Troubleshooting

- Apple Metadata Missing After Fileset Installation (macOS)
- iOS 12 / macOS 10.14+ and self-signed certificates
- M1 Silicon macOS and Recovery

Apple Metadata Missing After Fileset Installation (macOS)

Description

In some instances Metadata is added to items to provide additional features, however, this Metadata may not be transferred when the App is delivered as a standard Fileset. Where this occurs, the Metadata may be re-injected using a script. An example of this is highlighted in our KB on Deploying Folders with Icons.

Teamviewer is another example of this. The Quick Support version of the App has the option to include customisation, as per their guidelines. In fact, the Tool: FileWave QS App implements this to provide branding, user name and a personalised design.

When customisation is configured on this App, the App receives additional Metadata. If the Metadata were not restored, the customisation would be lost and the App would appear as the basic, standard looking App.

Instructions

To ensure the Metadata is re-applied after installation as a standard Fileset, the following should be followed:

- Use a command line tool to read the Metadata prior to making the Fileset
- Create an Activation or Postflight Script, to re-insert the Metadata, as part of the Fileset

To read the Metadata, open Terminal and run the following command, editing the path to match the required location. Using FileWave QS App as an example:

```
$ xattr -l ~Downloads/FileWave\ QS.app
com.TeamViewer.ConfigurationId: idcr6bwpyh
```

A script may now be created to re-instate this Metadata, again changing the path if the App is installed somewhere other than Applications.

```
#!/bin/zsh

xattr -w com.TeamViewer.ConfigurationId idcr6bwpyh /Applications/FileWave\ QS.app

exit 0
```

If using an alternative customised Teamviewer QS App, change the name to match the created App and use the reported value from the query to set the matching ID.

> Verification
> To ensure the script is run again if Verification actions a repair or re-instatement of the App, a Verification Script will also be required with the same contents.

On installation, all applied customisation should appear as expected. This same process may be applied to any additional Metadata that may be lost during Fileset installation.

Example Fileset

This example Fileset includes:

- Version 14 of Teamviewer FileWave QS
- Postflight Script
- Verification Script

FileWave TV QS Version 14.fileset.zip

When updated versions of Teamviewer FileWave QS are supplied, then the Fileset should be updated with this newer download, to replace the current application.

iOS 12 / macOS 10.14+ and self-signed certificates

iOS 12 and macOS 10.14 introduce more secured rules ; certificates must be generated from at least a 2048-bit RSA key ; certificates generated from a 1024-bit key will be rejected by the device.

If you are using a trusted CA issued certificate, you should be fine, most of the certificates you get on the market are fulfilling this requirement ; if you generated your certificated with FileWave 9.0 or later, you should be good as well, since in this version the key used to generate certificates is 2048-bit. If you are running a FileWave installation which has been setup before FileWave 9.0 with self signed certificate, or if you are using a 1024-bit key issued certificate, you need to update your setup to have iOS 12 devices trust your server.

How 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.

Recommended solution:

Use a third party, trusted Certificate Authority. Most organizations already have a wildcard certificate (for instance *.acme.org), installing this certificate on "filewave.acme.org" will make your server trusted automatically. If you don't have a certificate, several CAs provide SSL certificates which are trusted by Apple, Google or Microsoft. For more information about these trusted certificates please read this KB article.

Self-Signed solution:

If you decide to stay with a self-signed certificate, you don't have another choice than renewing the certificate ; please read this KB article on how to renew the certificate.

The best approach would then be:

1. Deploy a profile with "defer software update" set to 90 days restriction ; this will give you 90 days (starting from Monday, Sept 17th) during which devices won't be upgraded
2. Follow steps described in Renew FileWave Server Self-signed Certificate KB article:
   1. create new key and certificate
   2. deploy the new certificate via profile
   3. switch to the new certificate once all devices have the profile installed
   4. recreate DEP profiles (and associations, if required)
3. Already impacted devices can be manually "healed" by installing the profile (and trusting it explicitly for SSL in trust stored).

> If you have a pre-FileWave 9.0 certificate and devices have already upgraded to iOS 12, the only way to recover, assuming you can't use trusted certificate, is to manually add the new certificate in the trust store and give it permissions for SSL.

Related Content

- iOS 12+ Profile Installation Failed

M1 Silicon macOS and Recovery

Description

Apple M1 devices require an alternate method for Recovery Mode and other considerations may need to actioned.

> FileWave has seen instances where M1 macOS devices are no longer accessible after the first reboot following DEP enrolment. It is believed the trigger for this experience is centred around the Admin account having never logged in.

Erasing M1 devices

It is possible to use Apple Configurator to Restore Apple Silicon M1 macOS devices. This requires a second device along with the listed details from Apple's KB:

https://support.apple.com/en-gb/guide/apple-configurator-2/apdd5f3c75ad/mac

- Up to date Apple Configurator App
- Network access to Apple
- USB-C to USB-C cable (supporting both power and data)

Apple's guidelines should be followed to restore the device

Activation Lock

If Activation Lock was enabled on the device, then the above process will block access to the device once recovered; a request to enter Apple ID and password will be presented. However, it is likely there is no Apple ID associated to the device. In this instance Recovery Mode should be used to access the menus to add in the appropriate Bypass Code.

The ByPass Codes are available from the FileWave Admin Assistants drop down menu:

- Activation Lock Management

Recovery Mode

M1 Silicon devices have a newer method to boot into Recovery Mode; hold down the Power Button until the screen displays: 'Loading startup options'

https://support.apple.com/en-gb/guide/mac-help/mchl82829c17/mac

To enter the Activation Lock code:

- Choose 'Recovery Assistant' from the Menu Bar
- Select with MDM key
- Use the key from the Admin console Activation Lock Management window for this device

https://support.apple.com/en-gb/guide/mdm/apd593fdd1c9/web

At this point the device should be accessible again and a fresh enrolment may be actioned.

Failure to Personalise

There is an additional issue that Apple have identified:

- "An error occurred while preparing the update. Failed to personalize the software update. Please try again."

Again, Apple have a KB on this issue:

https://support.apple.com/en-us/HT211983

> The previous startup keys combinations used for Intel macOS devices do not apply to M1 Silicon macOS devices: https://support.apple.com/en-gb/HT201255