DATA SHEET
DIPLOMAT® MANAGED FILE TRANSFER
STANDARD EDITION

OVERVIEW

When secure file transfer is critical to your business, Diplomat MFT Standard Edition goes beyond secure FTP transfers to provide a more secure, integrated file transfer solution. You can use expanded transport types (like email, HTTP, HTTPS and SMB), deliver automated job status reports to both business and IT support users and integrate file transfer jobs with existing applications and processes.

JOB MANAGEMENT

Diplomat MFT Standard Edition lets you set up file transfers to or from FTP, SFTP, FTPS, HTTP, HTTPS, email or SMB servers. Diplomat's intuitive point-and-click interface means no more time-consuming programming with events, triggers, and "do" loops.

You can use Diplomat's built-in scheduler or folder monitoring to initiate file transfer jobs. Or, other applications can initiate file transfer jobs with Diplomat MFT Scripting Agent or the optional Diplomat MFT REST API.

Whether you use Diplomat's scheduler, Diplomat MFT Scripting Agent, or the optional Diplomat MFT REST API, you get all of the benefits of a Diplomat file transfer job, such as log files, archive files and email notifications.

Select files based on dates, sequence numbers or other wildcards and continue the job when all source files are available.

EVENT NOTIFICATIONS

You may need to notify a sender that a file was sent or notify a recipient that a file is ready to be picked up. Diplomat MFT can send email to you, others at your company or outside recipients at the completion of each file transfer job.

When a file transfer problem occurs, you need to know as soon as possible. You may have processing deadlines or service level agreements to meet. Diplomat MFT can send email or paging notifications that include the detailed information required to address a problem immediately – without searching through system log files.

PROBLEM RESOLUTION

File transfer errors are usually prevented when using Diplomat MFT Standard Edition. When a transient error occurs, like a dropped FTP session or a brief network outage, Diplomat MFT automatically attempts to recover and complete the transfer. Most transient file transfer problems are corrected so that the file transfer job succeeds without manual intervention.

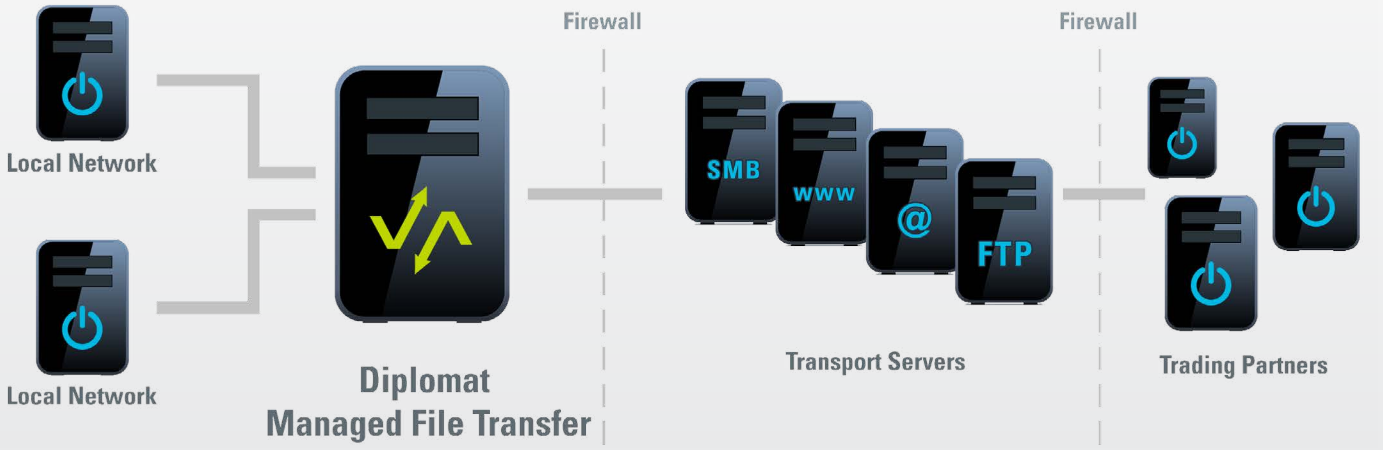
Unexpected problems may still crop up. You might have outdated FTP account login information. Files might not be ready for pickup. The wrong key might have been used to encrypt a file, so you cannot decrypt it. Diplomat MFT Standard Edition can send email or paging notifications that include the detailed information required to address a problem immediately – without searching through system log files.

In addition, Diplomat MFT logs all file transfer set-up and run-time events to a log file. Diplomat MFT's built-in log viewer makes it easy to locate the log entries you need to diagnose a problem.

Request Demo »

Free Trial »

Try Diplomat Online »



Diplomat MFT Standard Edition

SECURITY

Your data must be protected at all times – in transit and at rest. Diplomat supports OpenPGP encryption and various secure file transports. OpenPGP encryption lets you protect files at rest both inside and outside the firewall. Secure FTP or HTTPS ensures that both login information and data files are protected in-transit with SSH or TLS encryption.

Sensitive file transfer job set-up data (such as pass-phrases, passwords, and account logins) are encrypted before storage in a central Diplomat database. Batch files and registry entries do not contain sensitive data.

Diplomat uses secure HTTPS (TLS) connections for all communication between Diplomat components. No unprotected information is sent over your internal network.

Two-factor authentication protects Diplomat MFT from unauthorized use. Users are authenticated using their network identity or by entering a Diplomat username and password – or both.

An administrative dashboard lets you set user privileges, password policies, session expiration and manage user connections.

INTEROPERABILITY

Your secure file transfer solution needs to operate seamlessly with your partners' current tools and applications. Diplomat MFT works with existing technologies by adhering to industry standards, such as OpenPGP, secure FTP, SMTP, POP3 and HTTP/S.

Your business partners can continue to use the encryption and file transfer products they have in place. And, if you have existing applications or tools that use PGP keys, you can import all of your keys from your existing PGP key rings.

Diplomat MFT is designed to handle both expected and unexpected disruptions in your production environment. When you need to upgrade your production environment, you can create a single-file backup of Diplomat's internal database and restore it on any other system running Diplomat MFT Standard Edition. If your production system goes down unexpectedly, you can have a hot standby ready to run without a disruption in service.

To learn more call 781.210.3310.

Start Free Trial »

Try Diplomat MFT Standard Edition free for 15 days to see how it works in your environment.

Request Demo »

Schedule a live demo on how to control and monitor your file transfer jobs.

Try Diplomat Online »

Try Diplomat Sandbox to set up file transfer jobs without downloading and installing trial software.

TECHNICAL SPECIFICATIONS

COMPONENT & PLATFORM SUPPORT

Diplomat MFT Service

- Windows 7, 8 and 10 (64-bit)
- Windows Server 2008 R2, 2012 R2 and 2016 (64-bit)
- Red Hat Linux (64-bit; x86)

Diplomat MFT Client

- Windows 7, 8 and 10 (64-bit)
- Windows Server 2008 R2, 2012 R2 and 2016 (64-bit)

Diplomat MFT Web Launch

- Any system supporting Java Runtime Environment (JRE) 1.8 or higher

Diplomat MFT Scripting Agent

- Any system supporting Java Runtime Environment (JRE) 1.8 or higher

FILE TRANSFER SUPPORT

FTP

- FTP (RFC 959)
- FTPS (RFC 2228 with Secure FTP Using TLS)
- SFTP (RFC 4253)

Email

- SMTP (RFC 2821)
- POP3 (RFC 1939)
- IMAP (RFC 3501)

HTTP/S

- HTTP/S (RFC 2616)

SMB

- SMB 1.0, 2.0 and 3.0

OPENPGP ENCRYPTION

Symmetric Algorithms

- AES (up to 256-bit keys)
- Blowfish (up to 448-bit keys)
- CAST5
- DES (56-bit keys)[1]
- IDEA (128-bit keys)[1]
- Safer (128-bit keys)[1]
- Triple DES (up to 168-bit keys)
- Twofish (up to 256-bit keys)[1]

[1] Only supports decrypting existing messages encrypted with algorithm or encrypting to existing keys specifying algorithm as preferred cipher.

Asymmetric Algorithms

- DSA (1024-bit key only)
- El Gamal (up to 4096-bit keys)
- RSA (up to 4096-bit keys)

Hash Algorithms

- MD2[1], MD5
- RIPEMD-160
- SHA-512, SHA-384, SHA-256, SHA-224, SHA-1

Interoperability (RFC2440/4880)

- McAfee E-business Server v8.0 or later
- PGP Command Line v9.0 or later
- Any other RFC 2440 or RFC 4880 OpenPGP-compliant product

ABOUT COVIANT SOFTWARE

Coviant Software delivers Managed File Transfer solutions to improve the productivity of file transfer administrators. Diplomat Managed File Transfer software uses Intelligent File Transfer™ design with embedded secure file transfer logic, so file transfer experts can quickly design and deploy file transfer jobs with fewer errors and failed transfers.

COVIANT Software

www.coviantsoftware.com