FME® Cloud Security

SAFE SOFTWARE

Table of Contents

Safe Software's entire business is built on data, and we understand that it is among the most important assets of any organization. The security and privacy of your data is our highest priority.

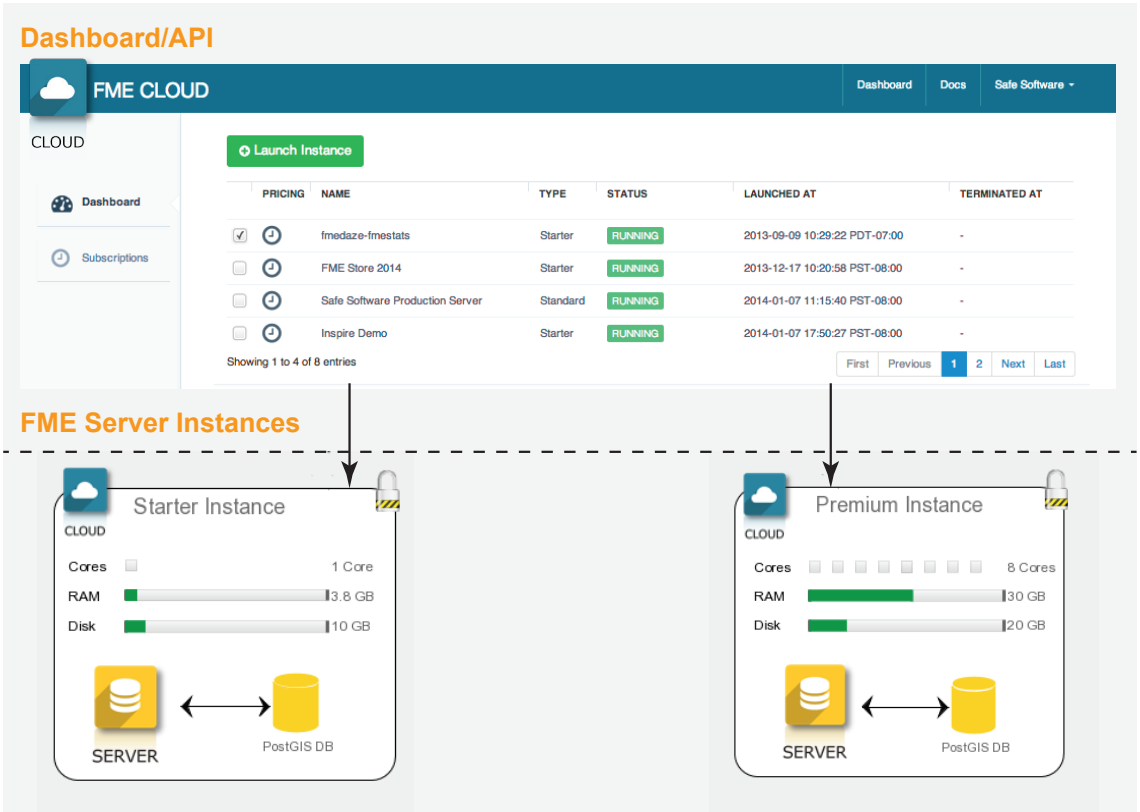
Safe Software's FME Cloud security features manage operational security, user security, data security, application security and transmission security. To keep you secure, we:

- Engage in secure design practices.
- Continuously identify and address security threats.
- Focus on operational processes.
- Employ third-party organizations to perform audits.

FME Cloud Architecture Overview

To understand FME Cloud security, a grasp on the architecture is crucial. Two components comprise FME Cloud. The first component is the dashboard/API, hereon referred to as the FME Cloud tier. This is a multi-tenant application where you sign up, launch/manage FME Server instances, and conduct billing and account management.

The second component are the FME Server instances. These are where you publish your workspaces and associated data. Each FME Server instance is a self-contained environment, isolated from other instances, and includes compute, storage, and database services. Unlike some other cloud providers, no functionality is shared between virtualized instances. Under our single tenancy model, customers own and operate their own instances. Since all FME Server functionality can be accessed via the web interface or API, there is no direct access to the server.



Secure Operations

Safe Software's internal policies control how we manage the infrastructure and developments of FME Cloud. These policies complement the controls that our IaaS provider, Amazon Web Services, provides.

Backup

FME Cloud Tier

Database backups are taken every 12 hours, and we keep the last 20. We also take a snapshot of the entire stack, every 24 hours, and these persist for 90 days.

FME Server Instances

- Backup created automatically every 24h while the instance is running.
- Backup created automatically after an instance is stopped.
- Backup created automatically before an instance configuration changes (such as a change in instance type).
- The last 15 automatic backups are kept.
- Backups can be triggered manually by the user. These are kept indefinitely until the instance is terminated or the user deletes them.

If the need ever arises to rebuild an instance, the customer can restore an instance from previous backups. Once an instance is terminated, all data associated with the instance is immediately destroyed.

Data Governance and Privacy

FME Cloud Tier

FME Cloud does not receive, process, or store customer credit card information in its infrastructure. Our billing page redirects to a third-party payment processing service, Braintree, that is fully PCI DSS compliant.

FME Server Instances

Your data is your own, even when stored on your FME Server instances.

Only your authorized users have access to data or workspaces stored on an FME Server instance. Safe Software employees and other customers do not have access to your data. The only exception is a small and controlled number of Safe Software system administrators who have access to the entire system. These administrators can only access your data under very controlled circumstances. You will receive an automated e-mail whenever an administrator accesses your instance, and all operations are logged.

Safe Software does access and monitor metrics on system utilization and performance, including disk usage, network throughput, server load, and application monitoring. By checking the performance and reliability of the server, we can alert you if there are any problems.

Destruction of Data

Upon termination of your FME Cloud account, assuming there is no outstanding balance, Safe Software destroys all data associated with your account, including any running instances and data associated with those instances.

Incident Reporting

Safe Software is committed to reporting any incident that may impact the customer as soon as possible, especially when customer data could be involved. Of course, it is our hope that we never have to notify you of such a reason.

If you believe you have discovered a bug in Safe's security, please get in touch at support@safe.com. We ask that you not publicly disclose the issue until it has been addressed.

Development

Safe Software engages in best practice techniques for software development, including code reviews, automated bug testing, and staging environments for manual testing. Continuous vulnerability testing is also in place to ensure any new threats are identified and addressed.

Working with a CISSP-certified third party, we incorporate on-board feedback to ensure we are always developing with security on our minds.

Customer Data Locations

All our physical infrastructure is hosted and managed by Amazon Web Services (AWS) via their secure data centers. An industry leader in cloud computing, AWS continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

AWS's data center operations are accredited under:

- ISO 27001
- SOC 1/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

For more information about AWS compliance, see the AWS Risk and Compliance whitepaper.

Application Security

FME Cloud Application Security

The FME Cloud tier is built and designed using industry-standard security practices. The web application is accessed via an SSL-encrypted user login. Password rules and a password strength meter are in place to encourage users to choose secure passwords. Two-step authentication can also be configured to add an extra layer of protection to the authentication process.

The API that provides programmatic access to various components of the applications is implemented using the OAuth 2.0 bearer token standard.

Upgrade and Maintenance

Both the operating system and database are upgraded/patched as releases become available. Patches are applied to the staging environment first to ensure they do not cause issues.

FME Server Application Security

Access to FME Server instances is limited to a web user interface and API (customers cannot use SSH). Like the rules for setting up an inbound network firewall, customers can control the protocols, ports, and source IP ranges that are allowed to reach your instance.

FME Server Configuration

FME Server has the flexibility to meet any organization's needs. FME Server ships with its own security module that gives an administrator full control over:

- Which resources should provide unauthenticated access?
- Which resources should users have access to, and what permissions should they have on those resources?

Roles

FME Server security controls access to resources with role-based access control. Within an organization, users are grouped into roles. FME Server ships with five roles by default. Roles are created for various job functions. Permissions to perform certain operations are assigned to specific roles. Custom roles can also be created for more control over who can access what.

For full details see Securing FME Server in the FME Server Documentation.

Upgrade and Maintenance

You are in control of how your FME Server instance is patched. We only apply security patches to running instances. When you launch an instance, you have three options:

1. **No patching:** We never apply security patches to the instance.
2. **Fully automated:** We apply security patches to the instance as they become available, and we will e-mail you if the instance needs restarting at any point.
3. **On restart/pause:** Whenever you restart or pause the instance, any available security patches are applied. (If this option is selected, keep in mind that if you do not restart the instance often, your server may become ome vulnerable.)

Risk Assessments

Application design is a combination of secure design practices and regular audits. To ensure the security of FME Cloud and FME Server, we worked with a third-party Certified Information Systems Security Professional (CISSP) and certified by Visa for PCI assessments (QSA, PA-QSA) organization to complete an application and network security audit. This included network vulnerability scanning, penetration testing, and an architecture review.

Shared Responsibility

Because the customer has a part to play in securing its FME Server instances, Safe Software, our IaaS providers, and our customers jointly share security responsibilities across different domains.

IaaS Provider (AWS)	PaaS Provider (FME Cloud)	Customer
▪ Virtualization layer ▪ Network security (including DDOS, spoofing, and port scanning mitigation) ▪ Physical and environmental security	▪ Operating system security ▪ Database security ▪ Network security (ports/ protocols) ▪ Vulnerability management, including patching and testing ▪ Support access	▪ Access control ▪ FME Server security configuration

Network Security

All connections are over SSL using high-grade encryption (128-bit, RC4). FME Server uses basic authentication to provide the user name and password to the server. HTTPS is configured on all FME Server instances, which encrypts the data and protects user names and passwords from malicious interception of transactions.

On-Premise Deployment of FME Server

Some customers require that their FME solution is completely isolated from the Internet, and therefore the Cloud offering is not feasible. FME Server technology can be deployed on-premise.

Please contact sales@safe.com for more information.

SAFE SOFTWARE