







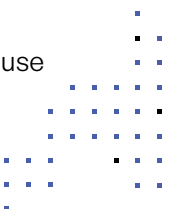


## Implementation Best Practices for MFT Encryption



MFT encryption is only as good as the tools, systems, and processes used to implement it. The following implementation best practices will help ensure a robust and secure encryption system for your managed file transfer solution and workflows.

-  **1. Use strong encryption algorithms:** Implement industry-standard encryption protocols like AES256- for data at rest and TLS 1.2 or higher for data in transit.
-  **2. Manage encryption keys:** Set up a robust key management system to generate, distribute, store, and rotate encryption keys. Use a hardware security module (HSM) for key generation and storage, regularly rotate keys, and ensure proper access controls.
-  **3. Employ end-to-end encryption:** Ensure data is encrypted before it leaves the sender's system, in transit, while at rest in any storage systems, and only decrypting data once it reaches the intended recipient.
-  **4. Implement access controls:** Use multi-factor authentication (MFA) and role-based access control (RBAC) to restrict access to encrypted data and keys.
-  **5. Perform regular security audits:** Periodically assess your encryption implementation to identify and address vulnerabilities. This includes penetration testing, code reviews, and assessing the strength of current encryption methods against emerging threats.
-  **6. Adhere to compliance regulations:** Ensure your encryption practices meet relevant industry standards and regulations like GDPR, HIPAA, PCI DSS, and any industry-specific or regional regulations that apply to your organization.
-  **7. Encrypt file contents AND metadata:** Encrypt file names and extensions, creation and modification dates, author or owner information, file size, and other attributes.
-  **8. Balance security with performance:** Use hardware acceleration for encryption when available, implement software encryption libraries, optimize network protocols for encrypted transfers, and use compression before encryption.



## Implementation Best Practices for MFT Encryption



**9. Invest in backup and recovery:** Implement a secure key backup and recovery system, testing recovery procedures regularly to ensure they work as expected. Use key escrow or split-key systems for critical data, and ensure backup and recovery processes are secure.



**10. Train employees and users:** Educate employees on the importance of encryption and proper handling of encrypted data and keys. Provide training on how to use encryption tools correctly and conduct simulations to test user understanding and compliance.

