



MobileIron AppStation 63 for Android Guide for Administrators

Revised: October 2, 2019

For complete product documentation see:
[MobileIron AppStation Product Documentation](#)

Copyright © 2019 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies' trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.



Revision history

TABLE 1. REVISION HISTORY

Date	Revision
October 2, 2019	<ul style="list-style-type: none">• In AppStation configuration steps overview, removed the requirement to disable Always require client for registration. If Always require client registration is enabled in Users > User Settings > Device Registration Setting in MobileIron Cloud, users automatically get emails for registering their device via AppStation.• Added the following sections:<ul style="list-style-type: none">◦ Configuring MAM-only in MobileIron Cloud◦ Add apps for distribution



Contents

Revision history	3
Contents	4
About MobileIron AppStation	5
MobileIron AppStation overview	5
MAM-only use cases with MobileIron AppStation	5
Android AppConnect app behavior with MobileIron AppStation	6
MAM-only deployment diagrams	6
MAM-only with AppStation	6
MAM-only with AppStation and MDM with other platform	7
MobileIron AppStation configuration	8
Supported configurations for managing apps through AppStation	8
Administrator actions supported for AppStation	8
Setting up MobileIron AppStation	9
AppStation configuration steps overview	9
Configuring MAM-only in MobileIron Cloud	9
Add apps for distribution	10
Verify the setup for AppStation	11
What users see in MobileIron AppStation for Android	12
Download and install AppStation for Android	12
Register with MobileIron Cloud	12
Launcher and Catalog	12
Settings	14



About MobileIron AppStation

The following provide an overview of MobileIron AppStation for Android:

- [MobileIron AppStation overview](#)
- [MAM-only use cases with MobileIron AppStation](#)
- [Android AppConnect app behavior with MobileIron AppStation](#)
- [MAM-only deployment diagrams](#)
- [MobileIron AppStation configuration](#)

MobileIron AppStation overview

Deploying a MobileIron unified endpoint management (UEM) platform allows you to secure and manage mobile devices as well as mobile apps in your enterprise. The term mobile device management (MDM) is used to describe the features, policies, and configuration used for securing and managing mobile devices. The term mobile apps management (MAM) is used to describe the features, configuration, and policies used for securing, managing and distributing enterprise apps to mobile devices. In most cases, you deploy MobileIron UEM to do both MDM and MAM. However, in some cases, you may want to manage only the apps on the device without having to manage the device itself. A deployment through which only apps on a device are managed is called MAM-only.

MobileIron AppStation is specifically designed as the UEM client for a MAM-only deployment with MobileIron Cloud. In a MobileIron AppStation MAM-only deployment, only apps available through AppStation are managed.

The following types of apps are supported:

- AppConnect apps (wrapped with Secure Apps Manager for AppStation)
- Non-AppConnect apps (in-house or from the Google Play Store)

MAM-only use cases with MobileIron AppStation

The following MAM-only use cases are supported with an AppStation deployment:

- You have employees or seasonal workers who need your relevant apps on their personal devices, but your privacy or legal requirements do not allow device management.
- You have contractors who need your relevant apps, but their devices are managed. The device may be managed by MobileIron Core or another MDM provider.

NOTE: A device that is managed with MobileIron Go cannot also at the same time be managed for MAM-only with MobileIron AppStation.

NOTE: If you already have a MAM-only deployment using MobileIron Go, you can continue with the deployment. However, MobileIron recommends using MobileIron AppStation for new MAM-only deployments. AppStation supports additional use cases that are not supported with MAM-only using MobileIron Go.



Android AppConnect app behavior with MobileIron AppStation

If a device has both Mobile@Work for device management (MDM), as well as MobileIron AppStation for MAM-only, AppConnect wrapped apps and AppStation wrapped apps continue to work as expected since the apps are wrapped with different flavors of Secure Apps Manager.

The AppConnect apps that work with MobileIron AppStation are wrapped with Secure Apps Manager for AppStation. The AppConnect apps that work with Mobile@Work are wrapped with the regular Secure Apps Manager. Therefore, Apps that are wrapped with Secure Apps Manager for AppStation work with AppStation only and apps that are wrapped with the regular Secure Apps Manager continue to work with Mobile@Work.

When wrapping an app in the AppConnect Wrapping Portal, you have the option to wrap it with Secure Apps Manager for AppStation. Apps that are wrapped with the AppStation option have the following package name:

- `appstation.<your app package name>`

For information about wrapping AppConnect apps, see the *MobileIron AppConnect for Android App Developers Guide*.

MAM-only deployment diagrams

The following provides a visual representation for a MAM-only deployment with MobileIron AppStation:

- [MAM-only with AppStation](#)
- [MAM-only with AppStation and MDM with other platform](#)

MAM-only with AppStation

The following shows a MAM-only with AppStation deployment. MobileIron Cloud is set up for MAM-only. The device is not managed, only apps on the device deployed through AppStation are managed.



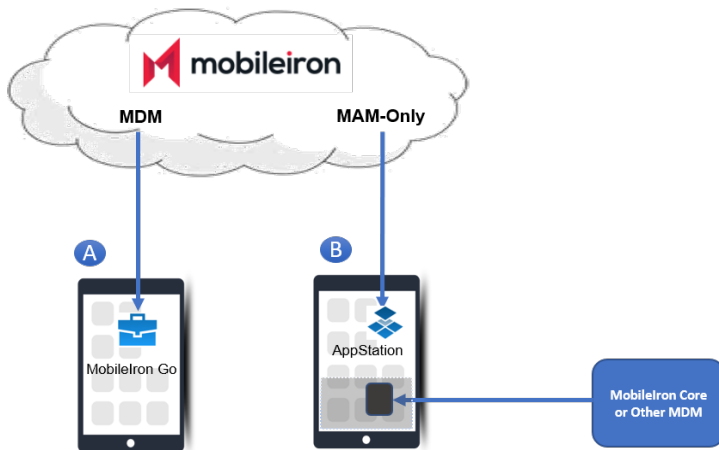
FIGURE 1. MAM-ONLY DEPLOYMENT



MAM-only with AppStation and MDM with other platform

The following shows a device on which apps are managed by MobileIron Cloud and AppStation, while the device is also managed with another MDM platform.

FIGURE 2. MAM-ONLY AND OTHER MDM ON A DEVICE



- Device A is managed (MDM) by MobileIron Cloud.
- Device B is not managed by your tenant of MobileIron Cloud. MobileIron AppStation is used for MAM-only. The device can also be managed by MobileIron Core or another MDM provider .

MobileIron AppStation configuration

Configurations for MAM-only with MobileIron AppStation are created in MobileIron Cloud. MobileIron AppStation receives the configurations when it registers with MobileIron Cloud.

Use the **MAM Only** configuration in MobileIron Cloud to set up AppStation. AppStation. For an overview of the configurations needed to set up AppStation see [AppStation configuration steps overview](#).

- [Supported configurations for managing apps through AppStation](#)
- [Administrator actions supported for AppStation](#)

Supported configurations for managing apps through AppStation

The following configurations in Cloud are supported for managing apps through AppStation:

- Certificate
- Identity Certificate
- AppConnect configurations and policies
- MobileIron Threat Defense
- Privacy
- VPN
- Wifi

IMPORTANT: MDM-related configurations other than the ones listed are not supported for MAM-only devices.

For information on setting up the configurations, see the [MobileIron Cloud Administrator Guide](#).

Administrator actions supported for AppStation

The following administrator actions through AppStation are supported:

- Force check in
- Retire
- Send messages



Setting up MobileIron AppStation

The following describe the setup required for MobileIron AppStation for Android:

- [AppStation configuration steps overview](#)
- [Verify the setup for AppStation](#)

AppStation configuration steps overview

The configurations for AppStation are done in MobileIron Cloud. The following provides an overview of the configuration steps for deploying AppStation and pointers to the relevant content in the *MobileIron Cloud Administrator Guide*:

1. Create a user group to distribute AppStation and manually add users to the group.
See "Creating a manually managed user group" in the [MobileIron Cloud Administrator Guide](#).
2. Create a dynamically managed device group with the rule "user group," which is equal to the user group created for AppStation.
See "Adding a device group" in the [MobileIron Cloud Administrator Guide](#).
NOTE: If devices had been previously enrolled for MDM in a Cloud tenant, users will not be able to register with the same Cloud tenant using AppStation. To use AppStation, delete the devices from the Cloud tenant, then register with the same Cloud tenant using AppStation.
3. Disable the Android enterprise configurations and change the distribution of the configurations to **No Devices**. The Android enterprise configurations are:
 - Android enterprise: Work Profile (Android for Work)
 - Android enterprise: Work Managed Device (Android for Work)
 - Android enterprise: Managed Device with Work Profile
4. Create a **MAM Only** configuration for AppStation and assign it to the dynamically managed device group created for AppStation.
See [Configuring MAM-only in MobileIron Cloud](#).
5. Add apps for distribution and assign the apps for distribution to the dynamically managed device group created for AppStation.
See [Add apps for distribution](#).
6. Notify users to download and register AppStation.
If **Always require client registration** is enabled in **Users > User Settings > Device Registration Setting** in MobileIron Cloud, users automatically get emails for registering their device via AppStation. Device users download AppStation to their device directly from the Google Play Store.
See [What users see in MobileIron AppStation for Android](#) for information about how device users can register their devices to your MobileIron Cloud instance and install apps from AppStation.

Configuring MAM-only in MobileIron Cloud

The **MAM Only** configuration in MobileIron Cloud allows you set up MAM-only for mobile devices.



Before you begin

1. Create a user group to distribute AppStation and manually add users to the group.
See "Creating a manually managed user group" in the [MobileIron Cloud Administrator Guide](#).
2. Create a dynamically managed device group with the rule "user group," which equals to the user group created for AppStation.

See "Adding a device group" in the [MobileIron Cloud Administrator Guide](#)

NOTE: If devices had been previously enrolled for MDM in a Cloud tenant, users will not be able to register with the same Cloud tenant using AppStation. To use AppStation, delete the devices from the Cloud tenant, then register with the same Cloud tenant using AppStation.

3. Disable the Android enterprise configurations and change the distribution of the configurations to No Devices. The Android enterprise configurations are:
 - Android enterprise: Work Profile (Android for Work)
 - Android enterprise: Work Managed Device (Android for Work)
 - Android enterprise: Managed Device with Work Profile

Procedure

1. In MobileIron Cloud, go to **Configuration > +Add**.
2. Enter **MAM only** in the search box, then select the **MAM Only** configuration from the search results.
3. Enter a name for the configuration.
4. Click **Next**.
5. Select a distribution option for AppStation.
6. Click **Done**.

Related topics

[MobileIron AppStation configuration](#)

Add apps for distribution

You distribute apps to MAM-only devices through MobileIron Cloud. Do the following in MobileIron Cloud:

1. Add the apps that you want to distribute to MAM-only devices.
2. Assign the apps for distribution to the dynamically managed devices group created for AppStation.

NOTE: AppConnect apps require additional AppConnect-related configurations as well.

See the [MobileIron Cloud Administrator Guide](#) for adding and configuring apps in MobileIron Cloud. Some relevant sections are: "Adding an app from a public store," "Adding an In-house app," "Configuring AppConnect Devices," "Configuring AppConnect Apps."

IMPORTANT: Ensure that AppConnect apps are wrapped with Secure Apps Manager for AppStation. AppConnect apps wrapped with the regular Secure Apps Manager will not work with AppStation. AppConnect apps wrapped with the regular Secure Apps Manager can be pushed to AppStation. For information about wrapping AppConnect apps for Android, see the [MobileIron AppConnect for Android App Developers Guide](#).



Verify the setup for AppStation

In MobileIron Cloud, go to **Devices > Device Groups**. Select the device group for AppStation to verify the configurations assigned to the group.



What users see in MobileIron AppStation for Android

The following provide information about the user experience with MobileIron AppStation:

- [Download and install AppStation for Android](#)
- [Register with MobileIron Cloud](#)
- [Launcher and Catalog](#)

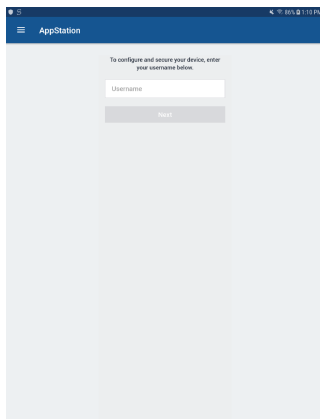
Download and install AppStation for Android

MobileIron AppStation is available in the Google Play Store. Search for MobileIron AppStation and follow the prompts to install the app on your device.

Register with MobileIron Cloud

When you first launch MobileIron AppStation, you are prompted to enter your username and password. Enter your enterprise username and password to register with MobileIron Cloud. When you register with MobileIron Cloud the Catalog with the list of available apps becomes available on your device.

FIGURE 3. REGISTER



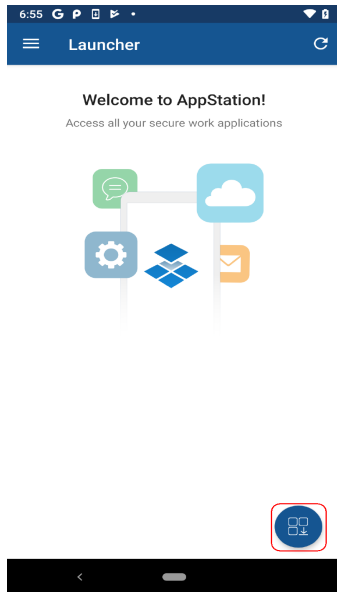
Launcher and Catalog

When you first launch AppStation, you see the welcome screen followed by prompts that take you through device setup and installing the needed configurations. You are then prompted to install apps that are available to you.



Follow the prompts to install the apps. After the apps are installed the Launcher becomes available. The Launcher displays the apps that are installed. If no apps are available to install, an empty **Launcher** screen is shown.

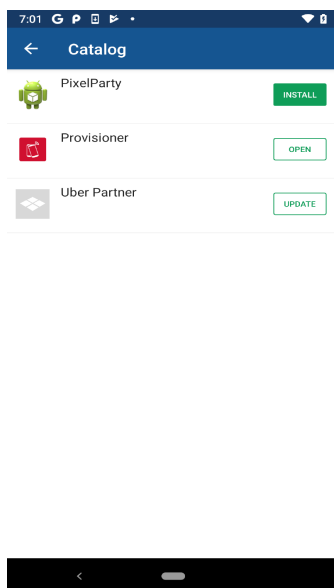
FIGURE 4. LAUNCHER WITHOUT ANY APPS



Tap the catalog icon to see the apps available to you. The following indicate whether an app is installed or not:

- **Install:** Indicates that the app is not yet installed.
- **Open:** Indicates that the app is installed.
- **Update:** Indicates that updates are available for the installed app.

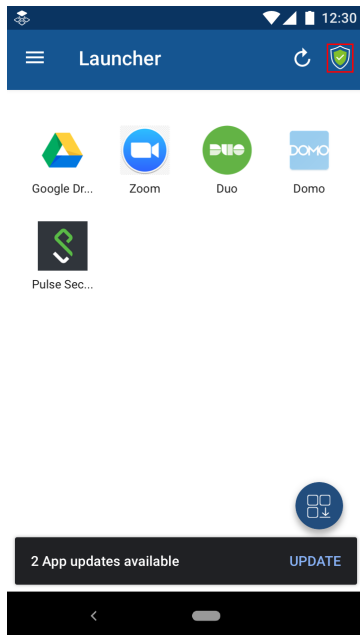
FIGURE 5. CATALOG WITH AVAILABLE APPS



To install an app, tap the app and follow the prompts. If the app is a public app, AppStation switches to the Google Play Store to install the app. After installing the app, the toggle changes from **Install** to **Open**. Click **Open** to launch the app.

If Mobile Threat Defense (MTD) is configured, the MTD icon is seen in **Launcher** and **Catalog**. Tapping the MTD icon, takes you to **Settings** where you have option to see the MTD status.

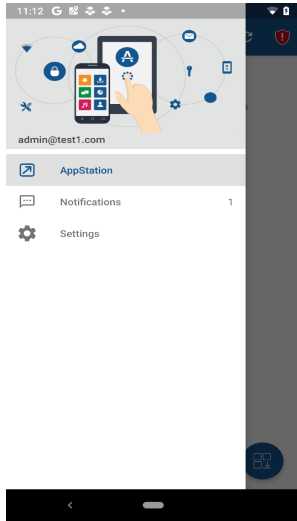
FIGURE 6. MTD ICON



Settings

Swiping from the left reveals additional options. These options provide more information about the app, device, and threat defense.

FIGURE 7. ADDITIONAL MENU OPTIONS



Settings provides additional information about the app and access to app logs. If Mobile Threat Defense (MTD) is configured and applied to the AppStation device group, MTD diagnostics is also available.

FIGURE 8. SETTINGS > ABOUT > DEVICE DETAILS

