Mobile Device Management for Everbridge Mobile App

Mobile Device Management-usually abbreviated MDM-allows mobile devices to be configured and controlled from a central location. Typically, it is used by enterprise-level organizations to impose minimum security standards, provide organization recommended apps, assist users in configuration, and protect company data on both organization-provided and BYOD devices.

The Everbridge Mobile App (hereafter, "EMA") includes support for configuration via MDM systems that support the AppConfig standard. This includes some custom configuration ability for EMA itself as well as functionality provided natively by the MDM systems.

Each MDM system works differently, and details can be found in the documentation of your MDM system. But this document provides some examples of MDM capabilities, as implemented by a sample MDM system (MobileIron Cloud), and lists the configuration settings currently available for EMA.

Note that MDM support is an ongoing effort, and additional configuration settings will likely become available over time.

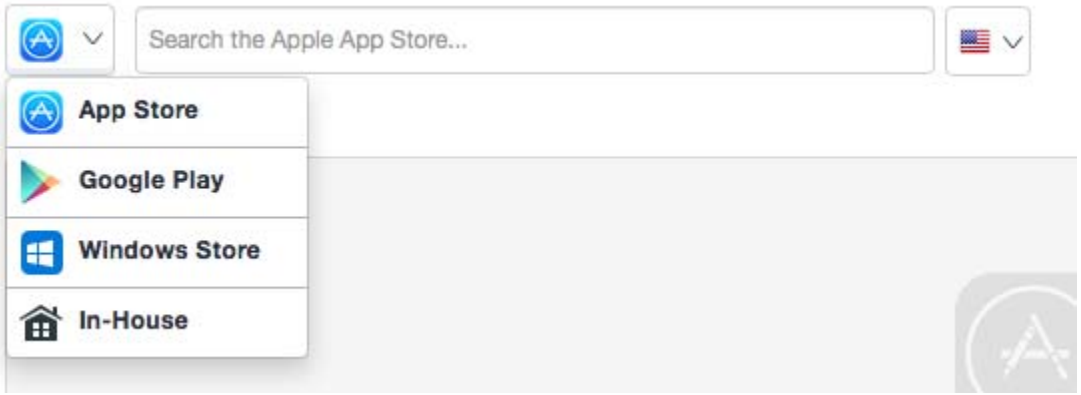
Internal App Store Distribution

MDM providers offer an "Internal App Store" mechanism which offers a selection of organization-curated apps that are either automatically or optionally installed on the users's device. How this is done varies between MDM providers.

On MobileIron Cloud, you access these configurations by:

- Select the "Apps" tab along the MobileIron Cloud top navigation bar.
- If necessary, select the "App Catalog" tab in the sub-navigation bar.
- Click the "+ Add" button

At this point, you can choose from a variety of methods to load your application, using the pull-down next to the Search box.



For EMA, select the "App Store" (for the iOS version) and/or Google Play (for the Android version), and type "Everbridge" into the search box. Once it's located, select it, and several screens of options will appear. On the final page ("Configure" on the left, "App Configurations" on the top), you can specify things like:

- Whether or not to force the app onto the user's device or let them choose it.
- Whether to convert unmanaged versions on the app to managed ones.
- Whether or not data from the app can be backed up to iTunes or iCloud.
- Application specific configurations (see "Set Custom EMA configuration Settings, below")
- Per-App VPN (protected networking).

NOTE: "AppConnect" is a proprietary MobileIron system, which extends certain apps with additional MobileIron-specific functionality. EMA is not an "AppConnect" managed app, so the following two AppConnect features will not function:

- AppConnect custom configurations will not apply (use the iOS Managed App Configuration option instead.
- AppTunnel (use the "Per App VPN" instead).

Once you have completed the steps and click "Done," the app will be made available to the devices of the users you specified. Note that this can take some time; it will not happen at all until networking is available on the device, and application downloads can take considerable time.

Remotely Wipe or Un-manage a Device

Removing a Single App

To remove a single app (such as EMA) from a device, set its distribution to "no one," or remove the device(s) from the current distribution group.

Return a Device to an Un-managed State/Remove all Managed Apps

You can also eliminate all management from a device: this will remove all managed applications and data. As usual, the method for this varies between MDM providers, as does the name. Some providers will call this "Unmanage," others will call it "Retire."

On MobileIron Cloud, you access these configurations by:

- Select the "Devices" tab along the MobileIron Cloud top navigation bar.
- If necessary, select the "Devices" tab in the sub-navigation bar as well.
- Check the devices you want to unmanage.
- From the "Actions" pulldown, select "Retire."

You will be asked to confirm your actions. After retirement, the device will operate as an unmanaged device and will no longer the organizations settings, security, or policies. Retiring a device can take a few minutes, and the device may or may not reboot to complete the retirement.

Wipe a Device Completely

Finally, you can "wipe" a device, deleting all applications and data on the device (including the user's own, unmanaged apps and data), and returning the device to its factory state. This is typically only done to protect data on a lost or stolen device, for organization-owned devices that will be re-purposed to a new employee, or when a device gets into an "unusable" state for whatever reasons.

On MobileIron Cloud, you access these configurations by:

- Select the "Devices" tab along the MobileIron Cloud top navigation bar.
- If necessary, select the "Devices" tab in the sub-navigation bar as well.
- Check the devices you wish to wipe.
- From the "Actions" pulldown, select "Wipe."

You will be asked to confirm your actions, since this is completely destructive to the data and apps on the device. One you confirm, the device will be erased, usually within a minute if it has network coverage. The device does not need to be unlocked for this to happen.

After wiping, the device will be restored to its out-of-the-box state. For devices that are still functional (that is, they have not been marked as stolen with their network), they may then be reconfigured as with any new device.

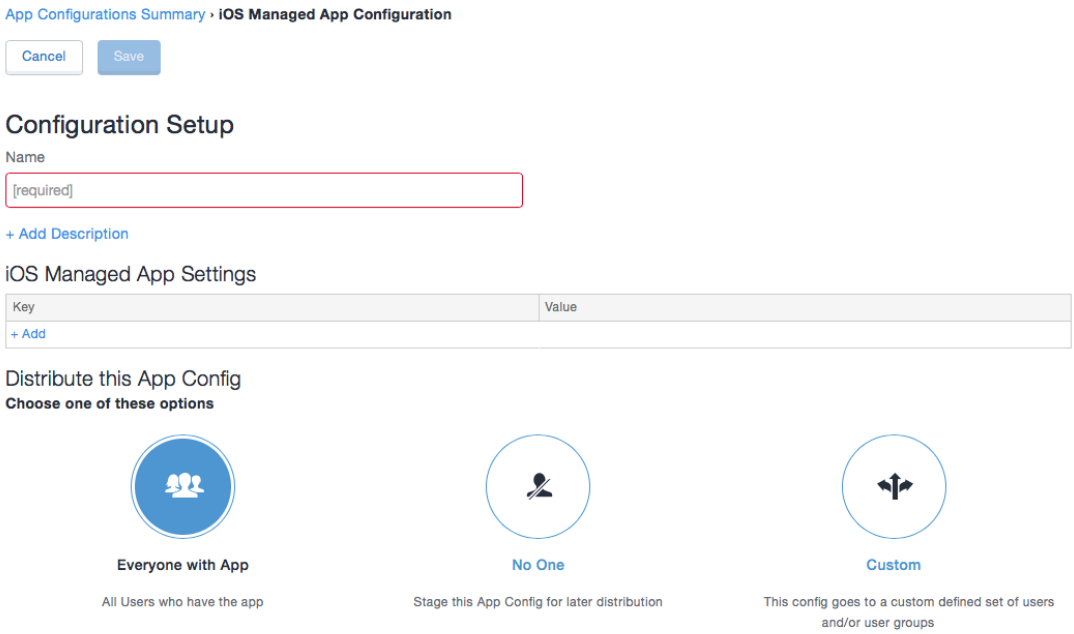
Set Custom EMA Configuration Settings

EMA supports sending application-specific configuration settings via the AppConfig standard. How this is done varies between MDM providers; it will typically be located in a "configurations" tab or button associated with the specific app.

On MobileIron Cloud, you access these configurations by:

- Select the "Apps" tab along the MobileIron Cloud top navigation bar.
- If necessary, select the "App Catalog" tab in the sub-navigation bar.
- Click on the "Everbridge" name (it will list as a hyperlink) in the App Catalog list.
- From the Everbridge application summary page, select the "App Configurations" tab.
- Select "iOS Managed App Configuration" (not "AppConnect Custom Configuration")

From this summary page, you can create, modify, delete, and activate as many sets of configurations as you like. To create a new one, click the "Add+" button.



Name the configuration whatever you like. On the bottom, you can choose which of your users will have the configuration applied; you can select "No One" if you want to try out configuration building without affecting your users (then apply it later if you desire).

The core of this screen, of course, is the configurations themselves. These are combinations of "keys" (the name for a specific setting) and "values" (what you want to set that setting to). You can specify as many of these as you like, but only settings whose "key" and "value" is supported by the application will take effect. Keys, in particular, must exactly match a setting name, including punctuation and case. That is, "EMA_allowcopy" is not the same as "EMA_AllowCopy". The specific key/value pairs supported by an application will be documented by the application provider; the supported pairs for EMA are listed below.

Everbridge Mobile App (EMA) Configuration Settings

The configuration settings currently provided for EMA are listed below. Note that this list will increase over time, so check for newer versions of this text.

All EMA settings begin with EMA_ ("EMA" and an underscore), and must be specified exactly, including upper/lowercase. Any setting not included in a configuration will have a specified default (unless provided by another configuration sent to the same device).

The available configurations are listed starting on the next page. Once a configuration set is chosen and sent from your MDM provider, the configuration should appear on devices in a very short period of time (no more than a few minutes), assuming the devices have network connectivity. Devices in areas without wireless access--or with that access disabled--will be configured when they next return to a wireless network.

Most configurations will take effect immediately upon the device receiving them; the application does not need to be killed or relaunched.

Name	Values	Default
EMA_AllowCopy	"true" or "false"	True

If set to false, the copy (and cut) command will be disabled in several locations in the application. Currently, this disallows the copying of notification message content; it will be expanded to disable copying in more locations over the next few versions of EMA. If you have a specific request for a control that should honor this setting (i.e., that you want to prevent copying), contact your Everbridge support or sales representative.

Note that setting this value to true will not enable additional copy/paste operations. For privacy reasons, many parts of EMA do not allow copy and/or paste, regardless of the value of this configuration.

This setting is used only on iOS. On Android, use your MDM provider's built-in policies to disable copy and paste globally.

Name	Values	Default
EMA_AllowPaste	"true" or "false"	True

If set to false, the paste command will be disabled in many locations in the application; it will be expanded to disable copying in more locations over the next few versions of EMA. If you have a specific request for a control that should honor this setting, contact your Everbridge support or sales representative.

Note that setting this value to true will not enable additional copy/paste operations. For privacy reasons, many parts of EMA do not allow copy and/or paste, regardless of the value of this configuration.

This setting is used only on iOS. On Android, use your MDM provider's built-in policies to disable copy and paste globally.

Name	Values	Default
EMA_AllowNotification Attachments	"true" or "false"	True

If set to false, notification attachments will not be available to the user in the messages list.

Name	Values	Default
EMA_SSO_Keyphrase	Any string	-none-

If provided, the "Enter Keyphrase" field in the SSO login dialog will be pre-populated with the specified value.