MobileIron AppStation 72 for Android Guide for Administrators

September 8, 2020

For complete product documentation see:
MobileIron AppStation Product Documentation Home Page

Contents

New features and enhancements

This guide documents the following new features and enhancements:

- **Rebranding**: MobileIron has updated the AppStation for Android icon and user interface color scheme. For more information, see What users see in MobileIron AppStation for Android.
- **Additional threat defense information**: If you have a MobileIron Threat Defense (MTD) deployment, users see additional threat defense information when they tap on the MTD icon in AppStation. Users see the device and network-specific threat details and descriptions on how to fix the threats.
  For information on the MTD user experience on AppStation, see Mobile Threat Defense.
- **Support for MobileIron Go and MobileIron AppStation on the same device**: The support allows for the MAM-only use case where you have contractors whose devices are already managed by another instance of MobileIron Cloud, however, you need to deploy required apps from your instance of MobileIron Cloud to the device.
  The supported MAM-only use cases are described in MAM-only use cases with MobileIron AppStation and MobileIron Go and MobileIron AppStation interaction.

About MobileIron AppStation

The following provide an overview of MobileIron AppStation for Android:

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 Cloud, MobileIron Core or another MDM provider.

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.

MobileIron Go and MobileIron AppStation interaction

The following behavior is seen when both MobileIron Go and AppStation are deployed to a device:

- All MobileIron Threat Defense actions are applied to the device irrespective of the tenant on which the actions are configured. For any particular setting, the stricter configuration takes precedence.
- In cases where the apps required from the MAM Cloud tenant (contractor) are blacklisted by the MDM Cloud tenant, the MDM Cloud administrator has to allow the apps for the contractor device registered to the MAM Cloud tenant.
- For anti-phishing policies, the last client, MobileIron Go or AppStation, used on the device becomes the default browser.
- The MDM Cloud tenant administrator can take actions, such as Wipe, which affect any app installed on the device, including AppStation.

For the configurations, apps, and actions supported for MobileIron AppStation, see MobileIron AppStation configuration.

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*.

Android AppStation and Android enterprise

If a MobileIron Cloud tenant supports both Work Profile for device management (MDM), as well as MobileIron AppStation for MAM-only, the Work Profile policies and configurations take priority.

Therefore, MobileIron recommends creating separate user groups for Android enterprise and for MAM-only. Do the following:

- Apply the MAM-only devices to the MAM-only user group.
- Do not apply Android enterprise devices, polices, and configurations, to the MAM-only user group. 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/Work Profile on Company Owned device

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

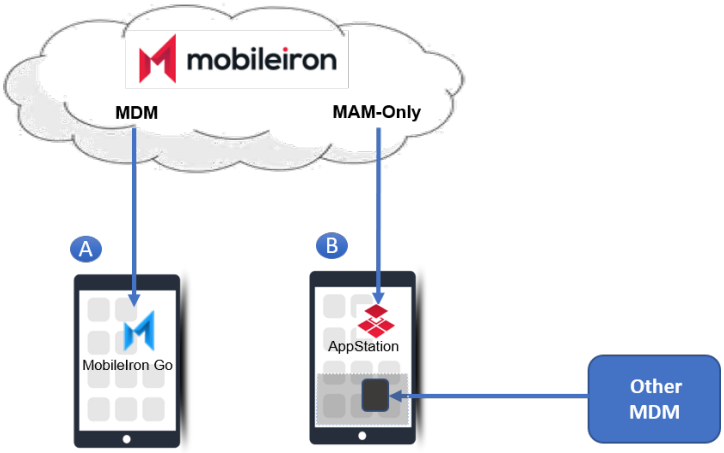
The following shows a MAM-only with AppStation deployment. MobileIron Cloud is set up for MAM-only. The device is not managed, only apps on the device deployed through AppStation are managed.

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, another MobileIron Cloud tenant, 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. 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
- AppConnect app
- 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 created 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 Android AppStation and Android enterprise for MobileIron AppStation behavior on Android enterprise devices.
   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: Devices previously enrolled for MDM in a Cloud tenant cannot be re-registered 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. 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 .
4. Add apps for distribution and assign the apps for distribution to the dynamically managed device group created for AppStation.
   See Add apps for distribution.
5. 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

- MobileIron AppStation configuration
- AppStation configuration steps overview

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**.

Next steps

- Add apps for distribution

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

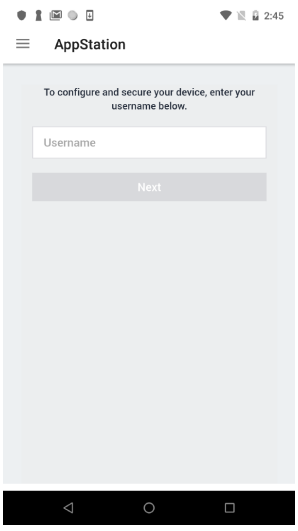
Download and install AppStation for Android

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.

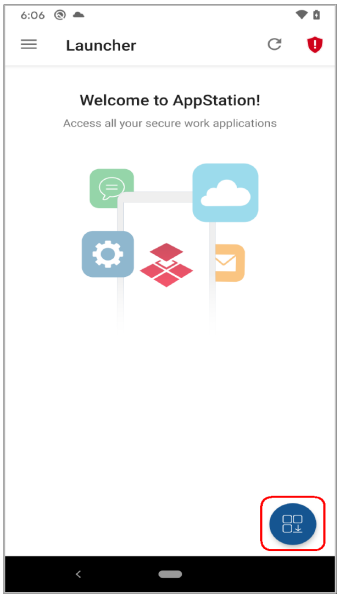
FIGURE 3. REGISTER



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 installed, an empty **Launcher** screen is shown.

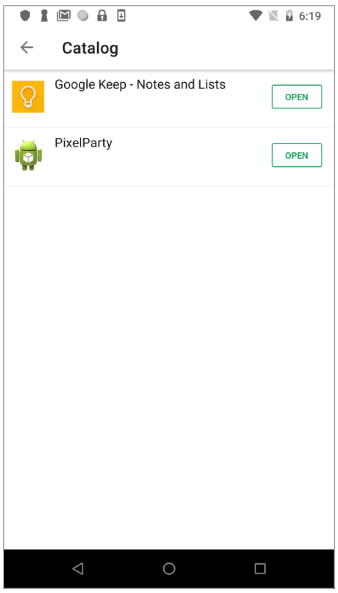
FIGURE 4. LAUNCHER WITHOUT ANY APPS



Tap the catalog icon on the bottom right corner 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

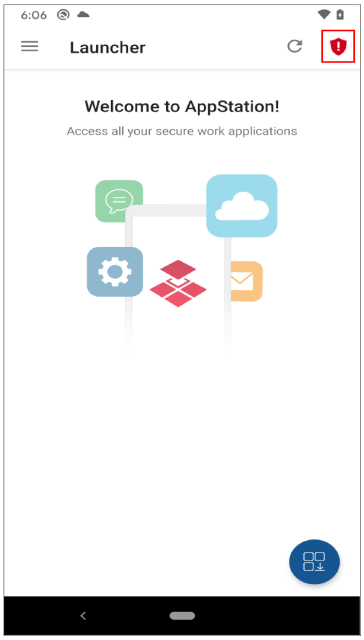


To install an app, tap the app and follow the prompts. If the app is a public app, AppStation switches to the Google Play Store to install the app. After installing the app, the toggle changes from **Install** to **Open**. Click **Open** to launch the app.

Mobile Threat Defense

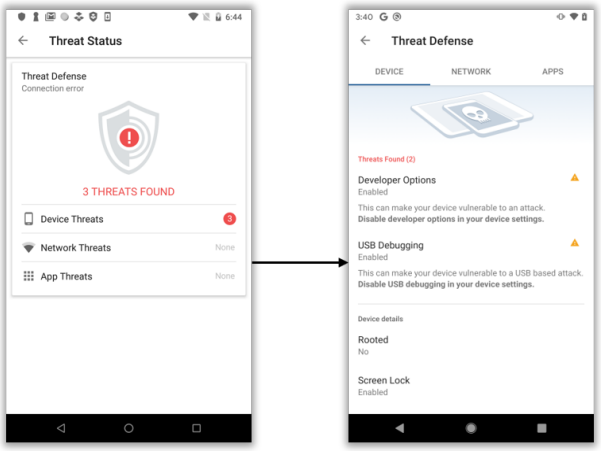
If Mobile Threat Defense (MTD) is configured, the MTD icon is seen in the top right corner of the screen in **Launcher** and **Catalog**. Tapping the MTD icon, takes you to **Threat Status** where you can see a detailed view of the threats specific to the device, network, and apps.

FIGURE 6. MTD ICON



Tap on one of the options, **Device Threats**, **Network Threats**, or **App Threats**, to see details for each threat and how to resolve the threat.

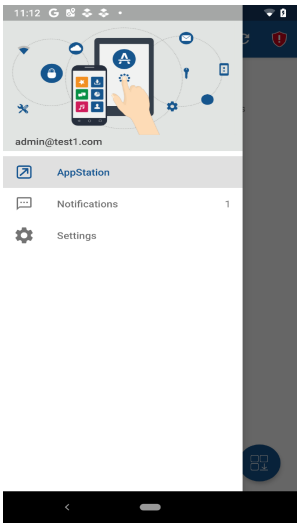
FIGURE 7. THREAT DETAILS



Settings

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

FIGURE 8. ADDITIONAL MENU OPTIONS



Settings provides additional information about the app and access to app logs.

FIGURE 9. SETTINGS > ABOUT > DEVICE DETAILS