

Troubleshooting

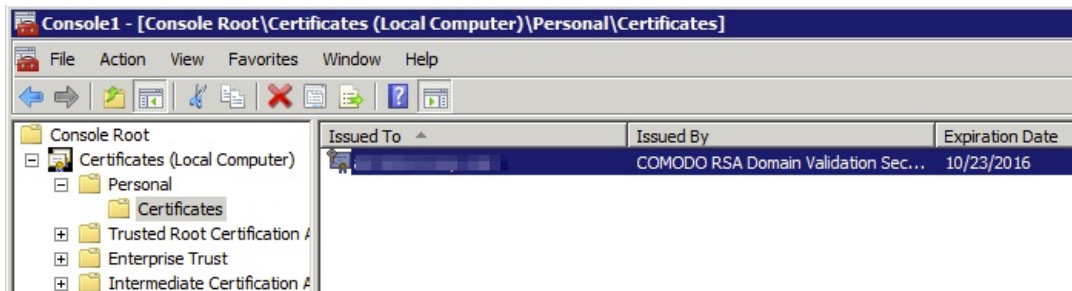
- [Export .p12 SSL Certificate from Windows](#)
- [Determine Correct Intermediates Bundle for SSL Certificate](#)
- [Self Signed Certificate Error during iOS OTA Enrollment](#)
- [SSL Server Certificates - iOS 13 and macOS 10.15](#)

Export .p12 SSL Certificate from Windows

When managing mobile devices, it is considered best practice to install a root trusted SSL certificate on the FileWave Server. This certificate is located in the FileWave Admin > Preferences > Mobile tab. If you generated the Certificate Signing Request (CSR) for your SSL certificate on a Windows based system and have completed the certificate generation process, the SSL certificate and intermediates bundle can be exported as a .pfx file directly from Windows. This bundle would contain all components (private key, public certificate, Root CA certificate, and intermediate certificate bundle). This .pfx file (after renaming the extension to .p12) can then be uploaded to the FileWave Admin > Preferences > Mobile tab without any modification.

Step-by-step guide

- Open a Run dialog and enter "mmc".
- Go to File > Add/Remove Snap-in.
- Add the Certificates snap-in and click the Add > button in the middle.
- Add for the Computer account.
- Pick Local computer and click Finish.
- Click the OK button.
- In the MMC console browse to Certificates (Local Computer) > Personal > Certificates on the left. If your certificate is not there, browse the rest of the Certificates (Local Computer) tree until you find it.



- Select your certificate in the middle pane, right-click, and pick All Tasks > Export.
- When prompted pick Yes, export the private key.



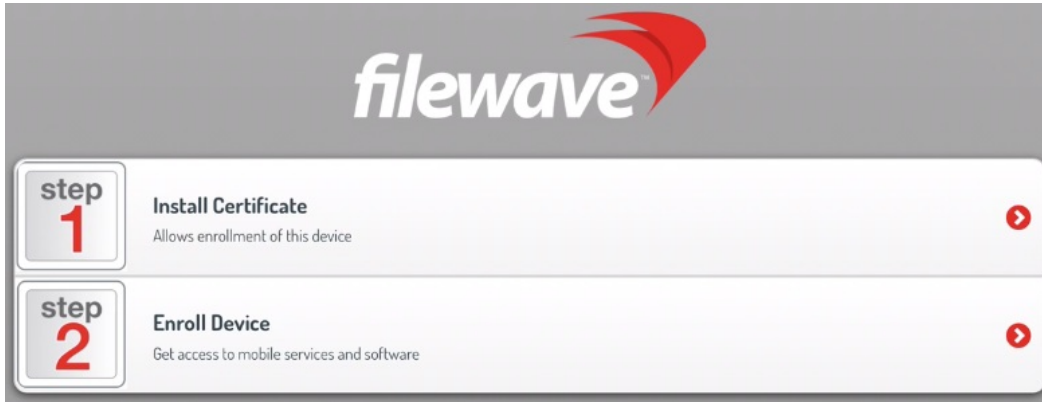
- Under Personal Information Exchange - PKCS #12 (.PFX) check Include all certificates in the certification path if possible. Leave the other 2 checkboxes unchecked.



- Click the Next button and specify an export password. The FileWave Admin will prompt you for this password when you attempt to upload the SSL certificate in the Preferences> Mobile tab.
- Save the file to your desktop.
- Change the file extension from .pfx to .p12.
- Upload .p12 file in the Mobile preferences tab of the FileWave Admin.

Determine Correct Intermediates Bundle for SSL Certificate

Some SSL providers include multiple intermediates certificate bundles along with your SSL certificate. Your SSL certificate must be merged with one of these intermediates bundles along with your private key to generate a .p12 certificate file that can be uploaded into the Mobile preferences tab of the FileWave Admin. If the incorrect intermediates bundle is used, two steps will appear during interactive MDM enrollment rather than one, like in the screenshot below. If the incorrect intermediates bundle is used, client devices will not be able to communicate with the FileWave MDM server correctly. There should normally only be one step listed, the one to "Enroll Device", if there are no certificate trust chain issues.



Step-by-step guide

Follow the steps below to determine the correct intermediates bundle to pair with your SSL certificate so that only one step appears on the interactive enrollment page.

1. Be sure to choose Apache format when downloading your SSL certificate from the your provider. If the certificate files do not have a .crt extension redownload them again and pick Apache format this time.
2. Go to the Intermediate Certificate Check page at <https://tools.keycdn.com/ssl>.
3. Paste the contents of your SSL .crt file from your SSL provider.
4. Follow it up with the contents of the desired intermediates .crt file right below it. The intermediates bundle may contain multiple certificates. Copy and paste them all into the Intermediate Certificate Check page below your SSL certificate.
5. Click the Validate button.
6. You'll receive a response stating either "No chain issues detected" in green or "Chain issues detected" in brown. If there are chain issues keep replacing the intermediates bundle with another one until there are no chain issues. The intermediates bundle that results in no chain issues is the one you need to use when generating your .p12 file for FileWave.

Decoder

This SSL check decodes your SSL certificates and validate intermediate certificate issues.

Certificate (PEM format)

```
-----BEGIN CERTIFICATE-----Certificate-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----Intermediate certificate-----END
CERTIFICATE-----
```

Q Validate

No chain issues detected.

Correct Intermediates Bundle

1. Subject CN: fw.lanrevcorp.com » Issuer CN: Go Daddy Secure Certificate Authority - G2
2. Subject CN: Go Daddy Secure Certificate Authority - G2 » Issuer CN: Go Daddy Root Certificate Authority - G2
3. Subject CN: Go Daddy Root Certificate Authority - G2 » Issuer CN:
4. Subject CN: » Issuer CN:

Decoder

This SSL check decodes your SSL certificates and validate intermediate certificate issues.

Certificate (PEM format)

```
-----BEGIN CERTIFICATE-----Certificate-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----Intermediate certificate-----END  
CERTIFICATE-----
```

Q Validate

Wrong Intermediates Bundle

Chain issues detected. Possible reasons are missing intermediate certificate or wrong order of the certificates.

×

1. Subject CN: fw.lanrevcorp.com » Issuer CN: Go Daddy Secure Certificate Authority - G2
2. Subject CN: Go Daddy Secure Extended Validation Code Signing CA - G2 » Issuer CN: Go Daddy Root Certificate Authority - G2

×

Self Signed Certificate Error during iOS OTA Enrollment

This article shows how to resolve an error if you are manually enrolling iOS 10.3+ devices in FileWave with a self-signed certificate.

It is considered a best practise to have a root trusted certificate defined in the FileWave> Preferences> Mobile> HTTPS certificate section. In FileWave v12+ it is easy to determine whether you have a self-signed certificate or not. Simply log into the FileWave Admin, open the preferences, go to the "Mobile" tab, and you will see in the HTTPS section, the following line:

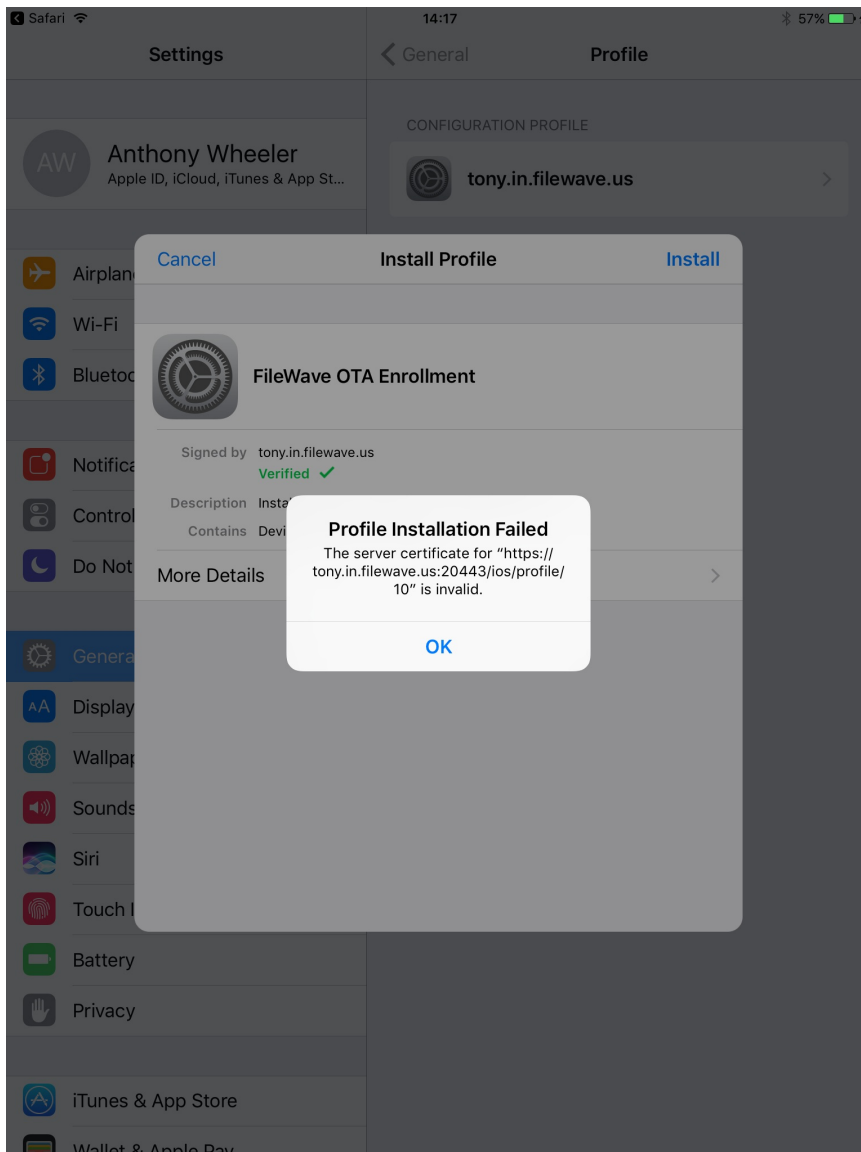
Warning: You are using a self-signed certificate. Your devices will need to trust the certificate to use FileWave. iOS 10.3+ devices require explicit trust before manual enrollment.

[Details...](#)

[Upload PKCS12 Certificate](#)

[Get Current Certificate](#)

If this is the case, you will still be able to enroll iOS 10.3+ devices through DEP. But if the device is iOS 10.3+ and you try a manual web enrollment (OTA), you will get the following error.



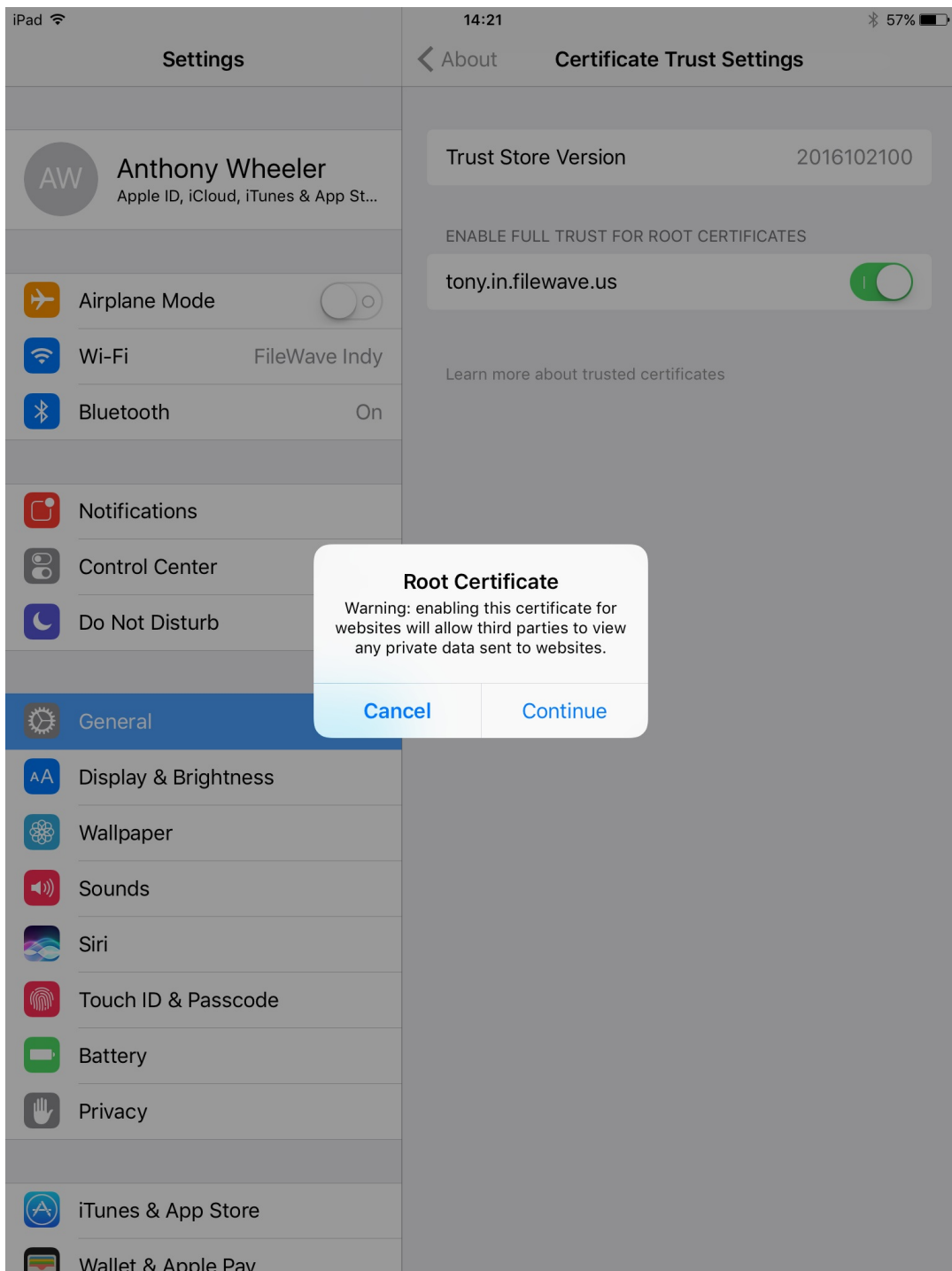
If you choose to retain your self-signed certificate, you will have to use the steps below to resolve the error. Alternatively, you can purchase a root trusted certificate, and you will not encounter this issue. Again, it is highly recommended that you purchase a root trusted certificate (can include a wildcard) so that you don't have to work around this trust issue, as described below.

Steps to Resolve (if you choose to keep a self signed certificate in place)

1. Navigate to the your manual enrollment address: <https://your.fw.server.DNS.here:20443/ios>
2. Select: "Step 1 - Install Certificate"

step 1	Install Certificate Allows enrollment of this device	➤
step 2	Enroll Device Get access to mobile services and software	➤

3. Once you have selected step one, the device will ask you to Install the cert, go through those three prompts by hitting Install each time and finally Done.
4. After the certificate has been installed, open the "Settings" app on the iOS device. Do not start Step 2 (This will prompt the error).
5. Go into General => About
6. At the bottom of the "About" section, tap the sub section called "Certificate Trust Settings"
7. You will see an option called ENABLE FULL TRUST FOR ROOT CERTIFICATES
8. Toggle that option for your newly installed certificate



Now go back to the manual enrollment page and finish the steps with "Step 2 - Enroll Device".

SSL Server Certificates - iOS 13 and macOS 10.15

Apple have updated their requirements for certificates for their new operating system releases: <https://support.apple.com/en-us/HT210176>

The new requirements can be broken down in the 3 major sections:

1. The mandatory presence of a Subject Alternative Name
2. Presence of an OID (1.3.6.1.5.5.7.3.1) designating the use of the certificate for TLS Web Server Authentication
3. Maximum validity period of 825 days

Requirement 1 is confirmed to render MDM clients unable to connect to the MDM server when not being met.

Requirements 2 and 3 are not currently (as of 24th of September 2019) interfering with MDM function when not being met. These two new requirements are not met by newly generated self-signed certificates as of FileWave Server 13.1.3 - so renewing your self-signed certificate will not mitigate this issue permanently. FileWave Server will be updated in a future release to accommodate these new guidelines in order to comply with self-signed certificates.

If you are using a self-signed certificate on a production server we recommend you purchase a valid 3rdparty certificate that has been signed by a [trusted root CA](#).

To verify whether your certificate is affected by a missing subject alternative Name, please run the following command on your Linux/macOS server :

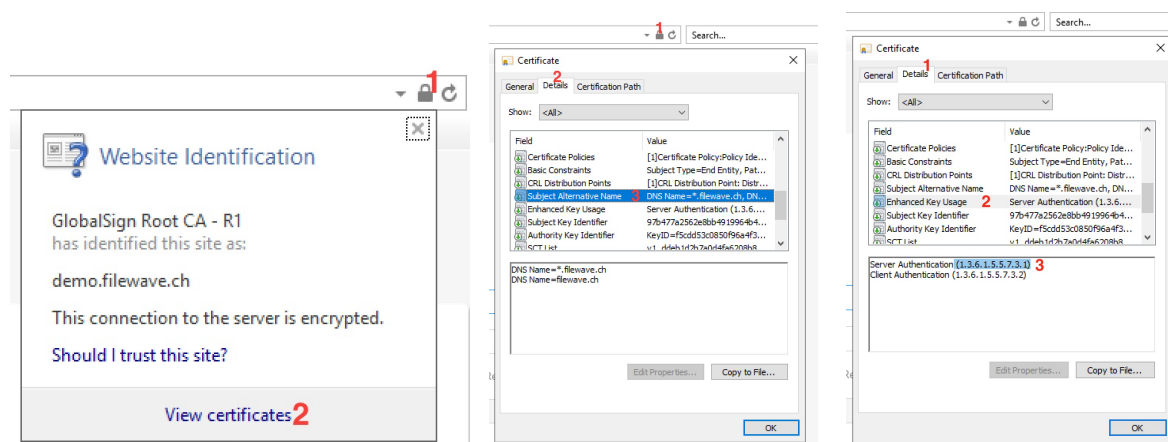
```
certSANCheck=$(openssl x509 -in /usr/local/filewave/certs/server.crt -text -noout | awk '/DNS/'; ); if [[ "$certSANCheck" == "" ]]; then echo "Certificate requires updating"; else echo "Certificate has SAN, no action required"; fi
```

If the above script returns "Certificate has SAN , no action required" , please verify the presence of the OID extension using the next snippet . Otherwise, please jump to "[Directions](#)" below to read on for instructions on how to mitigate this issue.

```
certOIDCheck=$(openssl x509 -in /usr/local/filewave/certs/server.crt -text -noout | awk '/TLS Web Server Authentication/'; ); if [[ "$certOIDCheck" == "" ]]; then echo "Certificate requires updating"; else echo "Certificate has OID, no action required"; fi
```

If the above script returns "Certificate has OID , no action required" , you can stop reading now . Otherwise, please check this page for updates on how to mitigate this issue .

To verify a Windows Server based Installation, please browse to your iOS enrollment page and verify the certificate as shown below :



If the above "Subject Alternative Name" is visible in the Certificate Details, and the "Enhanced Key usage" shows the OID 1.3.6.1.5.5.7.3.1, you can stop reading now. Otherwise, please read on for instructions on how to mitigate this issue.

Description

Apple have updated their requirements for certificates for their new operating system releases:

<https://support.apple.com/en-us/HT210176>

Some of these restrictions were in place with earlier versions of iOS and macOS:

Loss of Device Management



This could affect device communication if using non-compliant certificates. Certificate should be updated as per the following guide before updating devices or MDM device management will be lost.

Self-Signed and 3rd Party Certificates



Although this is likely to be an issue with older self-signed certificates, official 3rd party certificates could also be affected. Where 3rd party certificates are affected, contact your supplier for an updated certificate.

Information

Requirements:

- FileWave Server version 13.1.0+

Particular interest should be paid to the following:

- TLS server certificates must present the DNS name of the server in the Subject Alternative Name extension of the certificate. DNS names in the CommonName of a certificate are no longer trusted.

When using self-signed certificates, if the certificate does not have a SAN entry, it will no longer be trusted in Apple's new operating systems.

FileWave has an option to generate self-signed certificates:

```
sudo fwcontrol mdm generateSelfSignedCert --cn=fqdn [--country COUNTRY] [--state STATE] [--locality LOCALITY] [--organization ORGANIZATION] [--ou ORGANIZATIONAL_UNIT] [--email EMAIL] [--replace] [--ignore_name_mismatch]
```

However, earlier versions of FileWave did not generate a certificate with a Subject Alternate Name (SAN).

As of FileWave 13.1.0, fwcontrol generates a certificate that includes a SAN

Certificate Generation



Although a newer version of FileWave may be in place now, what is relevant here is the version of FileWave that was running when the certificate was generated.

Directions

This is a good opportunity to switch to an official SSL certificate, using our guide to ensure device management continuity:

[Root Trusted SSL Certificate \(Using and Renewing\)](#)

If you cannot make the switch at this time, please observe the following KB for distribution in profiles through MDM:

[Renew MDM self signed certificate](#)

For clients, the new certificate needs be added to the client's 'Trust Store' prior to making the pending generated certificate live. Details found on the following KB.

[Renew Self-signed Certificate - FileWave 13+](#)

Recovery

For devices upgraded when the server certificate did not meet requirements there are options:

- Obtain an official SSL 3rd party certificate (highly recommended)
- Manually install and trust the server certificate on each affected device
- Update the self-signed certificate as per the details then re-enrol all affected devices (may involve erasure of device)