IPSWITCH
FILE TRANSFER

Managed File Transfer and the PCI Data Security Standard

www.IpswitchFT.com

The Payment Card Industry (PCI) Data Security Standard (DSS) are intended for use by merchants, financial processors, point-of-sale vendors, and banks, credit unions and other financial institutions that transmit, process and/or store credit cardholder data. This document is intended to assist such companies to understand:

(1) how the standards apply to managed file transfer (MFT) products and solutions in general, and

(2) how the MOVEit™ MFT software products by Ipswitch can help them to both achieve and demonstrate compliance with the standards. This document begins with overviews of the PCI DSS and the MOVEit Central client and MOVEit File Transfer server products, and then goes into detail about the individual MFT-related DSS, together with explanations of how the MOVEit product capabilities assist with or enable compliance.

"The PCI Security Standard Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International."

– www.pcisecuritystandards.org/index.htm

PCI Data Security Standard v.1.2 – Important Dates

The PCI DSS version 1.2 is the global data security standard adopted by the card brands for all organizations that process, store or transmit cardholder. The PCI DSS version 1.2 contains many clarifications and explanations and is not considered a major change over the 1.1 version. The original 6 sections and core 12 requirements remain intact. The effective date of the PCI DSS 1.2 standard is October 1, 2008 and the effective End of Life date for PCI DSS Standard 1.1 is December 31, 2008.

The PCI DSS v.1.2 consists of these twelve critical data security requirements, organized into six sections. [1]

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

1 Source: PCI Data Security Standard version 1.2 at https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

MOVEit Central: Managed File Transfer Workflow Engine

MOVEit File Transfer and MOVEit Central are Windows-based enterprise-level MFT solutions that can be deployed together or on a standalone basis, depending on whether data transfer server and/or workflow automation capabilities are required. (Some MFT vendors combine functions in a single product, but Ipswitch offers them in separate products – MOVEit File Transfer and MOVEit Central– for security and value reasons.) When used together, there are benefits unique to such a combination.

The MOVEit Central workflow engine and file transfer process management system is a powerful tool that enables IT staff to automate the transfer and processing of files on a scheduled, event-driven, or on-demand basis. Central is an 'anything-to-anything' solution, able to move large files and large numbers of files between virtually any internal or external system, including MOVEit File Transfer servers. MOVEit Central typically resides on a company's internal, trusted network.
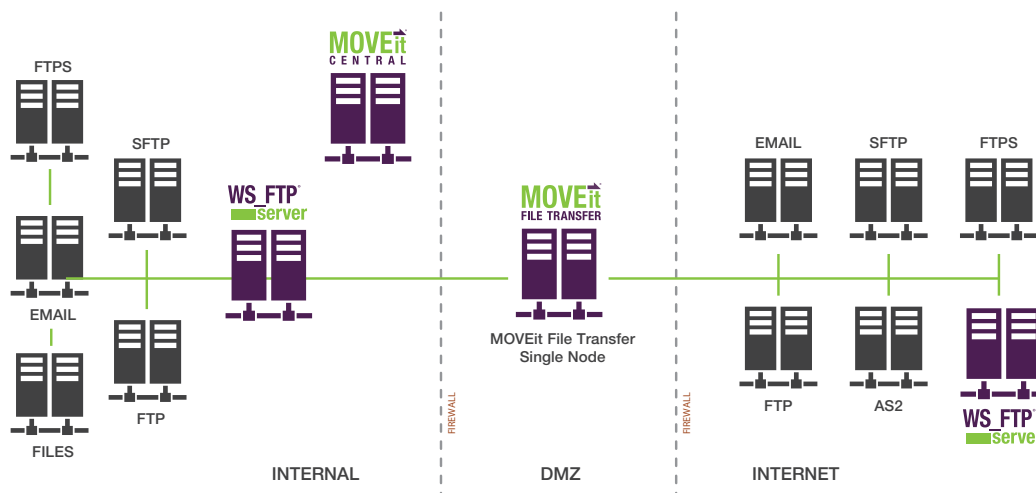
MOVEit Central moves files using easy-to-create tasks – scripting or other programming is not required. Tasks can use Central's built-in AS1, AS2, AS3, FTP, FTPS/TLS, HTTPS, SFTP/SCP2 and SMTP/POP3 clients, as well as its ability to copy to the local file system and/or to shared network folders.

Tasks can also automatically process files using a variety of built-in functions, including OpenPGP and SMIME encryption, and with sample and custom VBS scripts and the ability to run third-party applications.

MOVEit Central also includes several other abilities: an API interface that enables its tasks to be controlled by third-party programs (such as enterprise job or workflow schedulers) using the MOVEit Central API COM component and/or Java class; and the ability to deploy it on a high availability basis, providing automatic, unattended failover from a production to a continuously updated warm-standby copy of MOVEit Central.

MOVEit File Transfer: Managed File Transfer Server

MOVEit File Transfer is a security-hardened managed file transfer 'portal' through which applications and end-users can safely exchange files using Web browsers and a variety of MOVEit and third-party secure FTP clients that support any of these SSL or SSH2 encrypted methods: (AS1) AS2, AS3, FTPS, HTTPS, SCP2, SFTP or TLS. This, together with its unique, built-in, FIPS-140-2 validated AES encrypted data storage system, enables MOVEit File Transfer to support automatic end-to-end encrypted transfer and storage without using PGP.

MOVEit File Transfer is usually located in a DMZ, a network segment protected by a company's perimeter firewall(s). This location enables secure access to MOVEit File Transfer from the local internal network and from the Internet.
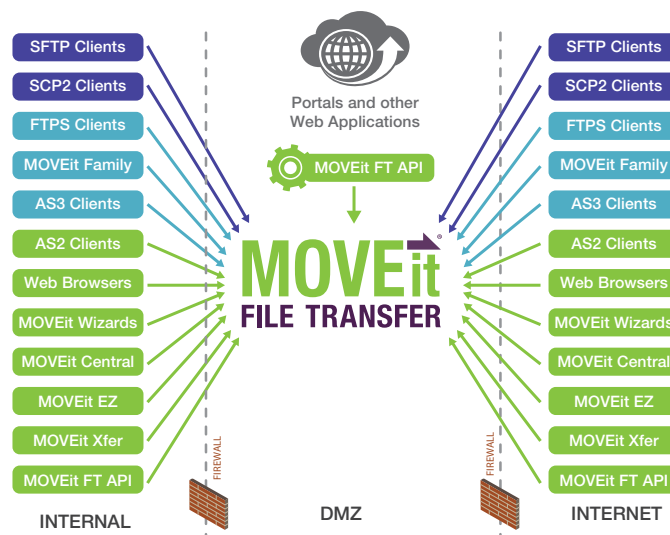
Unlike some MFT products, MOVEit File Transfer is strictly a server; it cannot initiate connections to other systems. As shown by the arrows above, all connections to a MOVEit File Transfer must be initiated by a suitable client, application, API or service, which means there is no need to open any firewall ports from the DMZ segment into the internal network.

DMZ-based MFT products that push files into the internal network, and MFT products that use DMZ-based secure file transfer proxies, typically require at least one open port from the DMZ into the internal network.

MOVEit File Transfer also includes several other abilities: an API interface that provides remote, secure, programmatic access to the product's file (and message) transfer, secure data storage, and user database services using the MOVEit File Transfer API COM component and/or Java class; French and Spanish language end-user interfaces; and the ability to deploy it on a high availability basis, providing scalability and automatic, unattended failover in a load balanced, multi-production server environment.

PCI DSS: Build and Maintain a Secure Network

1: Install and maintain a firewall configuration to protect cardholder data.

The MOVEit managed file transfer system was designed for use with the multi-layer, often multi-firewall network described by PCI DSS requirement 1. The MOVEit File Transfer secure MFT server was designed to live on a firewall protected DMZ network segment where it would be partially exposed to the Internet. The MOVEit Central MFT client was designed to live on an internal, trusted network, from which it can establish connections to the MOVEit File Transfer server through a firewall.

The following sections of this requirement are applicable to MFT products.

> **1.1.5:** These deal with specific protocols allowed under the standards. MOVEit File Transfer and MOVEit Central can perform all of their necessary file transfer functions under the HTTP/S (SSL) and SFTP (SSH2) protocols, both of which are explicitly approved by section 1.1.6. Note: When MOVEit uses FTP it is encrypted before being transferred using one of the following file encryption standards: AS3, FTP/S (SSL), PGP, or SMIME.

2: Do not use vendor-supplied defaults for system passwords and other security parameters.

For security reasons, the MOVEit Central client and MOVEit File Transfer server do not include any "vendor-supplied default" system passwords or other security parameters. The MOVEit installation packages, and the software itself, force the installer/administrator to set their own usernames and passwords during setup and configuration. Note: MOVEit File Transfer server has the ability to suggest unique, randomly generated passwords, which may be used or not as desired and also includes the ability for administrators to force strong passwords on all accounts.

IPSWITCH
FILE TRANSFER

The following sections of this requirement are applicable to MFT products.

2.2.1: This section says that only one primary function be implemented on each server. The MOVEit products help enforce this requirement by placing all file "collection" services on the server that hosts MOVEit File Transfer and all file "transfer initiation" services on the server that hosts MOVEit Central. Further, MOVEit File Transfer can be deployed in a tiered architecture across a segmented network with primary functions distributed across several servers. For example, the core MOVEit File Transfer application can be deployed on one server, the encrypted file system on another server and the database on a third.

2.2.2, 2.2.3 and 2.2.4: This section is about locking down or "hardening" server platforms. Ipswitch's CISSP and SANS-certified engineers have designed a "SecurityAuxiliary" utility that is bundled with the MOVEit File Transfer and MOVEit Central software. This utility performs many common hardening actions against the host platform when the MOVEit software is installed. MOVEit also comes with its own "SecAux" tool that automatically locks down over a hundred additional Windows settings (for example: permission to use the command-line utility, based on operational preferences). While it does not directly rely on the underlying Windows operating system, MOVEit File Transfer does attempt to protect the OS. For example, the MOVEit File Transfer installation instructions work with and recommend the use of automated OS security tools such as:

- URLScan

- IIS Lockdown Tool

- Windows Security Policies

- IPSec

- Windows Automatic Update

2.3: This section requires that all (non-console) administrative access must be encrypted. Administrative access to MOVEit File Transfer is via Web browser using HTTP/S – SSL encryption. Administrative access to MOVEit Central is via a Windows program using SSL-secured sockets.

PCI DSS: Protect Cardholder Data

3: Protect stored card holder data.

MOVEit Central and MOVEit File Transfer incorporate 'defense in depth' that provides a unique advantage over other file transfer products in regards to safeguarding stored cardholder data.

The MOVEit products were designed from the beginning with their own built-in user authorization, access controls and strong cryptography. These enable the MOVEit software to control exactly who can login, and what they can see and do in regards to commands, files, folders, logs and other users.

Both MOVEit products were also designed with their own built-in encrypted data storage system, which uses our MOVEit Crypto cryptographic software. MOVEit Crypto has been FIPS 140-2 validated by the US National Institute of Standards and Testing (NIST) and the Canadian Communications Security Establishment (CSE). MOVEit Crypto was one of the very first cryptographic software modules to earn FIPS 140-2 validation (Certificate #310 issued March 2003 to Standard Networks, now part of Ipswitch). MOVEit Crypto includes 256-bit AES encryption (used by the MOVEit software to securely store data) and SHA1 hashing (used to protect passwords and encryption keys and to perform file integrity checks).

These built-in authentication, access control, and cryptographic systems mean that the security of the MOVEit products, and the data they store, is independent of the security of the underlying OS.

The following sections of this requirement are applicable to MFT products.

3.1: Data Disposal. MOVEit Central and MOVEit File Transfer are each capable of doing scheduled, automatic and secure deletion of old files and folders in compliance with the National Institute of Standards and Testing (NIST) SP 800-88 erasure rules so the data cannot be retrieved later.

3.2: Authentication Retention. When passwords (or other credentials) are needed to access a remote system, MOVEit Central securely stores them using reversible strong encryption. When passwords are needed for local authentication, MOVEit File Transfer and MOVEit Central both use irreversible strong hashes. MOVEit File Transfer also has the optional capability to be tied into one or more "external authentication" sources such as LDAP servers to remove the need for any kind of local authentication at all. MOVEit File Transfer also supports strong password rules and policies on using previous passwords.

3.4: Protection of Stored Data. This section states that strong encryption must be used to protect credit card numbers (a.k.a. "Primary Account Number" or PAN) when storing such data. Most MFT systems lack the native ability to encrypt the data that they store. In contrast, the MOVEit File Transfer server and MOVEit Central client both include strong, native and independent of OS encryption. All data received by a MOVEit File Transfer server is encrypted before being stored using its strong, built-in, FIPS 140-2 validated 256-bit AES encryption. MOVEit Central MFT client has the built-in ability to apply PGP, SMIME, and/or AS2 cryptography to the files it handles.

3.5 and 3.6: Cryptographic Key Storage. These sections deal with very technical key storage elements that are beyond the scope of this whitepaper. Please contact Ipswitch MOVEit support if you would like to learn more details. But note that MOVEit software fulfills all of these PCI DSS key storage requirements.

4: Encrypt transmission of cardholder data across open, public networks.

The MOVEit MFT products provide support for a wide variety of encrypted transfer methods that can be used to exchange cardholder data over public networks, including the Internet, and VPN implementations.

MOVEit Central client can do transfers using secure FTP over SSL (FTPS), secure FTP over SSH2 (SFTP and SCP2), as well as secure file transfers using HTTP (HTTPS) and the AS1, AS2, and AS3 protocols. Central can also combine file-level PGP or S/MIME encryption with unencrypted transport protocols such as FTP and Windows SMB to achieve "encrypted transmission of data" in legacy or migration situations.

MOVEit File Transfer server supports transfers using secure FTP over SSL (FTPS), secure FTP over SSH2 (SFTP and SCP2), as well as secure file transfers using HTTP (HTTPS) and the AS2, and AS3 protocols.

PCI DSS: Maintain a Vulnerability Management Program

5: The MOVEit Central client provides tightly integrated antivirus protection and auditing when installed on a platform running McAfee, Symantec, or Trend AV software.

If any of these applications detects a virus, MOVEit Central will immediately and automatically do the following.

- **Stop the transfer.**
- **Delete the file on the system that MOVEit Central downloaded it from, or**
- **Remember the file characteristics and never transfer it again.**
- **Log the name of the file, virus, and AV software along with the time and date the infection was detected and what MOVEit Central did in response.**
- **Alert the appropriate persons via email.**

In addition, MOVEit Central client and MOVEit File Transfer server both feature tamper-evident FIPS 140-2 verified audit logs. This means their audit databases are protected by a chain of cryptographic hashes that make it difficult, if not impossible, for someone to add, delete or modify any audit records without being detected.

6: Develop and maintain secure systems and applications.

All of the requirements in this section have either already been implemented in the MOVEit products, or are recommended by MOVEit documentation for implementation when the MOVEit software is deployed. The complete list of requirements from developer-centric section 6.5 is repeated below to provide an idea of the kind of precautions that are taken in MOVEit software.

6.5: WebApplication Development Security. This section states that the development of web applications should be based on secure coding guidelines (such as those issued by the Open Web Application Security Project), involve the review of custom application code to identify coding vulnerabilities, and cover prevention of common coding vulnerabilities in software development processes, including all of the following:

> **6.5.1:** Cross-site scripting (XSS)
>
> **6.5.2:** Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
>
> **6.5.3:** Malicious file execution
>
> **6.5.4:** Insecure direct object references
>
> **6.5.5:** Cross-site request forgery (CSRF)
>
> **6.5.6:** Information leakage and improper error handling
>
> **6.5.7:** Broken authentication and session management
>
> **6.5.8:** Insecure cryptographic storage
>
> **6.5.9:** Insecure communications
>
> **6.5.10:** Failure to restrict URL access

6.6: All public-facing web applications are subject to either: 1) reviews of applications via manual or automated vulnerability assessment tools or methods or 2) installing an application-layer firewall in front of public-facing web applications

During development Ipswitch uses Hewlett Packard's popular "WebInspect" web application security assessment tool and several "fuzzing" applications to uncover security conditions before they are ever encountered in the field. These tools, dozens of other automated and semi-automated applications in our quality assurance testing suite and batteries of manual tests all help ensure that our products exceed PCI security requirements and remain that way from release to release.

To maintain the security of the MOVEit products in the field, Ipswitch support regularly posts security updates on the MOVEit support website (managed through the use of MOVEit Central and MOVEit File Transfer). Security alerts, as well as news about the results of OS security patch testing, are securely broadcast to licensees using the secure messaging capabilities of the Ipswitch corporate MOVEit File Transfer server.

All connections to the support site are via secure SSL-encrypted link, and login to the support site requires authentication and prior authorization. MOVEit licensees have the right to deploy patches and upgrades, at no additional charge, under their required annual software maintenance coverage.

IPSWITCH
FILE TRANSFER

PCI DSS: Implement Strong AccessControl Measures

7: Restrict accessto cardholder data by businessneed-to-know.

The MOVEit products allow the specific assignment of folder permissions, protocol access restrictions, IP address restrictions and other limited rights. All of these are typically "no access unless granted" items. MOVEit software also permits the delegation of authority so that an "administrator" need not have control over the entire MOVEit system, but rather only over a subset of folders, transfer tasks, or a group of users.

8: Assign a unique ID to each person with computer access.

The MOVEit products encourage the assignment of a unique ID to each person with computer access. One of the most helpful ways that it does this is to allow specific access to a single resource (folder, transfer task, etc.) by multiple users. For example, two users might have "read" access to a folder and a third might have "write" access. This specific assignment of rights to overlapping resources encourages people to use their own credentials rather than a more powerful "shared" account.

The following sections of this requirement are applicable to MFT products.

8.2: Authentication Credentials Beyond Username and Password. MOVEit Central client and MOVEit File Transfer server support the following additional methods of authentication.

- **Client Keys.** Used with secure FTP over SSH2 (SFTP and SCP2) and with PGP encryption.
- **Client Certificates.** Used with secure FTP over SSL (FTPS) and HTTPS, AS1, AS2 and AS3 as well as with S/MIME encryption.

8.3: Two Factor Authentication. While this section focuses more on network access than file transfer, MOVEit Central client and MOVEit File Transfer server are each fully capable of implementing two-factor (and even three-factor authentication) on all of its administrative and file transfer interfaces.

8.4: Credential Protection. The MOVEit products securely protect stored passwords and keys (as detailed in sections "3.2", "3.5" and "3.6"). Both products also use their secure SSL and SSH2 encrypted transport capabilities to securely protect credentials when they are being transferred.

8.5: Password and User Rules. The MOVEit Central client and MOVEit File Transfer server products have configurable password and user policies that enable them to fully meet all the rules in this section.

- **8.5.1:** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- **8.5.2:** Verify user identity before performing password resets.
- **8.5.3:** Set first-time passwords to a unique value for each user and change immediately after the first use.
- **8.5.4:** Immediately revoke access for any terminated users.

IPSWITCH
FILE TRANSFER

8.5.5: Remove/disable inactive user accounts at least every 90 days.

8.5.6: Enable accounts used by vendors for remote maintenance only during the time period needed.

8.5.7: Communicate password procedures and policies to all users who have access to cardholder data.

8.5.8: Do not use group, shared, or generic accounts and passwords.

8.5.9: Change user passwords at least every 90 days.

8.5.10: Require a minimum password length of at least seven characters.

8.5.11: Use passwords containing both numeric and alphabetic characters.

8.5.12: Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

8.5.13: Limit repeated access attempts by locking out the user ID after not more than six attempts.

8.5.14: Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.

8.5.15: If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.

8.5.16: Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

9: Restrict Physical Access to Cardholder Data.

Surprisingly, the MOVEit products can also help companies to address a few physical security requirements. For example, if someone was able to gain physical access to a MOVEit File Transfer server, they would be unable to read any of the cardholder data that it has stored because each file is encrypted with its own key and each key is individually encrypted at 256-bit AES?

9.5: Off-Site Backups. MOVEit Central client and MOVEit File Transfer server can easily and reliably handle the secure, automated transfer, processing and storage of large files, and large numbers of files. This enables them to be used to replace some tape-based physical backups.

> **9.7.2:** Courier Reliability. When MOVEit products are used to replace tape-based backups, the need to achieve compliance with this section disappears.

9.10: Media Destruction. While the MOVEit products cannot be used to physically destroy media, both MOVEit Central client and MOVEit File Transfer server provide NIST 800-88-compliant data erasure.

PCI DSS: Regularly Monitor and Test Networks

10: Track and Monitor All Access to Network Resources and Card holder Data.

MOVEit audit logging capabilities are among the most comprehensive offered by any MFT products. Many only create text-based logs that list little more than sign-ins, file transfers and when they occur. Such logs often have one or more of the following problems.

Log Data Security. Text-based MFT logs are often written out to the disk in the clear, which means they can be easily altered with a desktop editor to hide unauthorized activities. MOVEit Central and MOVEit File Transfer each have a built-in, commercially licensed database that they write their audit records to. Access to MOVEit databases requires authorization and authentication. To further guard against tampering, the MOVEit products include a cryptographic "hash chain" that provides proof as to whether the records in the databases have or have not been altered.

Administrative Log Data. Text-based MFT logs often do not include any record of administrative actions, such as the addition of users, folder permission changes, and other critical security changes. This makes it difficult or even impossible to discover any unauthorized administrative changes. The MOVEit products write detailed records to their secure databases of all administrative activities.

Ease of Use. Text-based MFT logs often must be processed by a third-party "log parser" in order to yield meaningful information. MOVEit products have the native ability to provide ad-hoc audit views. They also include built-in reports and customizable reports that enable administrators to quickly and easily track and monitor their MOVEit products – without having to use a third-party "log parser."

The following sections of this requirement are applicable to MFT products.

10.1-10.3: User Information. These three sections cover being able to link specific actions to specific users, what sort of actions should be audited, and the information the records should contain. MOVEit File Transfer server supports the unique user account per person concept in section 10.1 (see also #8) and exceeds the "what to log" and "how much information to log" rules in sections 10.2 and 10.3.

10.4: Time Synchronization. Time Synchronization. MOVEit products support time synchronization between computers, and provide utilities and documentation to perform this operation using standard time protocols.

10.5: Audit Data Protection. This section includes the following MFT-relevant sub-sections.

> **10.5.1:** Access Restriction. This section covers providing restricted access to audit records. Unlike MFT products that use text-based audit logs, MOVEit Central and MOVEit File Transfer record audit data to their built-in, commercially-licensed, access-controlled databases. These provide protection against unauthorized users that may gain access to or control of the underlying operating system. Access to MOVEit audit records is controlled so that people can only see events that relate to their organization and/or the groups, users, folders and transfer tasks under their control.

> **10.5.2:** Tamper Protection. This section covers the need to safeguard audit records from unauthorized modification. The MOVEit products address this by controlling access to the data (see section 10.5.1), by employing a cryptographic "hash chain" that checks file integrity to prove whether the data has been altered or not, and by issuing alerts if tampering is detected.

> **10.5.3:** Record Duplication. This section recommends the prompt copying of audit records, either to a centralized server or to "media that is difficult to alter" (such as a printed paper trail). MOVEit Central and MOVEit File Transfer provide instructions about how their audit records can be either sent to a centralized server (via SysLog or SNMP or spooled out to a print file.

> **10.5.5:** Integrity Monitoring. Using "file integrity monitoring and change detection software" to monitor for audit record changes is required by this section. As mentioned in section 10.5.2, MOVEit products do automatic file integrity monitoring and will issue alerts if problems occur.

10.6: Record Reviews. This section requires regular review of audit records, and recommends that such reviews be automated. MOVEit Central and MOVEit File Transfer have the built-in ability to provide ad-hoc audit data views, and to generate over 90 pre-defined reports covering file transfers, secure messages, user status, system performance, storage status and security. Reports can be run on-demand or on a scheduled basis, and can be generated in CSV, HTML, or XML formats.

The MOVEit products support automated reviews through their ability to integrate with centralized monitoring (see section 10.5.3). In addition, both products support the creation of custom reports, which can feed information into specialized systems used to detect particular anomalies.

10.7: Record Retention/Deletion. MOVEit products automatically purge their logs after a configurable time period, and can be set to automatically retain purged logs in an archive-friendly format for long-term storage.

11: Regularly Test Security Systems and Processes.

As discussed in section 6, Ipswitch encourages MOVEit Central and MOVEit File Transfer licensees to regular inspect and scan their MOVEit test and production systems. The MOVEit products also work with properly configured third-party application file change detection software as suggested in section 11.5.

IPSWITCH
FILE TRANSFER

PCI DSS: Maintain an Information Security Policy

12: Maintain a Policy that AddressesInformation Security.

The MOVEit Central and MOVEit File Transfer product documentation describes collections of configuration options, especially collections of security options, as "policies." This was a deliberate choice of terminology. MOVEit policies are designed to let licensees configure their software to enforce their corporate policies. The following sections of this requirement are applicable to MFT products.

12.2 and 12.5.5: Daily Operations. This section addresses daily security operations, including user account maintenance and log review procedures. MOVEit products provide maintenance-oriented administrative interfaces designed to manage hundreds of transfer tasks (MOVEit Central client) and thousands of users (MOVEit File Transfer server). "Show audit logs for selected user" and other context-sensitive options like look-up boxes aid the day-to-day security management of the MOVEit products, as does the automated generation and delivery of pre-configured and custom security reports.

12.5.2: Alert Monitoring andAnalysis. The MOVEit Central and MOVEit File Transfer products each write to event logs, which can be sent to SysLog, SNMP, or other central monitoring facilities.

12.5.4: User Management Delegation. MOVEit Central allows administrators to delegate control of specific transfer tasks to specified individuals, and MOVEit File Transfer administrators are able to delegate control over groups of users and their folders to specific "group administrator" users.

12.10: Partner PCI-DSS Compliance. This section addresses the need for PCI DSS compliance by business partners that your company exchanges cardholder data with. Many financial institutions and processors use MOVEit products, including 20% of the organizations on the PCI council's executive board and advisory council.

In Conclusion

The MOVEit products provide a comprehensive set of security and operational capabilities that can help companies to achieve and demonstrate their compliance with the PCI Data Security Standard, especially in the critical areas of secure cardholder data storage, transmission, access control, and audit records. That is one of the reasons that there is a significant installed base of MOVEit products amongst financial processors and banks, credit unions and other financial institutions in North America and Europe.

Ipswitch File Transfer provides solutions that move, govern and secure business information between employees, business partners and customers. The company's proven solutions lead the industry in terms of ease of use, allowing companies of all sizes to take control of their sensitive and vital information and improve the speed of information flow. Ipswitch lets business and IT managers govern data transfers and file sharing with confidence and enable compliance by balancing the need for end user simplicity with the visibility and control required by IT. Ipswitch File Transfer solutions are trusted by thousands of organizations worldwide, including more than 90% of the Fortune 1000, government agencies, and millions of prosumers. For more information on Ipswitch File Transfer and its products, go to www.IpswitchFT.com.

IPSWITCH
FILE TRANSFER