iOS / iPadOS

iOS and iPadOS are the operating systems developed by Apple for their mobile devices, including iPhones and iPads, respectively. Both operating systems share a similar foundation but have slight variations to cater to the specific form factors and functionalities of their respective devices. iOS and iPadOS provide users with a visually appealing and intuitive interface, seamless integration with Apple services, a vast selection of applications through the App Store, and advanced features like Face ID, Siri, and multitasking capabilities. They offer a secure and reliable platform for communication, productivity, entertainment, and more, empowering users to unleash the full potential of their Apple mobile devices.

- Block iOS TV App (iOS 10.2+)
- Does Inventory report data about iOS Applications?
- iOS 14 Compatible Devices (Query)
- iOS 17 Compatible Devices (Query)
- iOS Guided Access
- Unlock Token in iOS 13
- Return to Service feature for iOS/iPadOS
- Working with iOS Inventory
- iOS/iPadOS BYOD User Enrollment
    - iOS BYOD and VPP License Assignment Change
    - iOS BYOD User Enrollment Overview
    - Account-Driven User Enrollment for iOS/iPadOS BYOD Devices (v15.0+)
    - Managing BYOD User Enrollment
    - New Inventory Item -- Enrollment Type

- Troubleshooting
    - Apple ID prompt still appears even when Activation Lock Bypass Code is used during Remote Wipe
    - FileWave iOS Kiosk (IPA) Location Tracking Problem
    - iOS 12+ Profile Installation Failed

- Customising iOS Wallpaper
    - Customizing iOS Device Wallpaper with Dynamic Text
    - Custom iOS Wallpaper Dynamic Text Tips

- App Security on iOS

Block iOS TV App (iOS 10.2+)

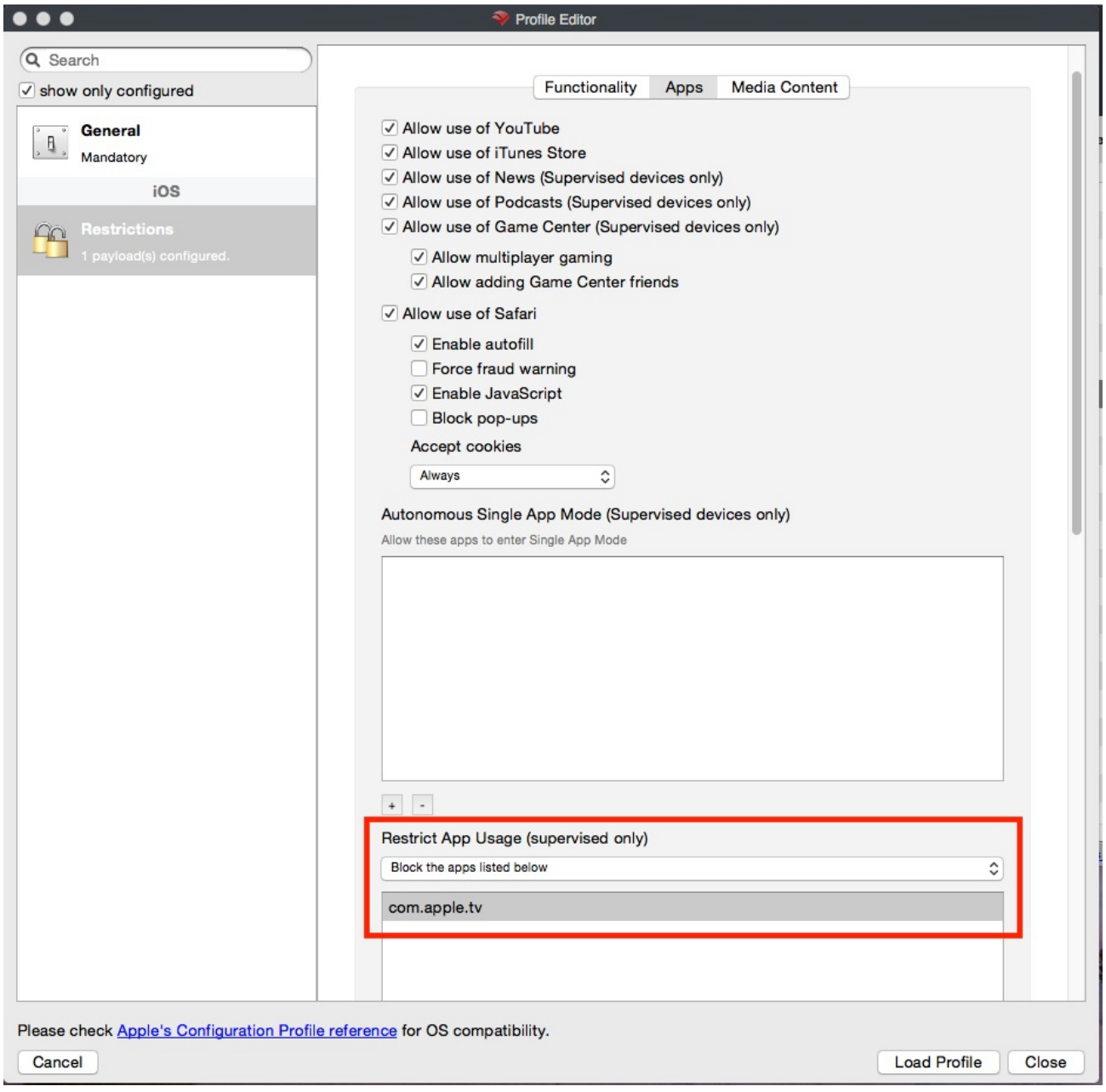
This article will show you how to block the TV app introduced with iOS 10.2 with your updated and supervised iOS devices. Your FileWave server will have to be version 11.2.2+.

Steps:

- Once in the Filesets view, select New Mobile Fileset at the top and then select the Profile option.
- Name the profile in the General payload. Other settings in this area are optional.
- Find the Restrictions payload in the left pane for iOS.
  Tip: Use the search feature at the top of the window to filter your payloads.
- Once you have found and selected your Restrictions payload for iOS, click the Configure button on the right pane to enable the payload for this profile.
- In the profile you will see three tabs across the top. Select the middle Apps tab.
- Scroll down to the section Restrict App Usage (supervised only) and from the drop down menu select "Don't Allow Some Apps".
- To create a new object, click the plus sign at the bottom left of the current pane that says:

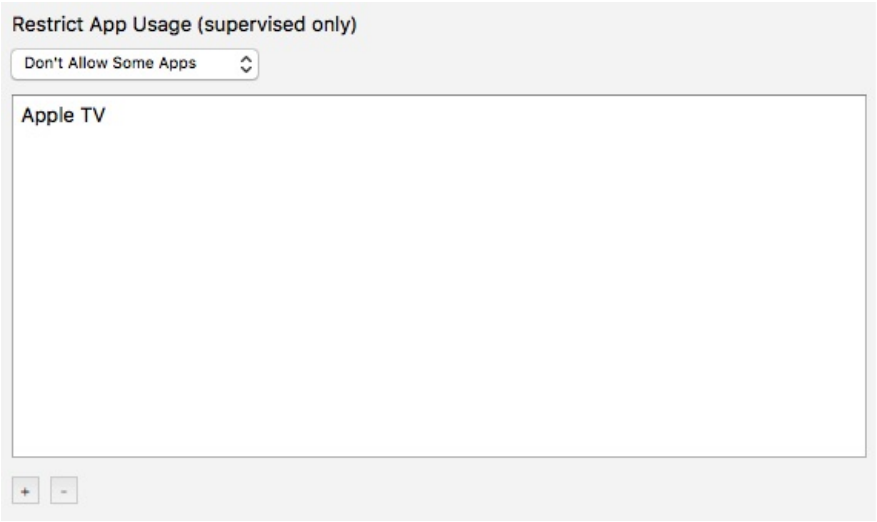
<click to edit app name>

- After you have double-clicked the new object, type in the following and then press enter/return to save the entry:
  com.apple.tv



- Hit the Save button at the bottom right of the Profile Editor window to save your profile.
  Please note: If you open this profile after it has been saved you will noticed the entry for com.apple.tv has been changed to "Apple TV" as seen below. You can do this for other apps as well by adding in it's payload identifier. (e.q. in the prior step if

you wanted to disable the Home app which has the identifier of com.apple.Home it will switch to just Home after saved.)



Congratulations, you are now ready to send this profile out to a few of your supervised iOS 10.2+ test devices before mass deployment!

Does Inventory report data about iOS Applications?

Yes and No.

The Inventory tracks lots of the same information for all devices. Including what applications are installed where.

The exception with iOS devices is that we are unable to obtain application usage like:

- Average Time Used
- First Launched Date
- Installed Date
- Times Launched
- Total Time Used

ADDITIONAL INFORMATION

This limitation is because there isn't an actual client running on the iOS device and Apple's MDM protocol does not currently contain information about Usage.

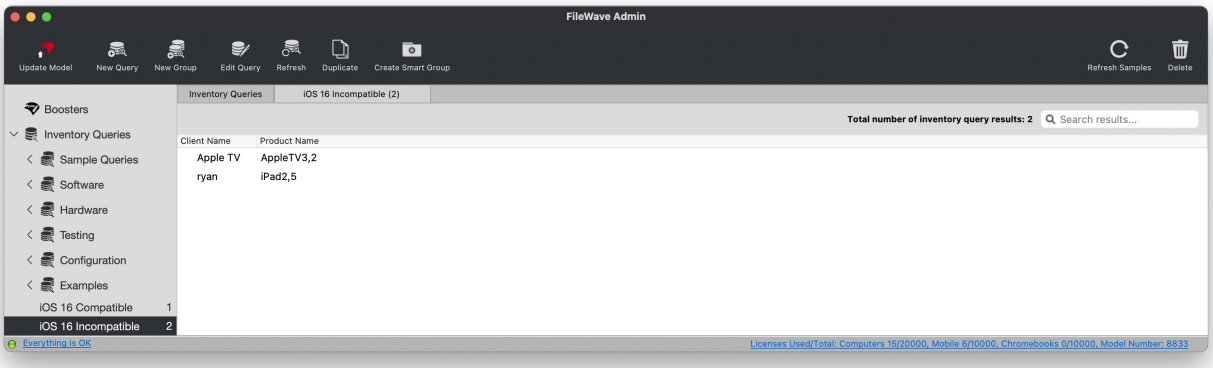
iOS 14 Compatible Devices (Query)

Description

Details on identifying compatible devices for iOS 14 using the Command Line API to create a Query in FileWave Central and FileWave Anythere.

iOS
Inventory Queries to list device compatibility

Example query view:



Ingredients

- Administrator Application Token (base 64)
- FW Admin Inventory Query

Compatible Query	Incompatible Query
ios14_compatible.json	ios14_incompatible.json

Directions

Requires the creation of Inventory Queries. Two queries are available, one listing incompatible devices and one listing compatible devices. To upload the queries involves using the FWAdmin CLI (Command Line Interface).

Obtain the Administrator Application Token (base 64), then use the following format to upload each Inventory Query to the server. For example:

- Token(base 64): eaIaY2Q2MjAkLTVmMzItMGU3AC1kYTcyLTU1NLc4NzNlNDc0An0=
- Server Address: mdm.filewave.ch
- File: ios14_compatible.json

Command Line API POST

You'll have the downloaded file in the same directory as where you run the below command. The below example uses the ios16_compatible.json but you can change that easily.

Shell Script:

```
curl -s -k -H "Authorization: eaIaY2Q2MjAkLTVmMzItMGU3AC1kYTcyLTU1NLc4NzNlNDc0An0="
https://mdm.filewave.ch:20445/inv/api/v1/query/ --header "Content-Type: application/json" -X POST -d
@ios14_compatible.json
```

PowerShell:

```
$uri = 'https://mdm.filewave.ch:20445/inv/api/v1/query/'
$headers = @{
    'Authorization' = 'eaIaY2Q2MjAkLTVmMzItMGU3AC1kYTcyLTU1NLc4NzNlNDc0An0='
```

```
    'Content-Type' = 'application/json'
}
$body = Get-Content -Raw -Path 'ios14_compatible.json'

$response = Invoke-RestMethod -Uri $uri -Headers $headers -Method Post -Body $body

# Process the response as needed
$response
```

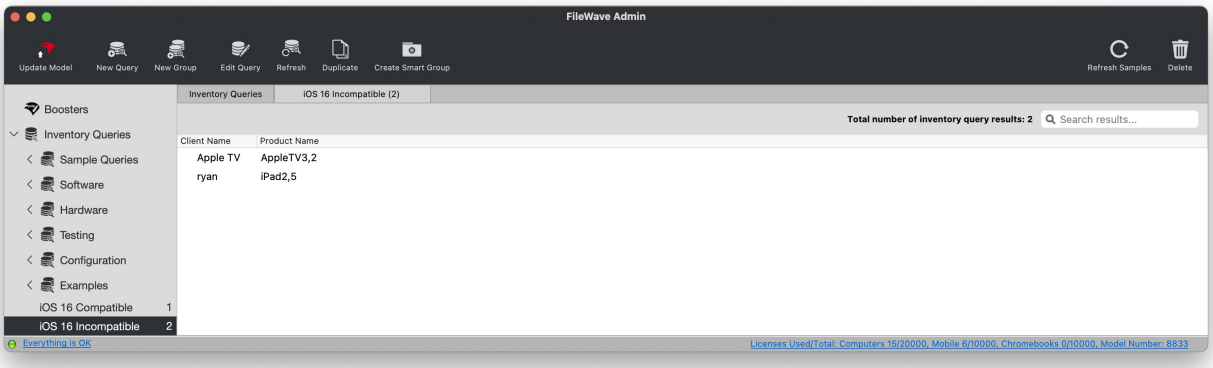
iOS 17 Compatible Devices (Query)

Description

Details on identifying compatible devices for iOS 17 using the Command Line API to create a Query in FileWave Central and FileWave Anythere.

iOS
Inventory Queries to list device compatibility

Example query view:



Ingredients

- Administrator Application Token (base 64)
- FW Admin Inventory Query

Compatible Query	Incompatible Query
ios17_compatible.json	ios17_incompatible.json

Directions

Requires the creation of Inventory Queries. Two queries are available, one listing incompatible devices and one listing compatible devices. To upload the queries involves using the FileWave Command Line API.

Obtain the Administrator Application Token (base 64), then use the following format to upload each Inventory Query to the server. For example:

- Token(base 64): eaIaY2Q2MjAkLTVmMzItMGU3AC1kYTcyLTU1NLc4NzNlNDc0An0=
- Server Address: mdm.filewave.ch
- File: ios17_compatible.json

Command Line API POST

You'll have the downloaded file in the same directory as where you run the below command. The below example uses the ios17_compatible.json but you can change that easily.

Shell Script:

```
curl -s -k -H "Authorization: eaIaY2Q2MjAkLTVmMzItMGU3AC1kYTcyLTU1NLc4NzNlNDc0An0="
https://mdm.filewave.ch:20445/inv/api/v1/query/ --header "Content-Type: application/json" -X POST -d
@ios17_compatible.json
```

PowerShell:

```
$uri = 'https://mdm.filewave.ch:20445/inv/api/v1/query/'
$headers = @{
    'Authorization' = 'eaIaY2Q2MjAkLTVmMzItMGU3AC1kYTcyLTU1NLc4NzNlNDc0An0='
```

```
    'Content-Type' = 'application/json'
}
$body = Get-Content -Raw -Path 'ios17_compatible.json'

$response = Invoke-RestMethod -Uri $uri -Headers $headers -Method Post -Body $body

# Process the response as needed
$response
```

iOS Guided Access

Description

Guided Access is a local equivalent to Single App Mode, which provides some additional features, e.g. select area of screen available. Additionally a local passcode is required.

Use Guided Access with iPhone, iPad, and iPod touch

Problem

This is a local passcode and cannot be controlled by MDM. Once set, without the passcode there is no way to locally exit Guided Access.

Solution

Despite MDM having no control over Guide Access, it is still possible to disable the Guided Access, without the passcode, through MDM. This can be achieved in a couple of ways:

1. Associate a Single App Mode profile through MDM
2. Set the device into Lost Mode

By providing a Single App Mode profile to the device, MDM will overrule Guided Access. On removal of the Single App Mode Association from MDM, the device will be back to normal

Setting Lost Mode should have the same impact. Once Lost Mode is de-activated, again the device will be back to normal

Related Content

- MDM Lost Mode (Apple)

Unlock Token in iOS 13

FileWave's MDM solution has the ability to unlock devices which are passcode protected. This can be very useful to recover devices without knowing the passcode set by students or users.

To achieve this, the device sends FileWave an Unlock Token, which is then sent back to the device with the ClearPasscode request. This ensures security as only the MDM solution where the device is enrolled can unlock the device - and access to user data.

Moving forward with security, Apple changed how this token is sent to MDMs in iOS 13: the token is sent only once during enrollment ; therefore it's extremely important to keep this token safe.

Apple recently clarified how this change would be effective: the device may still send a TokenUpdate message to the MDM server, but the message will not contain the token anymore.

Until FileWave 13.1.3, such a message (TokenUpdate without UnlockToken) was considered to be a message clearing the token ; therefore managing iOS 13 devices with a previous version can lead FileWave to clear stored tokens and then not being able to clear the device passcode.

It is therefore highly recommended to:

- regularly backup your FileWave instance, to keep sensitive data like unlock tokens in a safe place
- upgrade to FileWave 13.1.3 if you plan to upgrade your devices to iOS 13
- ensure iCloud backup is configured on iOS devices

You also have the ability to defer software updates by deploying a restriction profile (more information in this KB article)

Return to Service feature for iOS/iPadOS

What

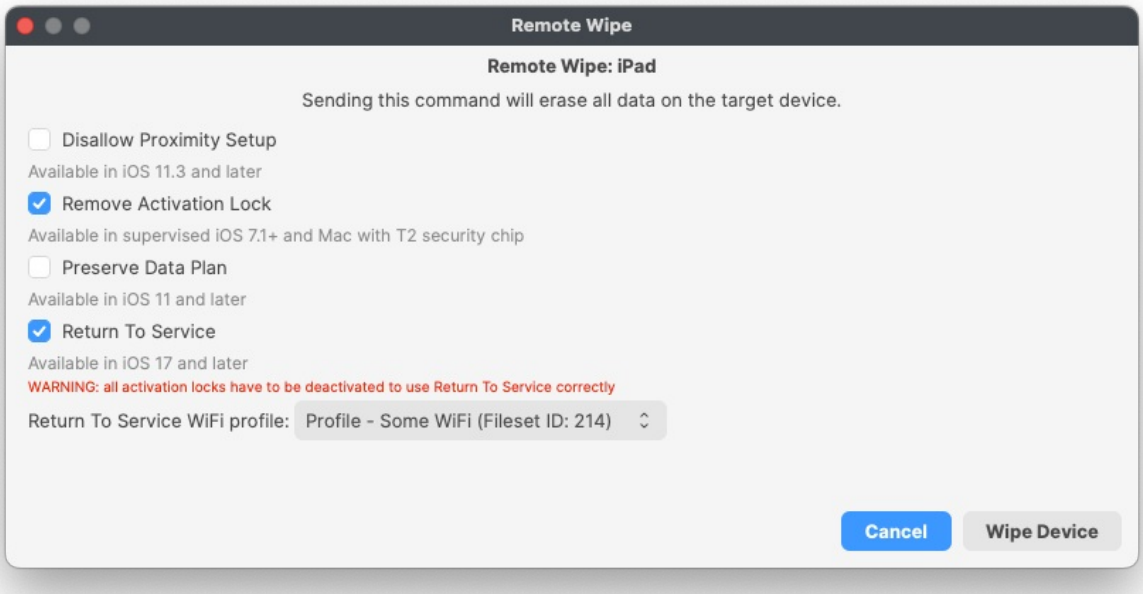
Even though devices can be erased remotely, getting them back into service is a manual process, as it requires someone to physically touch them and take them through Setup Assistant. Apple is removing the additional manual step with the introduction of Return to Service for iOS and iPadOS. This feature was added in FileWave version 15.1.0 for iOS 17.0 and iPadOS 17.0. As for FileWave version 15.5.0 this was also added for tvOS.

When/Why

Return To Service is the following process. The MDM server sends an `EraseDevice` command to the device. The command includes additional information which allows the device to reset, securely erase all data, connect to Wi-Fi, enroll into MDM, and get back to the Home Screen, ready to be used.

How

With FileWave 15.1.0 support of Return To Service was added. To use Return To Service open Remote Wipe dialog for iOS or iPadOS device. Checkbox Return To Service allows to specify whether feature should be enabled or disabled. It can be checked only if Remove Activation Lock checkbox is checked as well. The feature can be used only if there is at least one configured Wi-Fi profile (fileset containing Network payload with Network Interface “Wi-Fi“). Available Wi-Fi profiles are displayed on combobox.



What happens on the device?

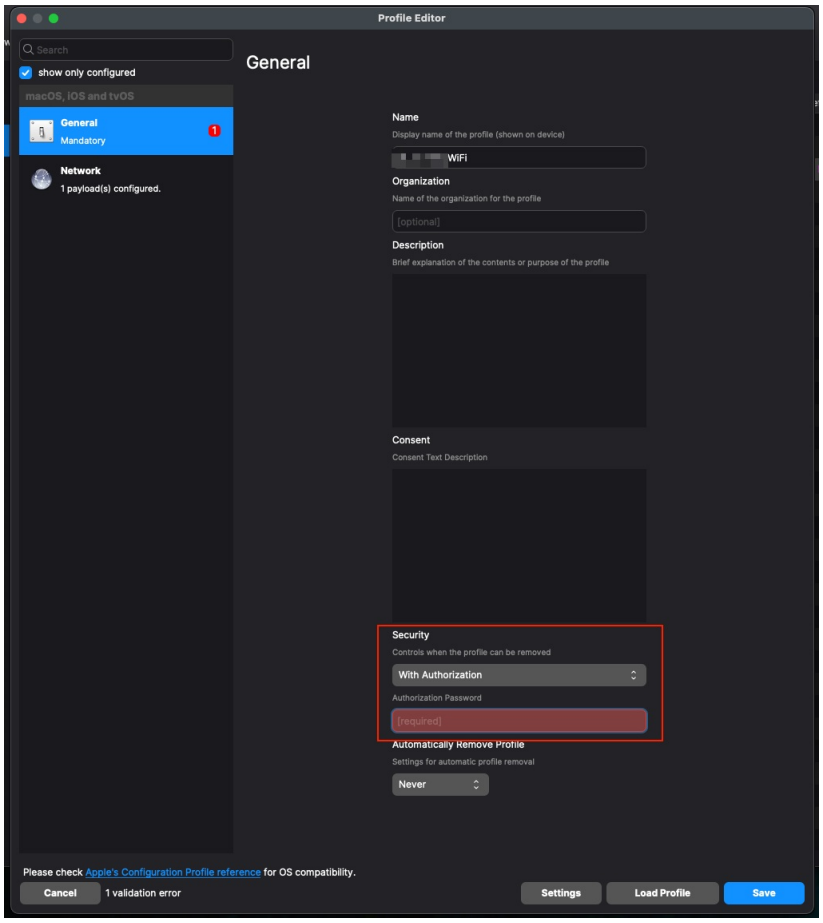
If Return To Service is enabled on FileWave side and then Wipe Device button is pressed, the device will be wiped and then connected to the Wi-Fi network specified in selected Wi-Fi profile without asking password. Also MDM profile will remain on the device, there will be no need for it to re-enroll in MDM.

Related Content

- FileWave Version 15.1.0
- Return to Service feature for tvOS

Troubleshooting

We have found that on the WiFi profile, setting Security to 'With Authorization' - even with the right password, will break Return to Service. What you will see is that the iPad will not be able to join the WiFi automatically when it boots up though you can manually join the WiFi.



Digging Deeper

When Remote Wipe dialog is opened the list of configured Wi-Fi profiles is loaded in format:

```
[(<file_id>, <fileset_id>, <fileset_name>, <payload_display_name>, <payload_identifier>),(...)]
```

`fileset_id` and `fileset_name` are displayed on the UI, `payload_display_name` and `payload_identifier` are used for tool tip. `file_id` is used as internal data for combobox.

When Wipe Device button is pressed, on the backend side is generated MDM command EraseDevice with dictionary field `ReturnToService` and fields `Enabled` and `WiFiProfileData` according to values specified on the UI, then command is added to command queue.

When command is grabbed from command queue and is being composed for sending to the device `MDMProfileData` is added to `ReturnToService` dictionary. This data matches the final payload that is provided by MDM server when /ios/profile URL is used for OTA enrollment. `MDMProfileData` is not added for DEP devices.

API Command

Sending the command to wipe via an API command requires the following data format.

```
'{
    "ids": [<integer>, <integer>],
    "command": "EraseDevice",
    "options": {
        "DisallowProximitySetup": false,
        "PIN": "",
        "PreserveDataPlan": false,
        "ReturnToService": {
            "Enabled": true,
            "WiFiProfileID": <integer>
        }
    }
}'
```

- 'ids' is a comma separated list of the Device IDs to be targeted
- 'WifiProfileID' is the File ID (this is not the Fileset ID)

To obtain the WifiProfileID, will require an additional query first. A full list of all Wi-Fi Profiles can be returned with the following API:

```
curl -X GET "https://${server_dns}/filewave/api/apple/profiles/wifi" -k -H  "Content-Type: application/json" -H
"authorization: ${auth}" | awk '{ gsub("\\]\\,\\[","\n"); gsub("\\]\\]",""); gsub("\\[\\[",""); print }'
```

Where:

- ${server_dns} is the server name as seen in FileWave Central -> Preferences -> Mobile
- ${auth} is the application token as shown in FileWave Central -> Manage Administrators (each user has one or more tokens)

The returned list might look something like:

```
750959,669526,"Profile - HOME WIFI","HOME WIFI","ml1063.lan.4bf6fba8-9cfc-48b5-ad74-
a251a65c8759.Configuration.4bf6fba8-9cfc-48b5-ad74-a251a65c8759"
780638,736322,"Profile - WLTC wifi","WLTC wifi","ml1063.local.7a00d6eb-9b4b-4e7e-b68b-
7ee7e6414051.Configuration.7a00d6eb-9b4b-4e7e-b68b-7ee7e6414051"
504184,411265,"Profile - Wi-Fi BT 2.4GHz","Wi-Fi BT 2.4GHz","FW1063.local.e285dc3b-9c4b-4a7a-84a9-
a3cd5169f92d.Configuration.e285dc3b-9c4b-4a7a-84a9-a3cd5169f92d"
504185,24571,"Profile - Wi-Fi BT 5GHZ","Wi-Fi BT 5GHZ","ML1063.local.02d6d9c3-5a7d-490c-afa8-
f160ba9b4e40.Configuration.02d6d9c3-5a7d-490c-afa8-f160ba9b4e40"
```

The first number is the File ID, whilst the second is the Fileset ID.

Example

Considering the following 3 devices to be wiped using 'Return to Service':

Server FQDN from Preferences	demo.filewave.ch
Authorisation Token	e2E1OTU4ZmYyLTg4ZTYtNDEzNC1iZjdhLWE0ZmJmMTViNmI5OH0=
"Profile - WLTC wifi" [File ID of Fileset: 'Profile - WLTC wifi']	780638
iPad001 [FileWave Device ID]	3425
iPad002 [FileWave Device ID]	4342
iPad003 [FileWave Device ID]	3312

The API data block might look like:

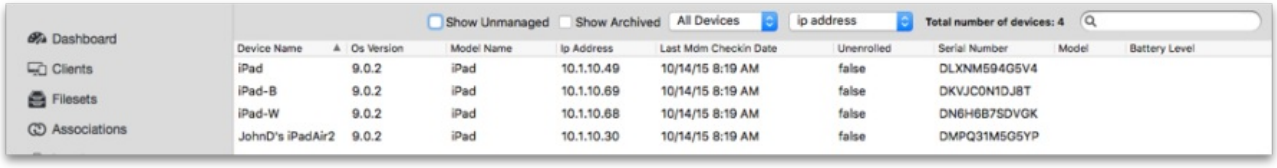
```
'{
    "ids": [3425, 4342, 3312],
    "command": "EraseDevice",
    "options": {
        "DisallowProximitySetup": false,
        "PIN": "",
        "PreserveDataPlan": false,
        "ReturnToService": {
            "Enabled": true,
            "WiFiProfileID": 780638
        }
    }
}'
```

and the command:

```
curl -X POST "https://demo.filewave.ch/api/devices/v1/devices/mdm-command" -k -H  "Content-Type: application/json"
-H "authorization: e2E1OTU4ZmYyLTg4ZTYtNDEzNC1iZjdhLWE0ZmJmMTViNmI5OH0=" -d  "<data block goes here>
```

Working with iOS Inventory

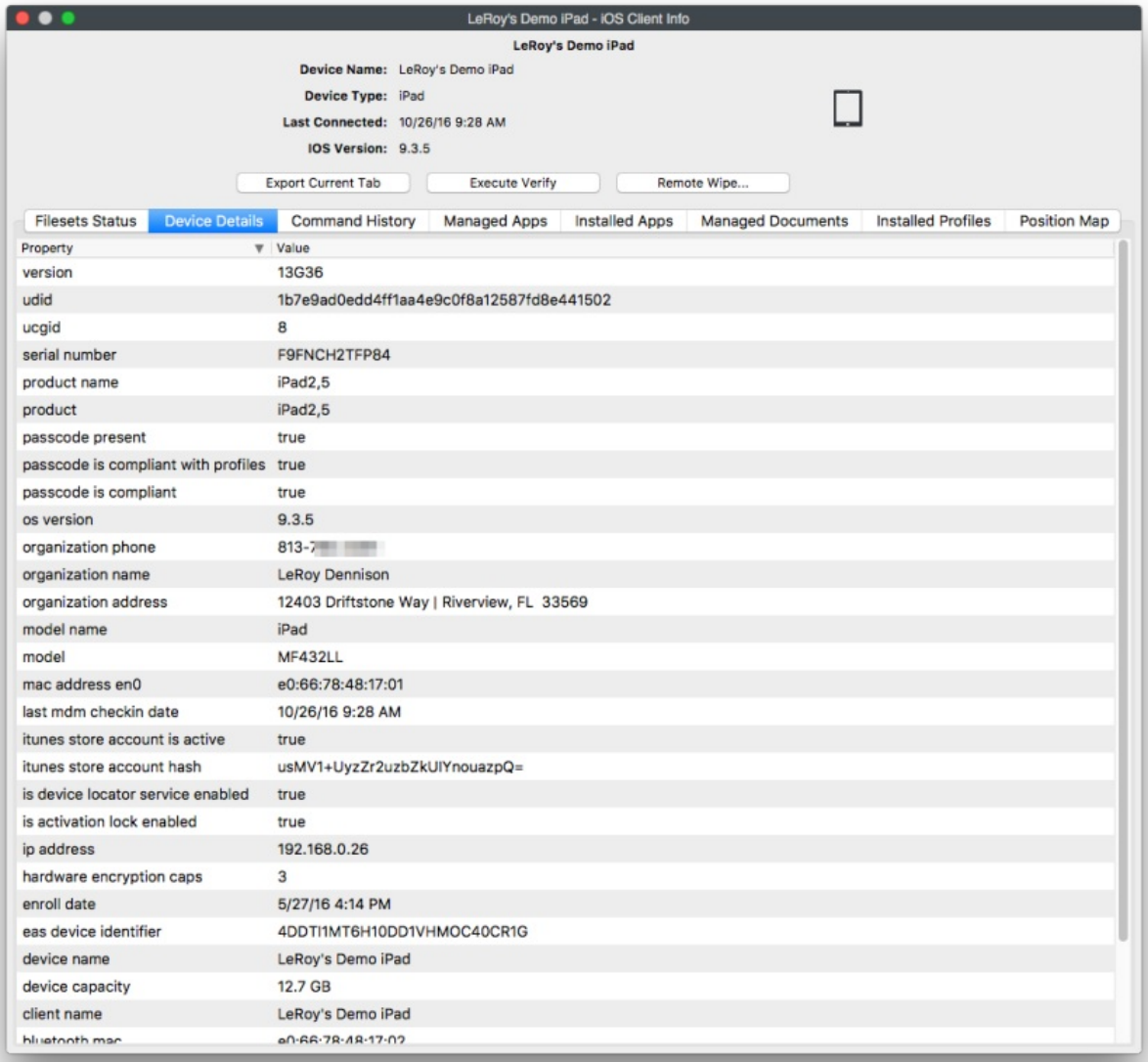
The iOS Inventory pane exists for you to have instant access to the attributes of your iOS devices. Unlike the normal Inventory pane, the iOS Inventory behaves more like a dashboard view of your iOS devices.



The iOS Inventory view is a read-only list of attributes for enrolled iOS devices. Each enrolled device automatically appears in this list which provides details retrieved about the device. The three toolbar items you use in this pane are the Device Info, Refresh, and Customize Columns.

Device Info

This window is identical to the one you see when you select Client Info in the Clients pane. The Execute Verify button forces the device to refresh all of its information with your FileWave server. The Remote Wipe... button allows the FileWave super administrator to remotely reset the iOS device, erasing all settings and content.



The window also provides all of the key details about your iOS device:

- Fileset Status – This shows the list of Filesets that have been installed on the device.
- Device Details – This displays technical information on the device to include UDID, serial number, etc.

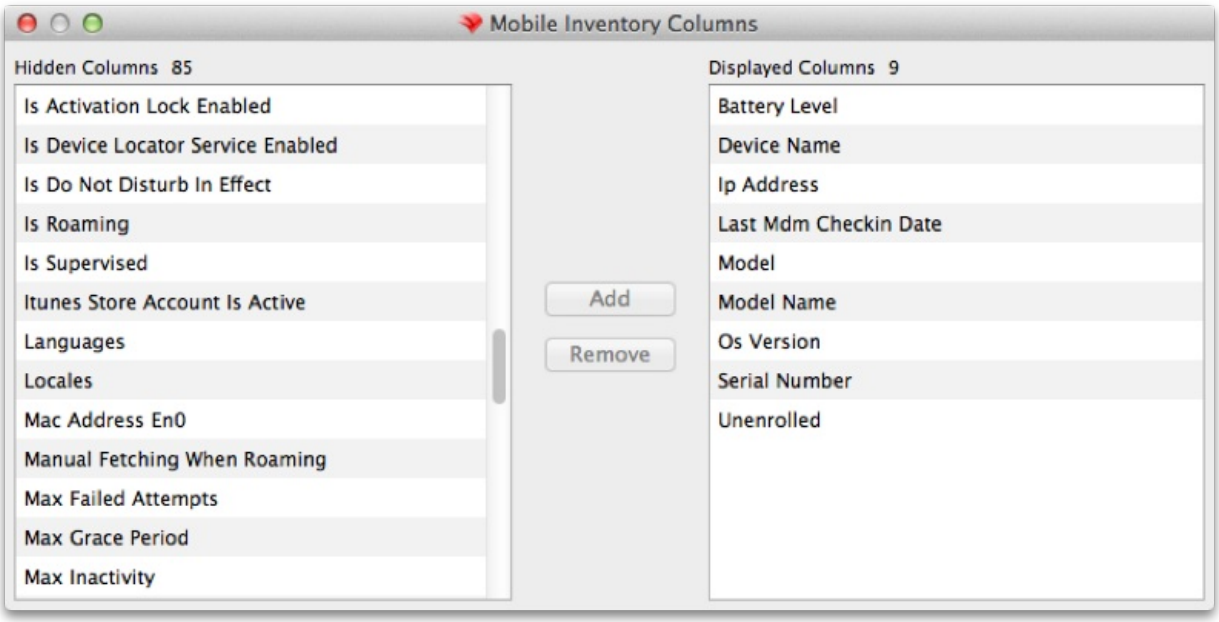
- Command History – This displays the commands sent from FileWave server to the device with actions and results.
- Managed Apps – This shows the applications sent from FileWave as Filesets.
- Installed Apps – This displays all applications, other than the built-in one, that were not sent by FileWave. It shows the applications installed by the user.
- Managed Documents – This shows a list of any documents that have been installed using a Fileset.
- Installed Profiles – This displays the profiles on the device from the the FileWave MDM server.
- Position Map – This shows a map displaying the last reported position for devices in which tracking has been enabled.

Refresh

This toolbar command forces the devices listed to be refreshed from information in inventory. The display window does not dynamically refresh. If the iOS database is very large, the refresh could take a long time.

Customize Columns

You can edit the display of your iOS devices by customizing the column view in the main window.

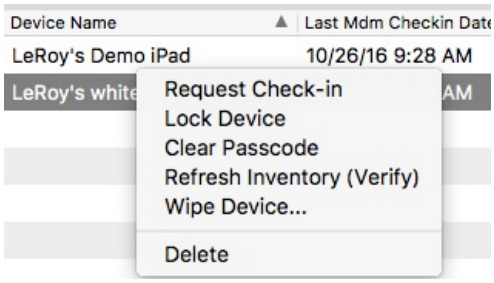


Searching and managing window contents

The main window can also be managed to view a restricted set of iOS devices depending on the specific devices you are looking for. You can select to see only iPads, iPods, or iPhones, and search for devices using the column data you have displayed. If you choose to see Unmanaged devices, it will show iOS devices you have added as clients that have not enrolled. These would be devices you added from a text file in bulk while preparing for a large roll out. You can also see a list of Archived iOS devices, if you have any that were previously enrolled, but have since been archived.

Contextual Menu

The contextual menu, from right-clicking a device, gives you a subset of the controls you see in the Clients pane. These include the ability to clear the passcode and lock the device remotely, which activates the screen lock.



iOS/iPadOS BYOD User Enrollment

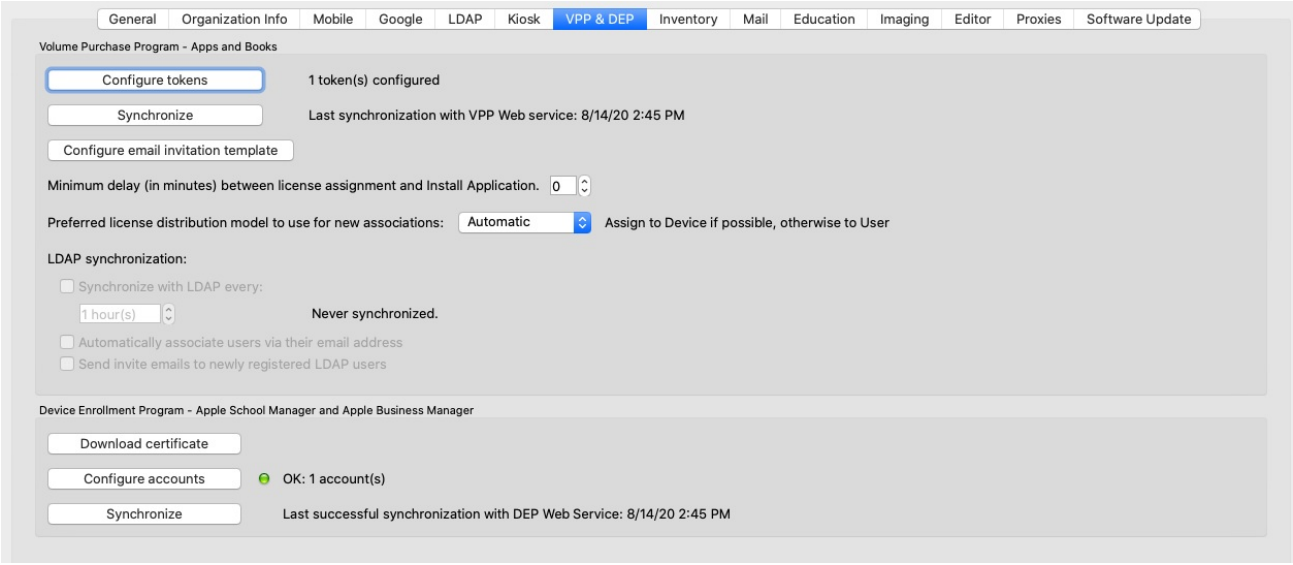
iOS BYOD and VPP License Assignment Change

What

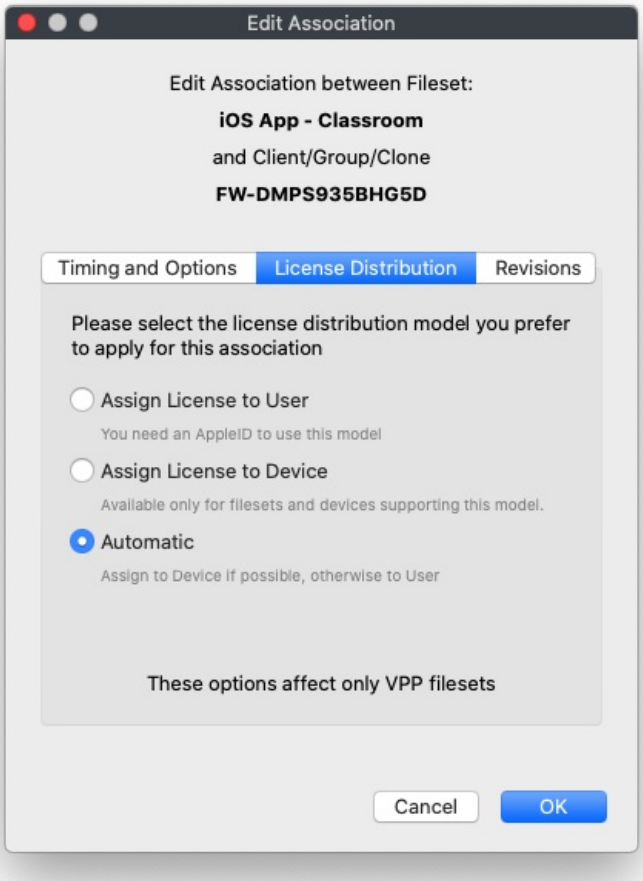
For a few years, device license assignment has been the preferred method for assigning licenses for managed iOS devices. But, with BYOD enrolled devices, licenses can't be assigned to the device... So FileWave have made some changes to how we handle this which make managing BYOD enrolled devices (and as a happy accident supervised devices) easier.

When/Why

Historically, when you created an association for a VPP app, you had a choice to assign the license to the Device, or to the User. And, in Preferences, there was an option to set your preference (which you most likely have set to Device). There is now a new option called "Automatic", which you will see below:



And, then on each Association that default can be overridden:



"Automatic" in this instance, basically means "Try to do a device license, but if you can't, then do a user based assignment"

Now, how does this make your life easier if you aren't going to manage BYOD devices? That is a great question! If you set your default setting in preferences to "Automatic", that means that all of your apps will assign to the device if they can, but if you have something that maybe you don't do much...like an app that can't do device based licensing, or an iTunes book for instance, then that association will still work even though you didn't manually change it over to "User".

How

We showed you above changing the preferences so that all new associations will be "Automatic" (which we think will work for almost all instances). But, what happens if you enroll a new BYOD device and put it in a group that has a "Device" based association? In short, nothing...the app will be associated, but can never install because device based license assignment can not be used. So, for best results, you may want to consider updating older associations to "Automatic" as well.

> The above may mean you have hundreds of associations to change...if that is the case, remember that you can mass-edit associations in the Associations view.

iOS BYOD User Enrollment Overview

What

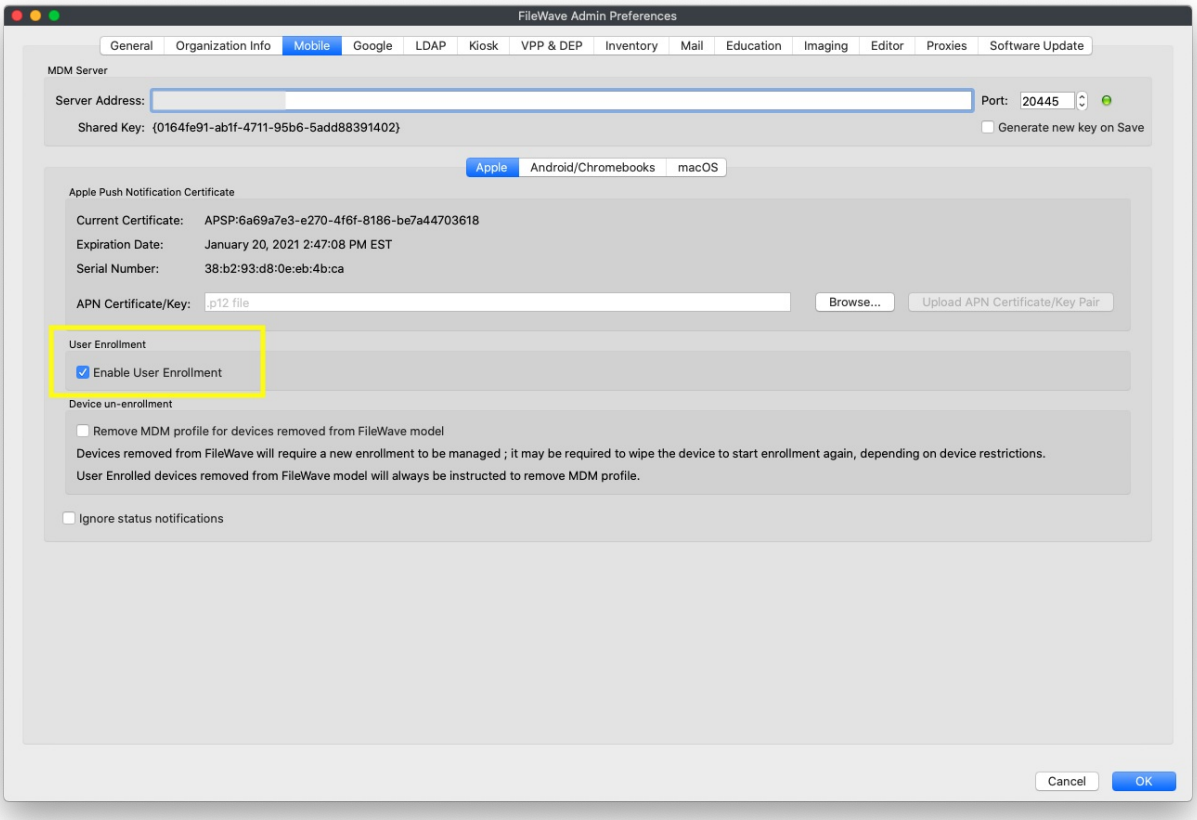
With Version 14(+) of FileWave, you can now BYOD (bring-your-own-device) enroll a device without giving total management of the device to the system admin.

When/Why

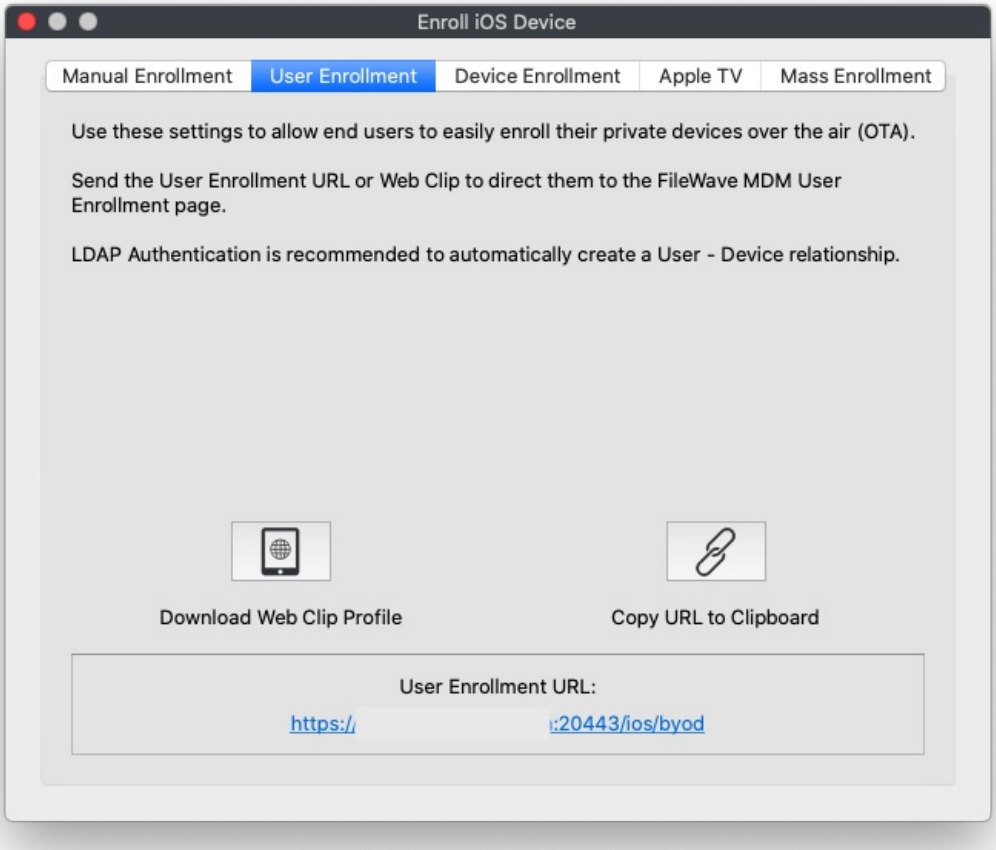
Typically, this option works best if the device to be supported is not company owned. For instance, an employee with their own iPhone may want to BYOD enroll a device to allow distribution of company-owned app licenses, but without giving their company the ability to manage their phone in other ways.

How

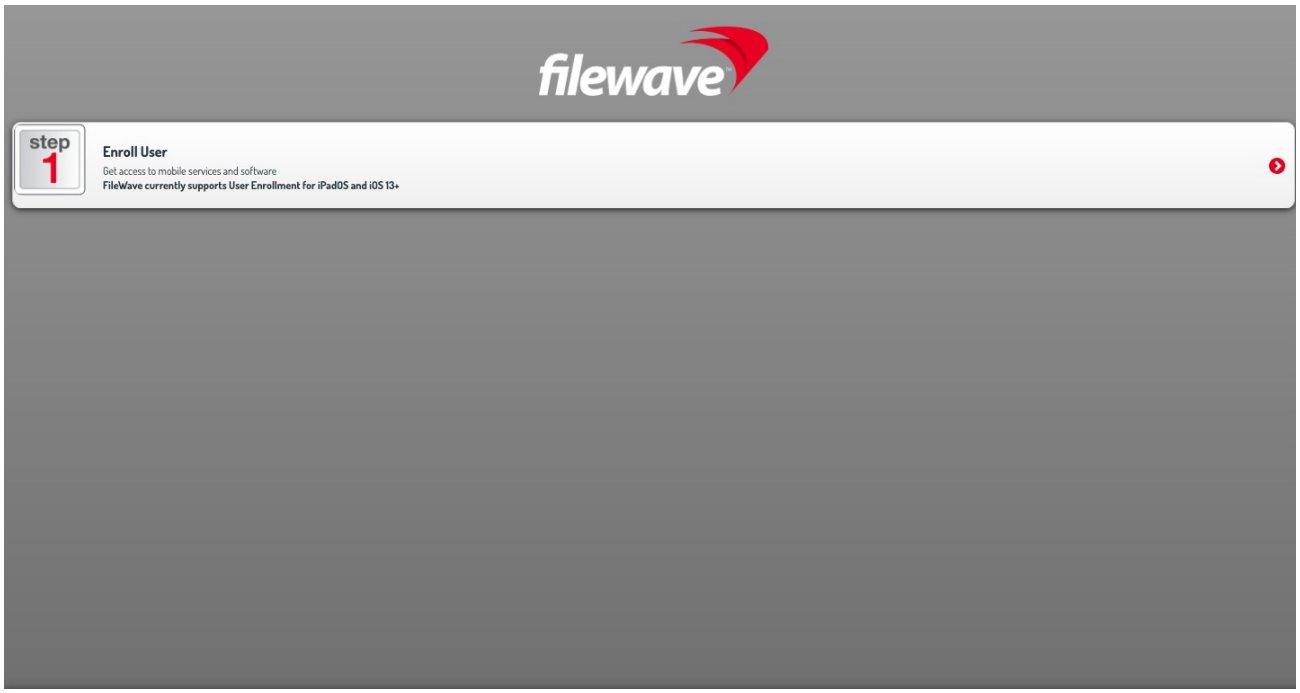
BYOD enrollment is off by default in FileWave, and must be enabled on the Mobile tab in preferences as shown below:



Once enabled, a new tab will be added to the "Enroll iOS Device..." Assistant:



And, once user enrollment is enabled, you can go to https://my.server.address:20443/ios/byod to see the user enrollment page:



Note that by BYOD's very nature the only way you will enroll BYOD devices is through this page. (i.e. it won't be through DEP). BYOD enrollment does require the use of managed apple ids from either Apple School, or Apple Business, Manager.

See below video of a BYOD device enrollment:

Unlike a DEP enrollment, you don't have to wipe the device first to BYOD enroll it. However, trying to enroll a device with a managed Apple ID that is already logged into iCloud on the device will result in an error.

Account-Driven User Enrollment for iOS/iPadOS BYOD Devices (v15.0+)

What

In 2021, Apple introduced Account-Driven User Enrollment, a new method for initiating Bring Your Own Device (BYOD) enrollments. With the releases of iOS 17 and iPadOS 17, profile-based User Enrollment is deprecated, and starting with iOS 18 and iPadOS 18, it is no longer supported. To align with these changes, FileWave 15.5 now supports Account-Driven User Enrollment (ADUE), enabling organizations to securely enroll BYOD devices using this new workflow.

When/Why

When to Use

- BYOD Environments: When employees use their personal iOS or iPadOS devices for work purposes and need access to corporate resources.
- Transitioning from Profile-Based Enrollment: As profile-based User Enrollment is being phased out, organizations should begin migrating to Account-Driven User Enrollment to ensure compatibility with future iOS and iPadOS versions.

Why This Feature Matters

Apple aims to enhance the security and privacy of BYOD deployments. Account-Driven User Enrollment offers several benefits:

- Improved Security: Separates personal and corporate data more effectively, protecting user privacy and corporate assets.
- Simplified Enrollment: Users can enroll their devices by signing in with their Managed Apple ID, streamlining the enrollment process.
- Modern Authentication: Utilizes OAuth 2.0 and OpenID Connect for authentication, providing a more secure and standardized method.
- Organizational Control: Shifts the responsibility of secure enrollment to the organization, allowing for better compliance with internal policies.

Account-Driven Enrollment relies on the Well-known URI mechanism for Mobile Device Management (MDM) discovery, ensuring that devices can locate the MDM server securely and efficiently.

How

Enrolling a Device Using Account-Driven User Enrollment

To enroll an iOS or iPadOS device using Account-Driven User Enrollment with FileWave 15.5:

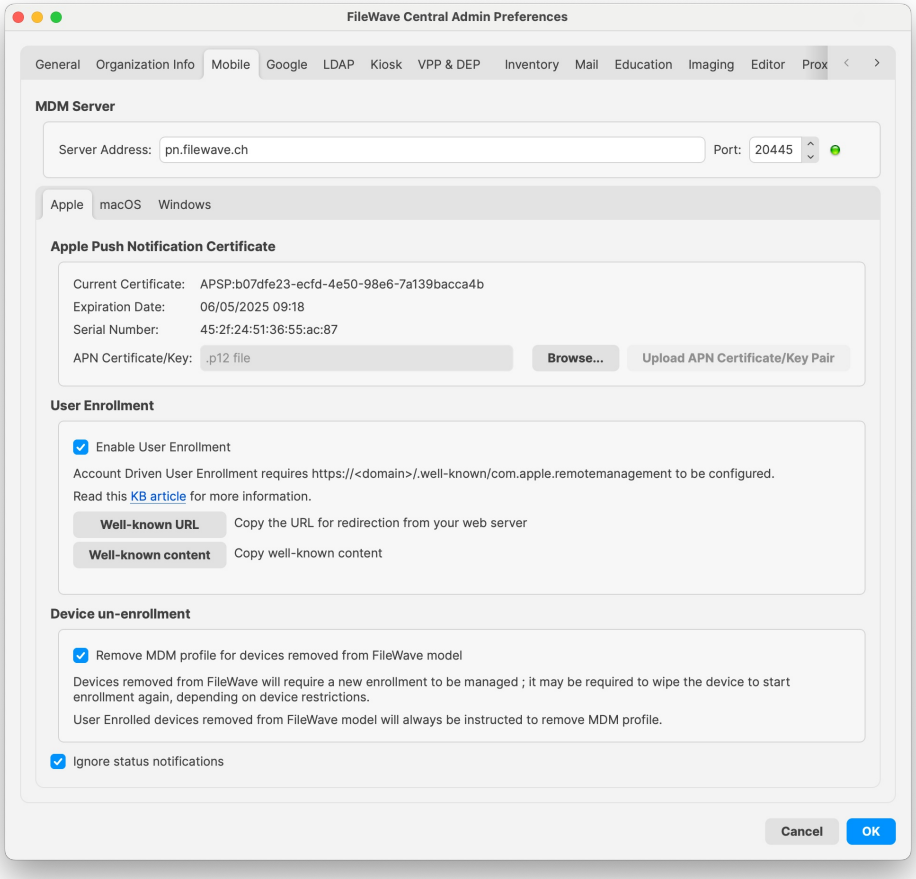
- On their iPhone or iPad, the user navigates to Settings > General > VPN & Device Management and taps Sign In to Work or School Account.

The email entered is used by the device to discover the MDM server. For example, if you enter “pn@widget.ch”, the device queries the widget.ch domain, specifically at https://widget.ch/.well-known/com.apple.remotemanagement.

This endpoint must return a specific JSON message containing all the information required to proceed with MDM BYOD enrollment. Therefore, organizations must have control over this URL, which could be an issue for those who completely outsource their website management (see below for potential workarounds).

FileWave Setup

The existing User Enrollment option in FileWave now enables both legacy BYOD and the new Account-Driven Enrollment (ADUE):



FileWave cannot manage your domain but provides some helpful options:

1. Retrieving the Well-Known Content (JSON):
   - If you prefer to host the required file yourself, you can easily obtain the necessary JSON content from FileWave.
   - Click the “Well-known content” button in the FileWave interface. The following JSON will be copied to your clipboard:

     ```
     {"Servers": [{"Version": "mdm-byod", "BaseURL": "https://pn.widget.ch:20445/ios/byod/enroll/"}]}
     ```

   - Create a file containing this JSON and serve it from your web server at the appropriate URL (https://yourdomain/.well-known/com.apple.remotemanagement).
2. Setting Up a Redirection to the FileWave Server Endpoint:
   - Alternatively, you can configure your web server to redirect requests from https://yourdomain/.well-known/com.apple.remotemanagement to the FileWave server endpoint.
   - Retrieve the endpoint URL by clicking the “Well-known URL” button in FileWave. For example, the endpoint might be:

     ```
     https://pn.widget.ch:20445/ios/byod/well-known/
     ```

   - Consult your web server documentation for details on setting up the redirection. For instance, to configure Apache, add the following directive inside the VirtualHost section:

     ```
     RewriteRule ^/.well-known/com.apple.remotemanagement https://pn.widget.ch:20445/ios/byod/well-known/ [R=301,L]
     ```

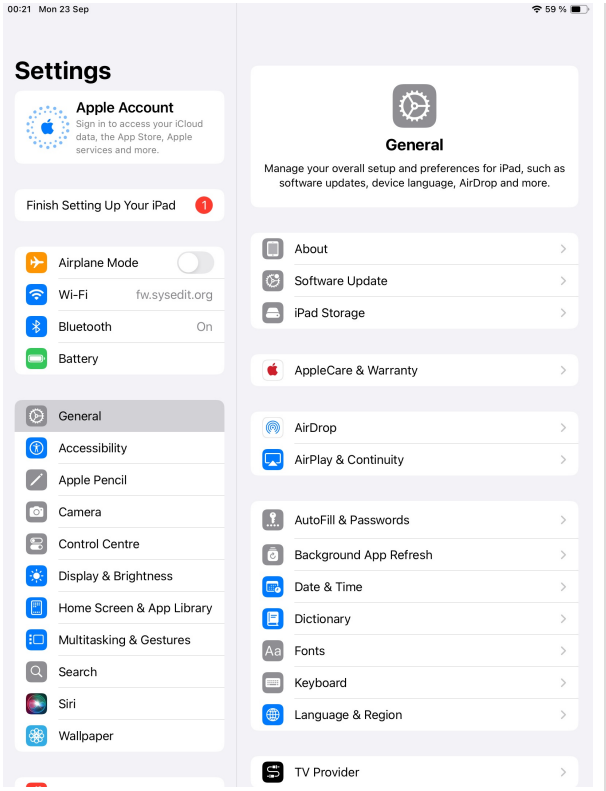
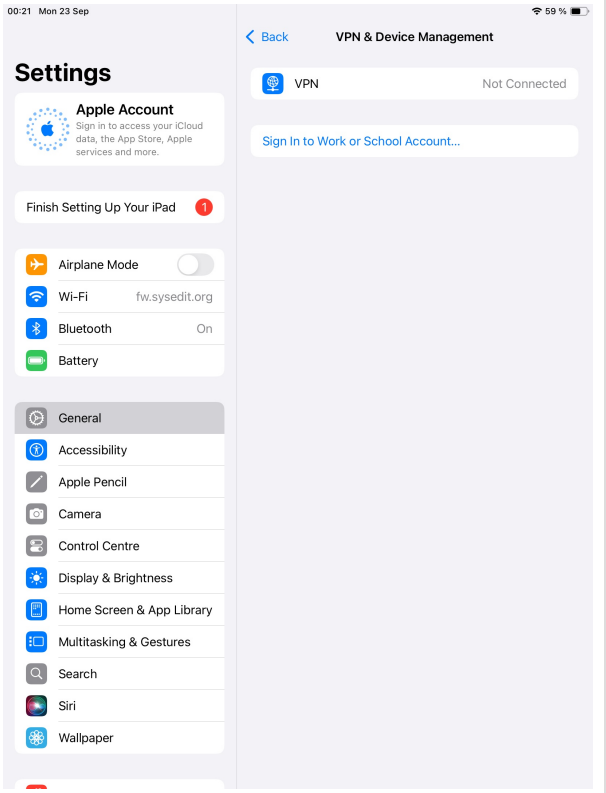
Related Content

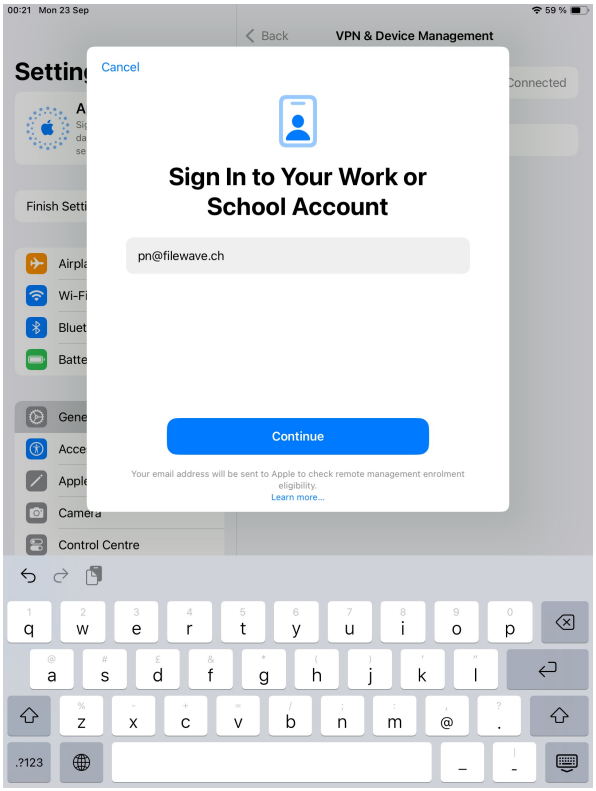
- Apple: User Enrollment and MDM
- Well-known URI
- Apple MDM Enrolment Methods

Digging Deeper

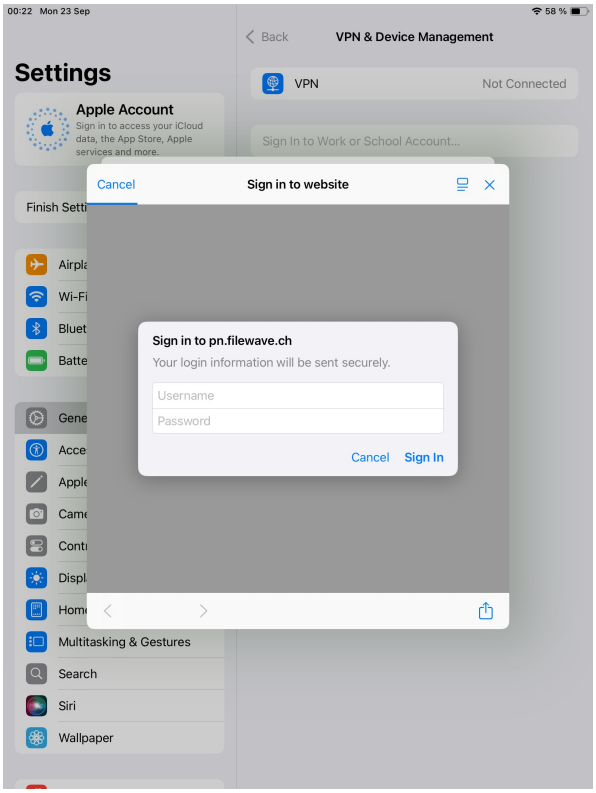
Device Enrollment Process Workflow

Navigate to Settings, General	

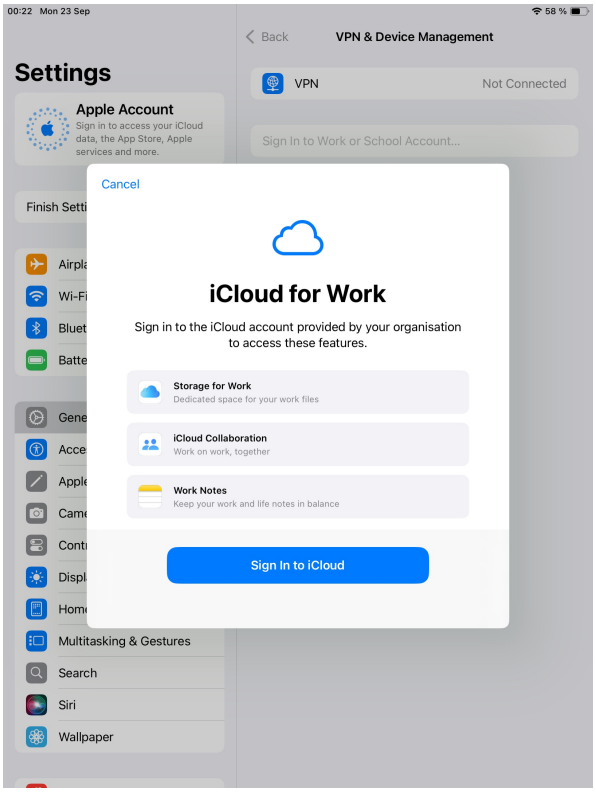
	
Navigate to VPN & Device Management	
Tap Sign In to Work or School Account...	



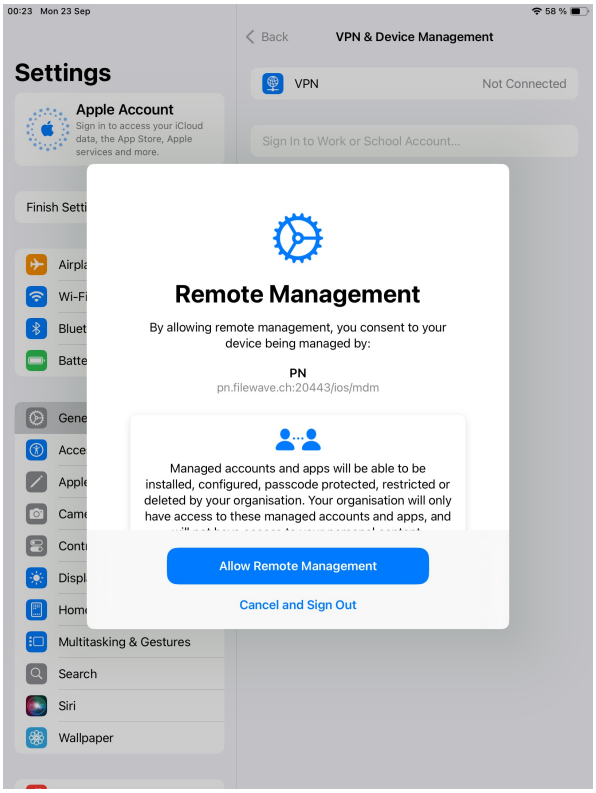
Enter your Managed Apple Account, press Continue.

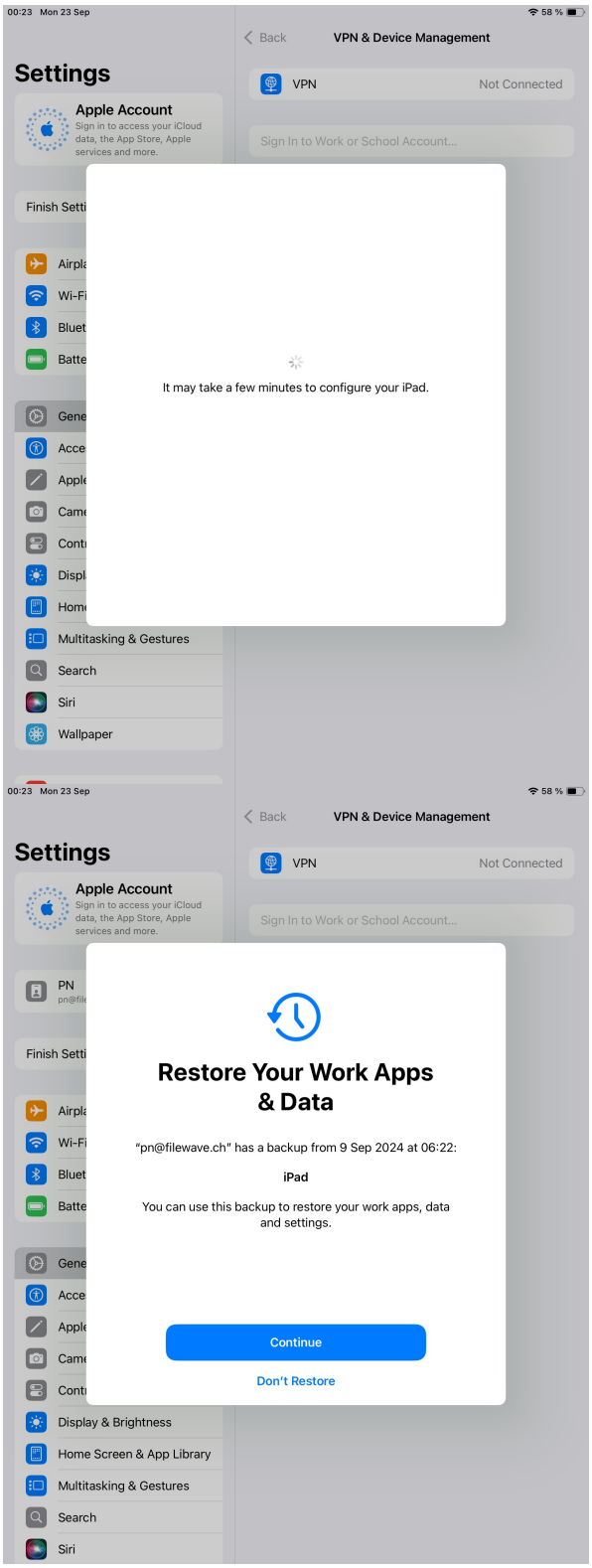


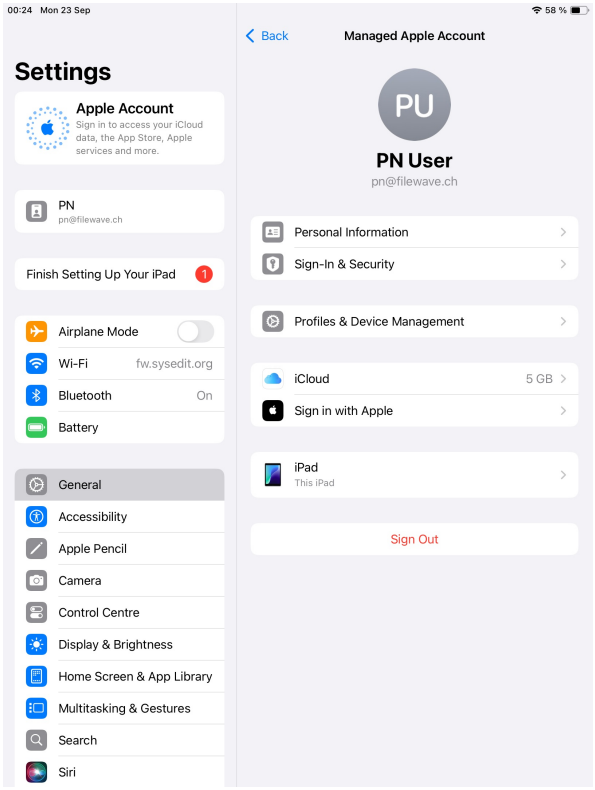
The device will now display the standard authentication page if configured; IDP login is also supported. Enter your credentials and tap Sign In.



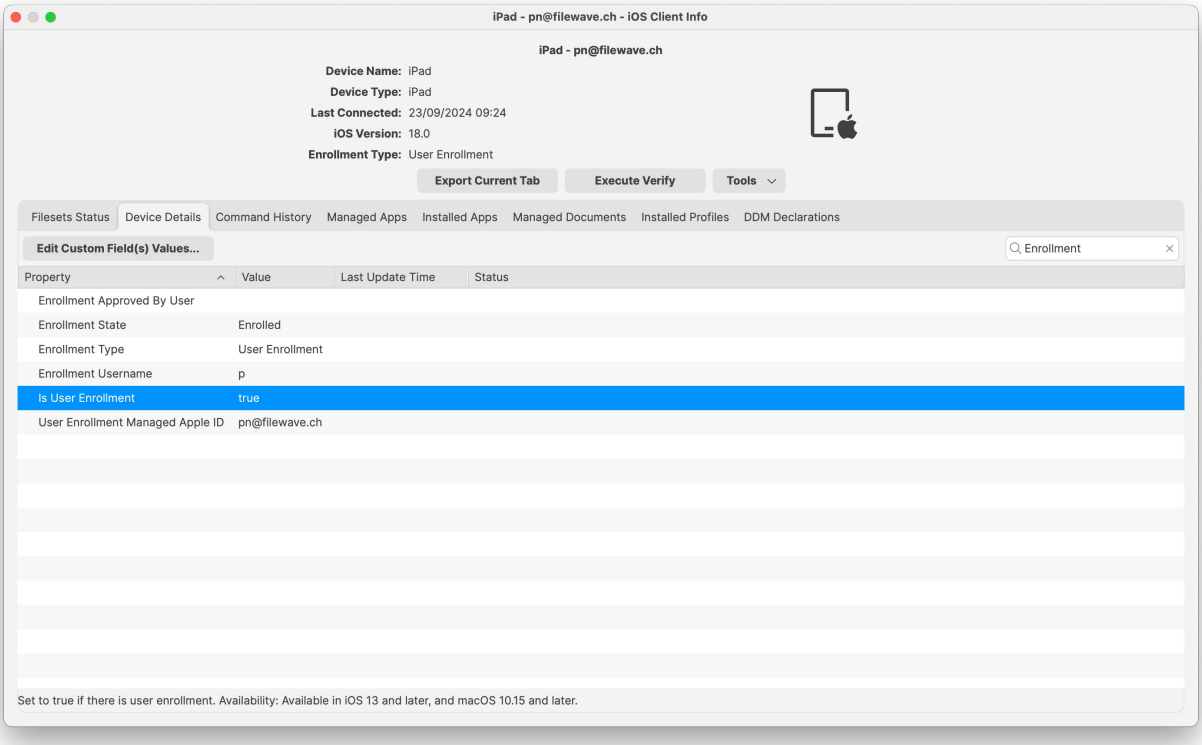
After a few seconds, the device will prompt you to sign in to iCloud. Tap the button and enter your Managed Apple ID password.



And then, press Allow Remote Management to start enrollment.	

After enrollment, device may prompt to restore iCloud data.	

Now the device is ready. As a final step, you need to add the device to FileWave. It will appear in the “New Mobile Client” dialog, or it will be automatically added to the model if Auto-Enrollment is enabled.



Managing BYOD User Enrollment

What

You have no doubt gotten used to managing supervised iOS devices, where you have the ability to manage most elements of the device. If you have previously had folks do a manual OTA enrollment, then you know you have less management of those devices than those that are supervised. BYOD user enrolled devices take that a step further, and even fewer capabilities exist (but for good reason).

When/Why

If you are going to utilize BYOD enrollment, it is because the devices to be enrolled actually shouldn't be managed by you, but they should have the ability to leverage the organization's resources. So, with BYOD enrollment, you can distribute VPP apps and licenses:

- An important feature provided through the Managed Apple IDs is the deployment of apps and media via VPP
- For User Enrollment, FileWave will automatically register and associate VPP users for each associated VPP asset on demand (because the licenses can't be associated to the device)
- Configuration profiles, like email settings and VPN settings are supported (to ease customer setup)

But there are also restrictions to management:

- No access to device-identifying information (e.g. serial number, universal device identifier (UDID), IMEI, or mac addresses)
- No access to personal data
- No access to personal apps (no taking management or removing)
- Limited control capability (no remote wipe, no restrictions, device is not supervised so no profiles requiring supervision)
- Not all profiles are supported (profiles that restrict the user are largely not permitted, e.g strict passcode requirements, configurations that proxy network traffic, restrictions that block content)

How

Once the devices are enrolled, associations for content are managed like you are used to, but there is one important (and helpful) change to the way FileWave is managing VPP license assignation. So please make sure and check out the article linked below on VPP License/Association Changes

> You may be saying to yourself: "If I have to assign these licenses to the user, doesn't that mean I'll have to create VPP users in FileWave and invite them?" And the answer to that is thankfully, no. For User Enrollment, FileWave will automatically register and associate VPP users for each associated VPP asset on demand.

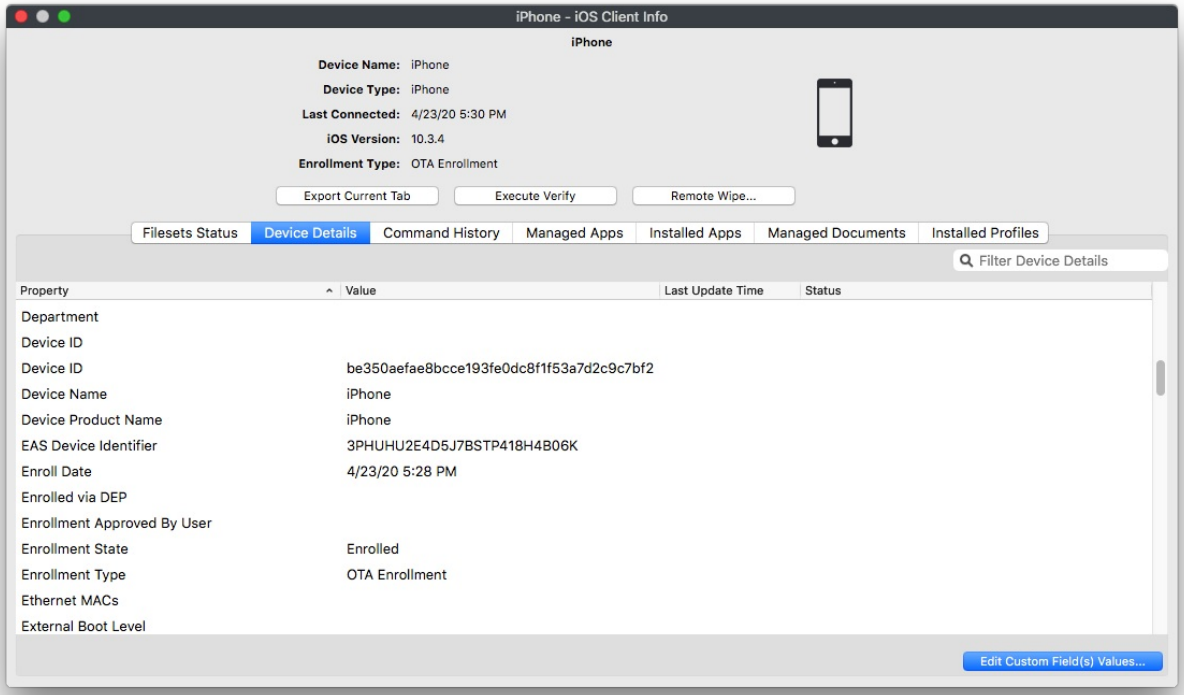
New Inventory Item -- Enrollment Type

What

There are now several methods of enrolling devices into FileWave and a new inventory field has been created to record the enrollment method.

When/Why

This field can be helpful when assigning content to devices. The field in question is called Enrollment Type as you'll see below:



How

There is nothing special about access the item...you can do it in any query or smart group, but the following are the breakdown of the values for the field:

Displaying information	Description
Enrollment via APK	Device was manually enrolled via installation of FileWave application
Enrollment via EMM_API	Device was enrolled via the Android Management API (through NFC or a QRcode)
OTA Enrollment	Device was enrolled over-the-air
User Enrollment	Device was enrolled BYOD
DEP Enrollment	Device was enrolled via Apple DEP
Enrollment via fwcld	Device was enrolled via fwcld
Enrolled	Enrollment of Chromebook
User approved enrollment	Device was enrolled over-the-air and approved by user
Presumed DEP Enrollment	Device is supervised iOS client that was enrolled before v14. "Presumed DEP" because there is no absolute concrete criteria to determine if it is DEP or Apple Configurator.
Not available	Enrollment type is not determined

Troubleshooting

Apple ID prompt still appears even when Activation Lock Bypass Code is used during Remote Wipe

PROBLEM

When executing a Remote Wipe against a Supervised iOS 7.1+ device and the "Remove Activation Lock" option is checked, the expected behaviour is that on activation of the iOS device, the AppleID username and password will not be required. Instead, the stored Activation Lock Bypass code (FileWave Admin> Assistants> Activation Lock Management...) should be used to remove the Activation Lock. In some circumstances, we have experienced that the username / password dialog is still presented to the user.

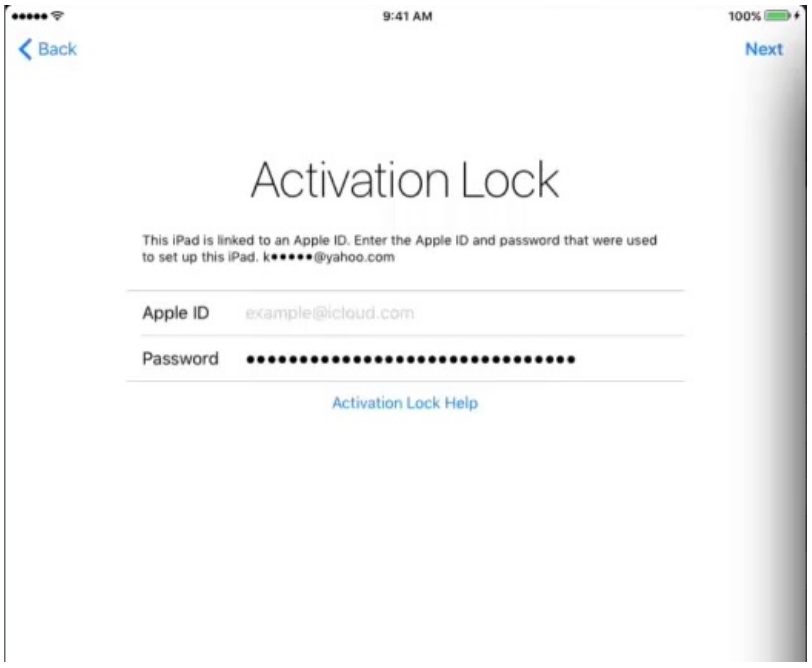
ENVIRONMENT

- iOS Supervised Devices
- FileWave MDM

RESOLUTION

Instead of entering the username and password in the dialog presented on the iOS device after the Remote Wipe command executes, enter the Bypass code for that device (found in FileWave Admin> Assistants> Activation Lock Management...) in the password field. Enter the code exactly as it appears in the Activation Lock Management dialog, as the code is case sensitive and also requires the dashes.

Keep the username (Apple ID) field empty.



ADDITIONAL INFORMATION

- Use Mobile Device Management and Find My iPhone Activation Lock

FileWave iOS Kiosk (IPA) Location Tracking Problem

We have been made aware of an issue with our FileWave Kiosk Enterprise IPA app with regard to location tracking. Simply put, iOS no longer allows our application to be approved once, and then allowed to collect geo-location information for all time.

Even when location tracking for the app is set to "Allow While Using", the application will re-prompt for permission on each application restart (usually multiple times).

We are currently investigating what changes will be required to make the Kiosk IPA less intrusive to your customers and will update here as we have more information. In the mean time, here are some mitigation suggestions:

1. Don't deploy the Enterprise IPA at all:
   - This may seem an odd suggestion, but this application was initially developed before the concept of "Lost Mode", and has largely outlived it's purpose
   - "Lost Mode" is much more effective at location lookup, because it doesn't suffer from the same pre-requisites that the IPA does, and it works even if the end-user has location services turned off
   - "Lost Mode" does not require the IPA
   - Outside of geo-location in "Tracked" mode, the IPA serves no other purpose, and tracking in this mode is delicate to manage at best, and largely ineffective since the user can disable it at any time
   - Apple, and other privacy advocates, are heavily leaning away from this type of location tracking, and before long it may not be possible at all
2. If you don't want to change how you are deploying the IPA currently, consider setting your devices to "Untracked"
   - The issue of user prompts is only seen if FileWave believes the device is in a "Tracked" state
   - By moving devices to "Untracked" you'll avoid customer complaints while we work on a possible fix for this issue

iOS 12+ Profile Installation Failed

Description

On attempting to enrol iOS 12 devices, we have seen some instances of the profile installation failing. In these cases it has been related to the server certificate. As of iOS 11 and macOS High Sierra, Apple introduced stricter rules regarding MDM server to device communication:

https://support.apple.com/en-gb/HT207828

However, it appears that these have not been fully implemented, until iOS 12, with respect to certificates. Certificates of RSA key sizes below 2048 have still managed to work on iOS 11. iOS 12 no longer allow this.

> Self-Signed Certificate
> As 3rd party suppliers have been supplying appropriate keys now for some time, this is likely to impact Self-Signed Certificates only.

Directions

The following command may be used to check the certificate RSA key size.

macOS, Linux:

```
openssl x509 -in /usr/local/filewave/certs/server.crt  -text -noout | grep Public-Key
```

Windows

```
C:\OpenSSL-Win64\bin\openssl.exe x509 -in C:\ProgramData\FileWave\FWServer\certs\server.crt -text -noout | FINDSTR
Public-Key
```

Windows does not have openssl installed as standard so you will need to go to https://slproweb.com/products/Win32OpenSSL.html and download the appropriate version of OpenSSL for your environment.

If the output is anything less than 2048, then the server certificate will need to be updated.

If you are using a Self-Signed Cert, you will need to either:

- Re-use your process for generating the certificate to update to ensure it has a RSA key size of 2048 or larger
- Consider moving to an official 3rd party certificate

Please take into consideration the following KB when moving to a new certificate: Root Trusted SSL Certificate (Using and Renewing)

Customising iOS Wallpaper

Customizing iOS Device Wallpaper with Dynamic Text

What

FileWave v14.10.0 introduced a new feature that allows customisation of wallpaper on iOS devices. This feature enables the additions of wallpaper text and with FileWave's parameters within Profiles, a single generic profile can be used to display Serial Number, Department and Assigned User, simplistically on all devices.

When/Why

Some suggestions of using text with wallpaper include:

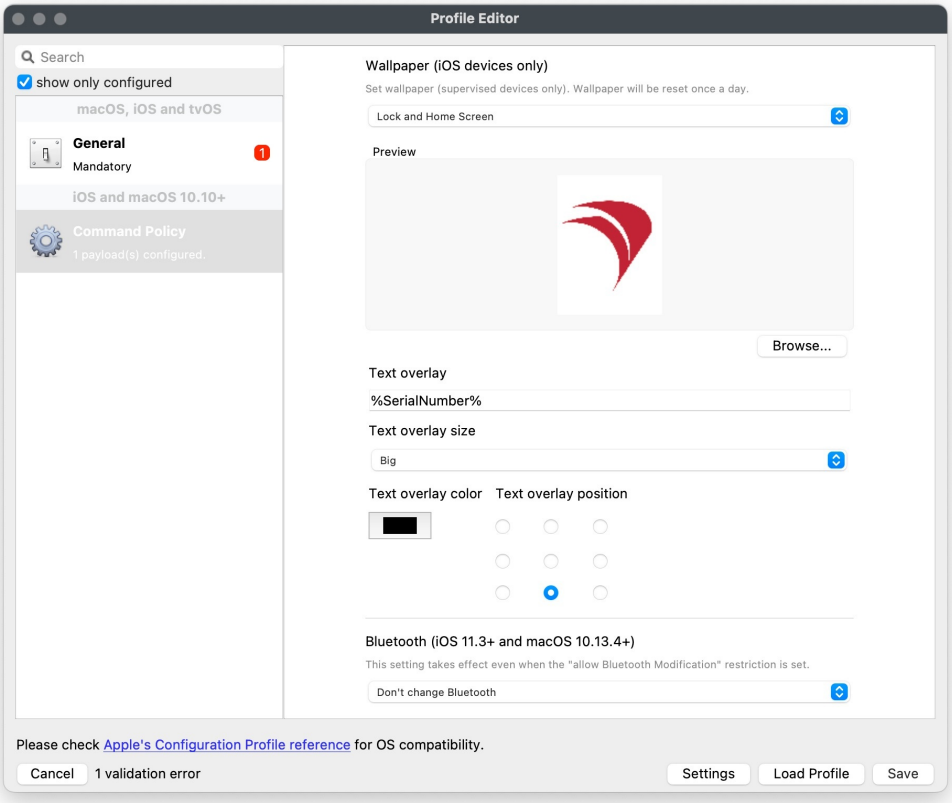
- Personalizing the device for an organization, department or individual
- Identifying a device with its unique Serial Number, which can be helpful in tracking and asset management
- Providing additional information that may be useful for the end-user or technical support team
- Displaying room names for wall mounted tablets outside meetings rooms, lecture theatres and hospital surgeries.

How

To utilise this feature in FileWave v14.10.0:

- Log in to your FileWave console.
- Create a new iOS Profile.
- Select the Command Policy item from the left list of profile types.
- In the Command Policy, add the desired text, e.g. Department, Telephone Number into the 'Text overlay' box.

Note this example demonstrates the use of a parameter to supply the device's Serial Number.



- Save the configuration and apply it to the chosen, targeted iOS devices.

It's that simple! Now your iOS devices will have a customized wallpaper that displays the information configured.

If the image's aspect ratio doesn't match the device's screen resolution, iOS or iPadOS will resize the image which may lead to portions of the image being cropped.

⚠ Even where an images resolution matches the screen resolution in one orientation, when rotated between landscape and portrait, this can no longer be the case. The consequence is a resize of the image, also leading to cropped edges.

The Text is burnt into the image and as such, if not placed with consideration, could also become cropped. Test the outcome of the image with text in both Portrait and Landscape.

Digging Deeper

Extensive details of image sizes with text placement and its impact is highlighted in:

- Custom iOS Wallpaper Dynamic Text Tips

Referencing parameters within all profiles (which can now be used to personalise the text on the wallpaper since FileWave v14.10.0) is also described in:

- Using parameters in iOS/macOS Profiles

Custom iOS Wallpaper Dynamic Text Tips

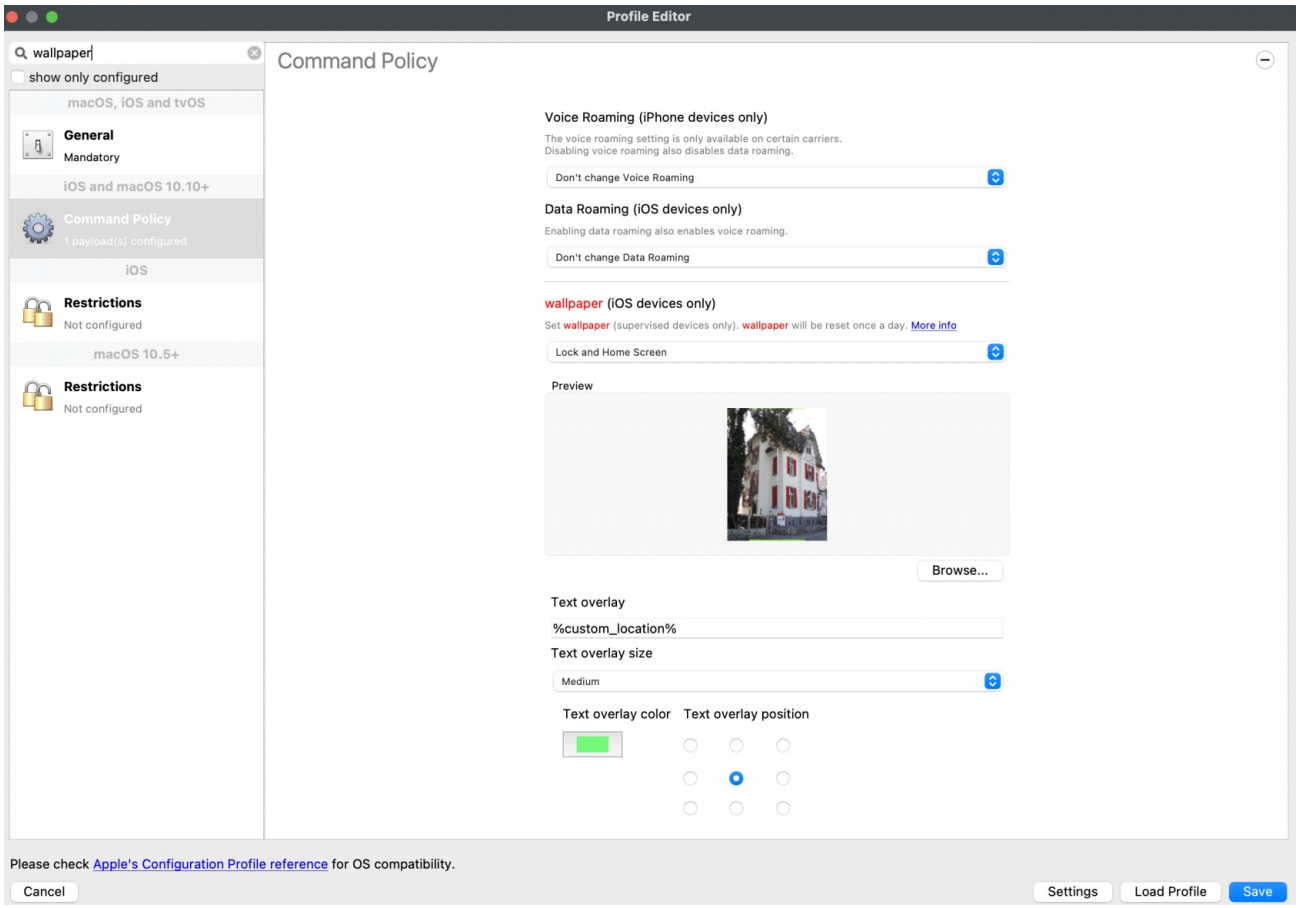
What

Consideration of the size and where to place the text being added to an Apple mobile device's Wallpaper.

When/Why

When adding text, there are 3 Font size options, plus 9 possible locations for placing text.

Note, the preview is portrait, but this is not necessarily how the image will appear on the device.



The Font used is GothicA1-Regular and the sizes refer to:

	SMALL	MEDIUM	BIG
FONT SIZE	65	80	95

> Image uploaded to FileWave must be smaller than 2MB to add text, to help protect against undue heavy load on the server.

How

Consider the devices currently managed. An image of the correct size should be required for each different device screen aspect ratio. Unfortunately, MDM cannot retrieve screen resolution from devices, but each device type resolution can be observed at the following:

https://www.ios-resolution.com/

Alternatively, a tool like Mactracker lists details for all Apple device types.

Smart Groups

Since a Wallpaper Profile Command Policy will be required for each screen resolution, devices need to be targeted appropriately.

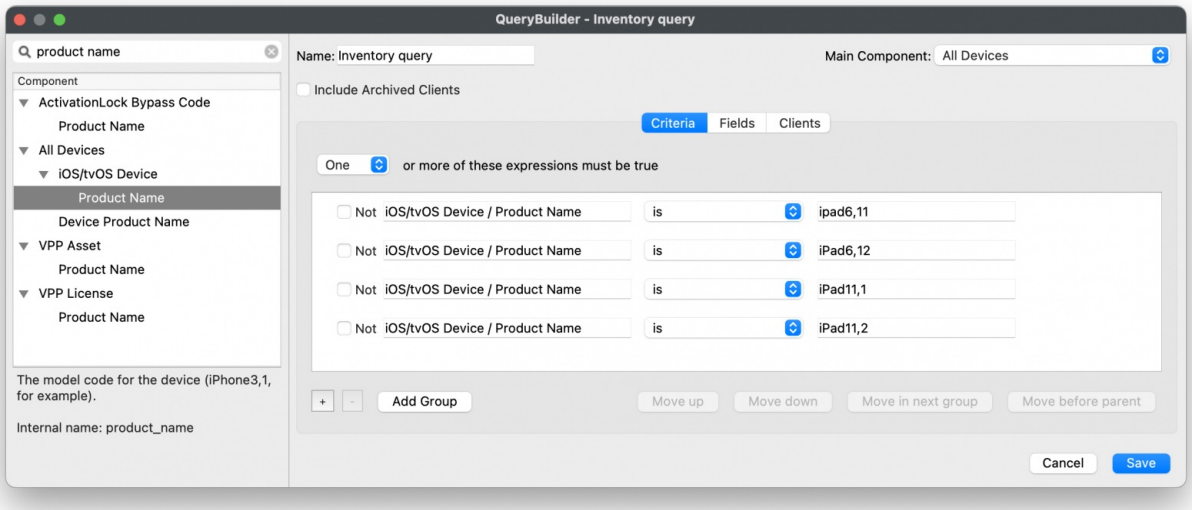
Consider the following method:

Obtain the Product Name for a device type to be managed (e.g. iPad6,11). Cross reference this with something like Mactracker to obtain details.

- Create a New Smart Group
  - Type: Inventory Query
  - Criteria: Product Name > is > iPad6,11
  - Group Name: (Something obvious)

> It may be sensible to include the screen resolution as part of the group name, but not use the Product Name. There is overlap with device types and resolution. E.g. both 'iPad 6th Gen' and 'iPad mini 5th Gen' have a resolution of 2048x1536, so one group could be used to target both device types. Example group name: iOS 2048x1536

Example of multiple device types for the Smart Group which all share the same resolution. Note the 'one or more expressions must be true' and the 'Main Component':



Copy the above process for each required resolution.

Image Preparation

Although there is an options to set the colour of text, complex images may hinder the visibility of the text. Image levels could be altered before uploading to FileWave. However, wouldn't it be better to test this first.

Additionally, text position can be of consequence, since devices may be rotated between portrait and landscape and the image will adjust accordingly. This will have the appearance of a cropped image, either at the sides or top and bottom, which in turn could crop the text.

Before commencing, download the Font and use Font Book to add the Font.

The following walkthrough should help assist with pre-planning the image and text visibility. Taking the above 2048x1536 as an example. The chosen starting image is:

FileWave Building

JPEG image - 1.2 MB

Information Show More

Created	Yesterday, 23:04
Modified	Yesterday, 23:04
Last opened	Yesterday, 23:04
Dimensions	2048×1365
Resolution	72×72

Note this image is currently the wrong resolution. Preview.app can be used to address this landscape image:

1. Open the image in Preview
2. Proportionally alter the height (which is currently too small) to match the height (y value in this example) of the device's screen resolution with the Adjust Size Tool. The image is now oversized, but will more than fill the entire screen in one axis and match in the other. (In this example, the height should now be 1536 and the width greater than 2048)
3. Zoom out so the entire image may be viewed
4. Select All
5. Move one of the sliders of the selection area, in this example left or right, until it reads 2048.
6. The selection can then be moved to the desired area

Copy this selection, open into a new Preview window and save.

Add an outline:

1. Alter the size of this new image, such that the smaller axis is set to match the larger. In this case alter 1536 to 2048
2. There will now be an image that is 2732x2048. Make a note of these values and undo.
3. Open Keynote
4. Select the Document button and alter the Document Slide Size to match this newly observed resolution: 2732x2048
5. From a blank slide, add a rectangle and remove the colour fill
6. Add a border line to the rectangle, choosing an obvious colour (for example bright green) and 5pt width should suffice
7. Alter the size of this rectangle, such that it matches the reverse dimensions of the device: 1536x2048
8. Centre the rectangle within the slide
9. Copy the rectangle
10. Alter the size of the new copied rectangle to match the resolution of the entire slide and centre: 2732x2048
11. Edit the Master Slide so that it has no background
12. Export the slide as a PNG with transparent background
13. Open the exported image into Preview
14. Resize the image, matching the resolution back to the target resolution, in this case: 2048x1536
15. Select All from Preview and Copy
16. Back in Keynote, create a new document and alter the slide size to the desired screen resolution: 2048x1536
17. Add the desired matching sized image to the slide, in this case the 2048x1536 FileWave building image
18. Paste the copied green boxes from Preview over the top

In Keynote there should now be an image, including the green inserted boxes, something like:

Since the green lines forming the boxes have a transparent background, the image behind may be altered, simplifying the testing of differing images.

Consider duplicating slides to test alternate images, in case the desire to revert is experienced!

Test Text

Keynote may now be used to test adding some text.

- Add a text box
- Set the Font as Gothic A1 Regular and a desired Font size, e.g. 80
- Select a colour for the Font
- Add the chosen text, ensuring it does not cross over the lines when centred

If the text does cross the lines, the smaller Font size of 65 could be chosen or reduce the amount of included characters.

If using variables, confirm the longest value from FileWave and then test with that value as text in Keynote

From Keynote, if the text is unclear, it is easier to adjust the text colour or even make adjustments with the image itself, to enhance the appearance of the text.

Once happy, copy the line of text.

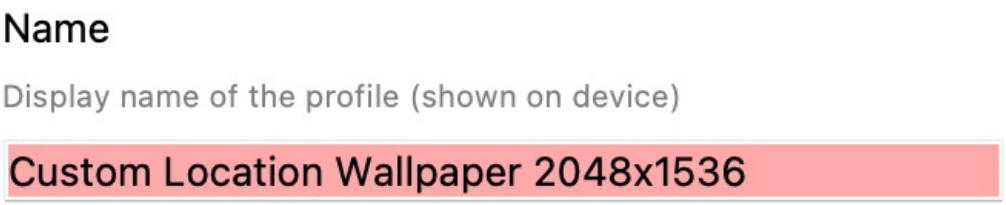
Create Fileset

Remove the text from the Keynote slide and save the slide as an image, using JPG (smaller size). Remember, the image to be uploaded needs to be less than 2MB.

Open up the Profile Editor in FileWave and search for Wallpaper, it should be located in the Command Policy. As per the directions in the prior KB article, choose the image just saved as the Wallpaper and paste the desired text into the text box. Clearly, alter the text to include any parameters if necessary. Don't forget to set the Font colour.

As per this example, the middle position is going to be chosen.

Save the profile and consider including the screen resolution as part of the name:



Test

Associate the Profile to a test device and Update Model, observing the Command History. The IntsallProfile command should appear and then disappear; this is not a permanent profile, but a one off command. However, the Settings command will persist. Further details in the following KB:

Profile Editor Command Policy

Turn the screen to confirm the look for both Portrait and Landscape.

Portrait


16%
Tuesday 19 September
05:58
Bruce Theatre
1
St. Gallerstrasse
filewave
Press Home to unlock
Device ID: 5e968b7947d74f064eb47ee2bcbbb67cb87eb133 Client Name: GCTV8F5THLF9

Landscape

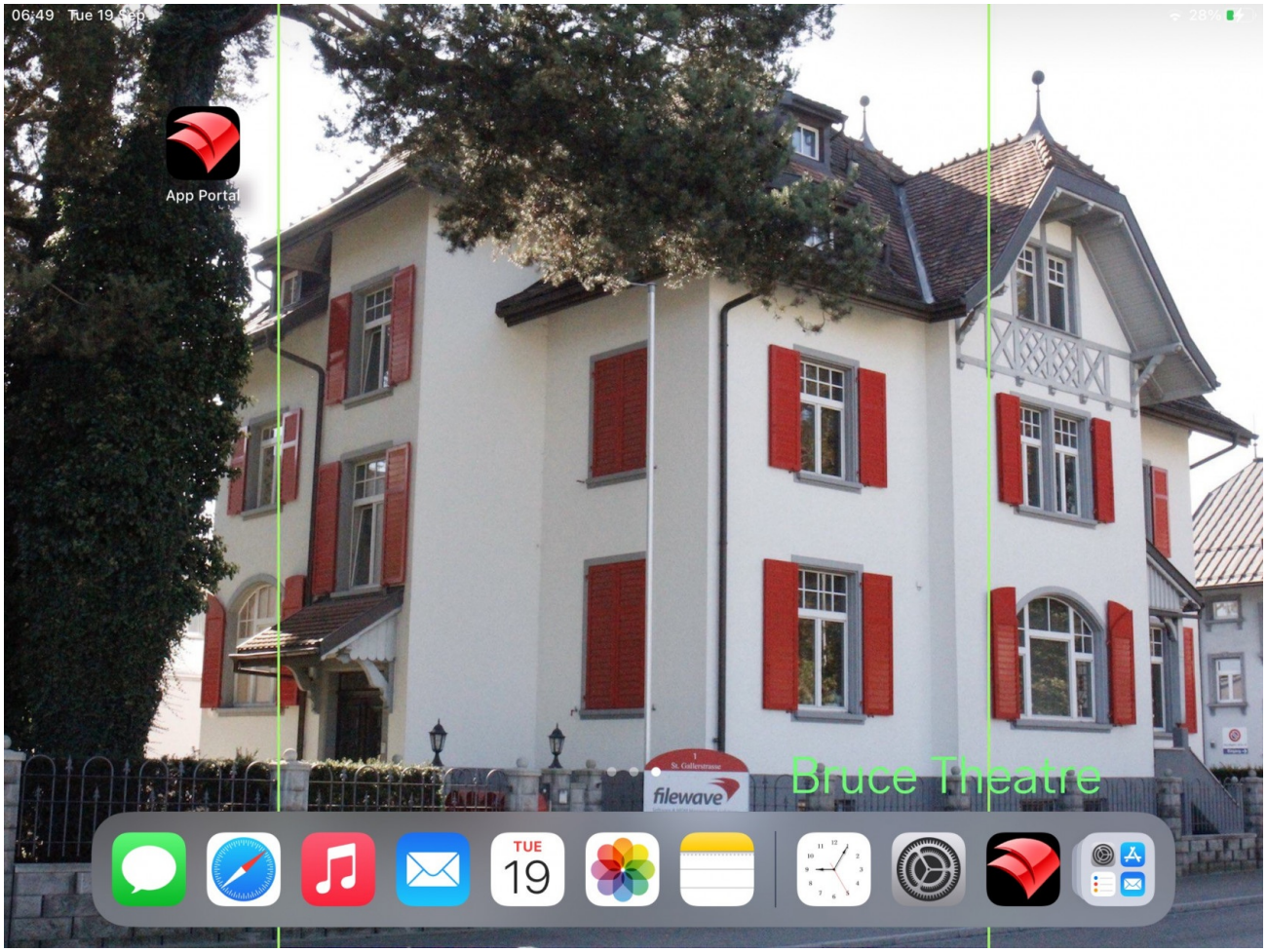
Additional Info

First, it is worth observing how Apple alter an image when the device is rotated between Landscape and Portrait.

Apple avoid having black bars around the image. As such, to alter the image, as can be seen above, The smaller, un-matching aspect is resized to match the size of the device's resolution. The impact of this is that the large matching aspect is now oversized and the overall effect is the image appears cropped.

The green lines from the image above show the crop position that will be seen in portrait when the device is turned from landscape. This has a consequence with the text. If the text position were bottom right instead, for example, the green box shows the text that would be lost:

Landscape



Portrait

Indeed, rotating the device into portrait shows the loss of text:

With this in mind, best practice would be:

- Where devices may be rotated
  - For a landscape image, only ever consider using Middle, Top Middle or Bottom Middle
  - For a portrait image, only ever consider using Middle, Left Middle or Right Middle
- Where devices will not be rotated
  - Any position could be chosen

Apple do not provide an option to prevent rotation, however, in some circumstances devices will not be rotated, e.g. wall mounted outside meeting rooms, lecture theatres, hospitals, etc.

Conclusion

Why use the profile, since the above has just made an image of the correct size and Keynote could have just added the text?

This is indeed a good question and the above is to assist with a guide on building out the image, ensuring that the text will display clearly and not be cropped on the image size. Chances are once you have done this for one resolution, that you need not bother for others and will already be armed with a good approximate example. However, the Profile still comes into its own!

The Profile can use parameters from FileWave, customising the text per device, based either upon built-in inventory or Custom Fields. This greatly exceeds the above method and is very much the beauty of this feature.

App Security on iOS

Description

Experienced being in a meeting and needing to pass an iOS device to someone else, but with the knowledge that there is sensitive data in some Apps or some Apps that not should be accessed at all?

To prevent temporary users of devices from accessing certain Apps, Apple introduced two new concepts: Hide and Lock.

- Allowance of Hiding Apps was introduced in iOS 18
- Allowance of Locking Apps was introduced in iOS 18.1

Hiding an App prevents the App from being visible, whilst Locking an App disallows the opening of a Locked App without an additional layer of security, e.g. Touch of Face ID. Hidden Apps are available from a visible folder called 'Hidden' within the App Library. Access to the Hidden folder and opening Locked Apps is by way of authentication.

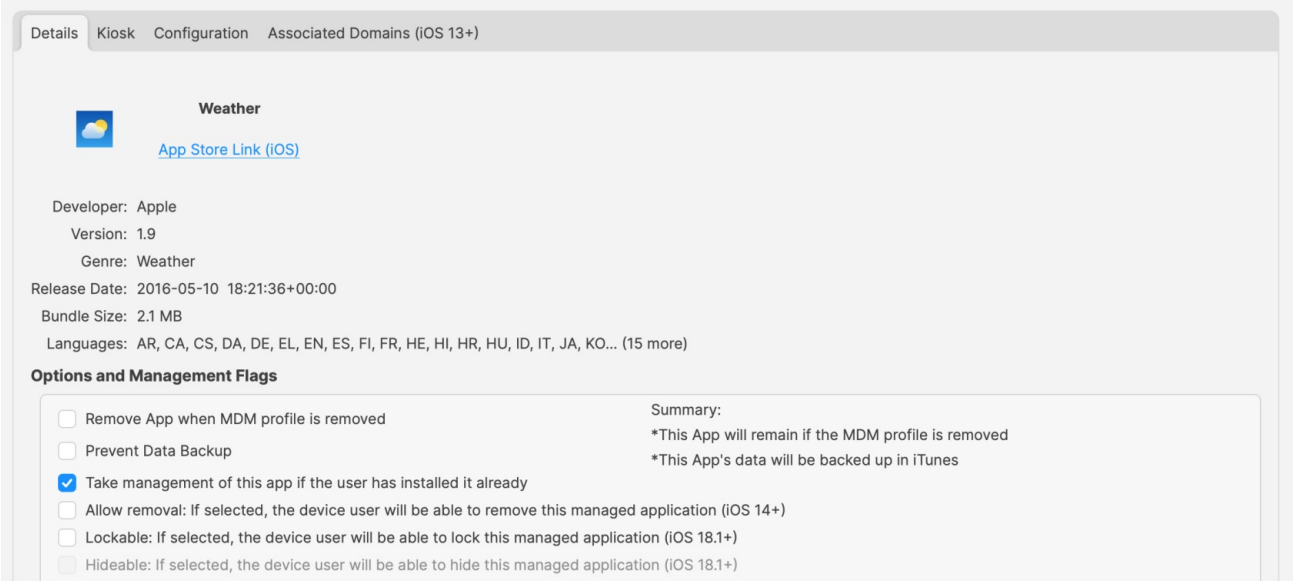
Further information may be viewed in Apple's KB: Lock or hide an app on iPhone

FileWave 16 included management for this feature.

Information

App Configuration

Each VPP App has two new options, one for Lock and one for Hide, allowing MDM to define Apps, on an individual basis, to be set as Locked or Locked and Hidden:

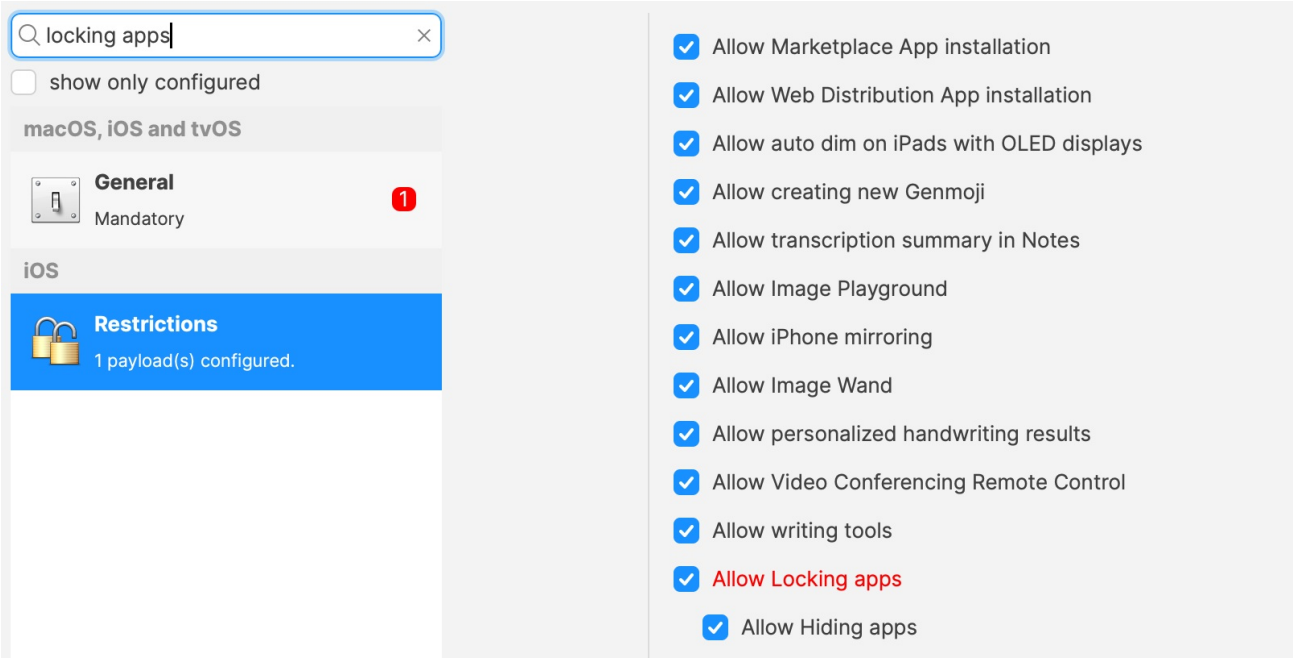


Hideable is only an option where Lockable is enabled.

As per Apple's above linked KB, not all Apps may be Locked or Hidden. Please review their KB for a list of Apps which may not be set.

Profile Configuration

As an addition to the VPP App setting, it is possible to allow/deny users from selecting Apps themselves to be either Locked or Locked and Hidden, by way of additional Profile options, within the iOS Restrictions Payload.


locking apps
show only configured
macOS, iOS and tvOS
General
Mandatory
1
iOS
Restrictions
1 payload(s) configured.
Allow Marketplace App installation
Allow Web Distribution App installation
Allow auto dim on iPads with OLED displays
Allow creating new Genmoji
Allow transcription summary in Notes
Allow Image Playground
Allow iPhone mirroring
Allow Image Wand
Allow personalized handwriting results
Allow Video Conferencing Remote Control
Allow writing tools
Allow Locking apps
Allow Hiding apps