Updated on 09/10/2025

Sign up

# MOVEit MFT Essentials training

3 days (21 hours)

## Overview

MOVEit MFT is a secure file transfer solution designed for mission-critical environments. It centralizes, automates and monitors all exchanges of sensitive files between users, internal systems and external partners.

Our MOVEit MFT Essentials training course will enable you to get to grips with the tool, set up secure file transfers via protocols such as SFTP, FTPS or HTTPS, and automate your flows using the MOVEit Automation engine.

You'll learn how to protect your files in transit and at rest, configure conditional workflows and trace every action via audit logs.

MOVEit integrates perfectly with DevOps, hybrid or cloud architectures, and will enable you to automate transfers in your CI/CD pipelines, while ensuring RGPD, HIPAA or PCI-DSS compliance. You'll also be able to leverage its REST API to trigger transfers from your applications or scripts.

Following this course, you'll be able to install, configure and operate MOVEit in a secure environment, as well as design robust, traceable transfer processes tailored to your business needs.

Like all our training courses, this one is based on the latest stable version of MOVEit.

## Objectives

- Understand the architecture and operation of MOVEit Transfer and Automation
- Set up secure file transfers between systems and users
- Create code-free automated workflows to orchestrate your exchanges
- Integrate MOVEit into a DevOps pipeline or hybrid architecture
- Apply security, audit and compliance best practices

- Supervise and diagnose transfer flows in a production environment

## Target audience

- DevOps engineers
- System administrators
- CISOS
- IT project managers

## Prerequisites

- Basic knowledge of networking
- Notion of DevOps

## Introduction to Managed File Transfer

- Understanding the challenges of secure file transfer
- Limitations of traditional FTP/SCP solutions
- Typical use cases in enterprise and DevOps environments
- Introduction to MOVEit MFT Essentials
- Positioning in relation to other MFT tools on the market

## MOVEit architecture and deployment scenarios

- Key components: MOVEit Transfer, Automation, Gateway
- DMZ architecture, perimeter security, DMZ Gateway
- On-premise, cloud or hybrid deployment
- Storage, database and high-availability management
- Integration into existing infrastructure

## Getting started with MOVEit Transfer

- Navigating the MOVEit Transfer web interface
- Creating users and managing groups
- Creating folders and configuring access rights
- Manual transfers via web interface and FTP client
- Using MOVEit Client and mobile applications
- Workshop: Configuring a user, a secure space and carrying out a file transfer via web interface and SFTP

## Exchange security and compliance

- Secure protocols supported: SFTP, FTPS, HTTPS

- Encryption of files at rest and in transit
- Local authentication, LDAP, SSO and MFA
- Granular access control and password policies
- Logging and auditing of user operations

## Automation with MOVEit Automation

- Overview of the Automation engine
- Code-free creation of tasks and workflows
- Triggers: scheduled, on-demand, event-driven
- Workflow steps: transfer, rename, notify
- Error handling and automatic resumption
- Workshop: Creating an automated transfer workflow + email notification in the event of failure

## Integration into a DevOps approach

- Using the MOVEit REST API: authentication, endpoints
- Calling up transfers from a script or application
- Integration into a CI/CD pipeline
- Automatic dispatch of artifacts or post-build reports
- Best practices for MFT industrialization in a DevOps IS
- Workshop: Integrating MOVEit into a CI pipeline to automatically deposit a file in a secure space

## Supervision and operational use

- Real-time transfer monitoring
- Configuration of automated alerts and notifications
- Log visualization and export for SIEM
- Activity reports (users, transfers, errors)
- Track quotas, expiration times and inactive files

## Advanced security and regulatory compliance

- Retention and file lifecycle management
- Encryption key rotation and FIPS security
- Regulatory compliance: RGPD, HIPAA, PCI-DSS
- Secure DMZ configuration with MOVEit Gateway
- Controlled remote access and data leakage prevention

## Best practices, auditing and long-term operation

- Naming policy, permissions and governance
- Backup, update and continuity planning
- Load tests and simulated downtime
- Maintaining compliance over time

- Synthesis, feedback and final Q&A

# Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

# Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

# Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

# Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

# Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

# Certification

A certificate will be awarded to each trainee who has completed the entire course.