerts and takes administrative actions when a user installs or uninstalls certain applications, Application Control prevents users from even attempting to make those changes. For example, prevent a certain game application from ever installing on a device, or allow only specific apps you’ve whitelisted to be installed on a device.

2. Configure General profile settings as appropriate.
3. Select the Application Control payload.
4. Enable or disable the following settings to set the level of control for your application deployments:
   - Enable **Prevent Installation of Blacklisted Apps** to enforce the automatic removal and/or prevent the installation of blacklisted apps defined in Application Groups.
   - Enable **Only Allow installation of Whitelisted Apps** to prevent the installation of any application that is not a whitelisted app defined in Applications Groups.
5. Select Save & Publish.

**Note:** For instructions on creating application groups, see Configuring an Application Group.