Return to Service feature for iOS/iPadOS

What

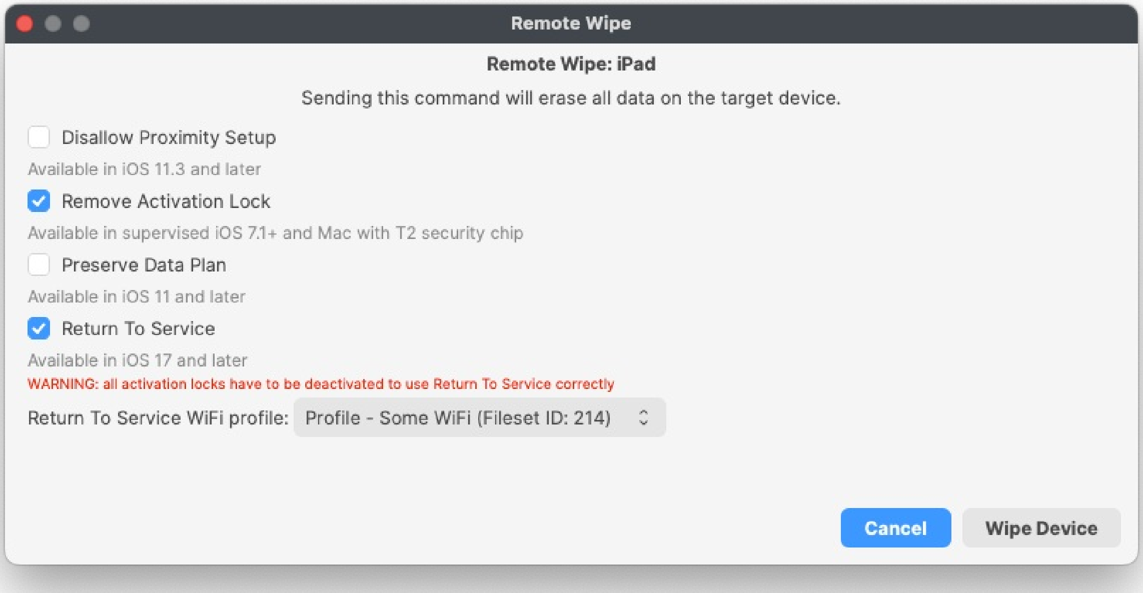
Even though devices can be erased remotely, getting them back into service is a manual process, as it requires someone to physically touch them and take them through Setup Assistant. Apple is removing the additional manual step with the introduction of Return to Service for iOS and iPadOS. This feature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

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.



Remote Wipe

Remote Wipe: iPad

Sending this command will erase all data on the target device.

☐ Disallow Proximity Setup
Available in iOS 11.3 and later

☑ Remove Activation Lock
Available in supervised iOS 7.1+ and Mac with T2 security chip

☐ Preserve Data Plan
Available in iOS 11 and later

☑ Return To Service
Available in iOS 17 and later
WARNING: all activation locks have to be deactivated to use Return To Service correctly

Return To Service WiFi profile: Profile - Some WiFi (Fileset ID: 214)

What happens on the device?

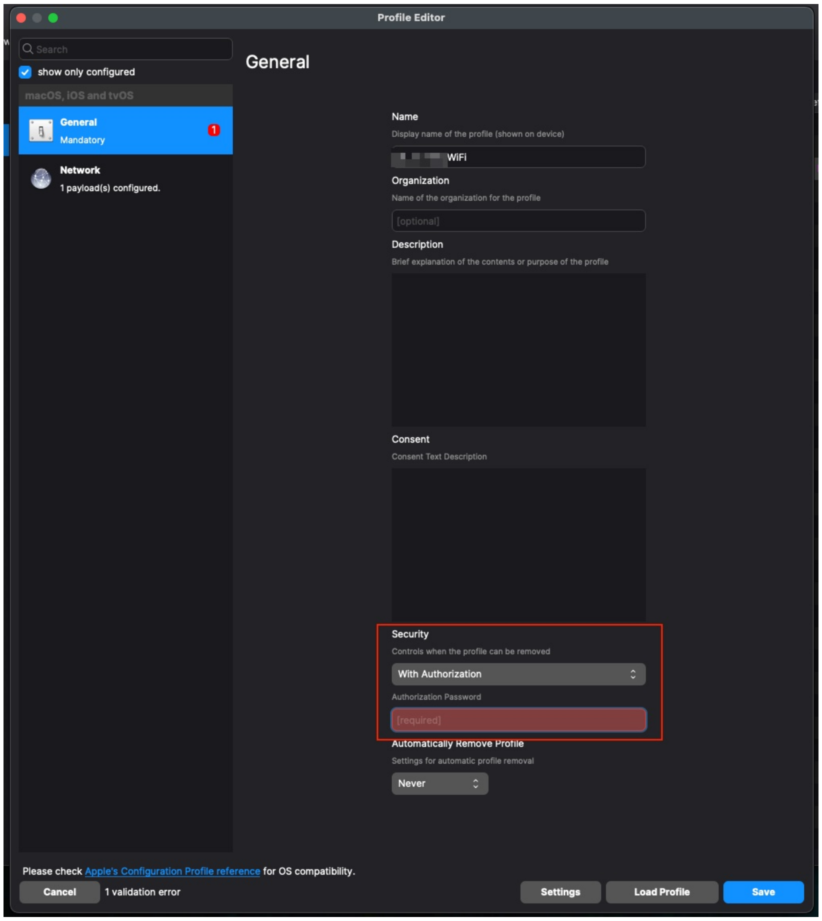
If Return To Service is enabled on FileWave side and then Wipe Device button is pressed, the device will be wiped and then connected to the Wi-Fi network specified in selected Wi-Fi profile without asking password. Also MDM profile will remain on the device, there will be no need to download it, set creds and install (fair only for OTA enrollment, DEP profile will redirect device to the right url which asks for creds).

Related Content

- FileWave Version 15.1.0

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.



General

Name
Display name of the profile (shown on device)
[redacted] WiFi

Organization
Name of the organization for the profile
[optional]

Description
Brief explanation of the contents or purpose of the profile

Consent
Consent Text Description

Security
Controls when the profile can be removed
With Authorization
Authorization Password
[required]

Automatically Remove Profile
Settings for automatic profile removal
Never

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

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>
```

Revision #12
★Created 7 September 2023 14:49:45 by Josh Levitsky
Updated 17 May 2024 16:22:52 by Josh Levitsky