VERSION 1 • FEBRUARY 2023

UNLEASH THE POWER OF SECURE AND CUSTOMIZABLE MOBILE APP

VMWARE WORKSPACE ONE UEM

Executive Summary

This paper describes the integration of FileOrbis with VMware Workspace ONE UEM.

FileOrbis is a secure content management and enterprise file sharing solution integrated with various security technologies.VMware Workspace ONE UEM is a solution for modern, over-the-air management of desktops, mobile, rugged, wearables, and IoT. It enables you to simply and securely deliver and manage any app on any device, anywhere.

The integration of FileOrbis mobile app with Workspace ONE UEM enhances security and ease of management for IT administrators, by utilizing the configuration and restrictions provided by the UEM solution.

1. Integration
1.1 About Workspace ONE UEM

VMware Workspace ONE is an industry-leading cloud platform for modern management and unified endpoint management (UEM) that gives IT teams control over the highly diversified device deployments found in so many organizations today while ensuring enterprise security outside the hardened perimeter. VMware Workspace ONE UEM provides device lifecycle management across all platforms in a single comprehensive solution that empowers IT to;

- Automate the onboarding process over the air
- Intelligently manage every device on every platform
- Flexibly support all use cases – BYOD, corporate-owned, frontline, or purpose-built
- Easily manage apps and provide a consistently positive self-service employee experience
- Make data-driven decisions and automate important repetitive processes
- Secure devices, apps, and data at rest and in transit

1.2 About FileOrbis

FileOrbis is an on-premise/on-cloud content management system equipped with unique operation and control features allowing you to:

·Enforce security scans and controls on your files

·Conduct content and sensitive data analysis on your files

·Share your files with internal and external users

·Manage permissions and access for your files

·Access your files from everywhere

FileOrbis is a consolidating platform that can manage file servers, user profile folders, user-specific file systems, and different types of file systems. With FileOrbis, you both create an access channel for all your file systems and have an integrated management system.

FileOrbis does not consider content management only through a single perspective such as access, authorization management, file sharing, logging, etc. but helps enterprises at any point related to content management. By integrating with security and content analysis solutions like endpoint protection, sandbox, CDR, DLP, etc. FileOrbis enables you to run all file environments together and/or in series and more effectively.

2. Challange

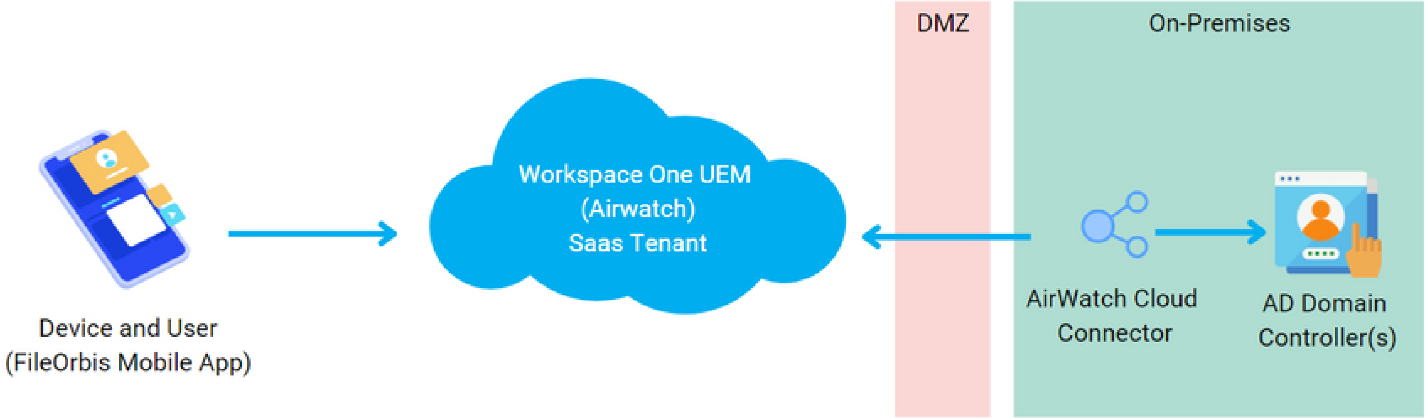
As digitalization continues to drive the growth of data, the need for quick and easy access to this information is paramount. However, with the rise of mobile devices, ensuring security has become a growing concern for organizations. Managing and protecting digital tools is becoming increasingly challenging, making it crucial for enterprises to have secure and seamless access to the data required for their daily operations. The demand for secure and efficient data access continues to grow as the importance of avoiding security vulnerabilities becomes more pressing.

3. Integrated Solution Overview

The integration of VMware Workspace ONE UEM and FileOrbis delivers a user-friendly and secure experience to end users. By combining the content management and security offered by FileOrbis with the application and device management capabilities of VMware Workspace ONE UEM, this integration provides an easy and secure solution for end users while also serving as a safeguard against potential security vulnerabilities caused by employees.

3.1 VMware AirWatch SAML Integration -SSO

The Single-Sign-On (SSO) architecture and federated authentication improve security and simplify user experience by reducing the number of necessary IDs and passwords. . VMware Workspace ONE UEM leverages SAML functionality by adhering to the defined SAML 2.0 standard protocols.



1.Device connects to AirWatch to enroll device, AirWatch server redirects the device to the client-specified identity provider

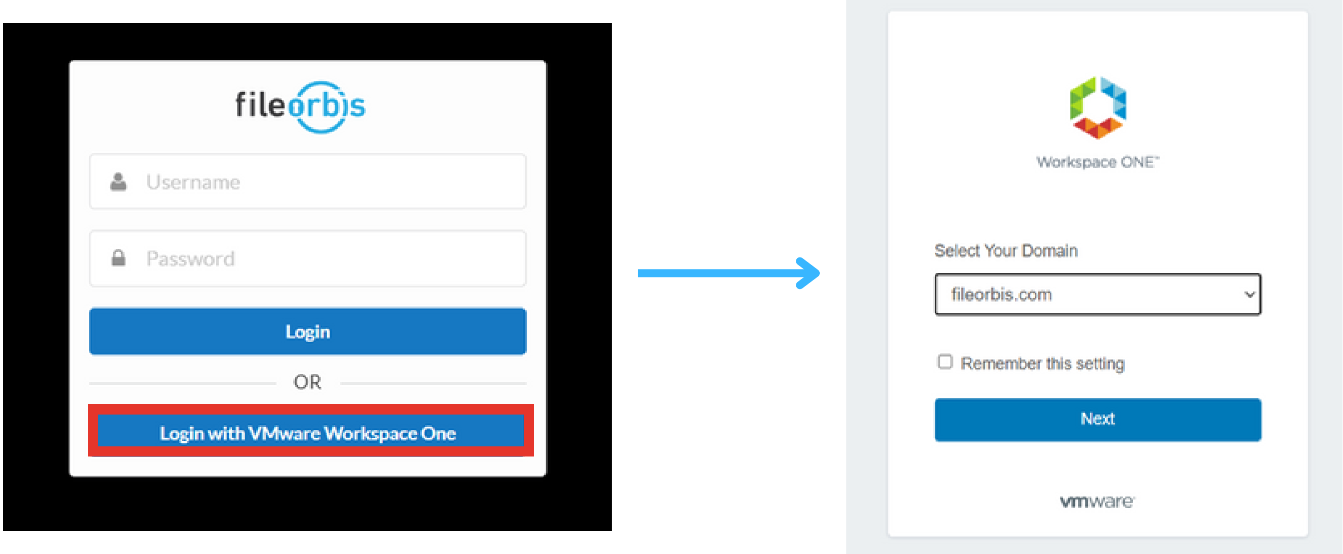
2.Device securely connects via HTTPS to client provided identity provider and user enters the credentials

- Credentials are encrypted during transport directly between the device and SAML endpoint

3. Credentials are validated against Directory Services

4.The identity provider returns a signed SAML response with the authenticated username

5.The device responds back to the AirWatch server and presents the signed SAML message; the user is authenticated.



Select Your Domain
fileorbis.com

Login with VMware Workspaca One

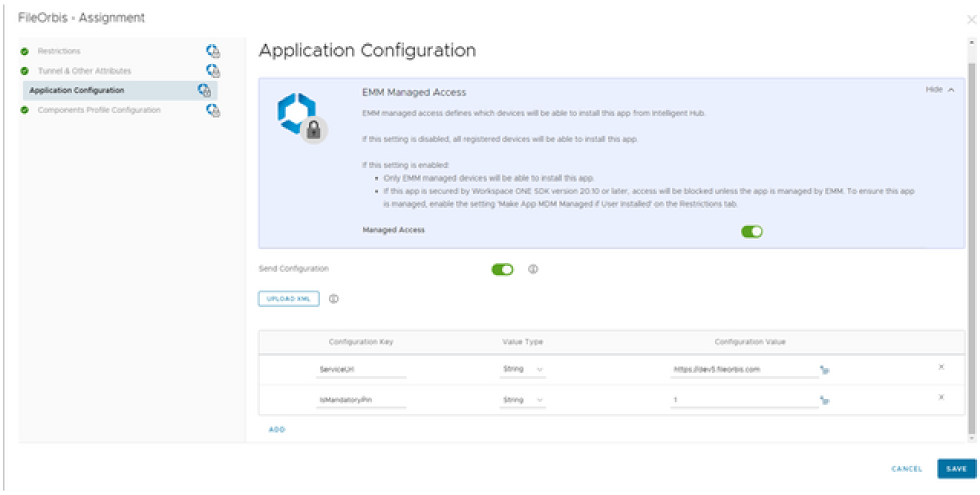
3.2 Management of FileOrbis App Through VMware Application Configuration

By integrating with VMware Application Configuration, the FileOrbis mobile app can be enhanced with user-friendly features and additional security measures for the end user. VMware Application Configuration can be utilized to incorporate selected features from the rule list created and developed by FileOrbis into the application.

The list of rules:

Rules	Definition
Service Url	It is the service URL information to be entered on the login page. If this parameter takes a string value and is set by the MDM administrator, the user will not be able to change the service url textbox on the login screen of the mobile application.
IsMandotoryPin	Adjustment the mandatory for pins
IsMandatoryBiometricAuthentication	Adjustment the mandatory for biometric pins (fingerprint or facial recognition).
DownloadStatus	Indicates the ability to limit download authority through MDM.
CreateLinkStatus	Indicates the ability to create link authority through MDM.
ShareLinkToAnotherAppStatus	Indicates if the ability to share a link with an external application will be restricted through MDM.
PreviewStatus	It includes the restriction to preview a file via mobile application.
ShareStatus	Allows the sharing authority to be restricted via MDM.

Rules	Definition
DisableScreenshot	Indicates the ability to take screenshots through MDM. (Only Android)
PreviewShareIsEnabled	It contains the enable/disable information of the share button via MDM during the preview phase of the downloaded file. (Only IOS)
DisableCamera	It allows to restrict the use of camera for uploading files with FileOrbis application.
UploadPrefix	It is the prefix information to be added in front of the file name while uploading. If this parameter takes a string value and is set by the MDM manager, the prefix determined is added in front of the name of the file uploaded in the mobile application. The user cannot delete or change this prefix.
UploadResolution	It allows the resolution of the uploaded photo to be adjusted via MDM.


FileOrbis - Assignment
Restrictions
Tunnel & Other Attributes
Application Configuration
Components Profile Configuration
Hide
UPLOAD XML
ADD
CANCEL
SAVE

Application Configuration

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

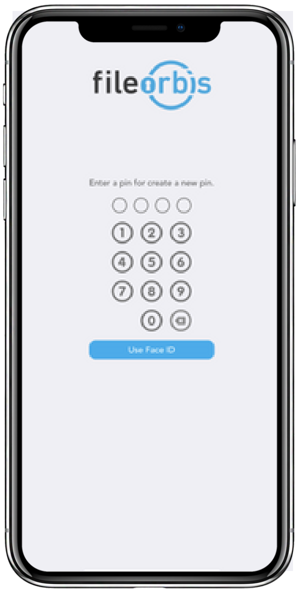
If this setting is enabled:

- Only EMM managed devices will be able to install this app.
- If this app is secured by Workspace ONE SDK version 20.10 or later, access will be blocked unless the app is managed by EMM. To ensure this app is managed, enable the setting 'Make App MDM Managed if User Installed' on the Restrictions tab.

Managed Access ●

Send Configuration ●

Configuration Key	Value Type	Configuration Value
ServiceUrl	String	https://dev5.fileorbis.com
IsMandatoryPin	String	1



Enter a pin for create a new pin.

IsMandotoryPin Rule Adding via VMware

IsMandotoryPin Rule on FileOrbis App

3.3 Management of FileOrbis App Through Airwatch SDK Integration

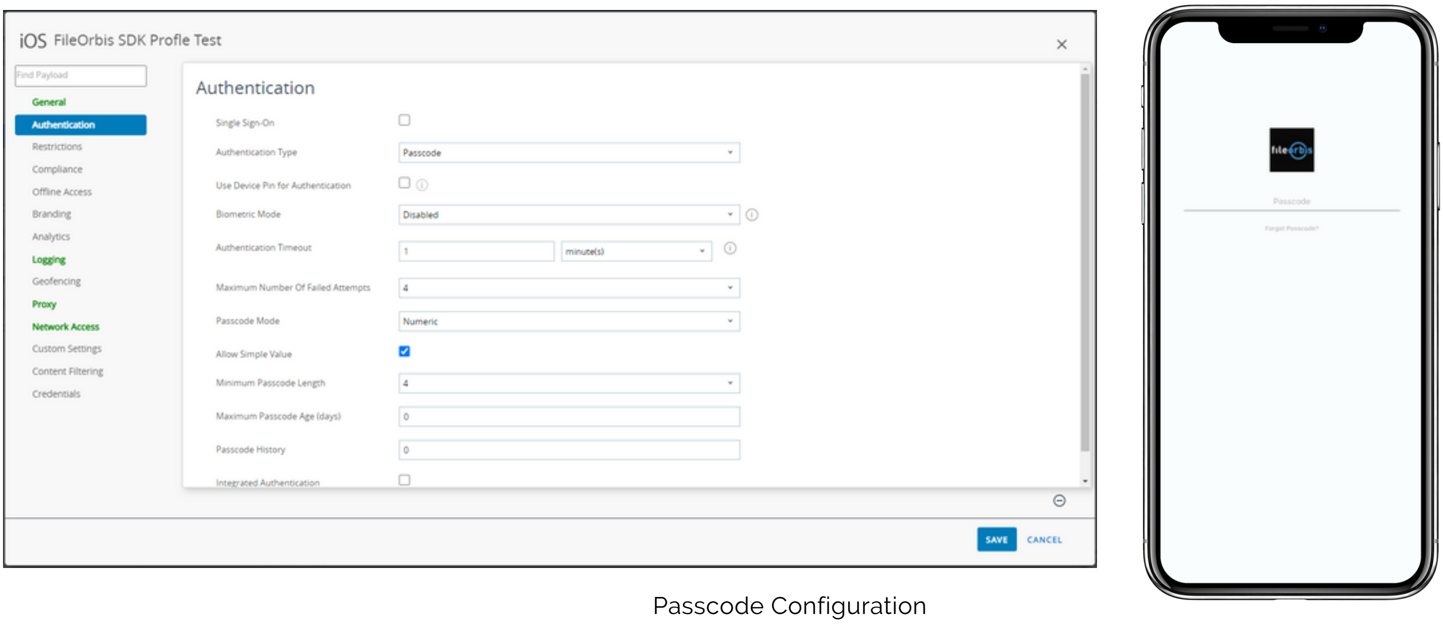
FileOrbis IOS application supports VMware mobile SDK rules with Airwatch SDK integration. The SDK rules that FileOrbis IOS app supports, following:

1.Passcode
2.Restrictions – DLP Rules
  a.Enable Camera
  b.Enable Copy and Paste Out
  c.Enable Copy and Paste Into
  d.Enable Screenshot
3.Branding
4.Network Access
5.Custom Settings

3.3.1 Passcode

The password feature can be used in the FileOrbis mobile application. When this feature is activated, the user will be faced with the passcode screen shown by VMware, when the FileOrbis IOS application is opened or to wake up the app from the background (passcode control will appear or not according to the session duration set while creating the profile).

If any FileOrbis user is logged into the FileOrbis mobile application and the passcode set by the user is entered correctly, the user will successfully continue his session in the mobile application. However, if the passcode is not entered correctly, the session of the FileOrbis user is terminated. The user is directed to the login page and is forced to login.



Authentication

Single Sign-On □

Authentication Type: Passcode

Use Device Pin for Authentication □

Biometric Mode: Disabled

Authentication Timeout: 1 minute(s)

Maximum Number Of Failed Attempts: 4

Passcode Mode: Numeric

Allow Simple Value ☑

Minimum Passcode Length: 4

Maximum Passcode Age (days): 0

Passcode History: 0

Integrated Authentication □

Passcode Configuration

3.3.2 Restrictions – DLP Rules

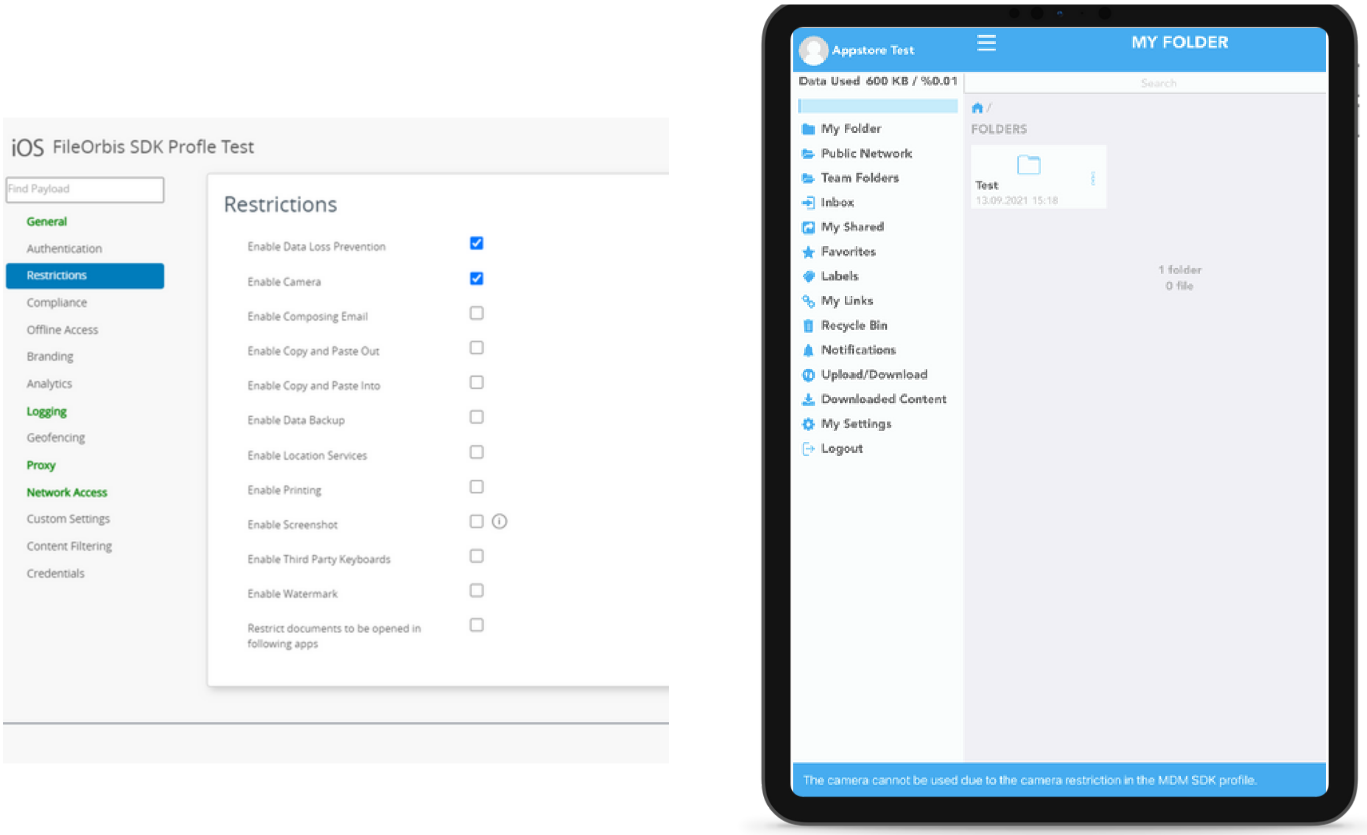
FileOrbis IOS mobile app supports the following features from Restrictions & DLP rules in VMware IOS SDK profile with Airwatch SDK integration.

3.3.2.1 Enable Camera

FileOrbis IOS mobile application supports the "Restrictions>Enable Data Loss Prevention>Enable Camera" feature in the VMware IOS SDK profile with Airwatch SDK integration. If the "Enable Data Loss Prevention" and "Enable Camera" options are turned on in the SDK profile, the user can upload to FileOrbis with the camera. While the "Enable Data Loss Prevention" option is on and the "Enable Camera" option is turned off, the user will not be able to upload to FileOrbis with the camera.

(This rule affects image upload and profile picture change operations with the camera.)

NOTE: If DLP rules (Restrictions) are not turned on in SDK profiles, the camera can be used if there are no other rules (such as device restrictions, etc.).



iOS FileOrbis SDK Profile Test

Find Payload

General
Authentication
Restrictions
Compliance
Offline Access
Branding
Analytics
Logging
Geofencing
Proxy
Network Access
Custom Settings
Content Filtering
Credentials

Restrictions

Enable Data Loss Prevention	☑
Enable Camera	☑
Enable Composing Email	☐
Enable Copy and Paste Out	☐
Enable Copy and Paste Into	☐
Enable Data Backup	☐
Enable Location Services	☐
Enable Printing	☐
Enable Screenshot	☐ ⓘ
Enable Third Party Keyboards	☐
Enable Watermark	☐
Restrict documents to be opened in following apps	☐

Appstore Test

MY FOLDER

Data Used 600 KB / %0.01

Search

My Folder
Public Network
Team Folders
Inbox
My Shared
Favorites
Labels
My Links
Recycle Bin
Notifications
Upload/Download
Downloaded Content
My Settings
Logout

FOLDERS

Test
13.09.2021 15:18

1 folder
0 file

The camera cannot be used due to the camera restriction in the MDM SDK profile.

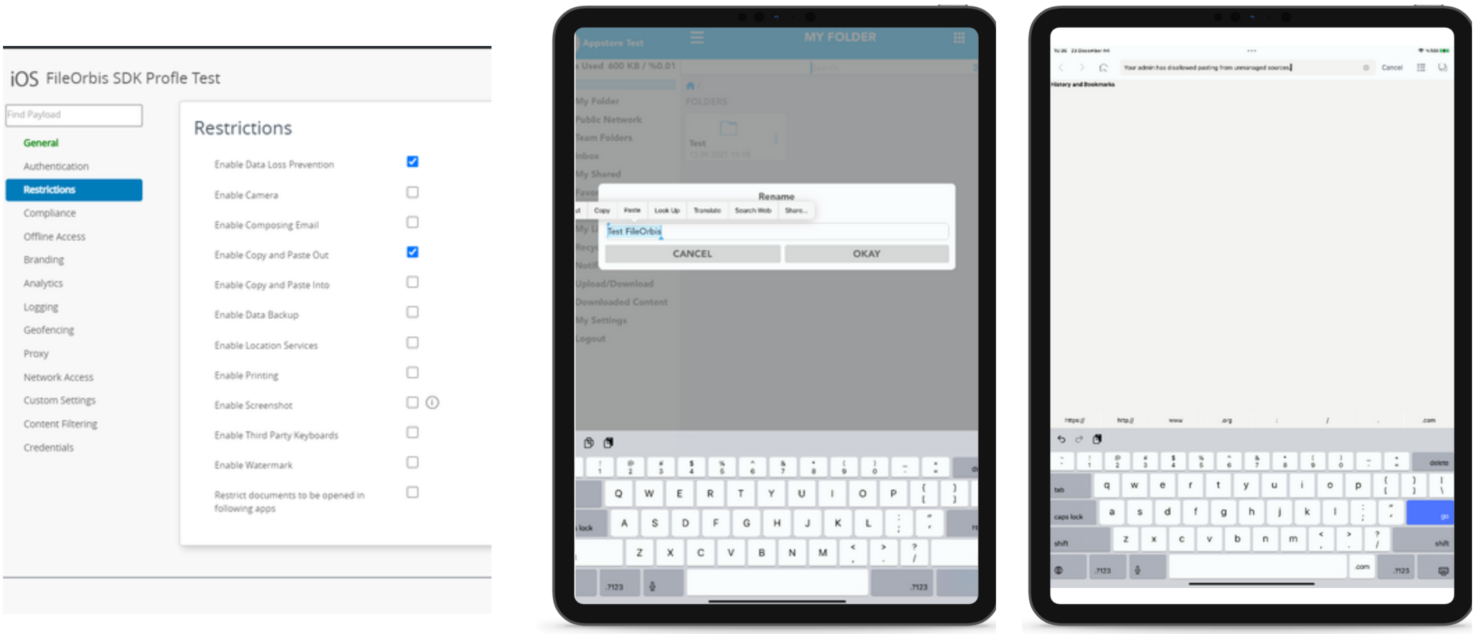
Camera Configuration

3.3.2.2 Enable Copy and Paste Out

FileOrbis IOS mobile application supports the "Restrictions>Enable Data Loss Prevention>Enable Copy and Paste Out" feature in the VMware IOS SDK profile with Airwatch SDK integration. If the “Enable Data Loss Prevention” and “Enable Copy and Paste Out” options are turned on in the SDK profile, the user can paste the text copied from the FileOrbis application to both managed and unmanaged applications, while the “Enable Data Loss Prevention” option is turned on. If the "Enable Copy and Paste Out" option is turned off, the user will be able to use the text copied from FileOrbis application only by pasting it in applications that are not managed with the VMware IOS SDK profile.

NOTE: If DLP rules (Restrictions) are not turned on in SDK profiles, the text copied from the application can be pasted anywhere, unless there are any other rules (such as device restrictions, etc.).

NOTE: If the "Enable Copy and Paste Out" rule is turned off, it should be noted that even if the link created as a result of link creation and the code generated on the FileOrbis authenticator page are copied to the clipboard, these texts cannot be used in other managed applications.



iOS FileOrbis SDK Profle Test

Restrictions

- ☑ Enable Data Loss Prevention
- □ Enable Camera
- □ Enable Composing Email
- ☑ Enable Copy and Paste Out
- □ Enable Copy and Paste Into
- □ Enable Data Backup
- □ Enable Location Services
- □ Enable Printing
- □ Enable Screenshot
- □ Enable Third Party Keyboards
- □ Enable Watermark
- □ Restrict documents to be opened in following apps

Rename

Test FileOrbis

Your admin has disallowed pasting from unmanaged sources.

Copy and Paste Out Configuration

3.3.2.3.Enable Copy and Paste Into

FileOrbis IOS mobile application supports the "Restrictions>Enable Data Loss Prevention>Enable Copy and Paste Into" feature in the VMware IOS SDK profile with Airwatch SDK integration. If the “Enable Data Loss Prevention” and “Enable Copy and Paste Into” options are turned on in the SDK profile, the user can paste the text copied from both managed and unmanaged applications on the device into the FileOrbis application. While the “Enable Data Loss Prevention” option is turned on and the “Enable Copy and Paste Into” option is turned off, the user can paste the copied text from the unmanaged applications on the device into the FileOrbis application, but the user will not be able to paste the copied text from the managed applications into FileOrbis.

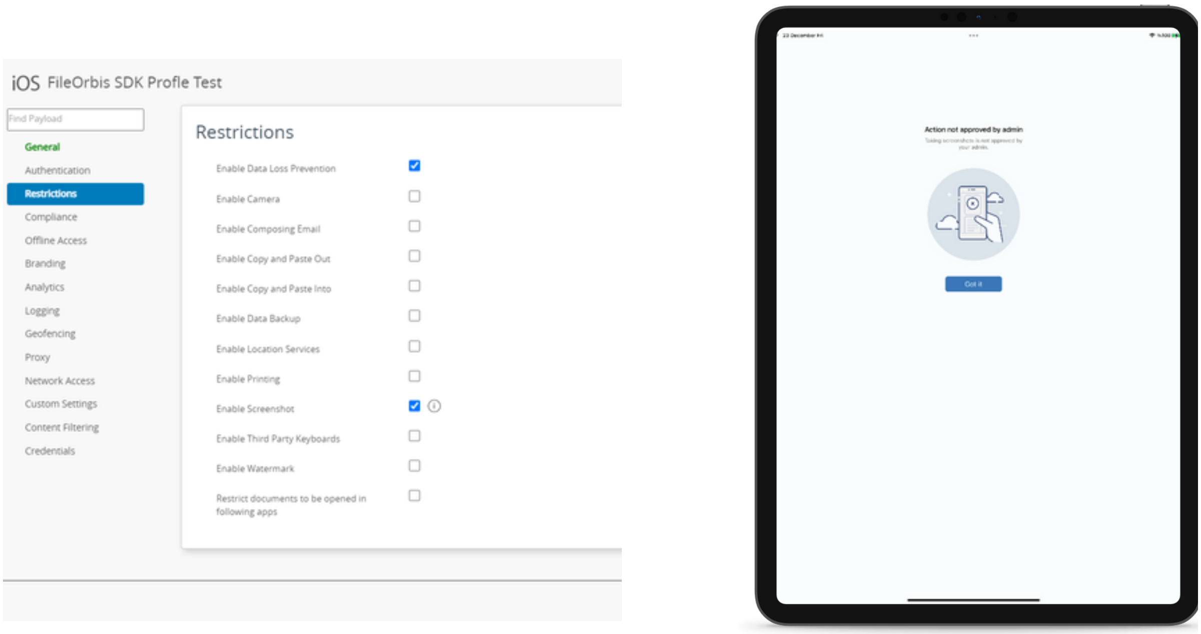
NOTE: If DLP rules (Restrictions) are not open in SDK profiles, all copied texts will be able to be pasted into the FileOrbis application if there are no other rules (such as device restrictions, etc.).

3.3.2.4. Enable Screenshot

FileOrbis IOS mobile application supports the "Restrictions>Enable Data Loss Prevention>Enable Screenshot" feature in the VMware IOS SDK profile with Airwatch SDK integration. If the "Enable Data Loss Prevention" and "Enable Screenshot" options are turned on in the SDK profile, when the user tries to take screenshot in the FileOrbis application, the user will see the screen containing the information that the screenshot process is blocked by the MDM admin. (However, taking screenshots still happens.)

IMPORTANT NOTE: If the screenshot in SDK profile is turned off, taking screenshots in FileOrbis application will not be blocked. Only after the screenshot is taken, the user will see a screen with information that this should not be done.

NOTE: If DLP rules (Restrictions) are not turned on in SDK profiles, if there are no other rules (such as device restrictions, etc.), FileOrbis application will not see any warning screen after taking screenshots.



iOS FileOrbis SDK Profle Test

Restrictions

Enable Data Loss Prevention ☑
Enable Camera □
Enable Composing Email □
Enable Copy and Paste Out □
Enable Copy and Paste Into □
Enable Data Backup □
Enable Location Services □
Enable Printing □
Enable Screenshot ☑
Enable Third Party Keyboards □
Enable Watermark □
Restrict documents to be opened in following apps □

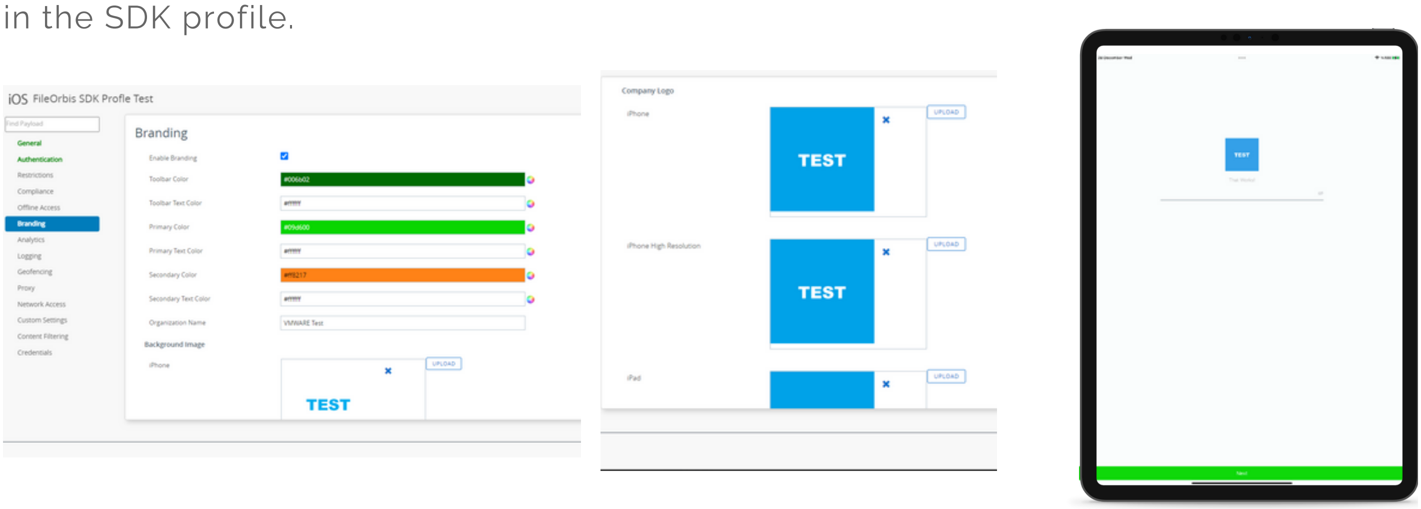
Action not approved by admin

Taking screenshots is not approved by your admin.

Screenshot Configuration

3.3.3 Branding

FileOrbis IOS mobile application supports the "Branding" feature in the VMware IOS SDK profile with Airwatch SDK integration. The icons, pictures and colors on the screens can be changed (These screens are the screens shown on the screens when the passcode feature is turned on) by opening the "Enable Branding" option under the "Branding" title in the SDK profile.



Branding

Enable Branding	☑
Toolbar Color	#006b02
Toolbar Text Color	#ffffff
Primary Color	#09d600
Primary Text Color	#ffffff
Secondary Color	#ff8217
Secondary Text Color	#ffffff
Organization Name	VMWARE Test

Background Image

iPhone

Company Logo

iPhone

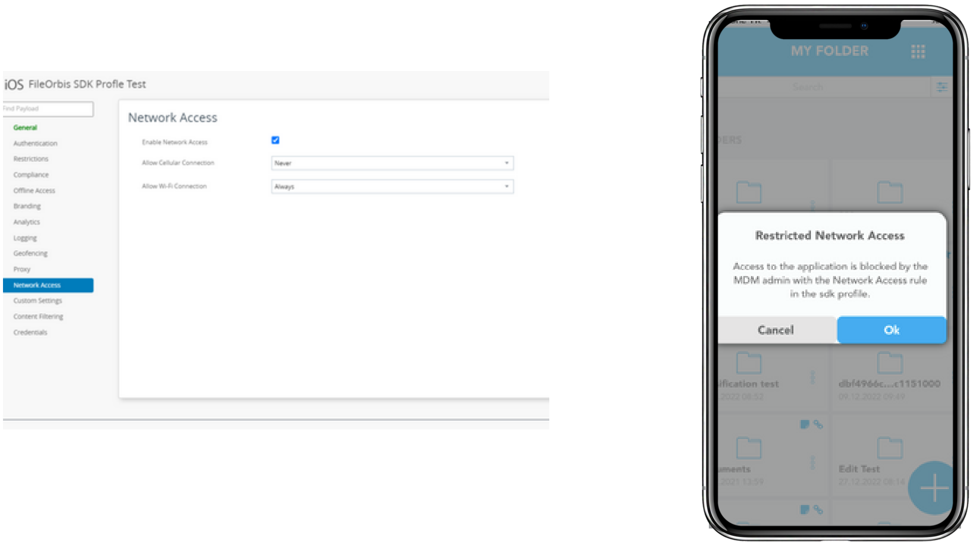
iPhone High Resolution

iPad

Brading Configuration

3.3.4 Network Access

FileOrbis IOS mobile application supports the "Network Access" feature in the VMware IOS SDK profile with Airwatch SDK integration. For this, the "Enable Network Access" option under the "Network Access" title in the VMware IOS SDK profile can be opened and how the application will react when the application is opened with a cellular or wifi connection can be set.



Network Access

Enable Network Access	☑
Allow Cellular Connection	Never
Allow Wi-Fi Connection	Always

Restricted Network Access

Access to the application is blocked by the MDM admin with the Network Access rule in the sdk profile.

Cancel Ok

Network Access Configuration

3.3.5 Custom Settings

FileOrbis IOS mobile application supports the "Custom Settings" feature in the VMware IOS SDK profile with Airwatch SDK integration. By activating the "Custom Settings" in the VMware IOS SDK profile and entering some rules predefined by FileOrbis in the Custom Settings textbox, the relevant changes can be made in the FileOrbis application.
The predefined custom settings rule by FileOrbis are:

Username: By using the "Username" key in Custom settings, what will be written in the username textbox on the login page can be determined. If "{EnrollmentUser}" is used as the “Value”, the username given to the user of the added device when registering the VMware-managed device to VMware will be written in the username field on the login page of the FileOrbis mobile application.

UsernameEnabled: The rule is set whether the username textbox on the login page can be changed by the user by using the "UsernameEnabled" key in Custom Settings. “True” or “False” values can be entered. If “True” is entered, the user using the FileOrbis mobile application will be able to change the username on the login page of the mobile application, if it is set to “False”, user will not be able to change username.