Cloud Hosting

- Cloud Hosting Product Information
- Cloud Hosting / Services Maintenance Schedule
- FileWave SaaS Service Level Agreement
- SSL Certificate Management for Custom Domains (FileWave-Hosted Servers)
- FileWave On-Premise Service Level Agreement

Cloud Hosting Product Information

Overview

Imagine you're running your FileWave server on a spare computer in your office. It seems like a cost-saving move at first, but then a power outage hits, and your server lacks a UPS. The database gets corrupted, and suddenly, your team scrambles to recover lost data. You realize the OS hasn't been patched in months, posing a security risk. When that old server finally dies, you're faced with the daunting task of migrating everything to a new machine. These are just a few scenarios that highlight the hidden costs and risks of self-hosting.

FileWave Cloud Hosting eliminates these concerns by handling backups, upgrades, and SSL certificates, allowing your team to focus on what they do best. It supports both FileWave Central and FileWave Anywhere administrative tools while maintaining your existing workflows.

Benefits of Hosted

Many benefits are outlined in the Cloud Hosting Current Customers.pdf, but key advantages include:

- Backups: No need to handle routine backups.
- Server Upgrades: Managed by FileWave.
- Business Continuity: Ensured in case of a disaster.
- Support Cases: Streamlined as access can be easily granted to support or development for issue diagnosis and resolution.

Differences from On-Premise

When transitioning to our Hosted service, there are a few differences to consider:

- FileWave Client IP Addresses - The FileWave server records the IP address the client is using to connect to the FileWave server. When clients are behind a router or firewall, the clients will only report their public (NAT) address to the FileWave server. This will not cause any issues with deployment or management of the clients.
- Fileset Uploads - Administrators should be aware that there is no "resume" feature for large Fileset uploads. If an upload fails, the incomplete Fileset will need to be deleted and the upload can be attempted again.
- Boosters - Since the Server is remote, if you have Windows or macOS systems, you must have Boosters to handle the traffic. There must be at least 1 Booster per 2000 systems that is Internet facing if clients will be outside of a LAN environment. Boosters will also cache Microsoft OS updates in addition to other Filesets.

Why Choose FileWave Cloud Hosting Over Self-Hosting?

While it might seem cheaper to run FileWave on a spare server, consider the hidden costs:

- Backups: Will you consistently perform and verify backups?
- Power Protection: Does your server have a UPS to prevent data corruption during power failures?
- Security: Are you regularly patching the OS for security updates?
- Hardware Lifecycle: When the server reaches end-of-life, are you prepared to migrate to a new machine without additional costs?
- Disaster Recovery: If the server's hard disk fails, can you quickly restore service?

These challenges are seamlessly managed by our dedicated cloud team, ensuring your FileWave server runs smoothly and securely.

Pricing

Please contact Customer Success for a quote. There is a one-time charge for the FileWave Server Migration and an annual charge based on the number of devices. The pricing is comparable to going directly to Amazon for their hosting.

Related Content

- Cloud Hosting / Services Maintenance Schedule
- Backup Procedures for FileWave Hosted Servers
- Your Hosted FileWave Server Has Been Upgraded - What Are Your Next Steps?

Cloud Hosting / Services Maintenance Schedule

Maintenance

This document serves as a detailed guide to the deployment and maintenance processes for FileWave's array of services. Our aim is to clearly present the methods and strategies employed to deploy and sustain the optimal functioning of our services. It encompasses a range of topics from maintenance schedules and procedures to deployment guidelines, providing our customers with a clear understanding of how we ensure the efficiency and reliability of our services in their diverse technological environments.

Regular Weekly Maintenance Period

This section outlines the standard weekly maintenance schedule relevant to our routine operations. It is essential to recognize that this schedule exclusively pertains to regular maintenance activities and does not encompass FileWave Version Upgrades, Incident Responses, or any additional maintenance intervals that may be communicated separately.

Region Name	Region ID	Weekday	Local Time	CET	CEST
US East (N. Virginia)	us-east-1	Tuesday	UTC 07:00 - 09:00	8:00 - 10:00	09:00 - 11:00
Europe (Frankfurt)	eu-central-1	Wednesday	CET/CEST 21:00 - 23:00	21:00 - 23:00	21:00 - 23:00
Asia Pacific (Singapore)	ap-southeast-1	Thursday	SGT 21:00 - 23:00	14:00 - 16:00	15:00 - 17:00
Asia Pacific (Tokyo)	ap-northeast-1	Thursday	JST 21:00 - 23:00	13:00 - 15:00	14:00 - 16:00
Asia Pacific (Mumbai)	ap-south-1	Thursday	IST 21:00 - 23:00	16:30 - 18:30	17:30 - 19:30

Special Maintenance Period

In our commitment to transparency and minimizing operational impact, we proactively notify customers about impending special maintenance periods. Notifications are typically issued at least one week in advance, accompanied by details of the anticipated duration of downtime for each service. The execution of these maintenance activities adheres to the specific time frames detailed in the accompanying table, ensuring clarity and predictability for our customers.

Region Name	Region ID	Local Time	CET	CEST
US East (N. Virginia)	us-east-1	UTC 05:00 - 10:00	06:00 - 11:00	07:00 - 12:00
Europe (Frankfurt)	eu-central-1	CET/CEST 21:00 - 06:00	21:00 - 06:00	21:00 - 06:00
Asia Pacific (Singapore)	ap-southeast-1	SGT 21:00 - 06:00	14:00 - 23:00	15:00 - 00:00
Asia Pacific (Tokyo)	ap-northeast-1	JST 21:00 - 06:00	14:00 - 22:00	15:00 - 23:00
Asia Pacific (Mumbai)	ap-south-1	IST 21:00 - 06:00	16:30 - 01:30	17:30 - 02:30

Emergency Maintenance

During emergency maintenance scenarios, our primary objective is the rapid resolution of the issue at hand. We commit to informing our customers about such emergencies at the earliest opportunity, with the timing of communication being carefully calibrated according to the incident's severity. This approach ensures that our focus remains firmly on swift resolution, while still keeping our customers duly informed as the situation progresses.

Deployment Guidelines

FileWave Server

- Major/Minor Version Upgrades: These upgrades are to be scheduled during the Special Maintenance Period. Customers will be notified one week in advance of the scheduled upgrade.
- Patch Version Upgrades: Depending on the severity of the fix, these upgrades should be scheduled either during the Special Maintenance Period or announced as Emergency Maintenance. Notification to customers will be given as soon as possible.

Infrastructure

- Non-Emergency Changes Causing FileWave Server Downtime: These are to be scheduled within the Regular Weekly Maintenance Period. No separate communication will be issued for these changes.
- Emergency Changes Causing FileWave Server Downtime: These changes can be scheduled at any time, with notifications to customers provided as soon as possible.
- Changes Not causing FileWave Server Downtime: These can be scheduled at any time and do not require prior communication with customers.

Related Content

- Cloud Hosting Product Information

FileWave SaaS Service Level Agreement

This Service Level Agreement (this “SLA”) is incorporated into the Terms of Service between FileWave and Customer (the “Agreement”).

The provisions of the Terms of Service resp. End-User License Agreement also apply to this SLA.

A. DEFINITIONS

“Designated Support Liaisons” means the two individuals specifically designated by Customer to coordinate error response and FileWave support.

*Note—Customer may request additional Designated Support Liaison(s) for an additional fee.

“Level 1 Error” refers to an error, excluding any Maintenance Period, that causes the FileWave server to cease operating, and which is likely to cause widespread or irreversible damage to the customer’s existing deployment or infrastructure.

“Level 2 Error” refers to an error, excluding any Maintenance Period, that causes the FileWave server to fail in regard to a critical or primary function in the current deployment environment, and which may cause reversible or localized damage to the customer’s existing deployment or infrastructure.

“Level 3 Error” refers to an error or product behavior, excluding any Maintenance Period, that causes a failure or undesired output from a minor component in the FileWave system, and while the error or behavior may be inconvenient for the customer, it does not cause imminent or irreversible damage to their deployment.

“Level 4 Error” refers to a minor error or unexpected product behavior, excluding any Maintenance Period, which includes user support for requests of best practices, templates, guidance for deployments, or feature requests.

“Maintenance Period” refers to any scheduled maintenance on the SaaS platform. FileWave will announce planned maintenance in advance to ensure minimal disruption. Details about scheduled maintenance, including timing and expected impact, will be available on our Cloud Hosting / Services Maintenance Schedule. Emergency maintenance may occur without prior notice.

“Response” refers to an email, telephone, or in-person acknowledgment of a Trouble Ticket.

“Trouble Ticket” means a written trouble ticket properly submitted to FileWave at help.filewave.com or help@filewave.com by one of Customer’s Designated Support Liaisons.

B. BACKUP

FileWave will perform daily backups of all Customer Data and securely retain these backups for a period of thirty (30) days. After this retention period, older backups will be automatically overwritten. FileWave is responsible for ensuring the accuracy and integrity of these backups and will take all reasonable measures to protect Customer Data during the backup process.

C. ERROR RESPONSE TIME AND REMEDY

Level 1 Error – Response Time: 2 Hours.

FileWave will work to restore the server to a state of normal operation. This may be achieved using a work-around, temporary solution while a more permanent solution is found.

Level 2 Error – Response Time: 4 hours.

FileWave recognizes that this emergency may be caused by outside factors (deadlines, deployments, unexpected load) and will work to resolve the issue as quickly as possible for the customer.

Level 3 Error – Response Time: 8 hours.

FileWave will assist the customer in navigating around this issue while working to determine the root cause. If the issue is found to result from a defect in the FileWave product, the FileWave support team will follow the procedures for a Level 1 or 2 incident. If the issue is due to incorrect or lack of documentation, the support team will ensure the documentation is appropriately updated.

Level 4 Error – Response Time: 24 hours.

FileWave is available to assist customers with questions regarding best practices or other issues with their deployments. Every effort will be made to ensure these questions are answered in a timely fashion and feature requests are properly documented and delivered to the correct departments.

D. SUPPORT AVAILABILITY

FileWave provides technical support 24 hours a day, 5 days a week (24/5), from Monday to Friday. Support requests submitted outside these hours, including weekends, may not receive immediate attention and could be addressed on the next business day.

E. CUSTOMER RESPONSIBILITIES

Server access:

For Level 1, 2, and 3 Errors, FileWave may need access to mission-critical servers and services (such as the customer's FileWave server and related infrastructure). To assist with this support, the customer agrees to provide FileWave with system-level control of FileWave servers and appliances, or to remain available during the performed work to grant access on an as-needed basis for the support team. Failure to provide access to the required servers may impede FileWave's ability to help resolve the issue.

Data collection:

FileWave may be required to capture a copy of the customer's database and logs to further investigate the issue with the development team by using our uploader tool (UT) or by a manual process.

Environment access:

For all levels of incidents, FileWave may require access to the customer's environment. This access will be provided using a screen-sharing tool or other remote access methodology to be determined during work on the incident.

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.

FileWave On-Premise Service Level Agreement

This Service Level Agreement (this “SLA”) is incorporated into the Terms of Service between FileWave and Customer (the “Agreement”).

The provisions of the Terms of Service resp. End-User License Agreement also apply to this SLA.

A. DEFINITIONS

“Designated Support Liaisons” means the two individuals specifically designated by Customer to coordinate error response and FileWave support.

*Note—Customer may request additional Designated Support Liaison(s) for an additional fee.

“Level 1 Error” refers to an error, excluding any Maintenance Period, that causes the FileWave server to cease operating, and which is likely to cause widespread or irreversible damage to the customer’s existing deployment or infrastructure.

“Level 2 Error” refers to an error, excluding any Maintenance Period, that causes the FileWave server to fail in regard to a critical or primary function in the current deployment environment, and which may cause reversible or localized damage to the customer’s existing deployment or infrastructure.

“Level 3 Error” refers to an error or product behavior, excluding any Maintenance Period, that causes a failure or undesired output from a minor component in the FileWave system, and while the error or behavior may be inconvenient for the customer, it does not cause imminent or irreversible damage to their deployment.

“Level 4 Error” refers to a minor error or unexpected product behavior, excluding any Maintenance Period, which includes user support for requests of best practices, templates, guidance for deployments, or feature requests.

“Maintenance Period” refers to any scheduled maintenance on the SaaS platform. FileWave will announce planned maintenance in advance to ensure minimal disruption. Details about scheduled maintenance, including timing and expected impact, will be available on our Cloud Hosting / Services Maintenance Schedule. Emergency maintenance may occur without prior notice.

“Response” refers to an email, telephone, or in-person acknowledgment of a Trouble Ticket.

“Trouble Ticket” means a written trouble ticket properly submitted to FileWave at help.filewave.com or help@filewave.com by one of Customer’s Designated Support Liaisons.

B. BACKUP

The Customer is solely responsible for performing regular backups of all Customer Data stored on the FileWave server. The Customer must ensure that these backups are conducted daily and securely retained for a period that meets their data retention and recovery requirements. FileWave is not responsible for the accuracy, integrity, or protection of Customer Data during the backup process. The Customer must take all reasonable measures to safeguard their data, including the use of appropriate backup tools and practices.

C. ERROR RESPONSE TIME AND REMEDY

Level 1 Error – Response Time: 2 Hours.

FileWave will work to restore the server to a state of normal operation. This may be achieved using a work-around, temporary solution while a more permanent solution is found.

Level 2 Error – Response Time: 4 hours.

FileWave recognizes that this emergency may be caused by outside factors (deadlines, deployments, unexpected load) and will work to resolve the issue as quickly as possible for the customer.

Level 3 Error – Response Time: 8 hours.

FileWave will assist the customer in navigating around this issue while working to determine the root cause. If the issue is found to result from a defect in the FileWave product, the FileWave support team will follow the procedures for a Level 1 or 2 incident. If the issue is due to incorrect or lack of documentation, the support team will ensure the documentation is appropriately updated.

Level 4 Error – Response Time: 24 hours.

FileWave is available to assist customers with questions regarding best practices or other issues with their deployments. Every effort will be made to ensure these questions are answered in a timely fashion and feature requests are properly documented and delivered to the correct departments.

D. SUPPORT AVAILABILITY

FileWave provides technical support 24 hours a day, 5 days a week (24/5), from Monday to Friday. Support requests submitted outside these hours, including weekends, may not receive immediate attention and could be addressed on the next business day.

E. CUSTOMER RESPONSIBILITIES

Server access:

For Level 1, 2, and 3 Errors, FileWave may need access to mission-critical servers and services (such as the customer's FileWave server and related infrastructure). To assist with this support, the customer agrees to provide FileWave with system-level control of FileWave servers and appliances, or to remain available during the performed work to grant access on an as-needed basis for the support team. Failure to provide access to the required servers may impede FileWave's ability to help resolve the issue.

Data collection:

FileWave may be required to capture a copy of the customer's database and logs to further investigate the issue with the development team by using our uploader tool (UT) or by a manual process.

Environment access:

For all levels of incidents, FileWave may require access to the customer's environment. This access will be provided using a screen-sharing tool or other remote access methodology to be determined during work on the incident.