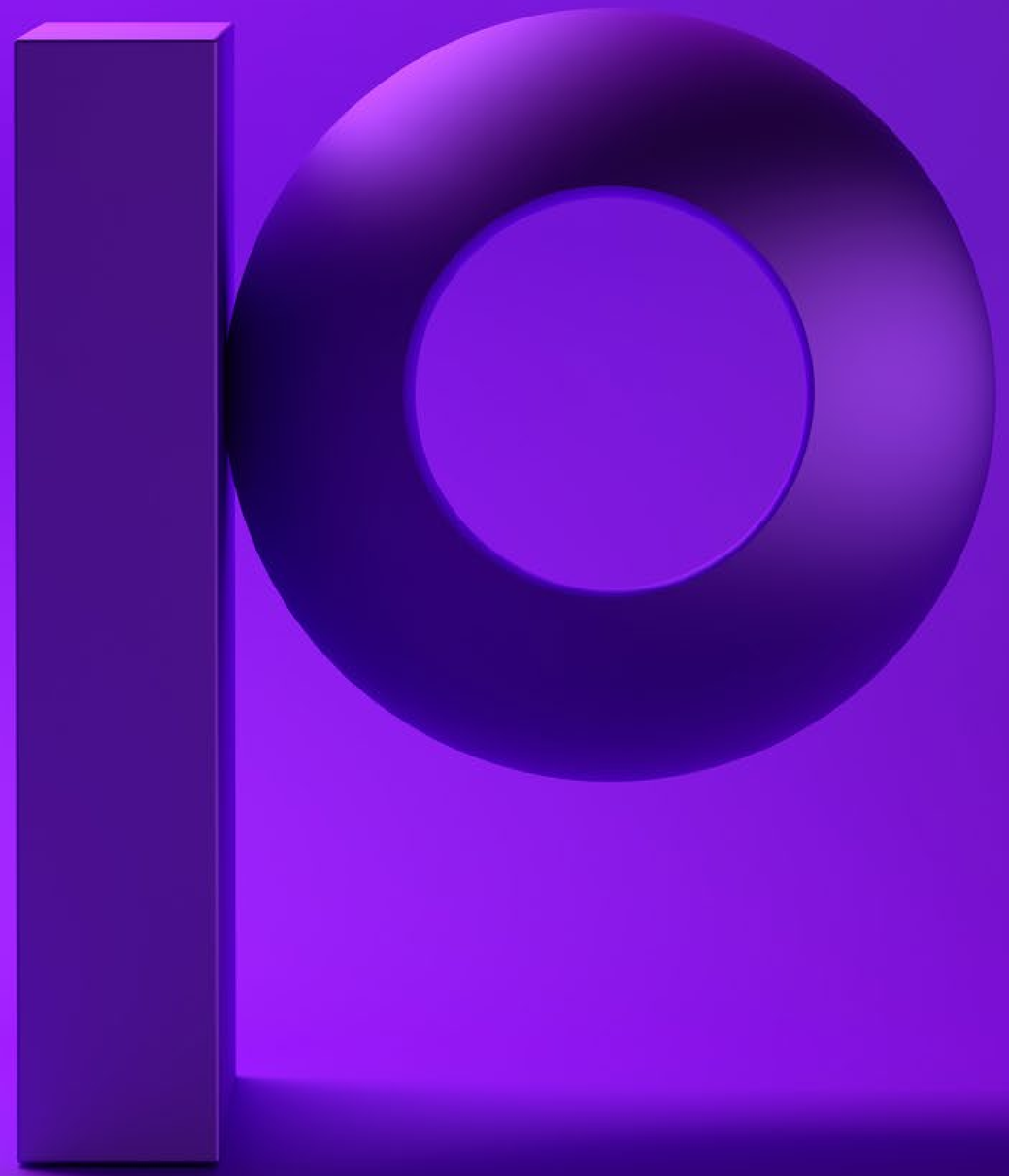
precisely

The Essential Guide to Secure and Managed File Transfers on the IBM i



Introduction

For many organizations, the IBM i plays a central role in the business-critical applications of an enterprise, often making it a hub for the sending and receiving of electronic files during the course of doing business. However, transferring files introduces significant risks unless proper security measures are taken. The standard open-source FTP protocol has been around for decades, and many free tools are available for this purpose, but these tools often don't include any inherent security. When a file containing sensitive information is transferred with this method, it could easily be intercepted by a hacker and viewed "in the clear." If your company is required to comply with one or more regulations, such as HIPAA, SOX, PCI DSS, 23 NYCRR 500, GDPR, etc., transferring unsecured files creates a huge exposure.

Security aside, there is the issue of manageability of file transfer processes. For companies that send and receive more than a handful of files, file transfers can be extremely time-consuming and error-prone without tools that provide automation, application integration, and other critical management functions.

Fortunately, third-party managed file transfer (MFT) solutions for IBM i are available that provide all necessary security functions in addition to a range of automation, integration, and management features. Consider the following examples of how a full-featured MFT solution can be utilized within an enterprise:

- A gaming and hospitality company needs to send files to their bank each night showing ACH fund transfers. The company's MFT solution is configured to automatically detect the files when these are ready to be sent, transfer the files to the bank using strong encryption, create an audit record of the transfers, back up the transferred files to an archive library, and notify relevant staff should any issues arise with any of these processes.

- A manufacturing company needs to rapidly process orders from its largest customer. The company's MFT solution is configured to automatically and securely connect to the customer's FTP server and "pull" all available order files to its IBM i server, after which a program is triggered that starts the process of moving the orders through the company's order-fulfillment applications.

As you can see, an MFT solution can help companies save significant staff time, reduce security exposures, meet Service Level Agreements (SLAs), and even create new competitive advantages.

Securing Transferred Files — First Things First

The trusted method for protecting files at all points of the file transfer process is encryption. With encryption properly in place, the contents of the file can be read only if the entity is in possession of a valid decryption key. But it's not always sufficient to encrypt the file while it is "in motion." For complete file transfer security, and as a general security best practice, the file must also be encrypted at the source and destination points so its contents cannot be viewed by unauthorized users at any time before or after the transfer. MFT solutions should provide all necessary encryption functions for transferred files, both while in motion and at all other stages of the file transfer process.

Encryption of Transfer Files While in Motion

Included in most MFT solutions are two primary methods, or protocols, that are used for creating encrypted tunnels when transferring files from one location to another: Secure SSL FTP (often referred to as FTPS) and Secure Shell FTP (often referred to as SFTP). The secure file transfer protocol that is chosen typically depends on how transfer sessions need to be established (password, key, certificate, etc.), how firewalls need to be negotiated (should this be a factor), required encryption standards, and other security requirements determined by the entities involved in the file transfer.

Encryption of Transfer Files at Source and Destination

Since SFTP and FTPS encrypt only the tunnels through which files are transferred, it is critical to also encrypt files before they are sent if it is expected that those files could be exposed for any period of time at the source or destination. In some cases, companies may choose to utilize file transfer repositories within their external-facing networks, and when files reside there for any length of time they can be vulnerable. The encryption method that is commonly utilized by MFT solutions on IBM i for this purpose is Pretty Good Privacy (PGP). PGP provides the necessary encryption functions, including the ability to utilize current ciphers (encryption algorithms) and encryption/decryption keys. If you are wondering if a file is doubly encrypted if it has been pre-encrypted with PGP and then is transmitted via SFTP or FTPS, the answer is yes; however, the extra layer of protection certainly doesn't hurt, and again, you never want to leave sensitive files unencrypted at any point in a process where they could be vulnerable. Bottom line: always encrypt at the source, only decrypt at a secured destination, and never let the data be unprotected in between.

Other Security Considerations

Not only should the MFT solution you choose be able to support all aspects of encryption required for file transfers, but it also needs to seamlessly integrate with the innate security functions of the IBM i OS, including user and object authorities, network access, etc. This integration can also ensure that any established journaling processes track all file transfer activity. But beyond these, MFT solutions often include other important security-related capabilities, including:

- Add-on rules or policies that can be used to define how FTP processes are to run
- Intelligent firewall negotiation and port management for firewall "friendliness"—For instance, some trading partners require the use of Clear Command Channel (CCC), which keeps the data encrypted yet allows FTP commands to be decrypted to negotiate a firewall
- Ability to easily execute encryption key exchanges with trading partners, particularly banks—For instance, you can load your trading partner's public key onto your IBM i by entering the DNS name for the partner's server in the MFT solution, which then finds and retrieves that key and installs it into your system
- Automated password authentication capabilities that accommodate trading partners who require the use of passwords to establish a secure connection
- Auditing and reporting functions (commonly using QAUDJRN journaling) that track all transfer activity in order to easily view a history of files transferred, date and time of transfer, identity of sender and receiver, success or failure of transfer, etc.—Regardless of whether IBM i journaling is used, the audit trail can be forwarded to a security information and event management (SIEM) solution if one exists. Comprehensive auditing and reporting are critical when there's a necessity to demonstrate compliance
- Native integration of PGP to automatically encrypt files immediately upon arrival in file transfer staging areas— and not only for Db2 and IFS files, but also for any save files and spooled files that are transferred

Integration of Secure File Transfers Within Business Processes

As mentioned at the outset of this ebook, MFT solutions can provide many benefits to an enterprise through an array of automation features that enable tight integration with business applications and other processes.

Certainly, an IT department can write its own scripts and programs to securely integrate file transfers within business processes, but these are time-consuming to develop and maintain, can cause unintended security issues, and often lack the flexibility needed to respond to one-off situations that invariably arise. In large IT shops without an MFT solution in place, it's not unusual for various developers to create file transfer scripts and programs in their own way, which creates enormous headaches when troubleshooting is required down the road. And then there's the consideration of properly logging transfer activity, archiving transferred files, and generating alerts when transfers aren't successful.

For these reasons and others, many companies choose instead to use a full-featured MFT solution that not only provides the latest encryption capabilities, but also includes a suite of powerful automation and integration functions with these capabilities:

- Monitor designated libraries/directories on local or remote servers for files to be sent and then automatically execute transfer processes based on predefined protocols. MFT solutions are also able to monitor designated libraries/ directories on remote servers for files to be received (e.g., from business partners) and then automatically pull those files to the remote system.

- Integrate file transfer processes within applications via commands and APIs with multi-step workflows that allow related business processes to be automated and reduce the need for human intervention. For instance, securely pull payroll files from a remote system to your local system and then automatically process data from those files within payroll applications.

- Schedule transfer processes so they occur at optimal times

- Perform automated retries when connections can't be made, and automatically resume any transfer that might be interrupted

- Archive transferred files automatically

- Create ZIP or PDF versions of files automatically before files are encrypted and sent, as well as provide automated processing of received ZIP files—for instance, unzipping and then processing all files contained therein

- Alert administrators when files are unsuccessfully sent/ received and provide clear information as to the cause. It shouldn't take a programmer to figure out why a transfer failed

- Scale to accommodate hundreds or even thousands of transferred files every day in a fully automated and secure manner

In addition to the above, an MFT solution should utilize open standards and protocols so that file transfers can easily interoperate with any business partner or reporting entity. It is important to avoid proprietary processes that require distributing special software to the entity that is to receive a transferred file. By the same token, your MFT solution must be able to accommodate any required processes and protocols from external trading partners; for instance, many major banks provide their trading partners with predefined send/ receive configurations.

Cross-platform functionality is also an important requirement for many companies, which is why some MFT solutions include the ability to pull transfer-ready files from a variety of internal IT platforms into a centralized file transfer-management hub from which the files can be managed and sent. Another crossplatform MFT function that's critical for many companies and their trading partners is the ability to receive and process PGP-encrypted files from systems beyond IBM i, such as Windows, Linux, UNIX, and IBM z.

Bringing It All Together

Whether executing transfers between business partners, government agencies, reporting bureaus, or intra-company departments, a full-featured MFT solution provides IBM i shops with all necessary file transfer security and management capabilities. With strong encryption, process automation, application integration, and a centralized, consistent method of handling every aspect of the file transfer process, administrators are assured of data security, and developers are freed up to focus their valuable attention on strategic priorities. Given the increasing pressure to meet compliance regulations and to do more with less, the functionality and affordability of today's MFT solutions bring many welcome benefits to companies of all sizes.

Assure Secure File Transfer

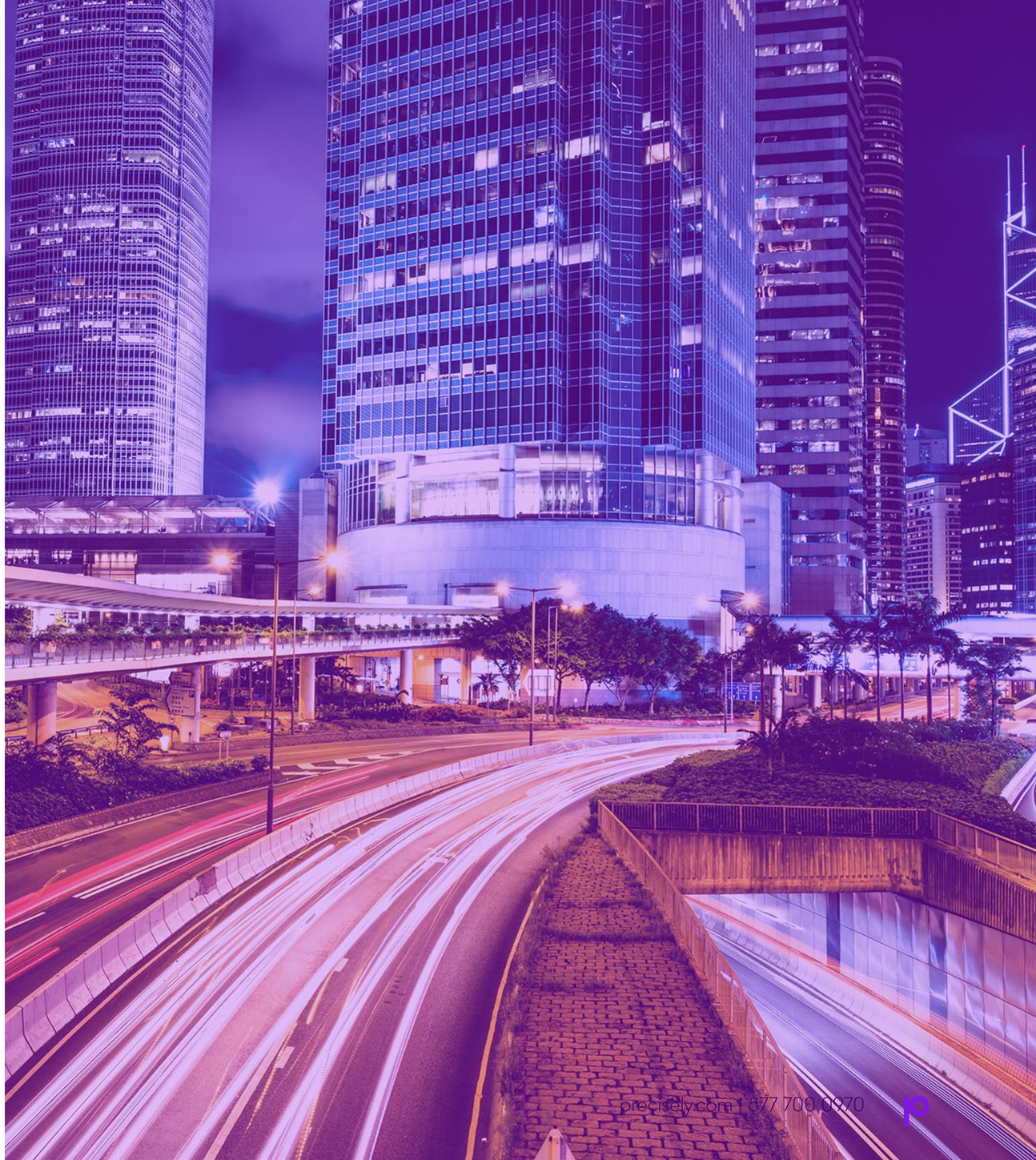
Providing secure, encrypted file transfers using the latest SFTP, FTPS, and PGP industry standards, Assure Secure File Transfer is designed to scale to any volume of transactions across multiple environments. This comprehensive MFT solution for IBM i includes a full set of commands, APIs, and automation features for maximum flexibility to help you exchange files without human intervention.

Other powerful capabilities include:

- Full interoperability with both commercial and open-source implementations of PGP—In fact, Assure Secure File Transfer is the only IBM i MFT solution that supports Symantec's commercial PGP implementation.
- Intelligent firewall negotiation capabilities, including Clear Command Channel (CCC)
- Support for a variety of file types: Db2, IFS, save file, and spool file
- Auto-scan facility that connects to remote FTP servers and automatically pulls files to your local system
- Centrally managed security policies
- Extensive automation/hands-off features

- Hub-and-spoke capabilities for centralized FTP management
- Detailed event logging and comprehensive audit trails that provide a permanent history of transfers to help companies meet compliance regulations
- Automated password support with SFTP to accommodate connection requirements of trading partners
- Support for key standards:
  - PGP is compatible with the OpenPGP standard documented in RFC 2440 as well as FIPS 140-2
  - FTPS is compatible with RFC 2228
  - SFTP is based on the OpenSSH implementation — a proposed Internet standard
- And numerous other security, automation. and integration capabilities

To learn more about all of Syncsort's security products and services, visit www.precisely.com.



precisely

About Precisely

Precisely is the global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely's data integration, data quality, location intelligence, and data enrichment products power better business decisions to create better outcomes. Learn more at www.precisely.com.

www.precisely.com