MDM Support

> (i) Support for Mobile Device Management (MDM) app configurations is available for the following FileCloud versions:
>
> - iOS 18.2.10
> - Android 18.2.1
>
> FileCloud support complies with the AppConfig Community Standards.

Mobile device management (MDM) is an industry term for the administration of mobile devices, such as:

- smartphones
- tablet computers
- laptops
- desktop computers

MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices.

Mobile devices can also be managed through:

- Enterprise Mobility Management (EMM)
- Unified Endpoint Management (UEM)

MDM is typically a deployment of a combination of the following:

- on-device applications and configurations
- corporate policies and certificates
- backend infrastructure

The reason for using MDM is to simplify and enhance the IT management of end user devices.

In modern corporate IT environments, the sheer number and diversity of managed devices (and user behavior) has motivated MDM solutions that allow the management of devices and users in a consistent and scalable way.

The overall role of MDM is to increase device supportability, security, and corporate functionality while maintaining some user flexibility.

How Do I Add FileCloud to My MDM?

> (!) Remember that MDM settings are case sensitive.
>
> When typing in configuration settings such as account and SSO information, make sure you are using lowercase letters.

When you enroll your device, you are issued an MDM certificate. This certificate is used to communicate with your MDM service.

Since there are many MDM providers and ways to enroll, please check your MDM documentation for instructions on how to enroll your device.

You must enroll your device! It doesn't matter to FileCloud if it is a personal or company-owned device.

- Personally-owned devices - in this scenario the MDM only manages some apps and those apps' configurations
- Company-owned devices - in this scenario the MDM manages everything, including the ability to remotely wipe clean all content from the device
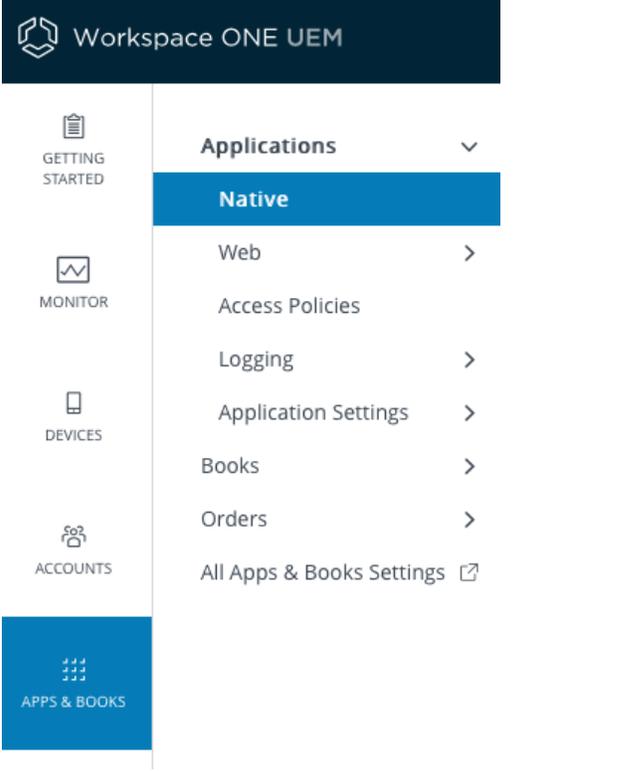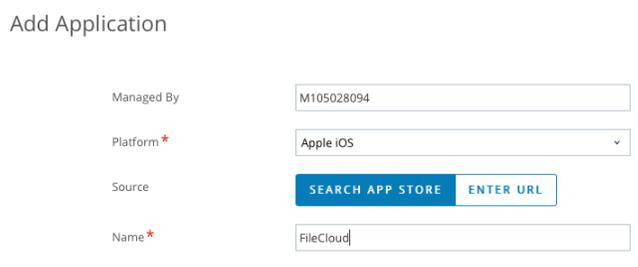
Since there are many MDM providers and ways to add applications, please check your MDM documentation for instructions on:

- how to add the FileCloud to your MDM software.

In general, the steps for adding FileCloud to your MDM will include:

1. Open your MDM software.
2. Search for the FileCloud app.
3. Choose to add the FileCloud App.

For example, in VMware's AirWatch MDM:

1. Open your MDM software.	
2. Search for the FileCloud app.	

3. Add the FileCloud App.	Apps & Books > Applications List View Internal **Public** Purchased Filters » ⊕ ADD APPLICATION

Once added you will need to complete the following steps:
 	
- Assign the FileCloud App
- Configure the FileCloud App
 	
These steps are discussed below in Steps 3 and 4.
	Add Application
	
	Managed By M105028094
	
	Platform * ✓ Select
	  Apple iOS
	  Android
	  Windows Phone
	  Windows Desktop
	
	Source
	
	Name

Workspace ONE® is powered by VMware AirWatch, which is the unified
digital workspace platform that simplifies and secures app
access and IT management.

Assignments allow you to edit the settings of an application to exclude or include specific devices, use Groups, profiles, and compliance policies.

- You can edit Assignment settings when adding the app
- To change or edit the settings, navigate to the app in your MDM software and find the Assignments section

In your MDM software, navigate to the FileCloud app	Apps & Books > Applications **FileCloud** Public | ✔ Status: Active | Details Devices **Assignment** Assignments Exclusions EDIT ASSIGN MORE ∨

Add an assignment OR Edit an existing one	**FileCloud - Update Assignment** **Assignments** Exclusions Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies ⊕ ADD ASSIGNMENT ✎ EDIT ✖ DELETE ⬆ MOVE UP ⬇ MOVE DOWN Name Priority App Delivery Method Managed Access 🔘 All Devices 0 Auto ✓ Enabled
For FileCloud, use the following assignments: *Managed Access* = Enabled *Remove On Install* = Disabled *Prevent Application Backup* = Disabled *Make App MDM Managed if User Installed* = Enabled *App Tunneling* = Disabled *Application Configuration* = Enabled 💡 Once you set *Application Configuration* to Enabled, you can configure FileCloud. To configure FileCloud, use the steps below in 4. Configure the FileCloud App	FileCloud - Add Assignment **Would you like to enable Data Loss Prevention (DLP)?** DLP policies provide controlled exchange of data between managed and unmanaged application To prevent data loss on this application, make it ""Managed Access"" and create ""Restriction"" Managed Access ENABLED DISABLED ⓘ Remove On Unenroll ENABLED DISABLED ⓘ Prevent Application Backup ENABLED DISABLED ⓘ Make App MDM Managed if User Installed ENABLED DISABLED ⓘ App Tunneling ENABLED DISABLED ⓘ Application Configuration ENABLED DISABLED ⓘ

Once you set *Application Configuration* to Enabled, you can configure FileCloud.

To configure FileCloud, you can do one of the following:

- Upload the XML configuration file. This populates the configuration fields for an administrator to configure.
- Manually enter the XML. If your MDM doesn't recognize any of the provided XML spec files, you can enter these values manually.

> ⊘ You can delete any configuration fields that do not apply to your organization.
>
> Sensitive information such as password are best removed from the configuration. When not present users will be prompted to input their password manually on the device once.

Upload a configuration file:

- FileCloud MDM specfile.xml
- FileCloud MDM specfile simple.xml

Values you can enter manually:

XML Tag	Type	Description
account	String	Enter the name of the account you want to setup
sso	Boolean	Set this value to true to create an SSO account
password	String	Password of the account to setup (for non-SSO accounts)
server	String	Server address / URL of your FileCloud server (MUST start with http:// or https://)
enforce_authentication	String	Either **code**, **sso** or **password**
enforce_lock	Boolean	Set to true to prevent login if an app-specific passcode has not been set
disable_edit	Boolean	Set to true to disable operations such as rename, copy, upload (if applicable)
disable_download	Boolean	Set to true to disable prevent file and folder downloads

disable_openwith	Boolean	Set to true to disable "Open with…"
disable_share	Boolean	Set to true to disable "Share" operation
disable_favs	Boolean	Set to true to disable "Add to Star" operation