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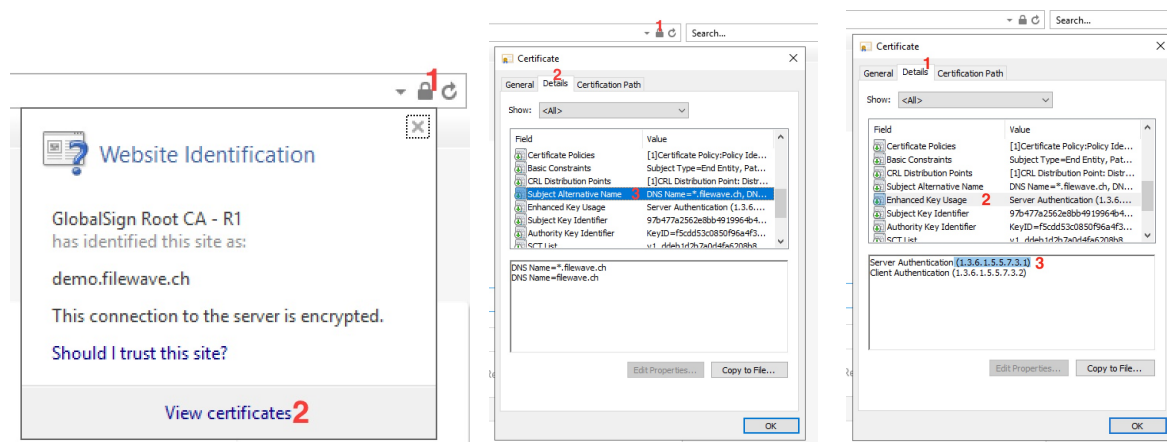
```
certSANCheck=$(openssl x509 -in /usr/local/filewave/certs/server.crt -text -noout | awk '/DNS/'; ); if [[
"$certSANCheck" == "" ]]; then echo "Certificate requires updating"; else echo "Certificate has SAN, no action
required"; fi
```

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.

> ℹ **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)

---