

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](#)

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:

The screenshot shows the 'VPP & DEP' configuration window. The top navigation bar includes tabs for General, Organization Info, Mobile, Google, LDAP, Kiosk, VPP & DEP (selected), Inventory, Mail, Education, Imaging, Editor, Proxies, and Software Update. The main content area is divided into two sections: 'Volume Purchase Program - Apps and Books' and 'Device Enrollment Program - Apple School Manager and Apple Business Manager'.

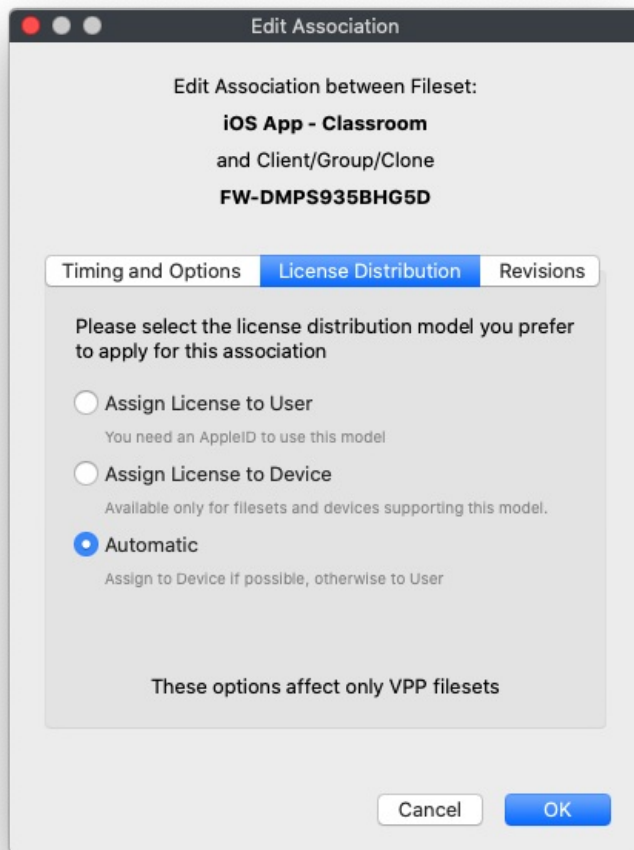
Volume Purchase Program - Apps and Books

- Configure tokens:** 1 token(s) configured
- Synchronize:** Last synchronization with VPP Web service: 8/14/20 2:45 PM
- Configure email invitation template:** (button)
- Minimum delay (in minutes) between license assignment and Install Application:** 0
- Preferred license distribution model to use for new associations:** Automatic (dropdown menu) Assign to Device if possible, otherwise to User
- LDAP synchronization:**
 - ☐ Synchronize with LDAP every: 1 hour(s) Never synchronized.
 - ☐ Automatically associate users via their email address
 - ☐ Send invite emails to newly registered LDAP users

Device Enrollment Program - Apple School Manager and Apple Business Manager

- Download certificate:** (button)
- Configure accounts:** OK: 1 account(s)
- Synchronize:** Last successful synchronization with DEP Web Service: 8/14/20 2:45 PM

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

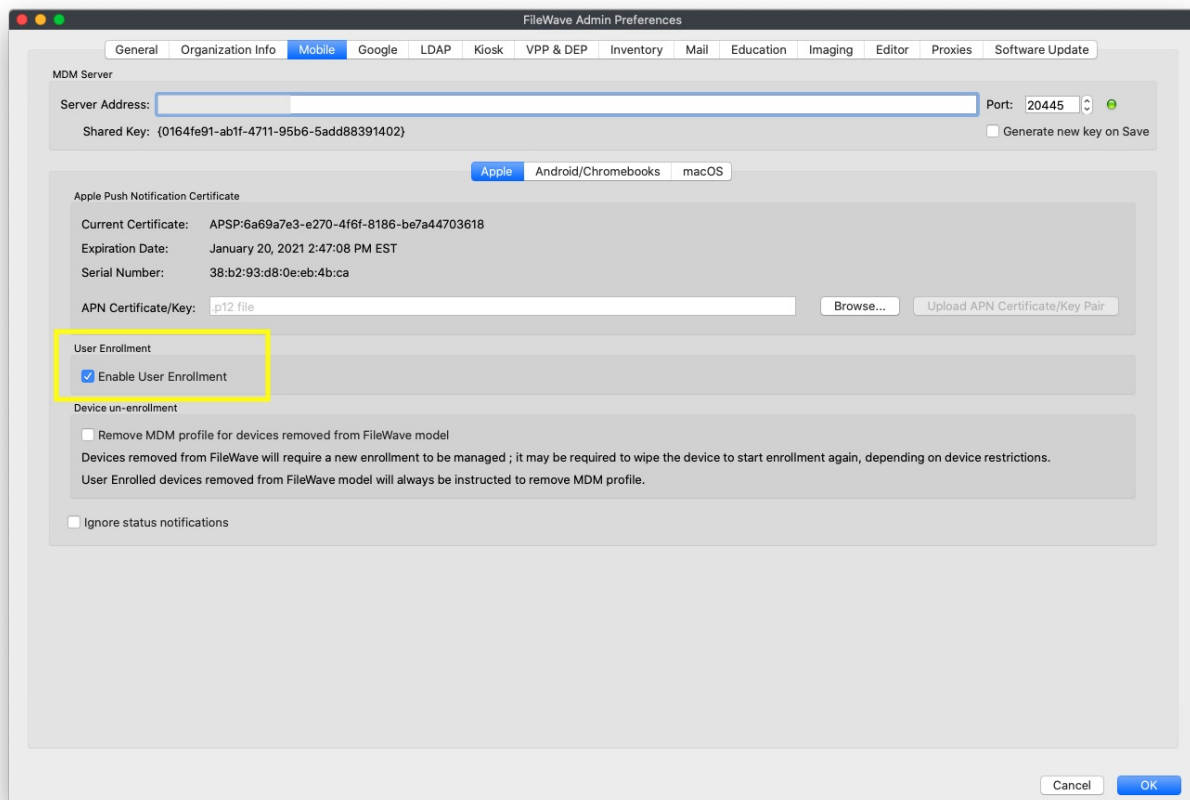
With Version 14(+) of FileWave, you can now BYOD (bring-your-own-device) enroll a device without giving total management of the device to the system admin.

When/Why

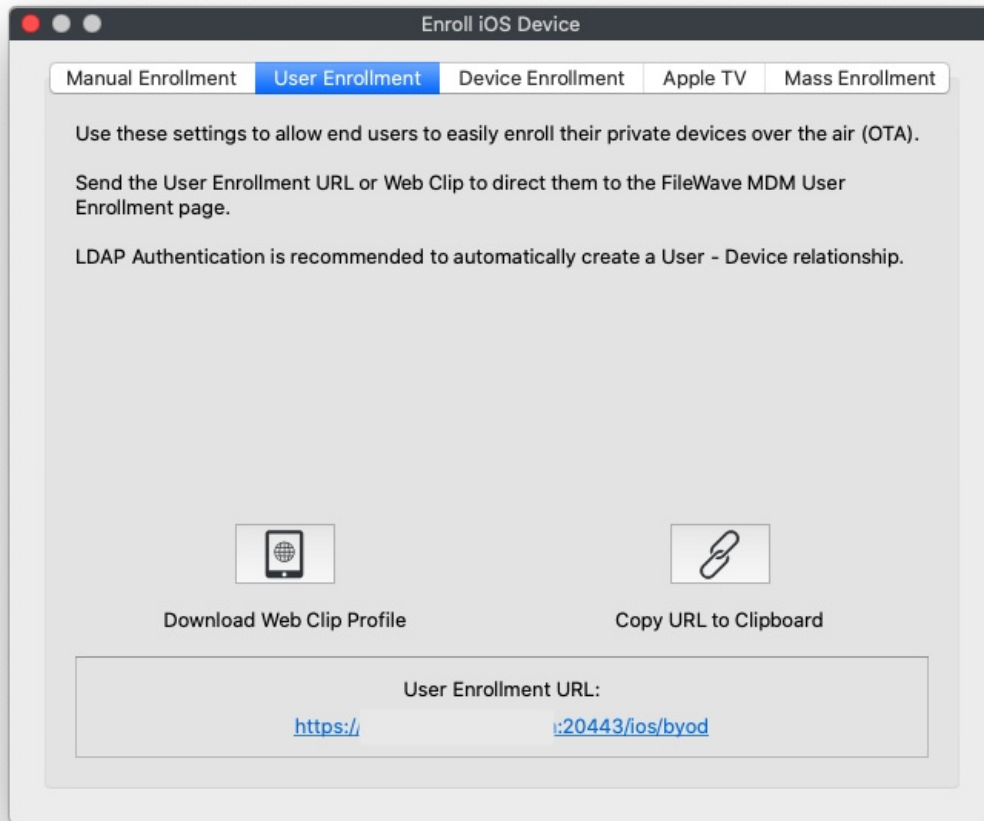
Typically, this option works best if the device to be supported is not company owned. For instance, an employee with their own iPhone may want to BYOD enroll a device to allow distribution of company-owned app licenses, but without giving their company the ability to manage their phone in other ways.

How

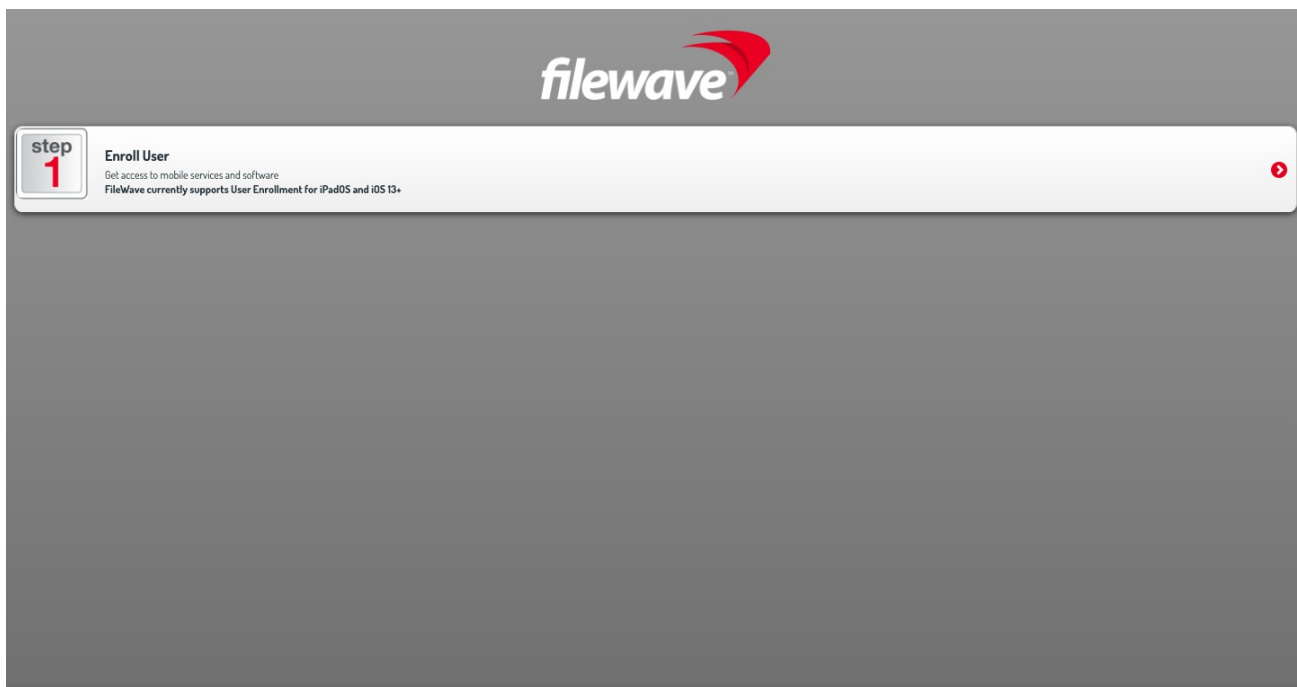
BYOD enrollment is off by default in FileWave, and must be enabled on the Mobile tab in preferences as shown below:



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:



Loading



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.

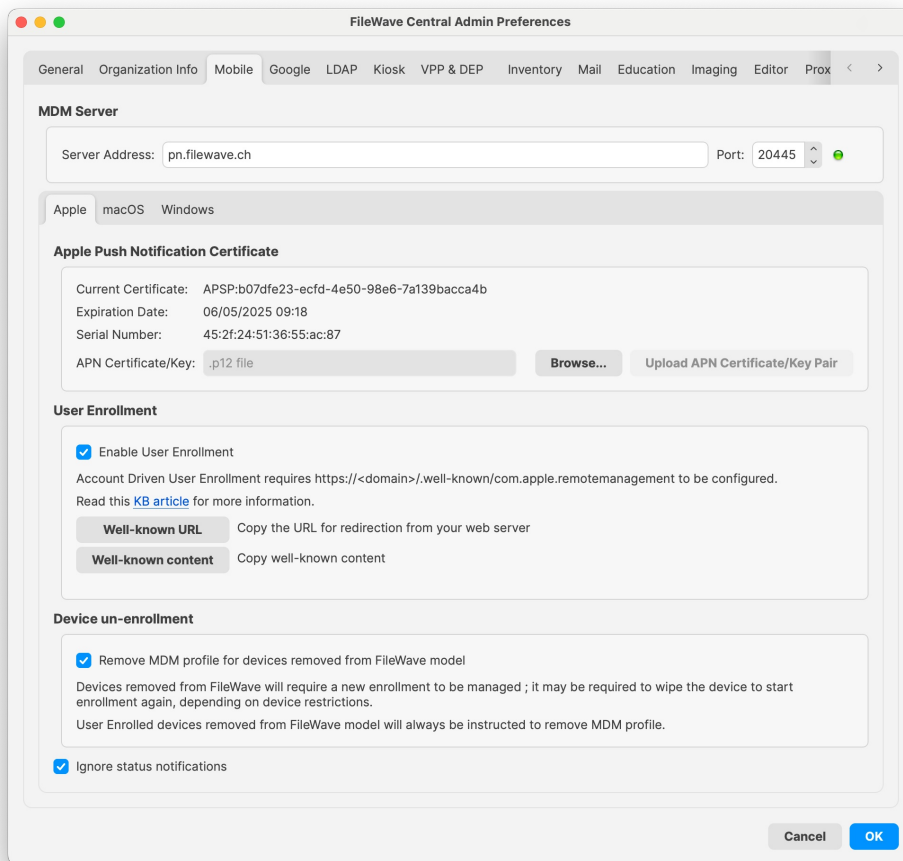


The email entered is used by the device to discover the MDM server. For example, if you enter “pn@widget.ch”, the device queries the widget.ch domain, specifically at <https://widget.ch/.well-known/com.apple.remotemanagement>.

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]
```

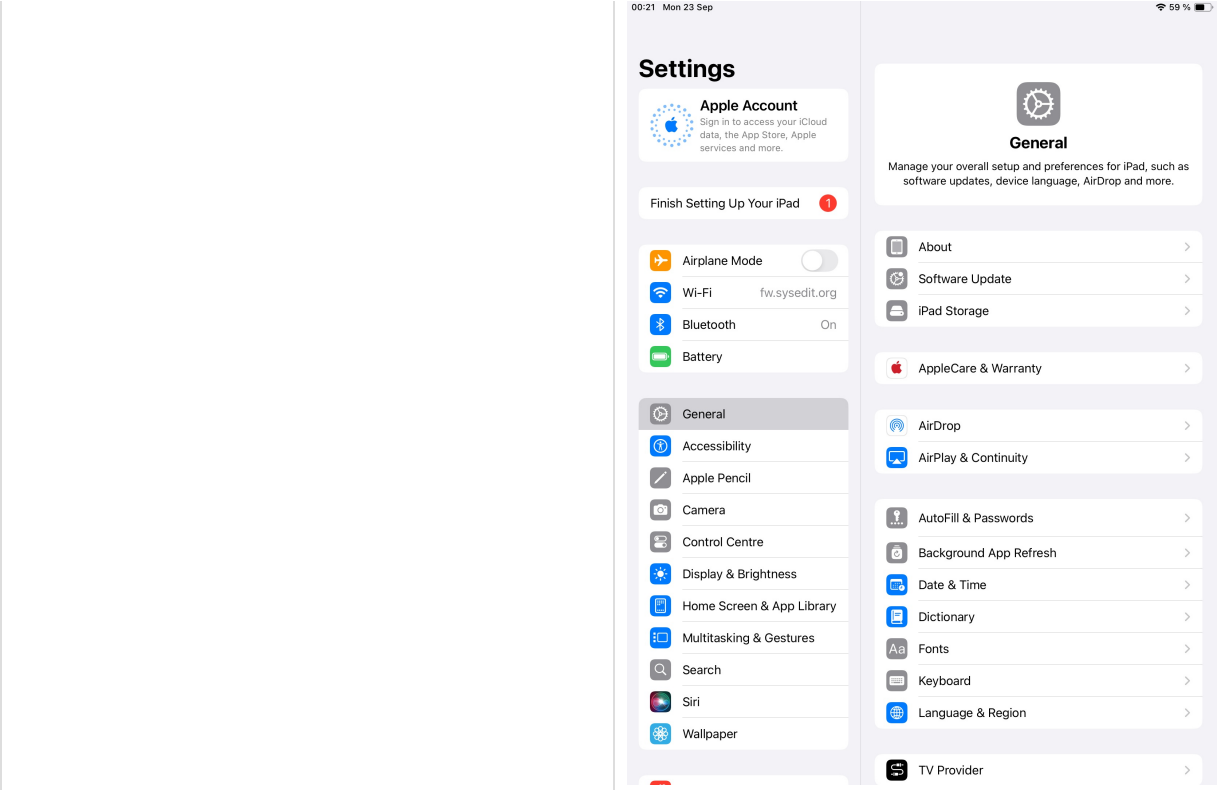
Related Content

- [Apple: User Enrollment and MDM](#)
- [Well-known URI](#)
- [Apple MDM Enrolment Methods](#)

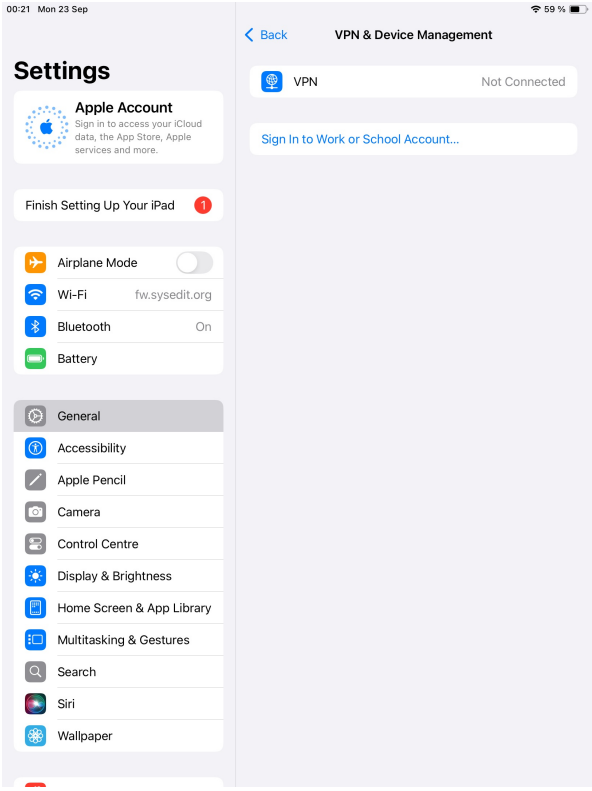
Digging Deeper

Device Enrollment Process Workflow

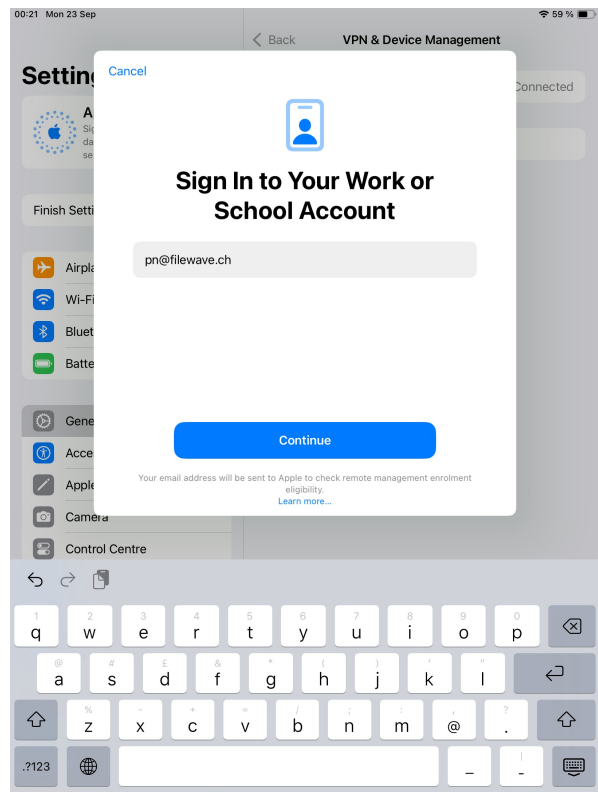
Navigate to Settings, General



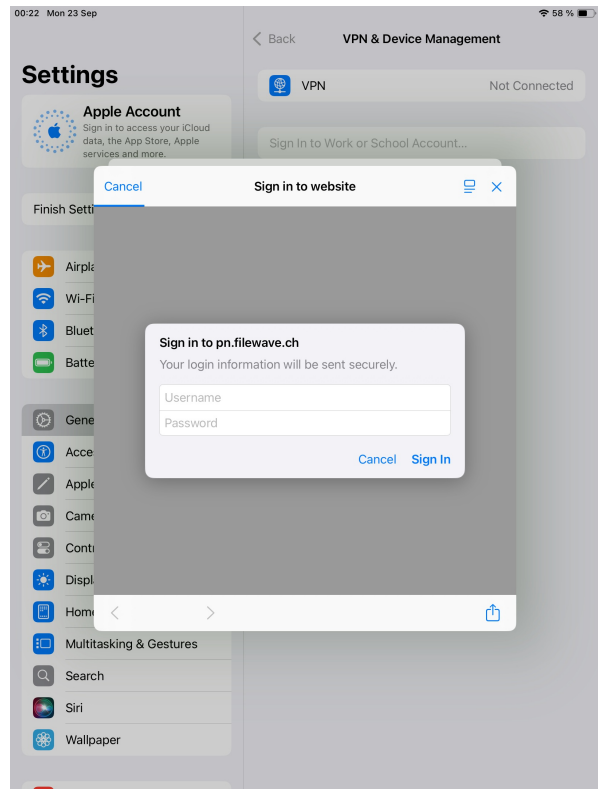
Navigate to VPN & Device Management



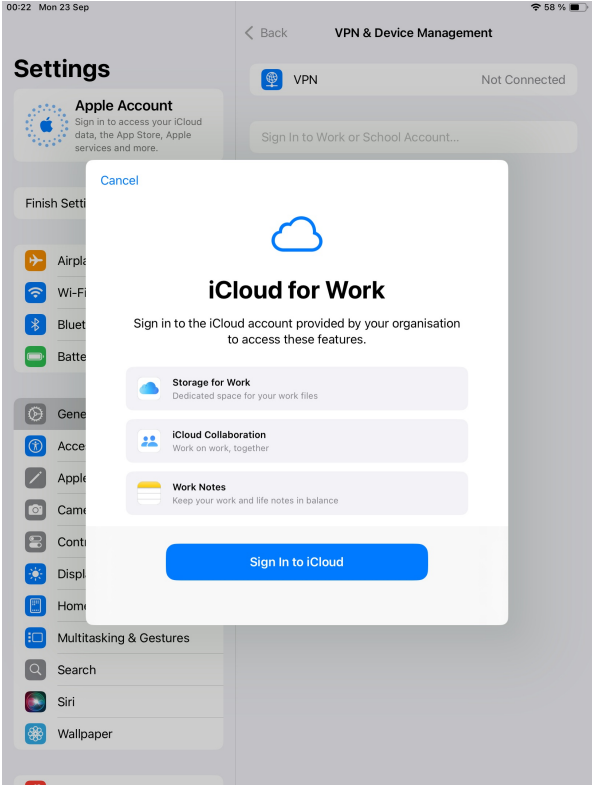
Tap Sign In to Work or School Account...



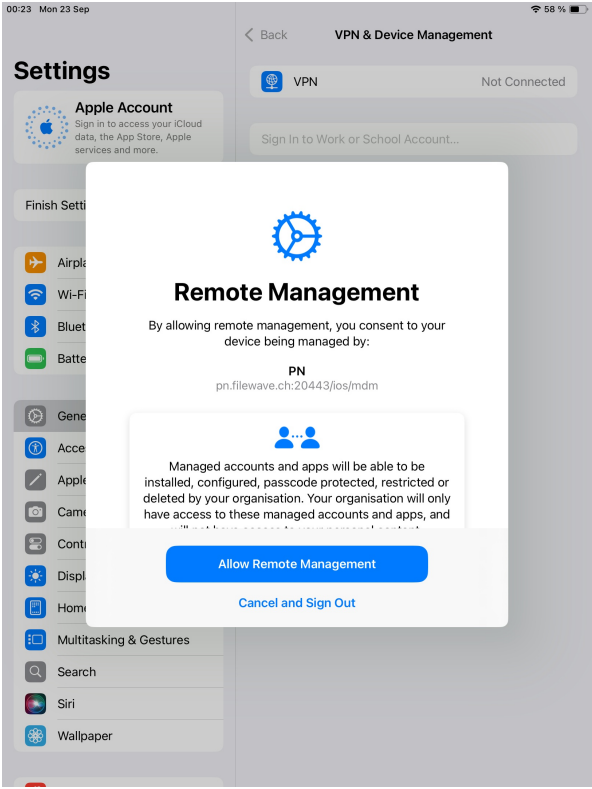
Enter your Managed Apple Account, press Continue.



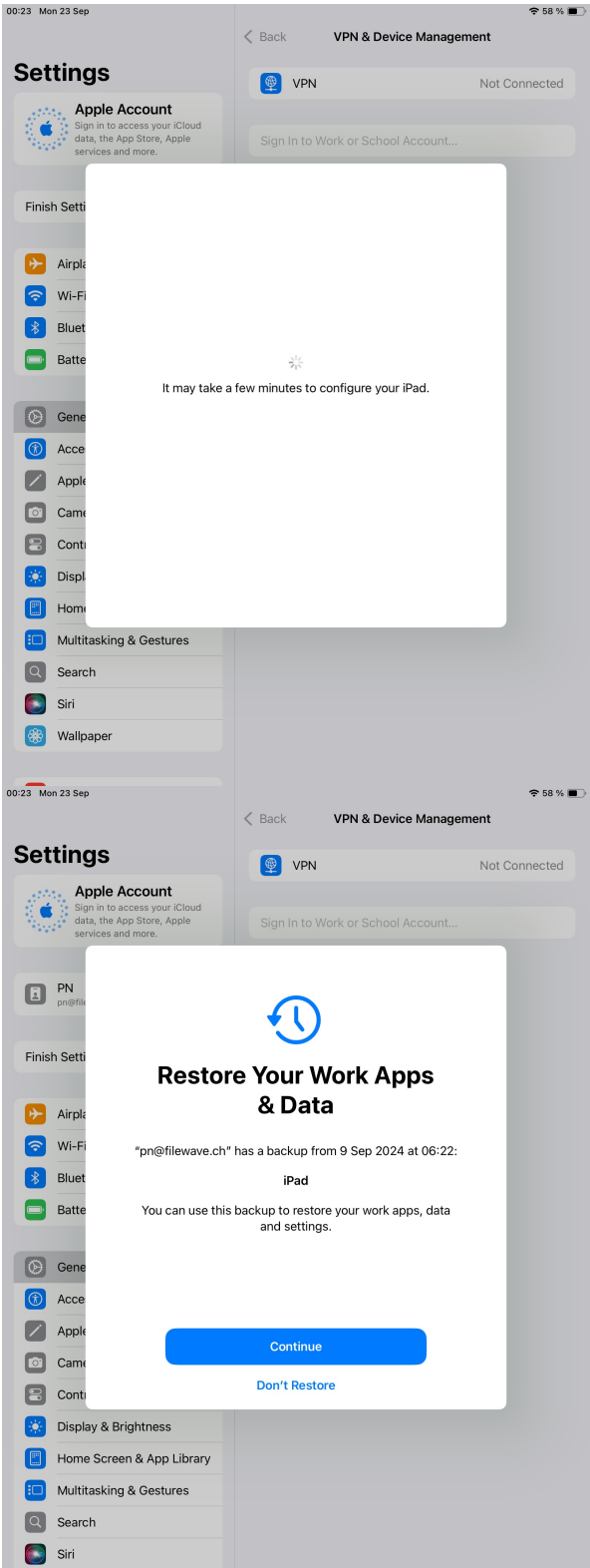
The device will now display the standard authentication page if configured; IDP login is also supported. Enter your credentials and tap Sign In.



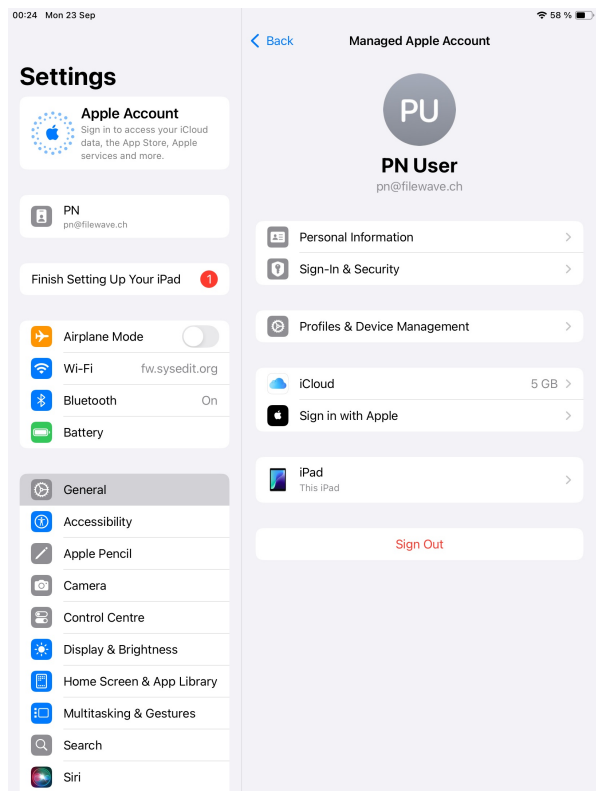
After a few seconds, the device will prompt you to sign in to iCloud. Tap the button and enter your Managed Apple ID password.



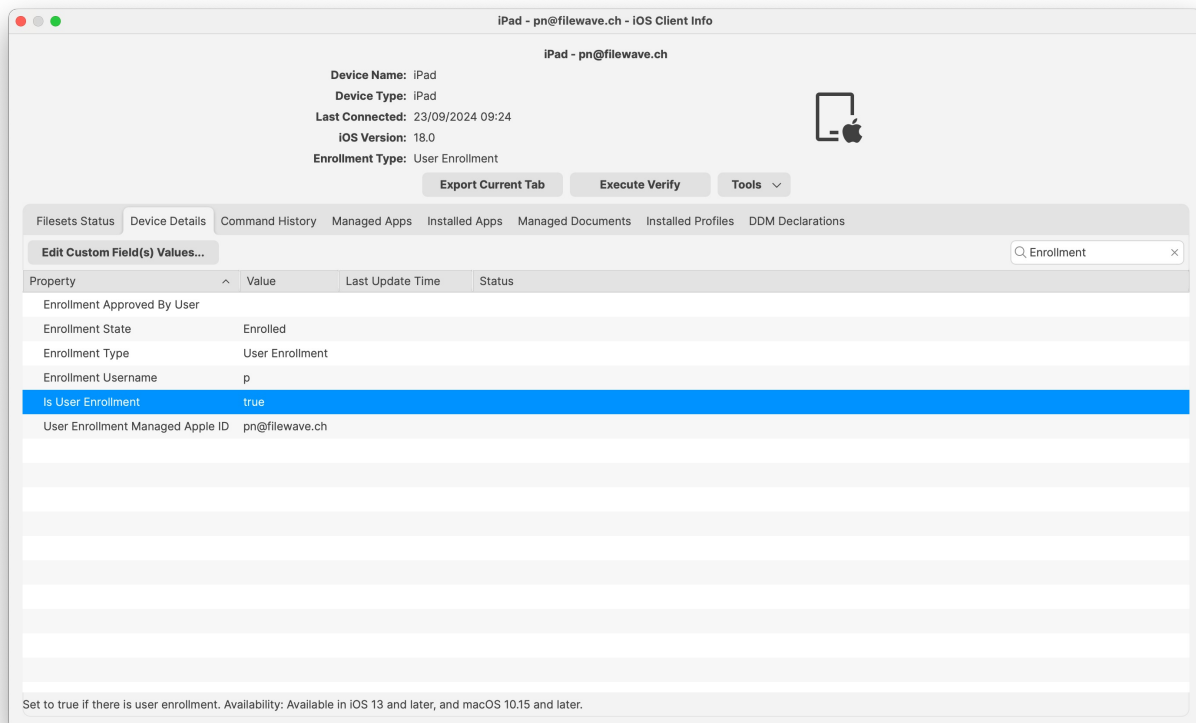
And then, press Allow Remote Management to start enrollment.



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.

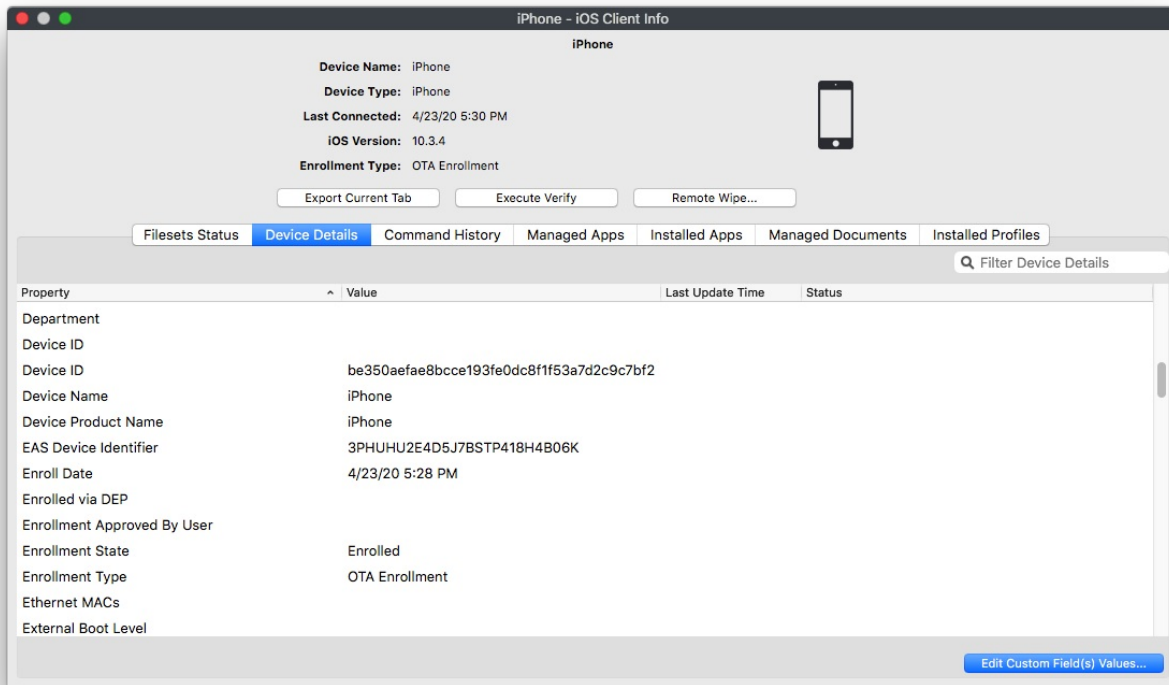
New Inventory Item -- Enrollment Type

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 fwclld	Device was enrolled via fwclld
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