Safe Software FME

Security Whitepaper

FME Form

2024.2 | V1.0

Contents

1 Introduction

Safe Software's operations are fundamentally centered on data, which is recognized as one of the most critical assets of any organization. Ensuring the security and privacy of data is the highest priority. This whitepaper outlines Safe Software's approach to security and compliance and describes the organizational and technical controls implemented to protect client data.

Security practices and safeguards are integrated across all technologies, programs, and processes. For over 30 years, Safe Software has collaborated with customers in highly regulated industries, including government, healthcare, and utilities. Each customer trusts FME to deliver data-driven solutions for improved decision-making.

This whitepaper provides an overview of how security practices are applied to FME Form, outlining critical considerations for administrators regarding the maintenance of product security, and offering guidance on how Safe Software can collaborate with organizations to ensure security throughout the lifecycle of these products.

2 System Architecture

FME Form, formerly FME Desktop, is a desktop-based application designed to enable the creation of data integration workflows through a visual interface. Data integration workflows can be authored in FME Form and automated or deployed using FME Flow, formerly FME Server. **FME Engine** is the data processor powering the data transformation, and is a core component of FME Form. This Whitepaper is inclusive of FME Form and its component, FME Engine.

FME Form is an on-premises solution, deployed by system administrators within an organization's environment. Additionally, FME Form offers various options for credential storage and transport, allowing organizations to balance functionality with security to suit specific use cases and environments.

Trust Relationships

FME Authors are trusted developers, designated and managed by the customer, who are responsible for creating the workflows, known as workspaces, that drive data transformation and integration within an organization. Utilizing FME Form, FME Authors configure various data manipulation tools, called transformers, to build custom workflows that best meet an organization's specific integration and transformation needs. FME Authors can establish connections to various data sources and destinations, such as databases, cloud services, APIs, and GIS platforms, enabling FME to integrate with other systems.

2.1 Storage Security

FME Form secures data at rest by utilizing the operating system's native cryptographic APIs to store credentials for third-party services and integrations. These credentials are accessible only to the current operating system user. For external web and database API connections, FME Form also applies a combination of AES and OS encryption algorithms, with keys securely stored in various types of OS vaults depending on the platform, ensuring enhanced credential protection.

FME Form provides options for securely sharing credentials across an organization, intended for managing connections to external systems that FME Form interacts with. System administrators control access to these shared credentials using operating system file permissions, ensuring that only authorized users can access and use them.

Credential data explicitly identified as a password type may also be stored within individual workspace files, where passwords are encrypted rather than in plain text.

2.2 Network Security

Data in transit between FME Form, FME Flow, and other client applications is encrypted using AES-128. FME Form employs a custom handshake over TLS to establish identity, followed by an exchange of temporary AES-encoded Data Encryption Keys (DEKs) over TLS. The data is then sent encrypted with the DEK, ensuring secure transmission. FME Form provides options to configure secure network transport settings where applicable, such as secure credential transport encryption to further enhance network security. In some cases, such as connections to FME Flow, the default state is to use more secure protocols like HTTPS/SSL, including support for TLS 1.2, for secure network transport.

FME Form offers administrators the flexibility to customize the installation and environment, including options to configure FME Form to connect through a proxy server, use certificate management, or apply other network-specific security protocols, features, or authentication methods.

FME Form accesses FME Flow to securely share credential data using modern encryption algorithms via Flow REST APIs, securely identifying itself to FME Flow. Credential data is only shared across the REST API when the API is called by FME Form. Additional controls are available for FME Flow administrators to manage credential access and prevent identity spoofing, including control over access frequency, token expiry, and user permissions.

FME Form connects to an internal AI Service via token-based authentication and sends encrypted traffic to and from the AI Server to maintain transport security for prompts, data, and responses. Connections to the AI Service may be blocked at the firewall level for the fme-ai-service.safe.com domain.

FME Form allows connection to FME Hub to access additional downloadable components that extend the functionality of the shipped product. FME Hub APIs are publicly accessible and use HTTPS transport encryption, though no additional authentication is required to access these resources.

Usage statistics for FME Form, if enabled, are anonymized and are intentionally devoid of credential data or personally identifiable information before being sent. These statistics are sent exclusively to Safe Software and used solely for product improvement. They are logged separately from translation logs.

FME Form readily integrates with third-party APIs, which may use various protocols and security features, depending on the API and its services. Examples of services include access to background maps, system integrations, and file or web service processing. Where applicable, FME Form enables customization of connection protocols and related options to align with the specific requirements of the API and its services.

2.3 Access Control

Access control is managed by FME Form administrators via the operating system, restricting permissions to critical default or user-selected path locations, such as the installer, user workspaces, and temporary folder locations. It is the organization's responsibility to enable and manage access according to their specific policies and requirements, forming the foundation for FME Form application security.

As noted, the organization's administrators provide the first layer of access control to FME Form through the configuration of local machine resources, such as file system and operating system access controls. These resources include default paths for user content, downloaded FME Hub components, application installation, and temporary files. FME Form allows customization of some of these locations to better suit the organization's environment and security requirements.

Additionally, FME Form offers the option to password-protect individual workspaces, custom formats, and custom transformers to manage access to these resources. With password protection enabled, only individuals who have been provided with the password can view or edit the protected resource. Furthermore, applying password protection encrypts the resource, providing another layer of security.

3 Application Security

Safe Software follows the principle that software should be built securely through all the stages of the development lifecycle. The following activities are undertaken to ensure that security remains a priority in the development of the products.

3.1 Security Requirements

Safe Software is actively pursuing alignment with the Open Worldwide Application Security Project (OWASP) Application Security Verification Standard (ASVS). A subset of Level 2 controls applicable to the system is being diligently adopted, ensuring that the application has the appropriate level of built-in security controls, based on this leading industry standard. To ensure authenticity, all our installers and principal executables are digitally signed.

3.2 Automated Security Testing

Multiple commercial and internally developed tools regularly monitor FME Form for potential security vulnerabilities. Static analysis and Software Composition Analysis (SCA) tools scan both first-party code and third-party libraries for vulnerabilities. Any identified security issues are triaged and addressed promptly, in accordance with vulnerability management guidelines, which are aligned with and based on the NIST Secure Software Development Framework (SSDF).

3.3 Threat Modeling

During the design phase of systems, Safe Software identifies security risks early by understanding how potential attackers could exploit application vulnerabilities. This proactive approach allows for the implementation of necessary protections before threats can materialize. The team is trained by application security experts in the principles of threat modeling, a structured process that systematically evaluates potential attack vectors, assets at risk, and the effectiveness of existing security controls. Threat modeling is applied throughout the product development lifecycle, ensuring that security considerations are embedded from initial design to final deployment. This approach enables the anticipation and mitigation of potential security threats as applications evolve.

3.4 Security Code Review

Mandatory, independent reviews of the source code are conducted to identify potential security issues before new code is integrated into applications. This approach significantly reduces the risk of introducing security vulnerabilities during product development.

3.5 Software Supply Chain Security Management

Safe Software's Software Supply Chain Security program ensures that all third-party components embedded in or shipped with FME comply with all legal and licensing obligations and internal security requirements.

Automated scanning tools, alongside dedicated personnel, are employed to continuously monitor, triage, and track known security vulnerabilities. This ensures that third-party components are updated promptly.

The FME Form license includes a Legal Notices file, located at <install directory>/res/FME Form Legal Notice.html. This file provides a list of Free and Open Source (FOSS) components used in the specific version of FME Form. A copy of the Legal Notices is also available on Safe Software's website FOSS page.

3.6 Vulnerability Disclosure Program

Safe Software welcomes feedback from security researchers and the public to help improve the security of its products. If a vulnerability, privacy issue, data exposure, or other security concern is identified in any Safe Software asset, reporting it is encouraged. The Vulnerability Disclosure Policy outlines the procedure for reporting vulnerabilities, including the requirements for submission and the expected response process.

Although monetary rewards are not offered for vulnerability disclosures, Safe Software values and appreciates the time and effort taken by individuals to report security vulnerabilities in accordance with this policy.

3.7 Third-Party Application Security Assessments

To thoroughly test and examine the third-party components of FME Form, Safe Software follows the best practices framework outlined in OWASP's Security Testing Guide (WSTG). This guide is a widely recognized cybersecurity resource, compiled by established cybersecurity professionals and volunteers in the field.

Guided by the WSTG framework, third-party security experts are regularly engaged to conduct comprehensive application security assessments, including but not limited to design reviews, threat modeling, code security assessments, and annual penetration testing. Any identified issues are reviewed and prioritized for resolution.

These third-party experts are employed by security firms and are former software developers with security industry expertise, applying their knowledge to identify significant product security vulnerabilities. Each expert follows the same established testing process and standards to ensure consistency and maximum testing effectiveness.

3.8 Security Guardians Program

Safe Software has a Security Guardians Program to empower developers to serve as security ambassadors within their teams. Security Guardians promote a "shift left" approach, fostering a security-conscious and resilient culture across the development organization. In collaboration with third-party mentors, Security Guardians actively discuss potential security scenarios and review design and architectural choices. This proactive approach ensures the efficient and secure delivery of the FME Platform while enabling Safe Software to meet security requirements.

4 Security Operations

4.1 Security Updates

Regular updates are released for FME Form to address identified vulnerabilities and enhance product security. Critical vulnerabilities are addressed promptly, and vulnerability fixes are committed to micro releases to ensure the protection of system assets. Fixes for lower-severity vulnerabilities, or those that are not exploitable based on the software architecture, are committed to the main development trunk and typically become available in the subsequent major or calendar year release of FME Form (e.g., FME 2024.0, 2024.1).

4.2 Data Governance and Privacy

FME Form should be installed by an organization's staff on machines within a computing environment exclusively under the organization's control. This ensures the data remains entirely under the organization's control, and Safe Software does not host or access the data in any manner. Please see the Privacy Policy for more information.

Safe Software does not receive, process, or store customer credit card information in its infrastructure. The billing page integrates with a third-party payment processing service that is fully PCI DSS compliant.

4.3 Data Lifecycle Security

Protecting data at all stages of translation and transformation is crucial. Data in motion is encrypted and protected using TLS 1.2 and 1.3 during communication across all environments.

4.4 High Availability

For high availability of FME Form, the Flexera License Manager for floating licenses can be configured with a failover option using a three-server redundant setup. This configuration ensures that the license server continues to function and distribute licenses as long as any two of the three servers are up and running. For more information, see About Floating License.

4.5 Offline Use

FME Form licenses can be borrowed for offline use if the application utilizes a floating license. As long as the license is available, the license can be borrowed and run for up to 30 days on a computer that is not connected to the license server. Once this period expires, the borrowed license is automatically checked back in and becomes available for other users. Additionally, most of the fixed licenses operate offline, ensuring that users can work without requiring a constant connection to the license server.

Please note that offline use may limit access to certain functionalities, including remote content from web services, connections, APIs, Form online help, and other FME Platform products such as FME Flow or FME Flow Hosted.

4.6 AI Assist

FME Form includes an Artificial Intelligence (AI) Assist feature that supports OpenAI and Azure OpenAI services, simplifying the generation of scripts for queries and custom functionality. AI Assist can be disabled and blocked across the organization by restricting access to the fme-ai-service.safe.com domain via a firewall. Individual users may also disable AI Assist via the FME Options dialog. For further details, please refer to the AI Assist in FME FAQ, and AI Terms of Use.

4.7 Incident Reporting

Safe Software is committed to reporting any incident that may impact the customer as soon as possible, especially when organization data could be involved. To receive notifications about any security advisories that affect the FME Platform, subscribe to the security advisory email at fme.safe.com/security.

If a security vulnerability is identified in Safe Software's products, it should be reported via email to security at safe.com. Public disclosure of the issue is requested to be withheld until the vulnerability has been addressed. For further details, please refer to the Vulnerability Disclosure Policy.

4.8 Inventory Management of Enterprise Software

The Safe Software Information Technology team manages the inventory of enterprise software and services. The Vendor Compliance Review process ensures the following risks are assessed before entering a business or contractual relationship with a vendor: compliance risk, reputational risk, operational risk, country risk, credit risk, and information technology risk.

4.9 Logging and Monitoring

FME Form generates a translation log with every workspace that is executed, and by default, this log is saved in the same directory as the workspace file. The log file provides a record of the most recent execution of a given workspace and includes key information about the workspace's various processes, any errors or warnings encountered during translation, and processing statistics. Users also have the option of appending to the existing log instead of overwriting the file, allowing for a continuous record of multiple executions. Some FME functionality is implemented using third-party components, so certain information in the log is reported directly from these products.

Please note that FME Form does not perform log file auditing for security purposes. This responsibility lies with the organization's FME Form administrator(s).

FME Form also manages password visibility in FME Form-generated log files when data is explicitly identified as a password type, ensuring that only masked password values are shown instead of logging passwords in plain text.

5 Staff Security

Safe Software takes appropriate measures to ensure all access to systems, assets, and data is properly managed, and staff receive high-quality, industry-standard training to address security issues before they become potential problems. Additionally, the recruitment process includes comprehensive verification steps, such as reference checks, and background checks, including a Canadian criminal background check, with additional background screening for sensitive roles.

5.1 Account Management and Access Control

Safe Software controls access to its infrastructure, applications, and data based on business and operational requirements, following the Principle of Least Privilege and the Need-to-Know principle. Access rights are restricted according to job roles, with personnel granted only the minimum level of access required to perform their job functions. These access levels are regularly audited to ensure continued need as roles evolve. The use of shared identities is restricted to enhance security.

Safe Software's password policy exceeds the U.S. National Institute of Standards and Technology (NIST) password guidelines and emphasizes the importance of password length. Additionally, multi-factor authentication for accounts is required wherever possible.

5.2 Security Training

Safe Software conducts security awareness training programs annually and upon hire for all employees. Programs are delivered via an e-learning platform and include a series of self-directed modules covering common application security issues as outlined in the CWE Top 25, along with key organizational security policies.

A secure software development training program is also conducted, specifically for the Safe Software Product and Software Development teams.

All training modules are reviewed and updated annually to reflect the latest cyber threats and to ensure employees fully understand our organizational security policies.

5.3 Endpoint Security

Endpoints are protected and managed by a suite of device management, monitoring, and endpoint protection software. Full disk encryption has been enabled on staff devices to protect data at rest. Events are monitored by a dedicated Security Operations Center team, staffed by analysts that maintain 24/7/365 vigilance, from alert validation through in-depth forensics and analysis of the internal network and users.

In addition to regular security reviews and compliance audits, Safe Software partners with trusted third-party security companies to perform penetration tests across the internal network.

6 Regulatory & Compliance

Safe Software complies with industry-standard certifications and global privacy regulations, such as ISO/IEC 27001, SOC 2 Type 2, the European Union's General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and the Payment Card Industry Data Security Standard (PCI DSS).

The Security and Compliance Program is based on the ISO 27001 Information Security Management System (ISMS). Safe Software has established guidelines that govern security policies and processes. These defined policies help guide updates to the security program to be consistent with applicable legal, industry, and regulatory requirements. Regular independent third-party audits are conducted, and efforts are continuously made to improve and expand coverage.

For inquiries, please contact Safe Software at security at safe dot com. Current FME customers are encouraged to create a support ticket for assistance. If FME was purchased through a Partner, please contact the Partner directly.