

SSL Certificate Management for Custom Domains (FileWave-Hosted Servers)

What

This article explains how FileWave can manage SSL certificates automatically using Let's Encrypt for customers who use their own custom DNS names (e.g., filewave.forrest.com) with FileWave-hosted servers. This eliminates the need for customers to manually renew SSL certificates, providing a more secure and convenient experience.

When/Why

When your FileWave Server is hosted by FileWave and you use a custom domain to access it, managing SSL certificates typically becomes your responsibility. However, FileWave now offers a way to automate this process using Let's Encrypt.

By delegating SSL management to FileWave:

- You no longer need to track certificate expiry or handle renewals manually.
- Your server remains secured with valid, trusted certificates.
- The process is seamless once set up—and currently free for hosted customers.

This option is ideal for organizations that:

- Use custom DNS names for branding or routing reasons.
- Prefer hands-off, automated certificate handling.
- Want to reduce reliance on third-party certificate management.

Note: While the service is currently free, FileWave may introduce a small future fee to support its ongoing development and maintenance. Customers will always be informed in advance and may choose to opt out and return to managing their own certificates.

How

To allow FileWave to manage SSL certificates for your custom domain, follow these steps:

1. Open a Support Ticket

Start by opening a ticket with FileWave Support via the IT Service Desk. Indicate that you want to enable SSL management for your custom domain.

The Support team will:

- Confirm your domain name of your FileWave Server.
- Open a ticket with the Cloud Team on your behalf.
- Provide you with the necessary DNS CNAME record value (based on a corresponding subdomain under filewave.net).

2. Add the Required CNAME Record to Your DNS

To allow FileWave and Let's Encrypt to automatically manage your SSL certificate, you need to add a CNAME record in your DNS settings. This record is used specifically for domain validation using the DNS-01 challenge method required by Let's Encrypt.

- Log in to your DNS provider's management console.
- Locate the area to add a new DNS record.
- Add a CNAME record with the following structure (values provided by FileWave Support):

Format:

```
_acme-challenge.<your-domain> IN CNAME _acme-challenge.<provided-subdomain>.filewave.net
```

Example:

```
_acme-challenge.filewave.forrest.com IN CNAME _acme-challenge.forrest.filewave.net
```

This CNAME allows the Let's Encrypt system to validate the domain through FileWave's infrastructure.

3. Check for Existing CAA Records

A CAA (Certification Authority Authorization) DNS record specifies which Certificate Authorities (CAs) are allowed to issue certificates

for your domain. If a CAA record exists and does not include Let's Encrypt (letsencrypt.org), then Let's Encrypt will not be able to issue or renew your certificate.

To enable FileWave to manage the certificate, ensure your DNS includes a CAA record like:

```
yourdomain.com. IN CAA 0 issue "letsencrypt.org"
```

If you already have CAA records that restrict certificate issuance to other CAs, you'll need to modify them to include Let's Encrypt.

 Need help with this? FileWave Support can assist in identifying and resolving any CAA-related issues during implementation.

4. FileWave Cloud Team Handles the Rest

Once the DNS CNAME record is in place, FileWave's Cloud Team will:

- Verify the DNS setup.
- Complete the configuration for SSL automation.
- Monitor and renew certificates automatically on your behalf.

Related Content

- [Cloud Hosting Product Information](#)

Digging Deeper

Let's Encrypt uses the ACME protocol to verify control of a domain before issuing a certificate. In this case, DNS-based challenges are used, where you prove ownership by creating a specific DNS record—an _acme-challenge CNAME pointing to a FileWave-managed subdomain.

By doing so, FileWave can securely respond to these challenges on your behalf, allowing the automation of issuance and renewal processes. This approach is especially useful when the server is behind load balancers, proxies, or hosted in environments where HTTP-based challenges (port 80) aren't feasible.

If you've ever missed a certificate renewal deadline or find SSL tedious to manage, this automation will save time and avoid outages due to expired certs.

🕒Revision #15

★Created 14 May 2025 15:30:34 by Josh Levitsky

✎Updated 22 May 2025 14:07:50 by Josh Levitsky