

FME Server Best Practices Guide for IT Ops and Server Admins

Updated June 17th, 2021

Introduction

After installing FME Server, there are some additional steps to perform to **enhance security** and sure that FME Server is being used to its **full potential**. The following is a list of actions to perform and links to the documentation that details how to perform these actions. If you have any questions along the way, contact [Safe Software Support](http://www.safe.com/support): www.safe.com/support

Passwords

- ❑ **Change the 'admin' user password immediately after installing:** As of FME Server 2019.0, the admin password is automatically set to *admin* at the time of installation. You will be prompted to change the password after installation before being able to log in. Note: It is important to double-check your admin password security and change it often.

Documentation:

- [Changing the Login Password:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/changing_login_password.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/changing_login_password.htm
- [Default User Accounts and Passwords:](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Default_User_Accounts_and_Passwords.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Default_User_Accounts_and_Passwords.htm

- ❑ **Enable Reset Password:** As of FME Server 2018.0, the server admin can grant users the option to reset their passwords if they were forgotten. This option also allows the server admin to create accounts for everyone and then have the user set up their new password when they first log in by clicking on the Forgot Password button.

Documentation:

- [Reset Password:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Reset-Password.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Reset-Password.htm

- ❑ **Enable Password Policy:** As of FME Server 2019.0, the server admin can enable a password policy to force users to create more secure passwords, such

as the password requiring mixed case, and/or numbers and special characters. As of FME Server 2020.0, this is enabled by default, but can be disabled.

Documentation:

- [Password Policy:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Password-Policy.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Password-Policy.htm

- ❑ **Enable Password Expiry:** As of FME Server 2020.0, the server admin can enable a password expiry. As of FME Server 2020.1, there is now a warning icon on the Users page indicating that the user's password needs to be changed.

Documentation:

- [Password Expiration:](https://docs.safe.com/fme/2020.1/html/FME_Server_Documentation/WebUI/Password-Expiration.htm)
https://docs.safe.com/fme/2020.1/html/FME_Server_Documentation/WebUI/Password-Expiration.htm

- ❑ **Change the Database Password:** As of FME Server 2021.0, during installation, the server admin will be prompted to set the password for the FME Server Database. For older versions of FME Server, we recommend updating the password for the FME Server Database following installation. If the password is not updated, a user with knowledge of the default settings for connecting to the FME Server Database may log in and make changes. For instructions on how to update the password see the documentation.

Documentation:

- [Install FME Server: Express Installation for Windows:](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/ExpressInstallation_Windows.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/ExpressInstallation_Windows.htm

Accounts and Roles

- ❑ **Role-Based and User-Based Account Access:** Once FME Server is installed, it is important to set up who has access to what. The server admin can create roles with various permissions and assign users to each role for quick control over security. It is a good idea to regularly audit roles to ensure the users still have the appropriate access.

Documentation:

- [Role-Based and User-Based Account Access:](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/AccessControl.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/AccessControl.htm

- [Role- and User-Based Access:](https://s3.amazonaws.com/gitbook/Server-Admin-2018/ServerAdmin3Security/3.01.RoleAndUserBasedAccess.html)
<https://s3.amazonaws.com/gitbook/Server-Admin-2018/ServerAdmin3Security/3.01.RoleAndUserBasedAccess.html>

- ❑ **Configure Directory Servers (and Import User/Groups):** As of FME Server 2021.0, Active Directory and Generic Directory can be configured under Directory Servers. Active Directory can be set up to allow users to use the same credentials on FME Server as they use to sign-on to their computer. It also allows for quick role assignment on FME Server as the roles can be imported from Windows.

Documentation:

- [Directory Servers:](https://docs.safe.com/fme/2021.0/html/FME_Server_Documentation/WebUI/Directory-Servers.htm?Highlight=directory%20servers)
https://docs.safe.com/fme/2021.0/html/FME_Server_Documentation/WebUI/Directory-Servers.htm?Highlight=directory%20servers
- [Active Directory:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Active-Directory.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Active-Directory.htm
- [Troubleshooting Active Directory Configurations:](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Troubleshooting_AD_Configs.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Troubleshooting_AD_Configs.htm

- ❑ **Configure Windows Services Account:** Optional step if setting up Active Directory, this allows Windows users to sign-on to FME Server using the Windows Credentials button. Additionally, setting this up would provide FME Server Core and Engines access to network locations.

Documentation:

- [Configuring Integrated Windows Authentication:](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/IWA.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/IWA.htm
- [Running the FME Server System Services Under Different Accounts \(Windows\):](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Running_System_Services_Under_Different_Accounts_(Windows).htm)
[https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Running_System_Services_Under_Different_Accounts_\(Windows\).htm](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Running_System_Services_Under_Different_Accounts_(Windows).htm)

- ❑ **Disable Multiple Web Sessions:** As of FME Server 2020.0, the server admin can disable multiple web sessions for each user. When a user is logged into one browser and then logs in to a second browser, the first one will be logged out. This restricts the user from running multiple FME Server sessions

simultaneously. Multiple web sessions is enabled by default and can be disabled in the General System Configuration settings.

Documentation:

- [Multiple Web Sessions:](http://docs.safe.com/fme/2020.0/html/FME_Server_Documentation/WebUI/Multiple-Web-Sessions.htm)
http://docs.safe.com/fme/2020.0/html/FME_Server_Documentation/WebUI/Multiple-Web-Sessions.htm

- ❑ **Disabled Default Accounts:** As of FME Server 2020.0, the Author, Guest and User default accounts are disabled with a new installation. These can be enabled under User Management.

Documentation:

- [Users:](https://docs.safe.com/fme/2020.0/html/FME_Server_Documentation/WebUI/Users.htm)
https://docs.safe.com/fme/2020.0/html/FME_Server_Documentation/WebUI/Users.htm

Security and Sharing

- ❑ **Set System Encryption to 'Restricted' (and Download Key):** FME Server encrypts sensitive data in the FME Server Database and passwords of FME Server configuration backups. By default, this encryption is managed using an encryption key that is common to any FME Server installation. You may wish to enhance encryption security by generating your own custom encryption keys, which you can apply on a rotating basis.

Documentation:

- [System Encryption:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Encryption.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Encryption.htm

- ❑ **Configure HTTPS/SSL:** HTTPS ensures that communication between the client and server is encrypted so that if it is intercepted, the third party cannot easily view or use the information.

Documentation:

- [Configuring for HTTPS:](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/configuring_for_https.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/configuring_for_https.htm
- [Configuring FME Server for HTTPS:](https://community.safe.com/s/article/Configuring-FME-Server-for-HTTPS)
<https://community.safe.com/s/article/Configuring-FME-Server-for-HTTPS>

- ❑ **Configure CORS:** Cross-Origin Resource Sharing allows the server admin to specify websites hosted on other domains that can access resources from FME Server through AJAX requests. Since FME Server 2017.0, CORS is set to open (Allow All) by default.

Documentation:

- [Cross-Origin Resource Sharing:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/CORS.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/CORS.htm

- ❑ **Configure Proxy:** FME Server can be connected to a proxy server on your organization's network to connect to external servers without compromising the security of the internal network. As of FME Server 2020.1, the proxy can be configured to use wildcards and exceptions.

Documentation:

- [Using FME Server with a Proxy Server:](https://docs.safe.com/fme/2020.1/html/FME_Server_Documentation/WebUI/Proxy.htm)
https://docs.safe.com/fme/2020.1/html/FME_Server_Documentation/WebUI/Proxy.htm

- ❑ **Encrypt Database Password:** As of FME 2021.0, the FME Server Database password is only stored in a new `fmeDatabaseConfig.txt` and the password is encrypted by default. In older versions of FME Server, the password that is stored in configuration files `fmeCommonConfig.txt` and `fmeServerWebApplicationConfig.txt` for the FME Server Database are not encrypted.

Documentation:

- [Encrypting the FME Server Database Password:](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Encrypt-FME-Server-Database-Password.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Encrypt-FME-Server-Database-Password.htm

- ❑ **Database and Web Connections:** Access to database and web connections can be controlled by modifying the permissions for each user or role. Connections should be audited regularly to maintain security.

Documentation:

- [Connections:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Connections.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Connections.htm

- ❑ **Create Broadcast Messages:** As of FME Server 2020.0, the server admin can create broadcast messages to be displayed for all users. In addition, the server admin can also dismiss broadcast messages created by Safe Software.

Documentation:

- [Broadcast Messages:](https://docs.safe.com/fme/2020.0/html/FME_Server_Documentation/WebUI/Broadcast-Messages.htm)
https://docs.safe.com/fme/2020.0/html/FME_Server_Documentation/WebUI/Broadcast-Messages.htm

FME Server Optimization

- ❑ **Configure System Email:** Before the FME Server system email can be used, it needs to be configured. This email will be used for sending emails about system events and password resets.

Documentation:

- [System Email:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/System-Email.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/System-Email.htm

- ❑ **Enable Version Control:** Version control allows access to previous versions of repository files. Optionally, version control can be set up to store to an external Git repository. Version control is not enabled at install and must be configured manually by an FME Server admin.

Documentation:

- [Version Control:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Version-Control.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Version-Control.htm

- ❑ **Enable Queue Control:** As of FME Server 2021.0, FME Server Engines can be set up with job queues, job routing rules, and engine assignment rules, which can help prioritize certain jobs or repositories to use different engines. This can be set up at the beginning or later on once job backlogs have been determined.

Documentation:

- [Queue Control:](http://docs.safe.com/fme/2021.0/html/FME_Server_Documentation/WebUI/Queue-Control.htm)
http://docs.safe.com/fme/2021.0/html/FME_Server_Documentation/WebUI/Queue-Control.htm

- ❑ **Review Scheduled Cleanup Tasks:** FME Server will automatically clean up old logs, system event history, and expired session tokens. Review these settings to

ensure that they correspond with your organization's data policy and are kept for the correct amount of time. If FME Server runs out of space, these files can be backed up externally.

Documentation:

- [Scheduled Cleanups:](https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Scheduled-Cleanups.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/WebUI/Scheduled-Cleanups.htm

- ❑ **Setup Backup Schedule:** It is a good idea to establish a regular backup schedule of the FME Server configuration. This can be done manually, but it can also be created as a scheduled task.

Documentation:

- [Performing a Scheduled Backup of an FME Server Configuration:](https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Perform_Scheduled_Backup.htm)
https://docs.safe.com/fme/html/FME_Server_Documentation/AdminGuide/Perform_Scheduled_Backup.htm

- ❑ **Data Published to Repositories:** As of FME Server 2020.1, on the repository/workspaces page, all the data uploaded with the workspace can now be seen and managed.

Documentation:

- [Manage Workspaces:](https://docs.safe.com/fme/2020.1/html/FME_Server_Documentation/WebUI/Manage-Workspaces.htm)
https://docs.safe.com/fme/2020.1/html/FME_Server_Documentation/WebUI/Manage-Workspaces.htm

- ❑ **View All Scheduled Automations:** As of FME Server 2020.1, all automations that are triggered by a schedule can now be viewed on the Schedules page by clicking on the Show Automations button. This is only available to the superuser role.

Documentation:

- [Schedules](https://docs.safe.com/fme/2020.1/html/FME_Server_Documentation/WebUI/Manage-Workspaces.htm)
https://docs.safe.com/fme/2020.1/html/FME_Server_Documentation/WebUI/Manage-Workspaces.htm