Apple Profile: ACME Certificate

What

The ACME Certificate profile is a new Apple Profile component introduced in FileWave 15.5.0 and above. This feature allows administrators to configure and manage ACME (Automatic Certificate Management Environment) certificates on Apple devices directly through FileWave. With this profile, devices can automatically obtain and renew digital certificates from an ACME server, streamlining certificate management and enhancing security across your organization's Apple devices.

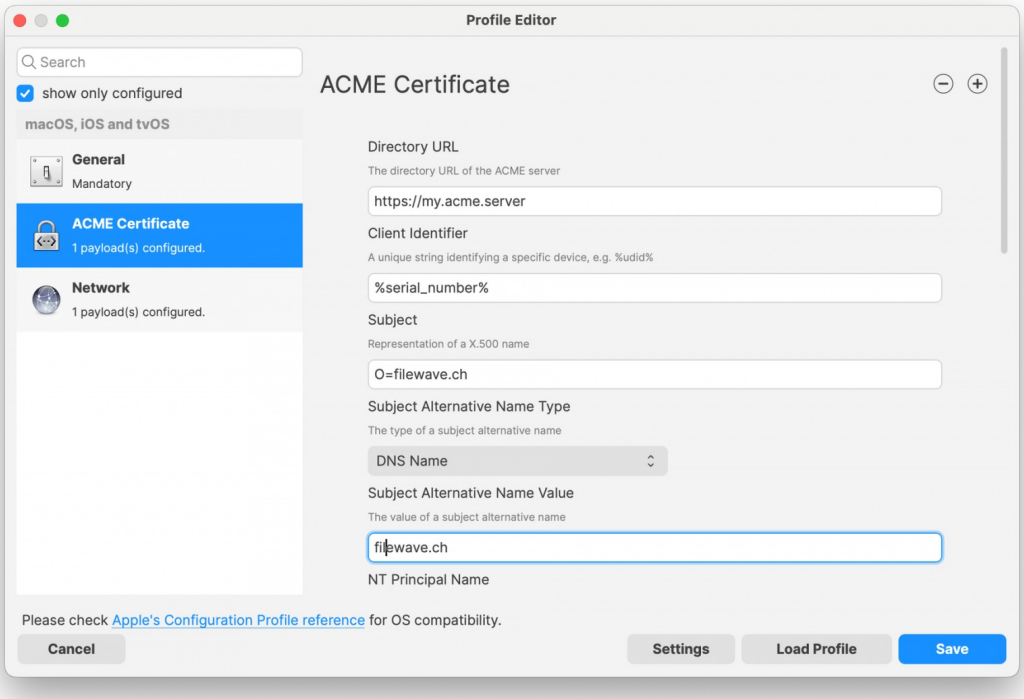
When/Why

Use the ACME Certificate profile when you want to automate the deployment and renewal of digital certificates on managed Apple devices using FileWave 15.5.0 or later. This is particularly useful for securing communications for services like HTTPS, Wi-Fi authentication, VPN connections, and email encryption. By leveraging ACME certificates through FileWave, you reduce administrative overhead, minimize the risk of service disruptions due to expired certificates, and ensure consistent security practices across all devices.

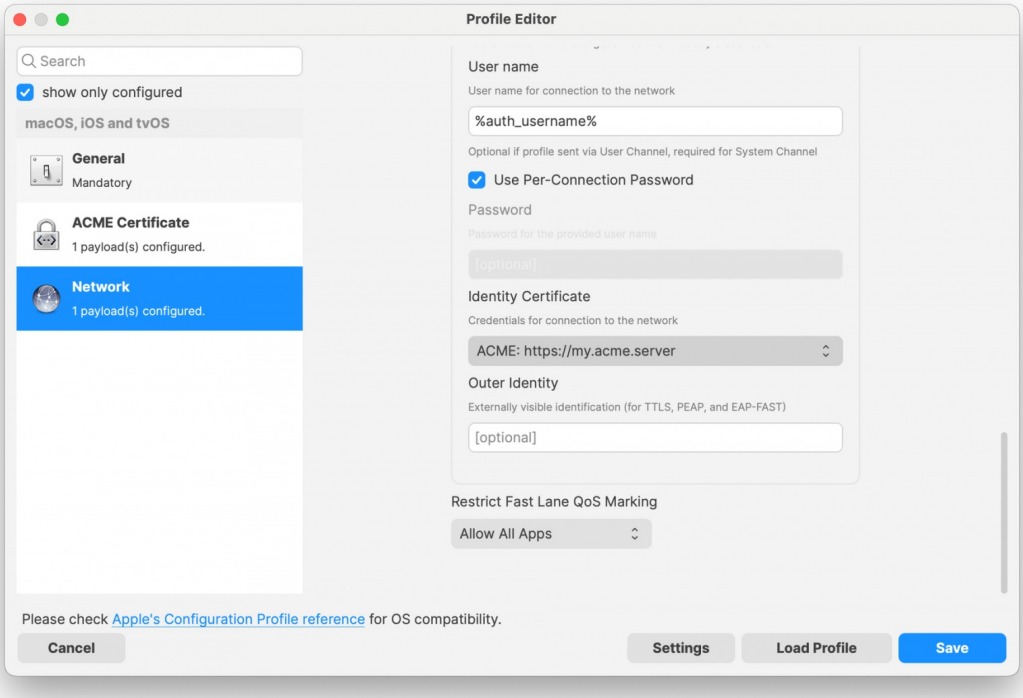
How

To configure the ACME Certificate profile in FileWave 15.5.0 and above:

1. Access the Profile Editor:
   - Open the Profile Editor within the FileWave Central or Anywhere interface.
2. Create a New Profile:
   - Select the option to add a new profile.
   - Choose the ACME Certificate payload from the list of available Apple Profile components.
3. Configure ACME Settings:
   - Directory URL: Enter the URL of your ACME server (e.g., Let's Encrypt).
   - Client Identifier: A unique string identifying a specific device (e.g., %udid%).
   - Subject: Specify the desired subject name for the certificate. (e.g., O=Company Name/CN=Foo).
   - Additional Options: Configure settings like key usage, extended key usage, and subject alternative names as required.



4. Reference ACME Payload in Other Profiles:
   - Other payloads, such as the Network payload, can reference the ACME Certificate payload, similar to how they would reference SCEP payloads.
   - This allows services like Wi-Fi configurations within the Network payload to utilize the ACME-issued certificates seamlessly for authentication.



5. Save and Deploy:
   - Ensure all required fields are completed correctly.
   - Save the profile and deploy it to the target Apple devices managed by FileWave 15.5.0 or later.

Note: The ACME Certificate profile is supported on devices running macOS 10.15 and later, iOS 14 and later, and iPadOS 14 and later. All profiles are signed according to the latest Apple requirements to ensure integrity and authenticity.

Related Content

- ACME Certificate Profile Documentation

Digging Deeper

With the introduction of the ACME Certificate profile in FileWave 15.5.0 and above, administrators can now integrate automated certificate management into their Apple device management workflows more efficiently. The ACME protocol automates interactions with certificate authorities (CAs), such as Let's Encrypt, to provision certificates without manual intervention.

A significant advantage of the ACME Certificate profile is its ability to be used alongside the Network payload within an Apple Profile. This means you can configure Wi-Fi or Ethernet settings in the Network payload and reference the ACME Certificate for authentication purposes. By doing so, devices can automatically obtain the necessary certificates for secure network access, streamlining the onboarding process for network services.

By allowing other configuration profiles to reference ACME payloads similarly to SCEP payloads within FileWave, you create a cohesive and efficient system for managing certificates across various services. This approach ensures that all network services relying on digital certificates have access to valid, up-to-date certificates, enhancing both security and user experience.

Implementing ACME certificates through FileWave 15.5.0 also contributes to cost savings by utilizing free certificate services like Let's Encrypt, eliminating the need for purchasing certificates from traditional CAs. Additionally, the automatic renewal feature reduces the administrative burden on IT staff and mitigates the risk of service outages due to expired certificates.

As security threats continue to evolve, automating certificate management with ACME profiles in FileWave 15.5.0 is a proactive step toward safeguarding your organization's data and communications. Regularly reviewing and updating your certificate policies in line with industry standards will further strengthen your security posture.

Revision #6
★Created 7 October 2024 13:36:22 by Josh Levitsky
✎Updated 4 November 2024 13:45:05 by Josh Levitsky