Microsoft Windows MDM

FileWave MDM services can manage Windows 10 and 11 by using the MDM protocol. The built-in management client is able to communicate with a third-party server proxy that supports the protocols to perform enterprise management tasks.

- Microsoft Windows MDM Setup
  - Pre-Requisites of Windows MDM Setup
  - Part 1: Custom FileWave Client
  - Part 2: Setting up Terms and Conditions
  - Part 3: Setting up the Portal App

- Integrating with Windows AutoPilot
- Manually enrolling a device into FileWave Windows MDM
- Reset Windows device through a script (FileWave Recipe)
- Windows MDM wipe command
- Configuration Service Providers (Profiles)
  - Windows MDM Policies (aka Profiles)
  - Windows MDM Software Updates CSP

- Troubleshooting
  - Windows MDM setup issue with custom domain

Microsoft Windows MDM Setup

Integration of FileWave with Microsoft Windows MDM requires some initial setup. This is likely a one-time configuration for your environment, depending on complexity.

On initial setup, we'll need to make sure we can satisfy the licensing pre-requisites, publish a custom FileWave client, set our acceptable use terms, and finally create and configure the AAD MDM application itself.

Pre-Requisites of Windows MDM Setup

What

FileWave can integrate and use the framework of Microsoft Windows MDM to manage Windows endpoints, but there are licensing requirements that need to be satisfied (outside of FileWave).

When/Why

Windows MDM requires certain licenses based on your organization's relationship with Microsoft. As far as FileWave-specific licensing is concerned, each endpoint need only have a FW client license.

How

All Windows MDM function relies on Microsoft Entra Active Directory, so that must be in place for your organization. Specifically Microsoft Entra Premium P1 or P2. Many of their license bundles include that license. Additionally, you'll need AutoPilot access and access to the Microsoft store for business:

Licensing requirements for AutoPilot:

Windows Autopilot licensing requirements | Microsoft Learn

(AutoPilot is the framework that allows your devices to enroll into FileWave when initially setup)

Information on Microsoft Endpoint Management / InTune for Business:

Endpoint Management at Microsoft | Microsoft Learn

Part 1: Custom FileWave Client

What

Windows MDM with FileWave is implemented in a hybrid-mode. That is, we can issue MDM commands (such as installing a policy), but also wish to leverage our native FileWave client capabilities.

When/Why

Our first step in setting up the integration for Windows MDM is to create and publish a customized FileWave client so that our newly MDM enrolled devices will have a functioning FileWave client installed upon enrollment.

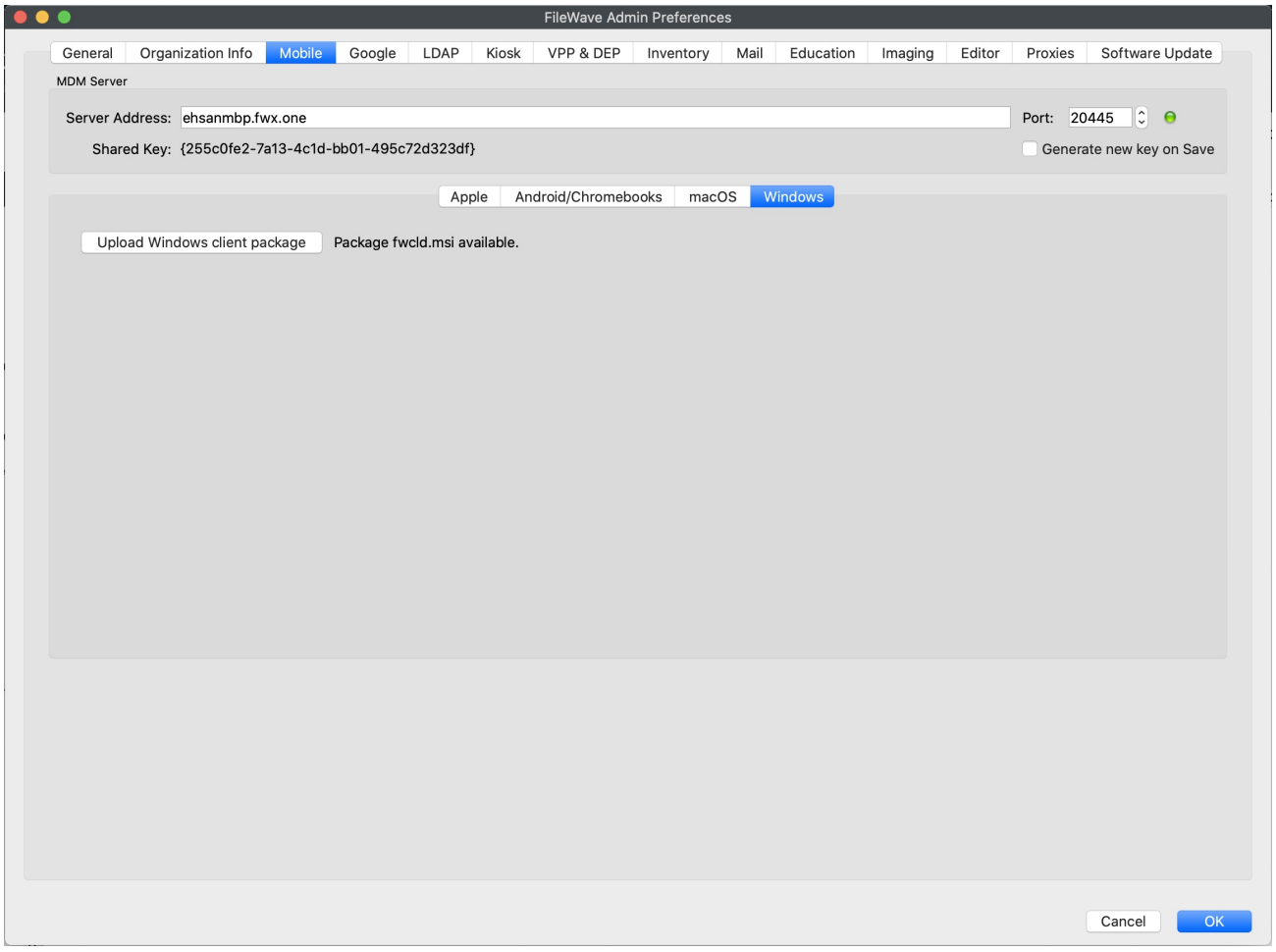
How

> ⚠ Before anything make sure that you have done following steps:
>
> Your FileWave server is running healthy, and backups are being performed.
> You have valid, trusted certificate installed on your FileWave server.
> You have at least saved FileWave preferences once (open preferences in the native admin and save it.)
> This will set important configurations on your FileWave server (shared keys, etc.)
> You have at least updated model once
> This will allow FileWave's internal URIs to be in place.

After you confirmed everything is ok, then you may upload the custom client MSI installer.

Upload fwcld msi package

1. Open the native admin and open preferences.
2. Go to the Mobile tab and look under the Windows sub-tab.
3. Upload your custom client.msi package on that tab as shown below. Create this installer with the Customer Installer Builder.



Part 2: Setting up Terms and Conditions

What

When a device is enrolled in Windows MDM, a custom end-user terms page is required for the Microsoft application we'll be building later.

When/Why

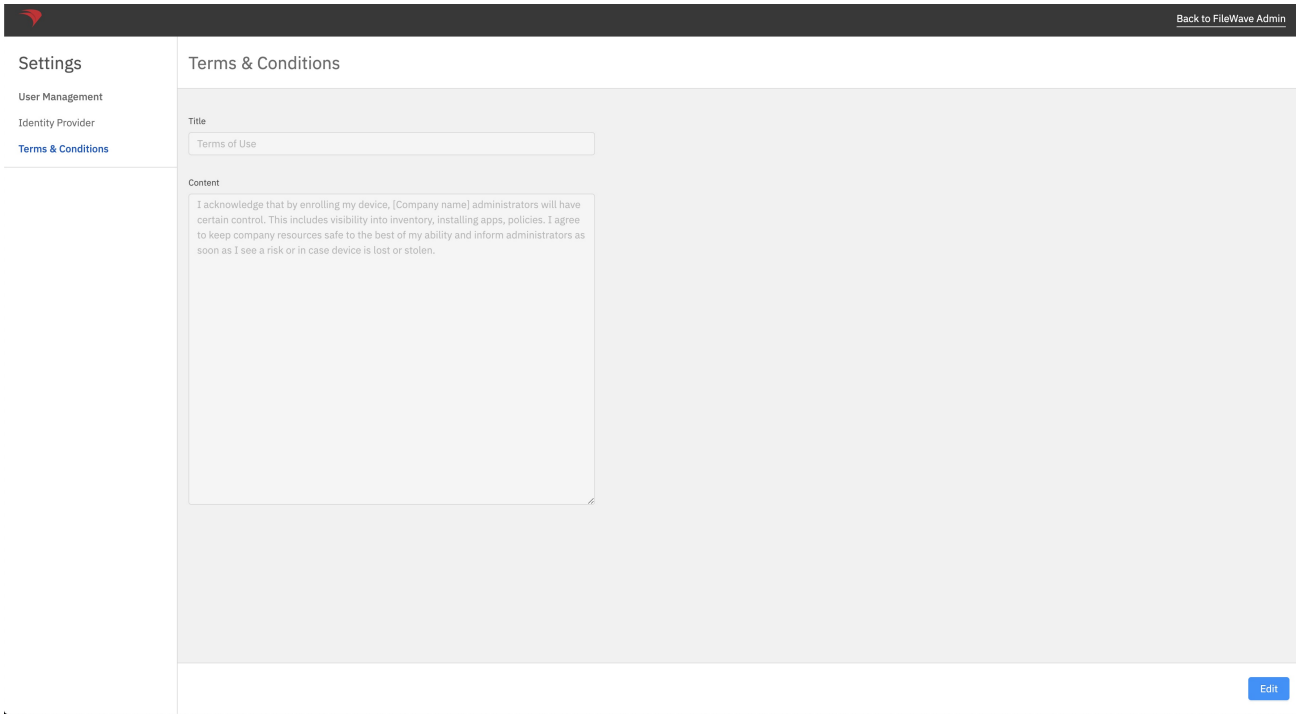
We'll need to establish our terms pages within the FileWave AnyWhere (Web admin), and they'll be used at enrollment time. These terms pages can be customized for your environment with the terms you prefer.

How

Editing Terms & Conditions

Terms & Conditions are for a page that are shows to users who are enrolling to your Server. You can customize this page via the FileWave Web Admin.

1. Click on the gear button next to Model update in FileWave Web Admin.
2. Navigate to Terms & Conditions tab.
3. Edit the title and/or the content of the page.



Part 3: Setting up the Portal App

What

The configuration of your Windows MDM integration will all be driven by an application you yourself create in the Microsoft Entra Portal.

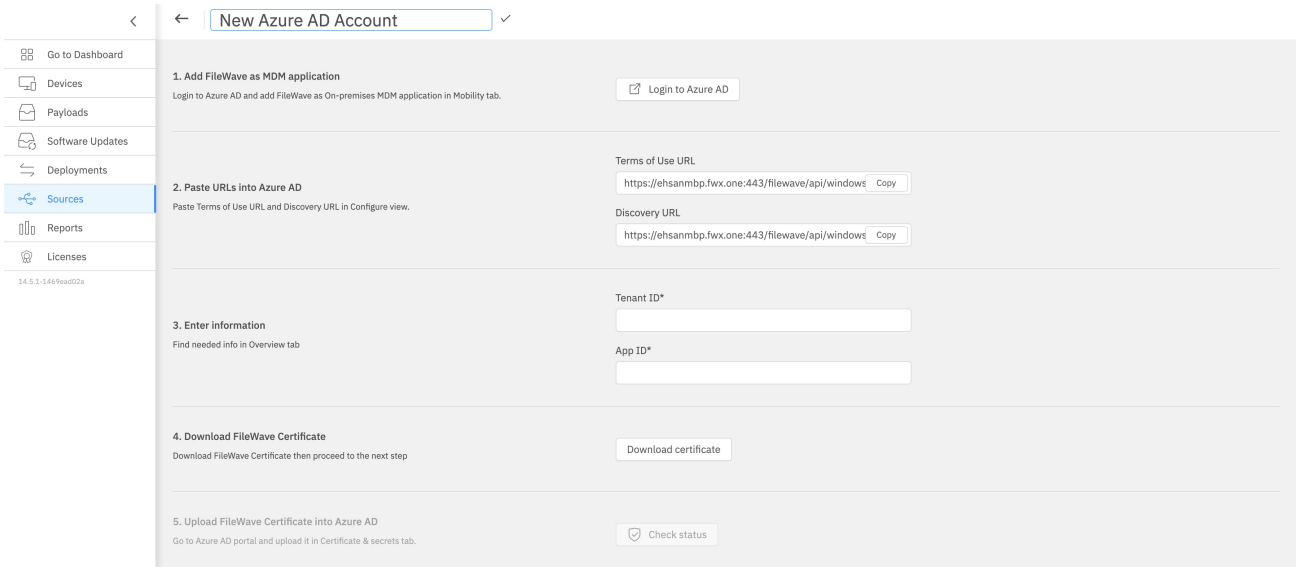
When/Why

This application is the linch pin that ties your devices (in AutoPilot), through your user accounts (the group associated with the app), into redirection to your FileWave MDM server. Detailed setup steps follow.

How

Add Microsoft Entra ID account in FileWave

1. Open your FileWave AnyWhere (Web Admin) page and navigate to sources.
2. Click the Microsoft tab.
3. Click on New account and you should see the following form:



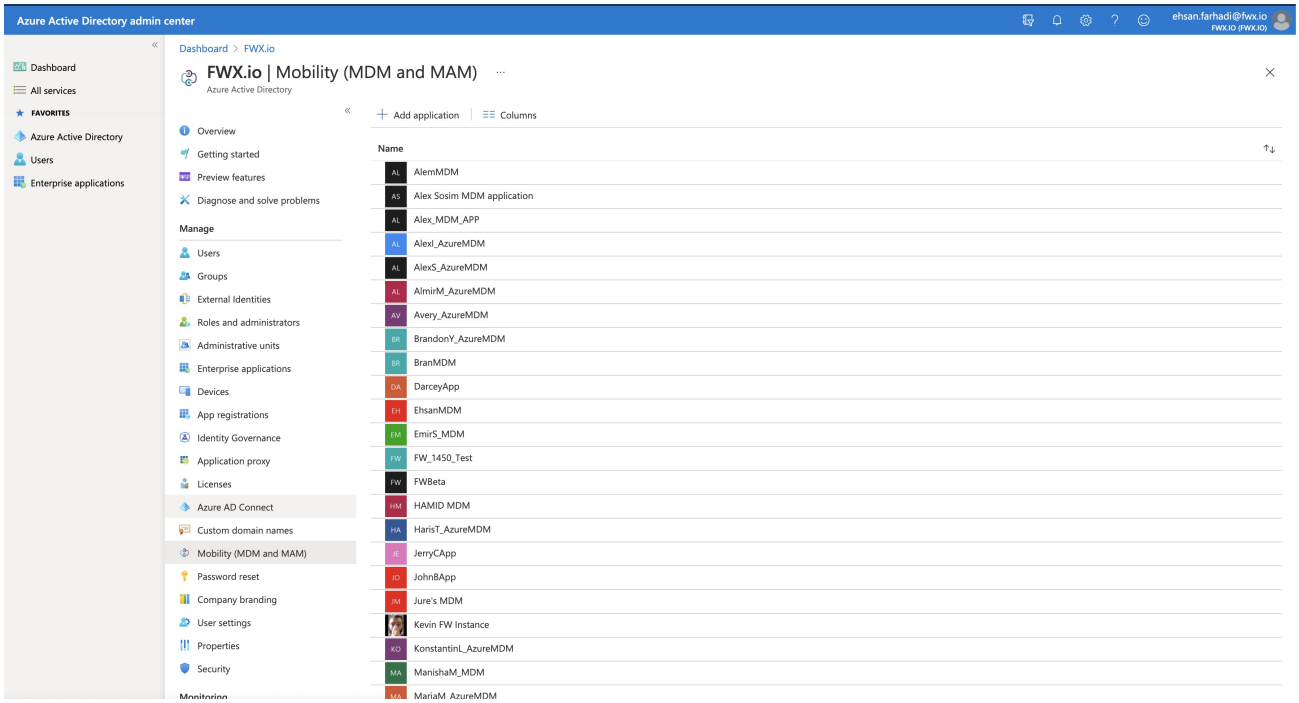
Keep this form open for completion in later steps.

Configuring Microsoft Entra ID

Creating MDM application

In order to enable MDM enrollment, first you need to configure your Microsoft Entra ID to recognizes your FileWave server as your MDM.

1. Go to your Microsoft Entra ID portal: https://aad.portal.azure.com
2. From dashboard navigate to Microsoft Entra Active Directory → Mobility (MDM and MAM) and then click Add application.
3. In new application form, select On-premises MDM application, give it a name and a log and click on add_._



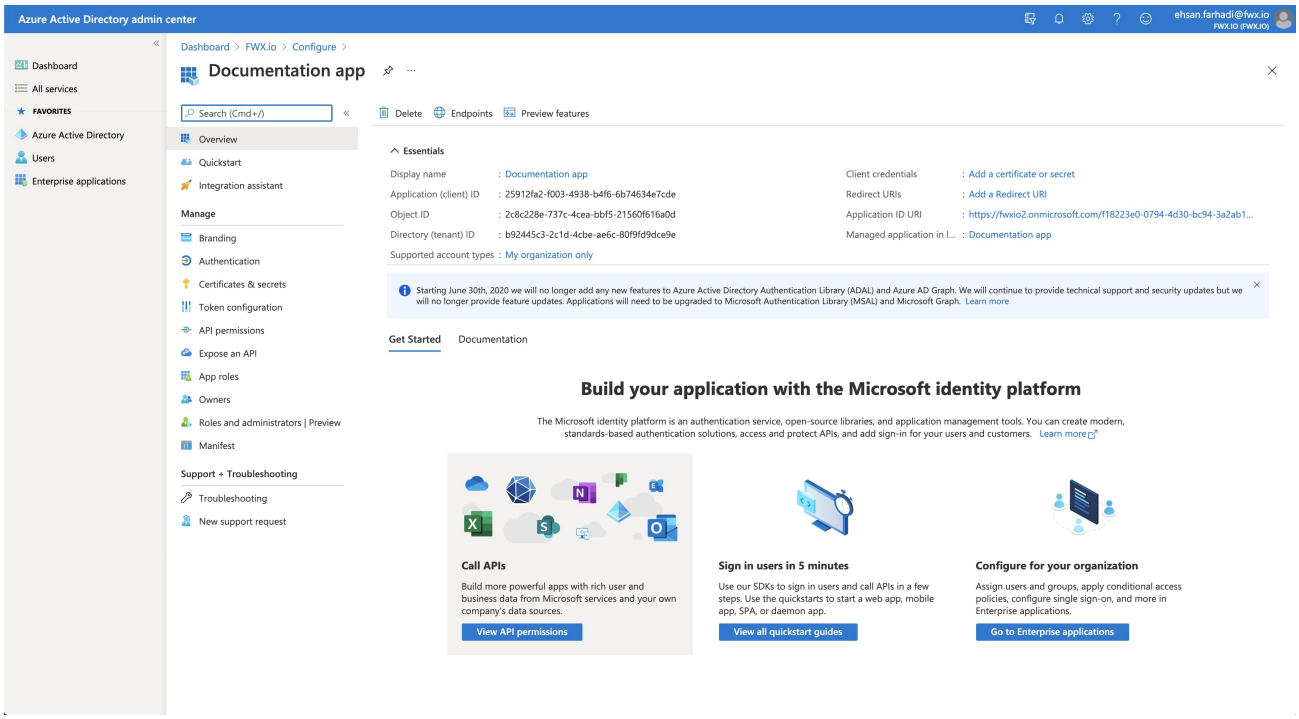
Configuring your MDM application

1. Go back to the list of MDM applications from step 2 above, and open the application you have just created. You should be able to see the following options:
    1. MDM user scope: This is where you indicate which users can enroll their devices using this MDM application. you can either choose:
        1. All: Force all users to use this MDM application. (Preferred)
        2. Some: You can select user groups which are allowed to use this MDM application to enroll their devices. If you do use this then you will need to make sure that you make a Group to restrict this, and add all of the users who will have their devices managed by MDM in that same group.
    2. MDM terms of use URL:
    Copy the value from the form you opened up in you FileWave AnyWhere (Web Admin) earlier.
    3. MDM discovery URL:
    Copy the value from the form you opened up in you FileWave AnyWhere (Web Admin) earlier.

It is very important that if you have another solution in place like InTune that you make sure that you do not have both InTune and FileWave enabled for the same users. You may get an error about not having permission to enroll devices. You can test this by disabling the Intune MDM (or another vendor) in Microsoft Entra by setting it to None and then wait 5 minutes and you would be able to enroll using FileWave. Think about which MDM solution you want to be for your different users in your environment. A single device can only really be in a single MDM. You can enroll to Intune for MDM and install the FileWave agent for instance, but then you could only push Windows Profiles from InTune. Everything else would work just fine in FileWave for those devices.

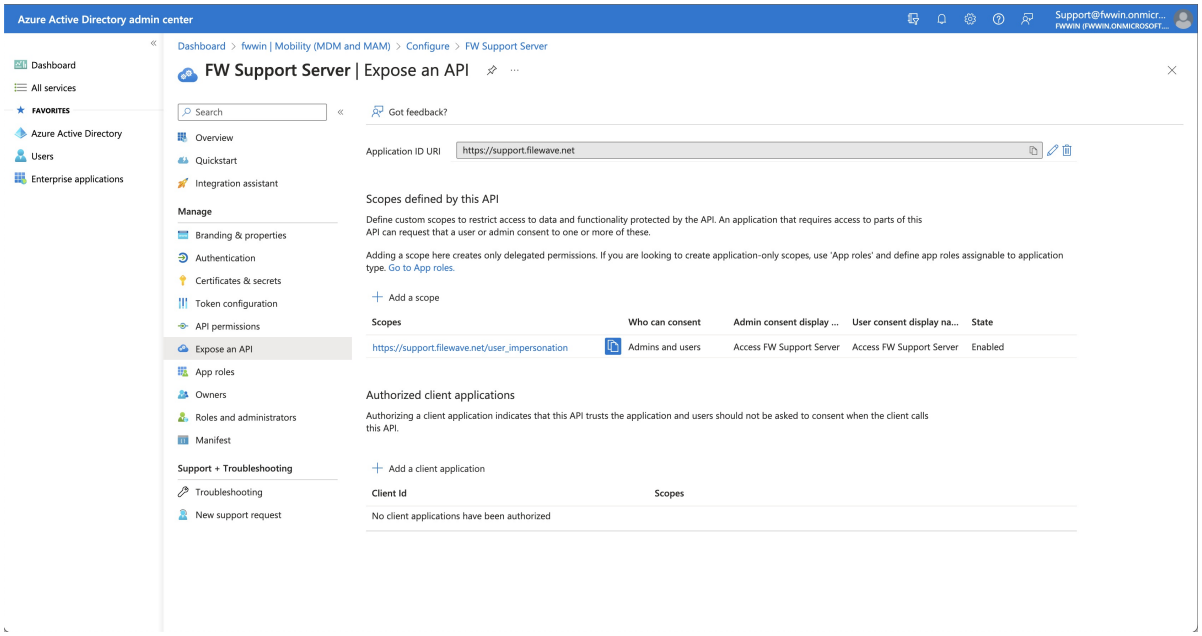
Integrating FileWave and Microsoft Entra

After configuring your MDM application, on the same page, you will see a small link that reads: On-premises MDM application settings. Click on it in order to open your on-premise application settings. You should see the following page:

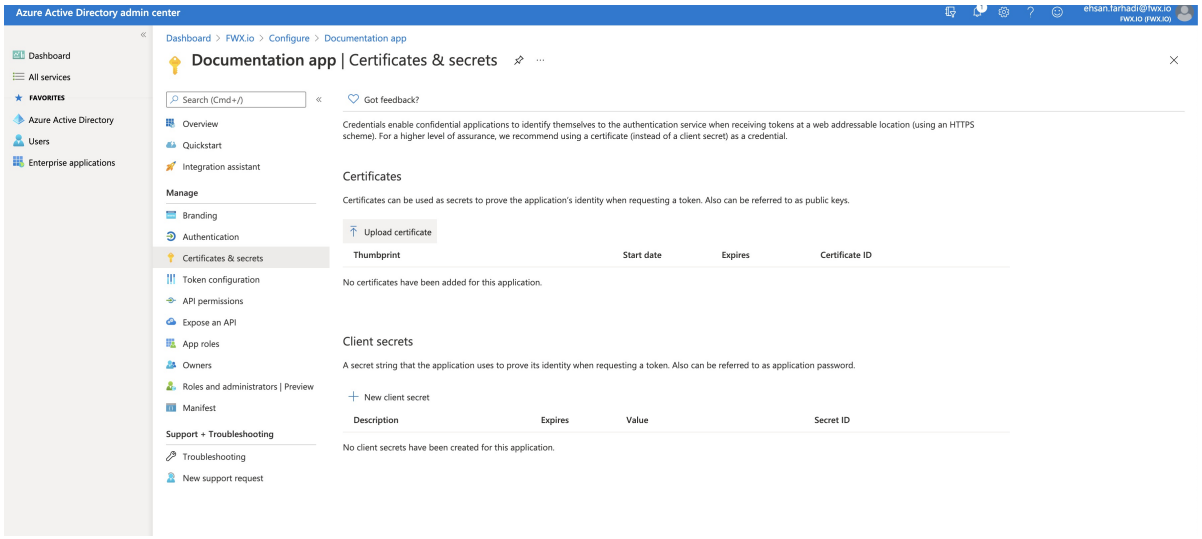


From here there are only few steps left!

1. Copy the Application ID and Tenant ID from this page and paste it in the Microsoft Entra Account form in FileWave AnyWhere (Web Admin) (which you kept open from earlier)
2. The Application ID URI value in your MDM app (in Microsoft Entra ID) must match your FileWave server URL, to fix that, go to "Expose an API" on the left side, and edit the URL there. The URL should be like https://example.filewave.net replacing that with your server's DNS name.



3. Go back to the Microsoft Entra account form in your FileWave AnyWhere (Web Admin), and download the FileWave certificate.
4. Once you have the certificate, go back to the Microsoft Entra ID portal, navigate to Certificates & secrets and upload your certificate to your Microsoft Entra MDM application there.



5. Once the Certificate is uploaded, wait couple of seconds, then go back to FileWave AnyWhere (Web Admin), in the already open Microsoft Entra account form and click on Check Status button.
6. As soon as you see the green light, go ahead and save your Microsoft Entra account.

You are now ready to enroll a device in to Windows MDM.

Application tenant or consent messages

You may see a message similar to below:

- AADSTS500011 – The resource principal named [URI] was not found in the tenant named [guid]. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You might have sent your authentication request to the wrong tenant.

If you're trying to log in from an application that doesn't support user consent flow or you're unable to use it otherwise, you can use the same special login URL crafting trick that I proposed in my article for resolving consent-related issues when getting error AADSTS650001, and create a URL like this:

- https://login.microsoftonline.com/[tenant_name_in_onmicrosoft.com-form]/oauth2/authorize?client_id=[appId]&response_type=code&redirect_uri=http://your-uri-here&nonce=1234&resource=https://graph.windows.net&prompt=consent.

If the application requires admin consent, you may replace "consent" with "admin_consent".

Integrating with Windows AutoPilot

What

AutoPilot is the Microsoft program that allows you to tie your devices into your organization for easy onboarding enrollment, and easy "re-imaging" by leveraging this process.

When/Why

Configuration of AutoPilot is very similar to what you may be familiar with if you manage Apple devices through DEP. We'll need to get our devices into AutoPilot, as well as create enrollment rules through an AutoPilot profile. Detailed steps follow below.

How

Getting the hardware hash to add to Autopilot

Microsoft provides technical details here - https://docs.microsoft.com/en-us/mem/autopilot/add-devices - but one option to add devices to Autopilot is to gather the hardware hashes from devices and upload a CSV file to Microsoft. The hardware hash for an existing device is available through Windows Management Instrumentation (WMI), as long as that device is running a supported version of Windows. You can use a PowerShell script (Get-WindowsAutoPilotInfo.ps1) to get a device's hardware hash and serial number. The serial number is useful to quickly see which device the hardware hash belongs to. For more information about running the script, see the Get-WindowsAutoPilotInfo script's help by using "Get-Help Get-WindowsAutoPilotInfo.ps1".

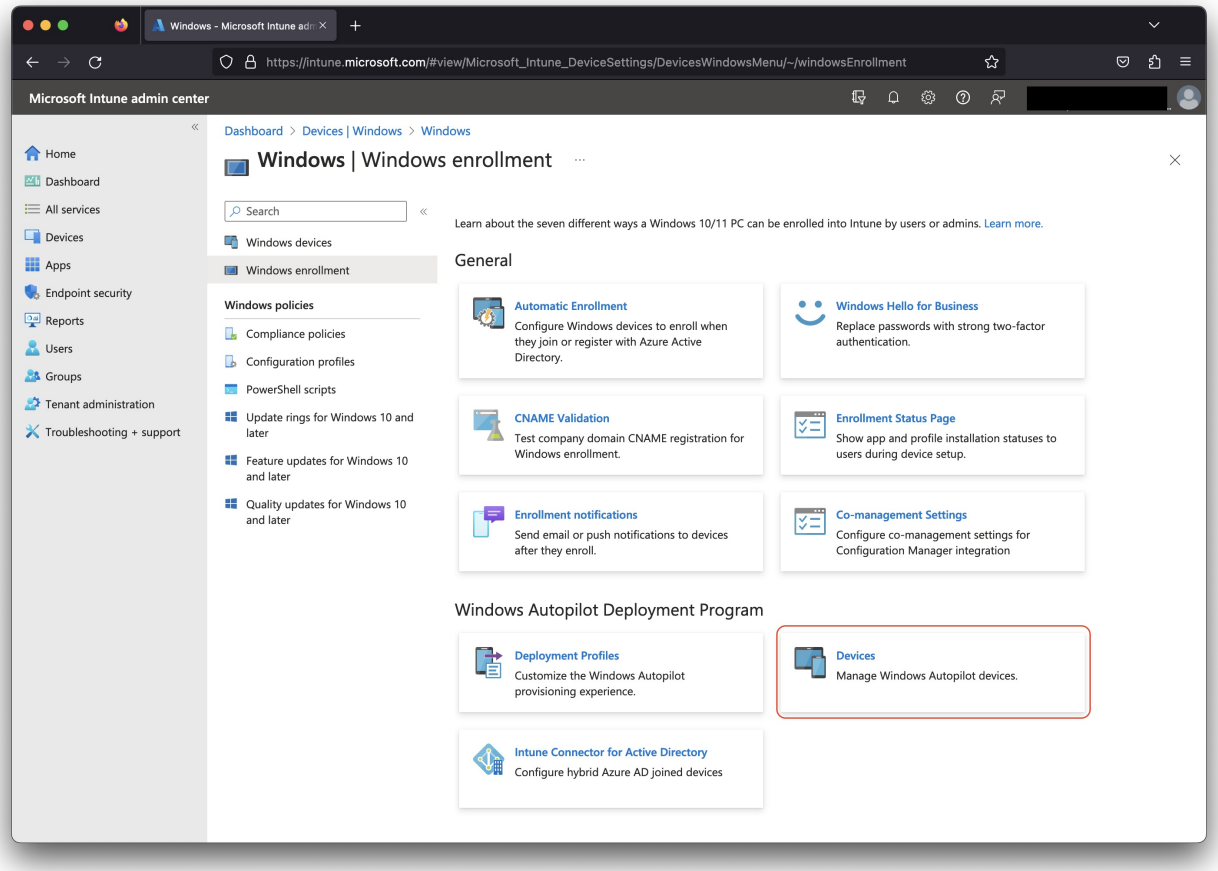
To make this step easier we have created a custom field that will populate a custom field called Windows Autopilot Hash so that you can easily export a list of serial numbers and hashes to later import in to Autopilot. Download the Custom Field and then import it in the Native Admin in Assistants → Manage Custom Fields.

Windows AutoPilot Hash Custom Field

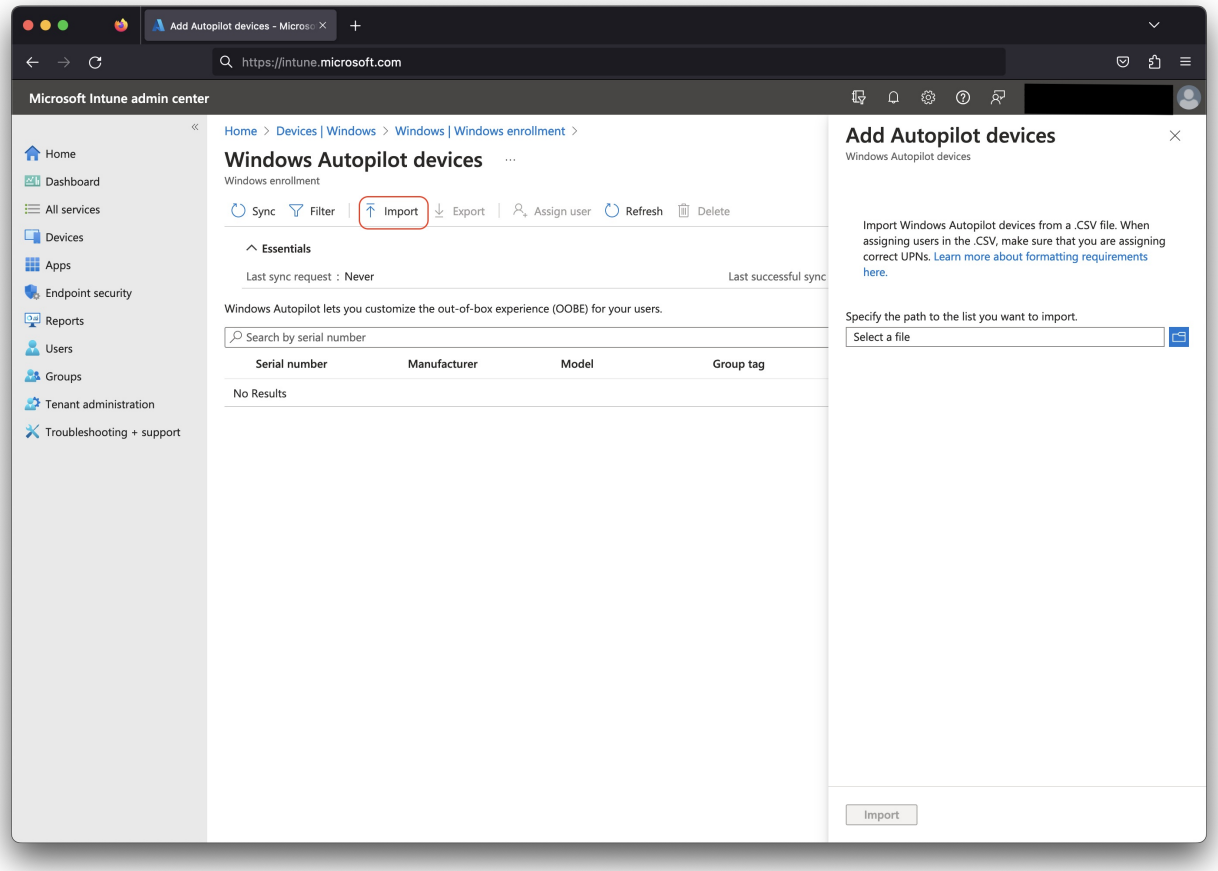
Importing device hashes in to Autopilot

Now that you have captured hardware hashes in a CSV file, you can add Windows Autopilot devices by importing the CSV file. The following are instructions to import the CSV using the Microsoft Intune admin center.

In the Microsoft Intune admin center, choose Devices, choose Windows, choose Windows Enrollment, then under Windows Autopilot Deployment Program, select Devices.



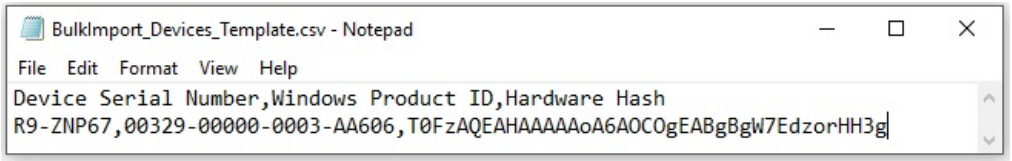
Under the Windows Autopilot devices, select Import to upload your .CSV file.



Browse to a CSV file listing the devices that you want to add. As per the documentation, the CSV file should list:

- Column A: Device Serial Number
- Column B: Windows Product ID (optional, typically blank)
- Column C: Hardware Hash

Here's a sample device information file. Please note that the header row is important or the import will not work:



You may select a group on the next dialog or simply pick "No, thanks" and continue.

Assigning Autopilot Profile

After the import is complete, choose Devices → AutoPilot deployment → Create new profile to create an MDM profile if you have not done this before. Once created then you can select your imported devices, and click on AutoPilot deployment and then pick to apply the MDM profile that you created.

Enrolling the Windows Device

At this point you will want to follow the steps in either Manually Enrolling a Device Into FileWave Windows MDM or Reset Windows Device through a script (Recipe) depending on if you are setting up a new device that you have or resetting a device in the field.

Manually enrolling a device into FileWave Windows MDM

What

Windows MDM allows you to manually enroll a device based on appropriate Microsoft Entra ID credentials.

When/Why

Enrolling a device in this manner isn't scalable. You would probably never use this method for a production rollout, but it is exceptionally handy to test your initial configuration to ensure you can enroll. And it doesn't have the AutoPilot complexity added.

How

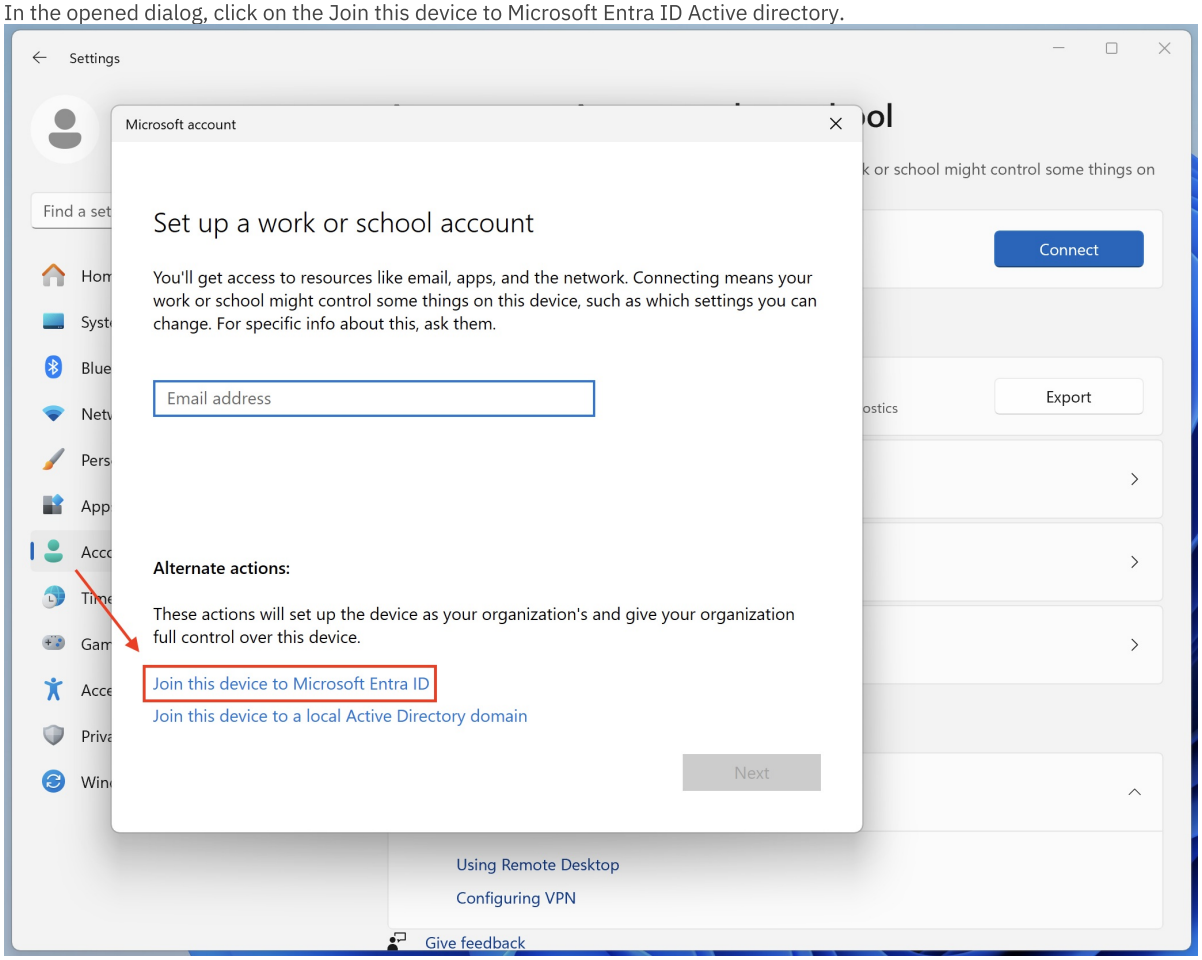
Manual Device Enrollment

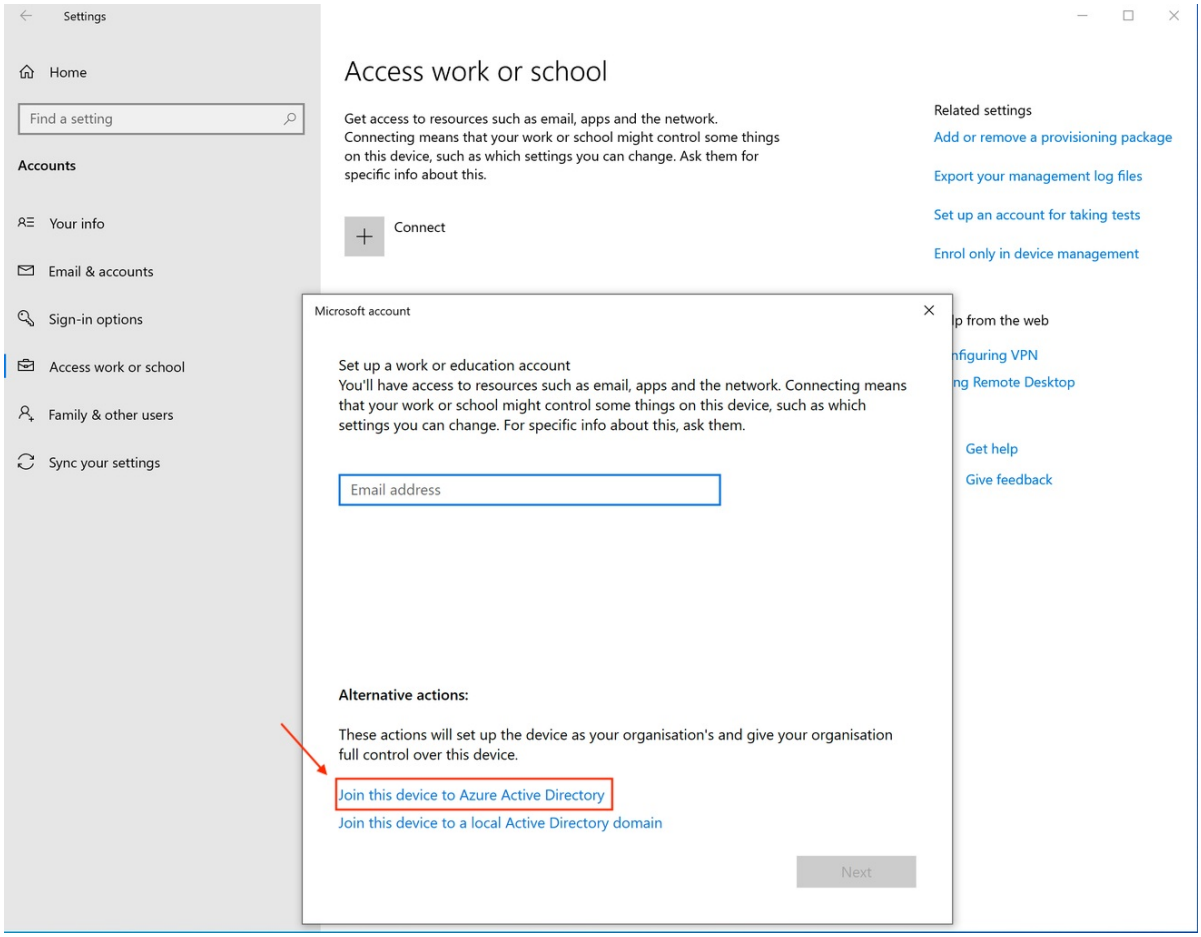
At this point, the hard part of the setup of the link between FileWave and Microsoft Entra is behind us, and we just simply have to enroll our devices. These steps are similar for both new (not previously enrolled in FileWave) and existing (via fwcld) FileWave clients.

Make sure your client can communicate with your server (you can ping server, correct ports are opened on firewall, etc.)

Also make sure you are not using Windows Home or Starter editions because they do not allow you to bind them to Microsoft Entra in this way.

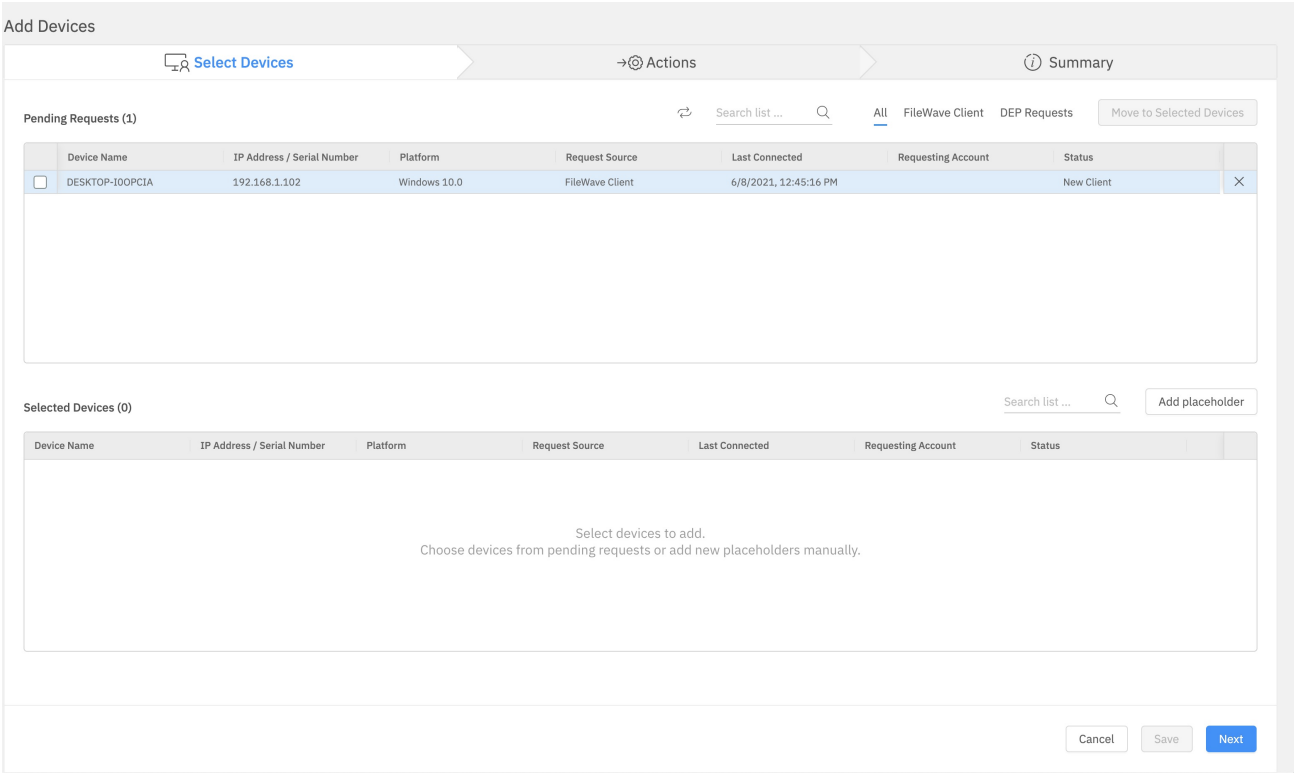
1. Navigate to Settings ➞ Accounts ➞ Access work or school
2. Click on Connect button
3. In the opened dialog, click on the Join this device to Microsoft Entra ID Active directory.





4. From here, just enter your Microsoft Entra credentials (as the user who wants to enroll their device) and follow the steps in the wizard until you're done.
5. You can verify the details of the MDM enrollment by clicking on the new account and opening Info.

If your device is newly enrolled, after a few minutes, you should be able to see the client show up as new on the FileWave Serve. Add it to your server.



Existing FileWave clients will not show up as a new client. They simply are updated to the new version.

You can verify if a device is truly MDM enrolled by checking the enrollment type in device info in Native Admin, as seen below:

DESKTOP-I0OPCIA - Client Info

Last Connected: 08.06.21 12:47
From: 192.168.1.102
Free Space: 40.4 GB
Platform: Windows 10.0
Model: 2
Version: Not connected
Enrollment Type: Enrollment via AZURE AD

Export Current Tab | Client Monitor | Get Log | Verify | Tools

Filesets Status | Device Details | Users | Policies

Edit Custom Field(s) Values...

Filter Device Details

Property	Value	Last Update Time	Status
Archived			
Building			
Client ID	217		
Client Name	DESKTOP-I0OPCIA		
Content Caching Enabled	false		
CPU Count	2		
CPU Speed	2.7 GHz		
CPU Type	Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz		
Created by conflict resolution	false		
Current Upstream Host	ehsanmbp.fwx.one		
Current Upstream Port	20017		
Date of Last Enterprise App Validation			
Date of Last State Change	08.06.21 12:45		
Deleted from admin	false		
Department			
Device ID	3ab7088b31f65dc998aa48c8e25c190ce9554b9a		
Device Manufacturer	VMware, Inc.		
Device Name	DESKTOP-I0OPCIA		

Reset Windows device through a script (FileWave Recipe)

What

AutoPilot assigns devices to your organization. This, coupled with the ability to "reset" a Windows 10 or 11, device allows you to be able to "re-image" a Windows device without necessarily wiping it out. What is described in this article is a method to wipe a device which could be used for Autopilot, but can also be used independently of Windows MDM.

When/Why

As of FileWave v14.8.0, a command to "reset" your Windows devices will be included in FileWave itself, but that requires the device to be enrolled in MDM. In this Fileset in this article, we are providing you with a method of doing the device reset through a PowerShell command that does not require MDM. It goes without saying that this reset is destructive to data on the device, so appropriate caution should be utilized.

How

Wiping a device to reset it in the field

Windows Autopilot Reset - https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset - takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically, Windows Autopilot Reset:

- Removes personal files, apps, and settings.
- Reapplies a device’s original settings.
- Maintains the device's identity connection to Microsoft Entra ID.
- Maintains the device's management connection to Intune.

The Windows Autopilot Reset process automatically keeps information from the existing device:

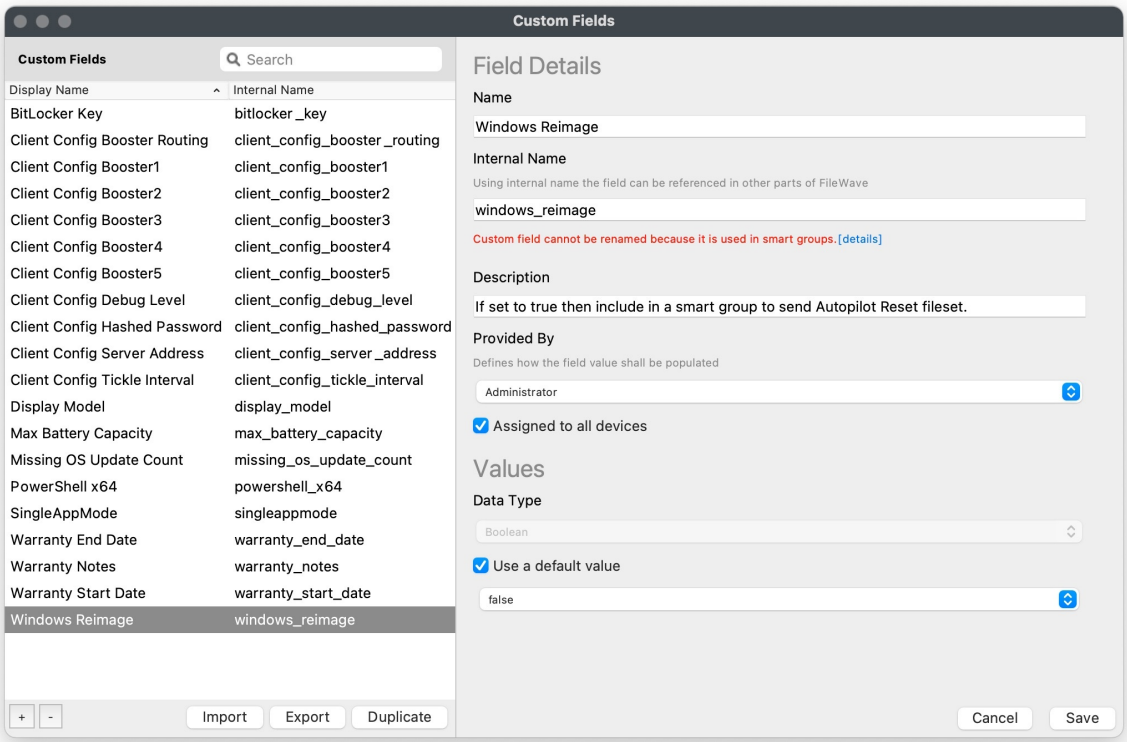
- Set the region, language, and keyboard to the original values.
- Wi-Fi connection details.
- Provisioning packages previously applied to the device
- A provisioning package present on a USB drive when the reset process is started
- Microsoft Entra Active Directory device membership and MDM enrollment information.

Windows Autopilot Reset will block the user from accessing the desktop until this information is restored, including reapplying any provisioning packages. For devices enrolled in an MDM service, Windows Autopilot Reset will also block until an MDM sync is completed. When Autopilot reset is used on a device, the device's primary user will be removed. The next user who signs in after the reset will be set as the primary user.

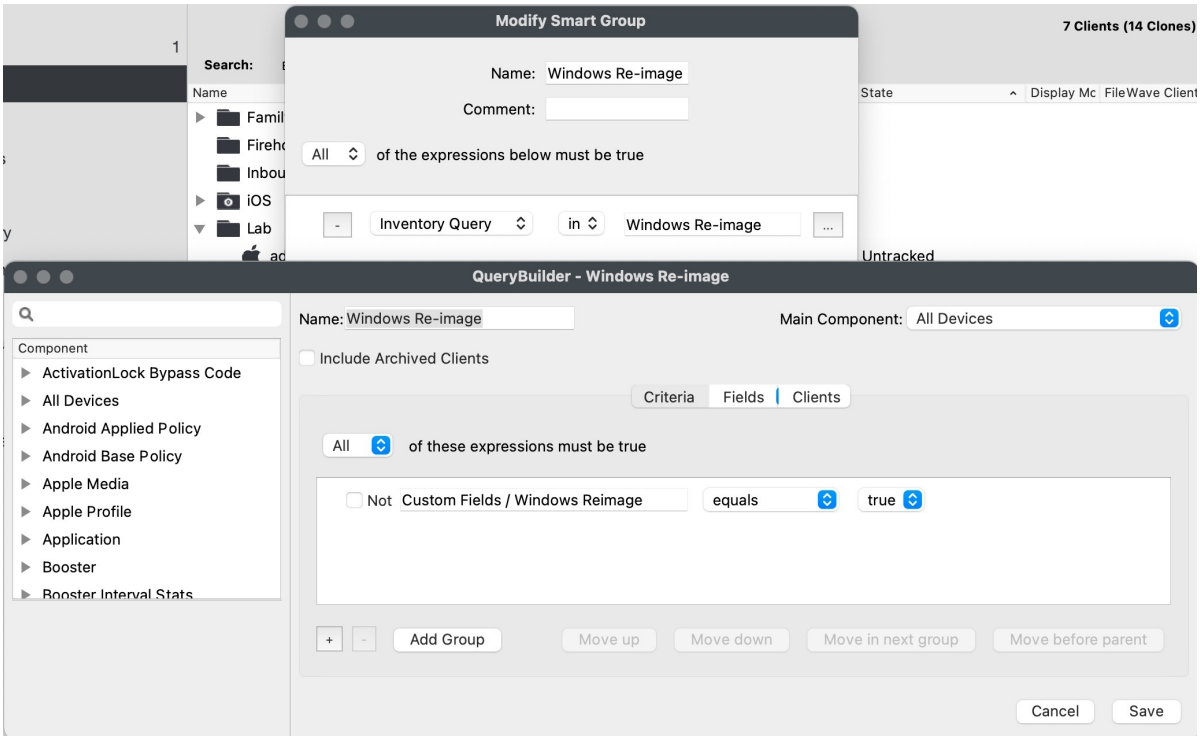
Initially FileWave does not directly issue the Autopilot Reset via MDM, but there is still a way to accomplish Autopilot Reset for a FileWave enrolled device. The below fileset will execute the above PowerShell. It will also enable the Windows Recovery Environment so that this can be successful. If using Windows 10 1703 or newer you can change the methodname to doWipeProtected so that the wipe will continue even if a user reboots in the middle of it.

Directions

1. Ensure that you have your device in Autopilot as outlined here: Integrating with AutoPilot
2. Create a custom field with the internal name of windows_reimage as seen below. The field should be Boolean and have a default value of "false".



3. Create smart group that looks for windows_reimage to be True as seen below.



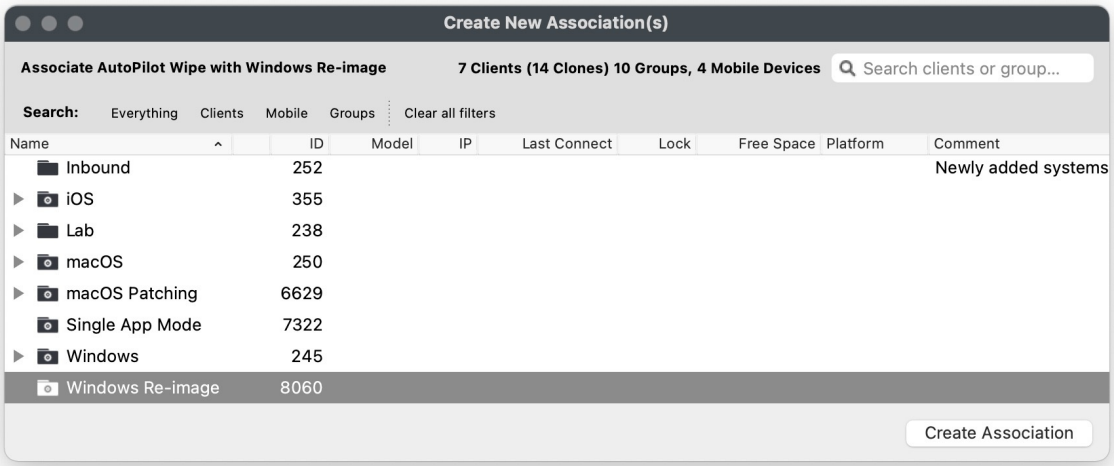
4. Add this Fileset to your server. You can unzip it and then drag the Fileset into the Fileset window. Note that this Fileset uses the section of code below that can be edited to change "doWipeMethod" to "doWipeProtectedMethod" or to use any other method as outlined here but be sure to add "Method" to the one you want to use: https://docs.microsoft.com/en-us/windows/client-management/mdm/remotewipe-csp

```
# This part wipes the system
# https://docs.microsoft.com/en-us/windows/client-management/mdm/remotewipe-csp
# methodname can be doWipeMethod or doWipeProtected but the later needs Win 10 1703 or newer
$namespaceName = "root\cimv2\mdm\dmmap"
$className = "MDM_RemoteWipe"
$methodName = "doWipeMethod"

$session = New-CimSession

$params = New-Object Microsoft.Management.Infrastructure.CimMethodParametersCollection
```

```
$param = [Microsoft.Management.Infrastructure.CimMethodParameter]::Create("param", "", "String", "In")
$params.Add($param)

$instance = Get-CimInstance -Namespace $namespaceName -ClassName $className -Filter
"ParentID='./Vendor/MSFT' and InstanceID='RemoteWipe'"
$session.InvokeMethod($namespaceName, $instance, $methodName, $params)
```

AutoPilot Wipe Fileset

5. Select the Fileset and click the Scripts button in the Native Admin. Right click on the Reset.ps1 script and pick Properties. You must change the first Environment Variable for that script to be the API token you want to use. You can get this from the Native Admin from Manage Administrators → Select an admin → Application Tokens. This token is used by the script to set the custom field for windows_reimage to false. If you don't update this then your device will be stuck in a loop of wiping once you enable it.
6. Associate the Fileset with the Smart Group that you created.



7. To wipe a device you will set the windows_reimage custom field to True. This will cause the device to appear in the Smart Group, and will cause the Fileset to be applied. The Fileset will set windows_reimage to be False while it runs, will enable Recovery Environment, and then will initiate a wipe.
8. Because the fileset sets windows_reimage to False the device leaves the smart group that would cause the AuotPilot Wipe Fileset to apply to it so it won't be caught in a re-image loop.

Windows MDM wipe command

What

14.8+ FileWave introduces the option to Wipe MDM enrolled Windows devices from the Web Admin console.

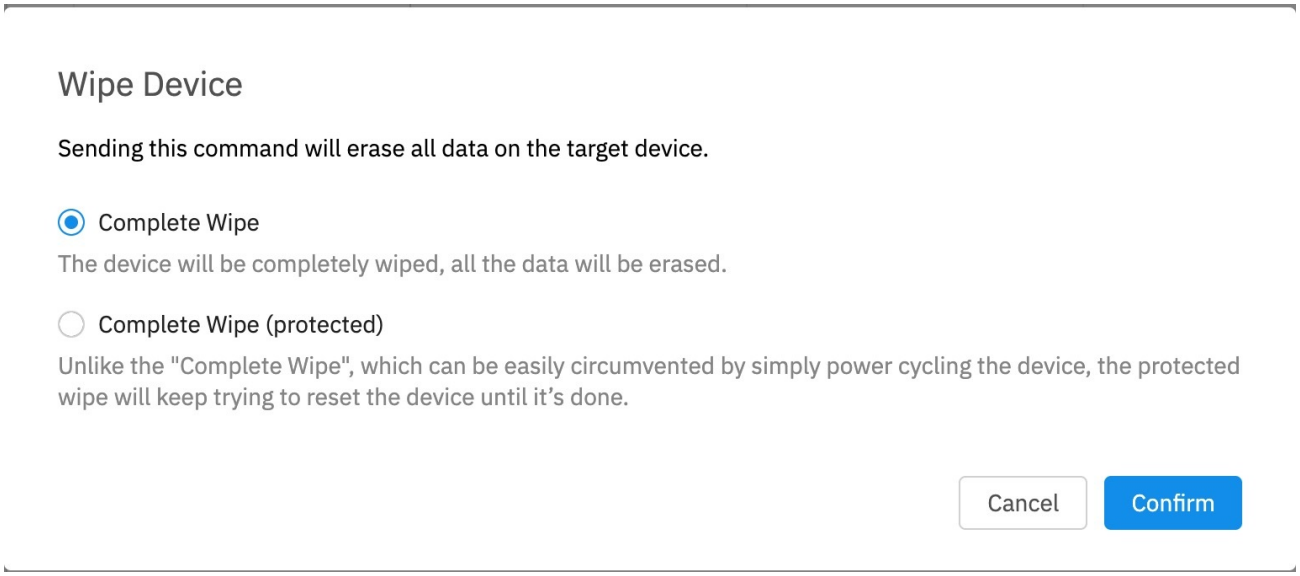
When/Why

The options from the ellipsis now include the Wipe option.

Option to Wipe will only be visible for Windows devices which are MDM enrolled.

How

- Select device
- Select ellipsis
- Choose Wipe option



Configuration Service Providers (Profiles)

Windows MDM uses CSPs which are profiles that configure Windows.

Windows MDM Policies (aka Profiles)

What

Windows Configuration policies enable you to define and enforce settings on your Windows devices that are enrolled in Mobile Device Management (MDM). For example, you can restrict features like Bluetooth by setting policies such as “Bluetooth is not allowed.” While these policies are conceptually similar to Apple Profiles, they are specifically designed for Windows MDM-enrolled devices. These configuration policies offer management capabilities similar to what you might have previously achieved using Group Policy Objects (GPOs).

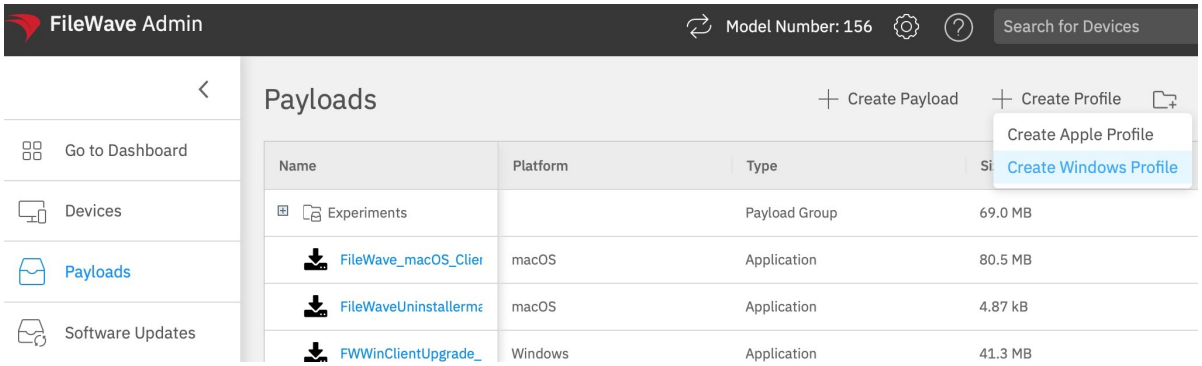
When/Why

We'll use configuration policies whenever we want to configure Windows endpoints for items that ease setup, or restrict device usage. Policies will always be a work in progress as more and more are added to the platform over time. In this iteration we start with the critical core policy settings.

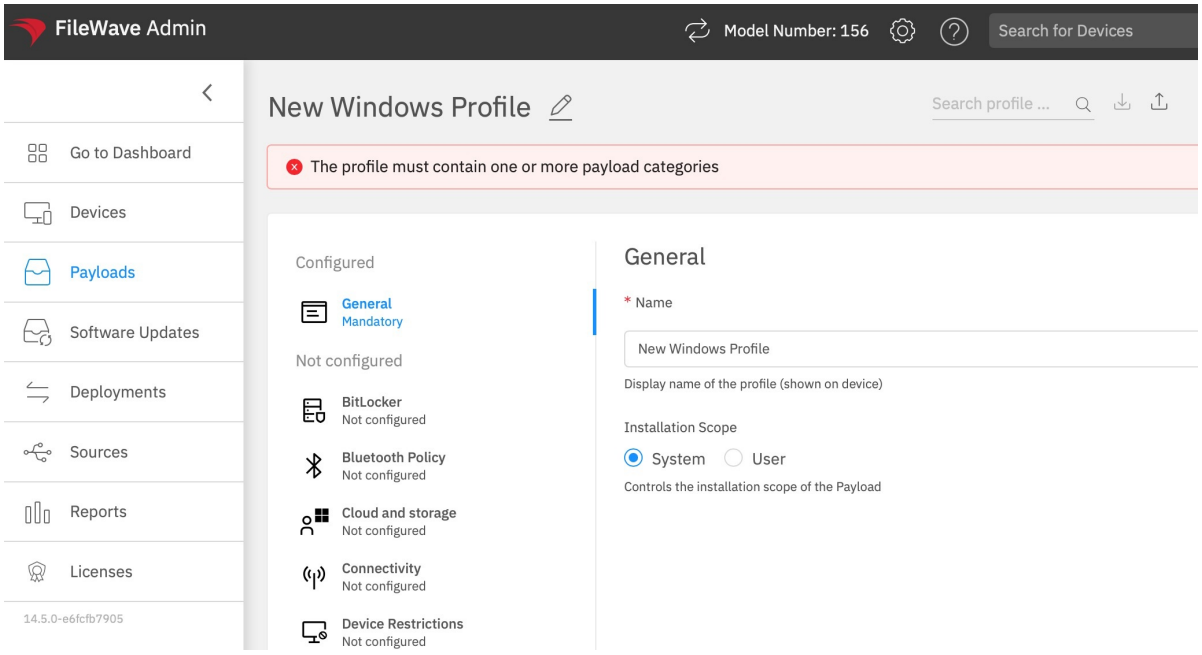
How

How can a FileWave administrator create the Windows policies?

1. Open the FileWave WebAdmin → navigate to payloads → click on + button.
2. Click Create Windows Profile.



3. Here you will be able to select what should be controlled by the profile and the settings for those controls



4. Once the profile is saved you can deploy the profile to the single or group of devices using deployment view.
5. The FileWave server will reach to the devices using push model via WNS (Windows notification services.)
6. The device will now reach to the FileWave server and sync for the assigned payloads. In case the device is not online there is a caching mechanism built to retry for several hours.

You have now deployed a profile to manage settings!

> Note that at this time there is no method for seeing command history in the FileWave admin with regard to policy installation,

but this feature will be coming in a later update.

Windows MDM Software Updates CSP

What

What is CSP? A configuration service provider (CSP) is an interface to read, set, modify, or delete configuration settings on Windows devices, and the options available have been expanded in FileWave 14.8+ to include Microsoft Software Update management.

When/Why

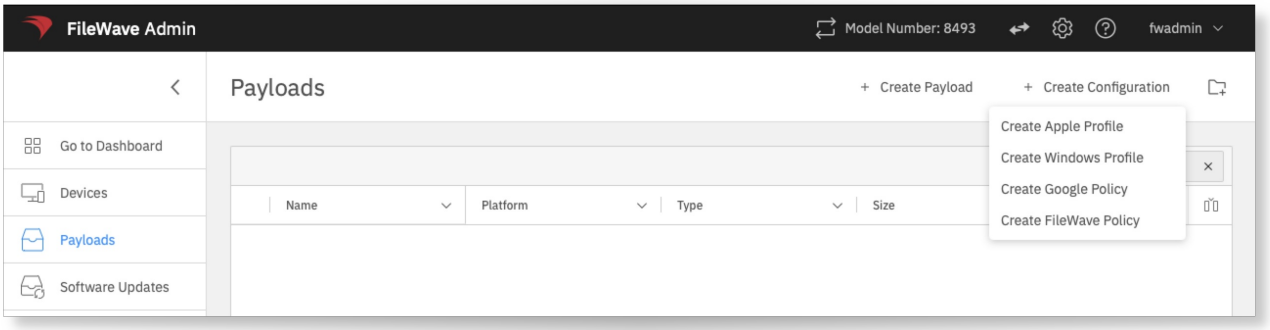
Windows profiles may be built via the FileWave Web Admin. Using this new CSP you can control many options around Windows Update on Microsoft Windows 10 and 11 devices.

> Microsoft Profiles are only available through the FileWave Anywhere

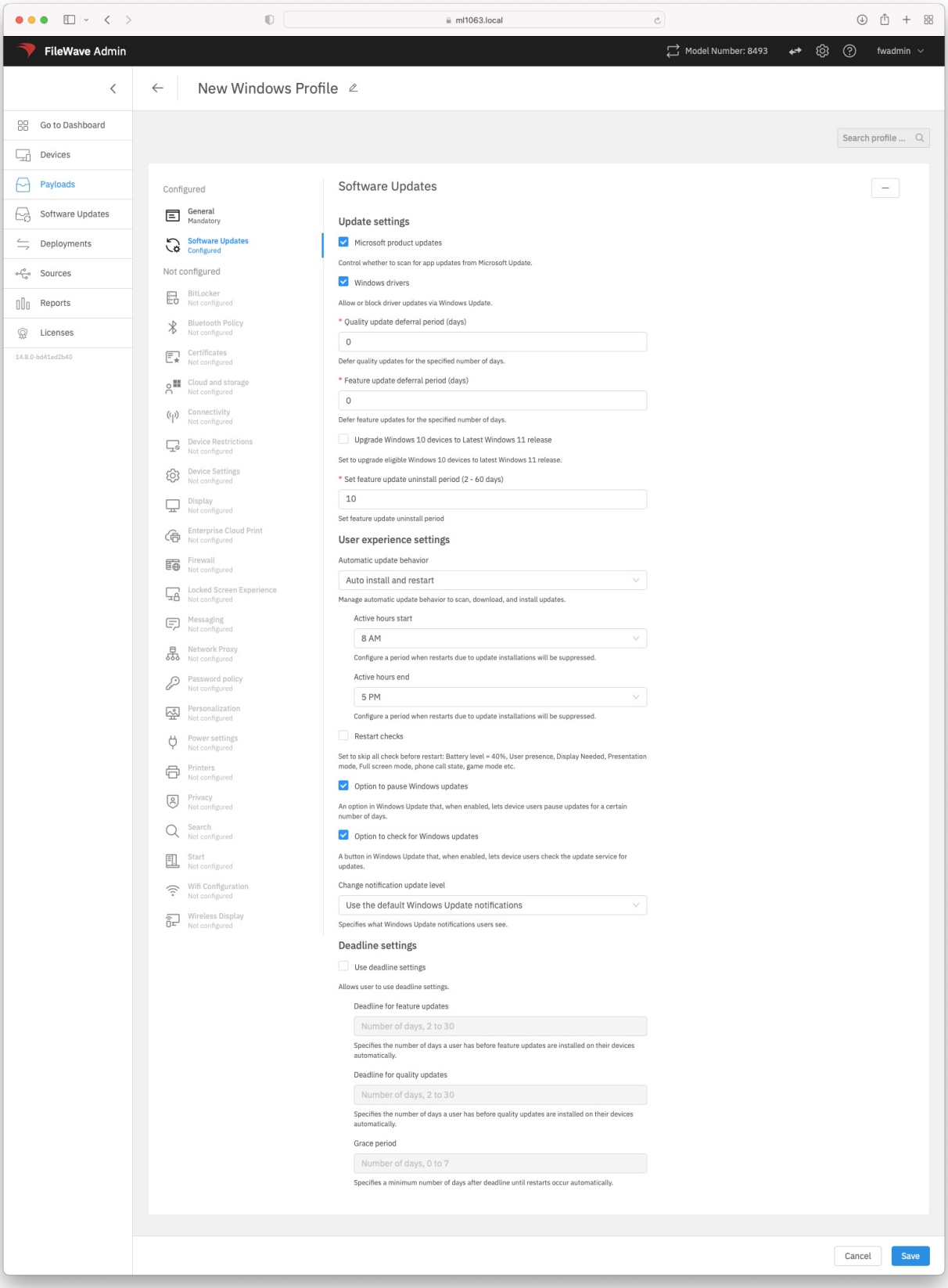
How

To build a Windows Profile, select:

- Payloads > Create Configuration > Create Windows Payload



As you go through configuring the Software Updates CSP you will see that each option is clearly explained and allows you easy control over the Software Update experience.



Related Content

- Windows MDM

Troubleshooting

Windows MDM setup issue with custom domain

What

When configuring FileWave's Windows MDM integration with Microsoft Entra ID, and the On-premises MDM application is added to the Microsoft Entra tenant, attempting to add the URL of the FileWave server to the Expose an API blade results in an error message stating:

"Failed to update Application ID URI application property. Error detail: The Application ID URI must be from a verified domain within your organization’s directory."

When/Why

Microsoft instituted a breaking change in Microsoft Entra on 10/15/2021 to require the use of verified domains in all apps. See https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-breaking-changes#appid-uri-in-single-tenant-applications-will-require-use-of-default-scheme-or-verified-domains for more information.

This change impacts customers using the On-premises MDM app from Microsoft in that the configuration of that app requires the URL of the FileWave server to be added to the Expose an API blade of the app. Previously, a FileWave SaaS environment, such as filewave.net could be added to the configuration. With this change, it is not possible to add an unverified domain.

Customer environments using the On-premises MDM app from Microsoft who had Microsoft Entra configured prior to the breaking change can continue to use that configuration as long as they do not attempt to change the URI on the Expose an API blade. Any new customer environments attempting to use the On-premises MDM app will not be able to use that app to integrate a FileWave SaaS tenant that has a filewave.net domain name with Microsoft Entra ID.

How

For customers who have a FileWave environment that is using a domain name of your own, you can continue to use the On-premises MDM app, but you need to verify ownership of your domain through Microsoft. The process for verifying ownership of a custom domain is documented at:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain

Customers who are on a FileWave SaaS tenant that currently uses a filewave.net domain name, and did not setup Windows MDM prior to 10/15/2021 would need to migrate to a server that uses a domain name that you can control so that it can be added to your Microsoft Entra tenant.