Adapting to Apple's TLS Server Certificate Validity Limits

What

This article provides guidance on adapting to Apple's updated policy regarding the maximum allowed lifetimes of TLS server certificates. Effective from September 1, 2020, 00:00 GMT/UTC, TLS server certificates must have a validity period no greater than 398 days. This policy, part of Apple's efforts to enhance web security, affects TLS server certificates issued from Root CAs preinstalled with iOS, iPadOS, macOS, watchOS, and tvOS.

When/Why

The policy is critical for administrators using FileWave to manage Apple devices. It ensures that device profiles and their associated TLS server certificates comply with the new security standards. Non-compliance results in network and application failures, and can prevent websites from loading on affected Apple devices.

How

To comply with Apple's policy:

1. Certificate Issuance and Renewal: Certificates should be issued with a maximum validity of 397 days to avoid edge case issues.
2. Check Existing Certificates: Certificates issued before September 1, 2020, are not affected by this change. However, their renewal must comply with the 398-day limit.
3. Profile Deployment in FileWave: Ensure all TLS server certificates embedded in profiles for Apple devices meet these validity requirements.
4. Monitoring and Planning: Regularly monitor certificate expiration dates and plan renewals accordingly.

Related Links

- Apple's Certificate Policy Announcement - Details on the TLS server certificate validity limit.
- RFC 5280, Section 4.1.2.5 - Reference for certificate validity period definition.

Digging Deeper

This policy shift reflects a broader move towards enhancing digital security and trustworthiness in online environments. By reducing certificate lifetimes, Apple aims to mitigate risks such as certificate compromise and mis-issuance. For FileWave users, adapting to these new requirements is essential for maintaining secure, reliable, and compliant management of Apple devices across various environments.