

AN ACCELLION WHITE PAPER

# No More FTP

## Eliminate FTP Issues with a Secure File Transfer Appliance

COMPLIANT, EASY TO USE, AND EASY TO MANAGE



Accellion, Inc.  
1900 Embarcadero Road  
Suite 207  
Palo Alto, CA 94303

Tel +1 650 739-0095  
Fax +1 650 739-0561  
[www.accellion.com](http://www.accellion.com)  
[info@accellion.com](mailto:info@accellion.com)

FTP and overnight delivery of CDs do not meet the stringent tracking and audibility requirements of business processes that must comply with government mandates.

## Executive Summary

Today's business environment requires ad hoc and instantaneous sharing of information. Driven by new applications that create massive amounts of data as well as globalization, systems for sending large files have not kept up with the business need.

Existing solutions for sending large files fall short in several regards: E-mail does not handle large files (even just 10MB) efficiently and FTP is too difficult to manage, administer and use. End users often resort to time-consuming workarounds such as burning CDs and sending them via overnight mail.

More seriously, FTP and CD sending do not meet the stringent tracking and audibility requirements of businesses processes that must comply with government and industry mandates such as Sarbanes-Oxley Section 404, FDA 21 CFR Part 11, and HIPAA.

A new appliance-based solution for secure file transfer has been developed to provide a compliant, easy-to-use and easy-to-manage system to send large files. Companies who have implemented secure file transfer based on a *Secure File Transfer Appliance* have eliminated FTP servers, improved the performance of e-mail, reduced storage requirements, and created compliant business processes.

Most companies need to move at electronic speed and are using a very unlikely tool to send their data: FTP.

## The Growing Need to Send Large Files

Today's business environment is changing more rapidly than ever before. Globalization and increased competition are driving new business models and collaboration needs. For example, outsourcing is creating new demands to synchronize business processes across companies and increase the sharing of information. Another example is the always on, distributed company that has to make faster decisions, which requires more information to be available and shared more broadly. *Business users are demanding new tools for instantaneous ad hoc communication and data transfer.*

Information and how we share it has evolved as well. Five years ago, most people would use e-mail to share spreadsheets and Power Point presentations. For other data sharing, they typically relied on custom systems. Today, presentations and spreadsheets are much bigger and are used much more broadly. In addition, application files and sometimes even whole databases are regularly shared as part of new business processes. Examples of large files that are routinely sent today range from closing documents for complex financial transactions, design documents for engineering firms, research databases for pharmaceutical companies, and video files for advertising and media firms. *Many of these files are so big that e-mail cannot be used to deliver them.*

Finally, many business processes have changed so rapidly that the supporting IT systems are out of sync with the businesses they support. While people used to rely on corporate systems to integrate a company, we are now seeing much more data being shared outside the formal IT systems, using alternative or non-standard solutions. While some organizations have resorted to more cumbersome and costly solutions, such as CD burning and overnight mail, most companies need to move at electronic speed and are using a very unlikely tool to send their data: FTP.

## Why FTP Falls Short For Today's Business Requirements

FTP falls short as a scalable business application in several areas that are more serious and costly than inconvenienced business users.

FTP, or File Transfer Protocol, was one of the first protocols generated by the early Internet back in 1973. FTP was developed so that people could share files between computers on the Internet. It was designed by programmers to share files with other programmers with the usage metaphor of manually copying files through a command line interface. It rapidly became a ubiquitous programmer tool but it is very unlikely that it would ever have become a business tool had there existed reasonable alternatives.

When FTP is used in a business environment it is typically implemented as follows: An FTP administrator creates one or more FTP directories where files that need to be shared are put. People who want access to some or all of these files are granted access to one or all of these directories. Recipients (or downloaders) download files through a browser from the directories they have access to.

For business collaboration, FTP is often unfamiliar, inconvenient, and difficult to fit into the normal work flow. However, FTP falls short as a scalable business application in several other areas that are more serious and costly than inconvenienced business users.

#### **Lack of security is the most dangerous shortcoming of FTP**

When FTP was designed, the security environment was much more benign. Now, with the need for greater controls and tracking digital assets, FTP represents a security risk for most companies. Security and control have become the responsibility of the over taxed IT administrator who must minimize file exposure to the wrong parties, delete files, setup and manage accounts, maintain complex file directories, and securely distribute passwords. Frequently, the system breaks: passwords are shared amongst multiple users, files are left for months in the FTP directories, and confidential documents may be exposed. Many of the security vulnerabilities have been alleviated with new flavors of FTP (e.g. SFTP, FTPS, EFTP) which typically require that special client programs be installed on user's computers. However, requiring ad-hoc recipients to install a program for file delivery imposes a time consuming overhead, which limits adoption.

Now, with the need for greater controls and the tracking of digital assets, FTP represents a security risk for most companies.

#### **FTP Account set up is time consuming for IT**

An FTP system account has to be created for both up-loaders and down-loaders. Waiting for this to happen is frustrating for business users who may have an immediate need. Apart from administration overhead, this causes further security issues because users start sharing accounts and passwords and outside recipients have login access to a computer behind the corporate firewall.

#### **File management on FTP servers is an administrative burden**

Over time, FTP directories tend to fill up as people upload more files. Unfortunately the people who up-load files rarely remove them. The result is directories of hundreds of large files and little knowledge as to which files should be deleted. The FTP administrator will likely guess based on file name, type and date with somewhat unpredictable results and potentially upset users. Because of the lack of automatic cleanup of files in FTP, valuable digital assets are frequently left unprotected in an FTP directory for extended periods.

#### **FTP is not a good collaboration tool**

The usage metaphor of FTP is quite different from e-mail, the standard ad hoc collaboration tool for business. Users have to download a file when they believe that a new version has been uploaded. The up-loader will not know when someone downloads a file. There is very little ad hoc about FTP because of the account set up structure. From a user perspective, the preferred way to send a large file is as an e-mail attachment. However because of the burden on the e-mail infrastructure (specifically storage and server performance), large attachments are often prohibited on many e-mail systems, forcing FTP on end users and left for IT to maintain.

Business processes that routinely rely on FTP to deliver information or other digital assets are not auditable and are not compliant.

### FTP does not meet compliance requirements

New regulations such as HIPAA, FDA 21 CFR Part 11 and most notably Sarbanes-Oxley, require that companies prove that the intended information, and only the intended information, was shared or exchanged (HIPAA); administrative controls are in place when electronic systems and records are used in place of paper or manual systems (FDA); and that business processes have integrity and are auditable (Sarbanes-Oxley). In these environments, FTP does not have the required control capabilities. The only way companies can prove that data deliveries took place is if the delivery system keeps records of all transactions and that these records can be retrieved later. But FTP doesn't keep records of each download. This makes sense: FTP was designed to be an open protocol for programmers to share files and not to be an auditable business tool. *Still, business processes that routinely rely on FTP to deliver information or other digital assets are not auditable and are not compliant.*

And although FTP is *free*, when the above factors are taken into account, the cost is clearly significant and the possible risks even more costly. This had lead to some organizations developing their own applications but this approach is hard to maintain and scale with the business usage needs both internal and external to the company.

*So, what compliant, secure, and effective alternatives are there to FTP?*

## An FTP Alternative: the Secure File Transfer Appliance

Until now, the few alternatives to sharing large files have not been easy to use or deploy, nor suitable for meeting widespread requirements for security, scalability, usability, and maintenance. The ideal file transfer system needs to have the following characteristics:

Until now, the few alternatives to sharing large files have not been easy to use or deploy, nor suitable for meeting widespread requirements for security, scalability, usability, and maintenance.

**Auditability and traceability.** This can be considered one of the key drivers of a better file transfer system. Government regulations now demand that companies have in place *auditable business processes*. Large file sharing is often part of critical business processes. See Table 2 for a list of major compliance regulations.

**Security.** Large files often represent digital assets that need to be managed securely rather than being sent 'out in the open'. FTP is insecure by design, with no encryption or secure channels for upload or download.

**Easy to manage and maintain.** How easy a system is to manage and maintain is more important than the purchase price to the system's total cost of ownership.

**Efficiency.** Although bandwidth and storage may be getting cheaper, the cost of managing the storage and utilizing the bandwidth capacity can be several fold the purchase cost. Given the exponential increase in file size and the need to share more and more versions of these files with more and more people, any file transfer system must be able to optimize the storage and bandwidth available.

A new solution has been developed to meet the need for ease of use, easier to maintain, and more secure large file sharing. A *Secure File Transfer Appliance* is easy to use and requires nearly zero administration for IT. This system addresses the limitations of FTP by:

**Sharing any size file securely**

A Secure File Transfer Appliance gives business users an easy and intuitive way to send up to gigabyte sized documents to both internal and external recipients. All data transfers use secure tunnels. Senders receive a download receipt whenever a file is downloaded.

**Eliminating the administration burden**

Users send files through a Web interface as easily as sending an e-mail with an attachment. The recipient receives an e-mail with a link to the file and downloads the file by simply clicking on the link's Web URL. Optionally, the system allows external recipients to self-register to send files back to the originating company. This eliminates the need to have system accounts laboriously set up, monitored, and deleted for both sender and recipient.

**Managing digital assets**

Any file sent and downloaded is tracked, the sender receives a download receipt, and files can be automatically deleted or archived after a system configurable length of time. The only way files can be accessed is through the embedded e-mail links.

**Enabling compliant processes**

Because of the secure and auditable design of the Secure File Transfer Appliance, it can be part of business processes compliant with government regulations. The next section highlights some of the regulatory requirements that the system supports.

Any file sent and downloaded is tracked, the sender receives a download receipt, and files can be automatically deleted or archived after a system configurable length of time.

### Providing operational efficiencies

A Secure File Transfer Appliance optimizes both storage and bandwidth. Any type of storage – NAS, SAN, offline, etc. can be integrated with the appliance for long term archival. Automated retention and deletion rules can be put into place that make the system self-managing. The system is able to fill available bandwidth, such as point-to-point lines, for maximum speed of transfer. It enables optimum service levels because spikes for sending large files are smoothed and files can be prioritized for sending. Furthermore, the system can be configured to be redundant with failover capability and is able to scale seamlessly as the business need grows.

**Table 1: Comparison of File Transfer Methods**

	FTP	Newer FTP (SFTP, FTPS, EFTP)	E-mail Attachments	Secure File Transfer Appliance
<b>Business</b>				
Suitable for ad-hoc file delivery	No	No	Yes	Yes
<b>Security</b>				
System Account Based	Yes	Yes	No	No
Login Security	No	Yes	Depends	Yes
Transport Layer Security	No	Varies	No	Yes (SSL)
Can Virus Scanner be integrated	Cumbersome	Cumbersome	Yes	Yes
<b>Administration</b>				
Required End User Client Installation	No (Browser)	Yes	No	No (Browser)
Manual Account Creation and Deletion	Yes	Yes	No	No
Manual deletion of files	Yes	Yes	Shifts problems to Mail Server	No
Reporting and Visibility	Log files	Varies	Difficult	Yes
<b>User</b>				
Learn and Install New Client	No	Yes	No	No
Send very Large Files	Yes	Yes	No	Yes
File up Mailboxes	No	No	Yes	No
Require Administrator Intervention (create accounts)	Yes	Yes	No	No
Guaranteed Recipient receipt notification	No	No	No	Yes

## Compliant File Transfer Applications

There are numerous government regulations where a Secure File Transfer Appliance would aid in compliance. The table below summarizes several U.S. regulations that address data permanence, data security, data privacy, and data traceability. A Secure File Transfer Appliance can support a compliant business process in these areas:

Any business process that incorporates the transfer of large files and needs to verify authenticity, maintain an audit trail, and retain a record of file transfer, will benefit from incorporating a Secure File Transfer Appliance.

**Table 2: U.S. Regulations regarding Data permanence, security, privacy and traceability**

Legislation	Vertical Segment	Requirement	Impact
Sarbanes-Oxley (SOX) Act, Section 404	Industry-wide	Requires public companies to verify that their financial-reporting systems have the proper controls, such as ensuring that revenue is recognized correctly. Requires testing and monitoring of internal controls via establishing, documenting, and auditing business processes.	Audit trails, authenticity, record retention
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare	Addresses security policies and procedures of insurance companies and providers regarding personal health information and services.	Record retention, privacy, protection, service trails
21 CFR Part 11	Life Sciences	Regulates life science and pharmaceutical companies involved in biotechnology and manufacture of medical equipment, food, and beverage concerning electronic and paper record retention.	Record retention, authenticity, confidentiality, audit trails
Department of Defense (DOD) 5015.2	Government	Concerns all defense-related government agencies' and contractors use of technologies relating to records.	Authenticity, protection, secure shredding
Securities and Exchange (SEC) Act Rules 17a-3 4 (17 CFR 240,17a-3,4)	Financial Services	Requires broker retention of sent and received communication, including interoffice memos, e-mails, sales training manuals, advertisements, and account records	Protection, audit trails Record retention, authenticity

Any business process that incorporates the transfer of large files and needs to verify authenticity, maintain an audit trail, and retain a record of file transfer, will benefit from incorporating a Secure File Transfer Appliance. Because the system is easy to use for both sender and recipient, it can be integrated into any compliant business process to ensure that a file, document or any other digital asset has been 1) delivered to the intended recipient at the intended time, and 2) deleted or archived for the required time.

## Solutions for an Appliance-based File Transfer System: Accellion

Accellion has the premiere appliance-based secure file transfer solution on the market today. Accellion pioneered the use of an appliance-based model for secure file transfer and Accellion's enterprise solution is cost-effective, auditable, secure, and easy to use for business users and IT management.

### Accellion Secure File Transfer System

**ACCELLION APPLIANCE** The Accellion Appliance is used to temporarily store large files as they are being transferred. When a large file is sent via Accellion the file is first uploaded to an Accellion Appliance, then the recipient is sent an email containing a secure link to the file. The recipient then clicks on the secure link to download the file from the Accellion Appliance. The Accellion secure file transfer solution can be implemented as a single site installation with a single Accellion appliance or quite typically in an enterprise installation multiple Accellion appliances are installed in different geographic locations to provide a secure file transfer network. The Accellion appliance is placed in the DMZ for delivering attachments to external recipients. Accellion Appliances require minimal maintenance because the operating system and software are maintained as an appliance, so issues with operating system compatibility do not exist. The appliance is available in multiple models to fit the capacity needs of any size enterprise.

**ACCELLION WEB USER INTERFACE OR EMAIL PLUG-IN** Accellion users have the choice of sending a large file either via the Accellion web interface or the Accellion email plug-in for Microsoft Outlook or Lotus Notes. Using either user interface the Accellion user composes an email to the intended file recipient and attaches the file. Using the Accellion email plug-in the user will make use of an Accellion Attach icon located in the email toolbar. When the e-mail is sent, the file is not included in the e-mail; only a secure link to the file is included. The attached file is instead sent to the Accellion Appliance. The recipient clicks on the link in the e-mail and downloads the file from the Accellion Appliance.

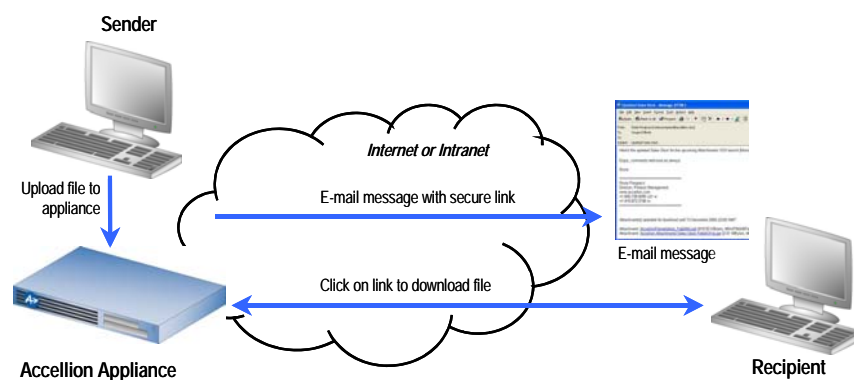
**ACCELLION ADMINISTRATION USER INTERFACE** Initial setup and minimal ongoing maintenance are accomplished through a Web-based Administrative interface. Appliances can be managed remotely with just a standard Web browser. Initial setup will configure replication and retention policies based on the amount of time required to store a file, the type of file, user groups and other parameters. Statistics and usage can be reported for a particular appliance or a network of appliances. Charge back grids can be established to bill clients or internal departments.

### How Accellion Works

Accellion sends large files outside the e-mail infrastructure, yet provides all the convenience of e-mail for both the sender and the recipient. The sender sends through a Web-based User Interface. The recipient receives an e-mail message with an embedded, secure link.

Accellion sends large files outside the e-mail infrastructure, yet provides all the convenience of e-mail for both the sender and the recipient.

Figure 1: How Accellion Secure File Transfer Works



### How Accellion Secure File Transfer Works

By not including the file in the e-mail, the created e-mail is tiny and will not be blocked for being too large by any recipient's e-mail system. When the recipient receives the e-mail and clicks on the embedded link, the file is downloaded from the Accellion Appliance using SSL. The file transfer is secure and compressed and performance is exceptional.

The most important feature, from a compliance perspective, is the fact that the Accellion secure file transfer system keeps records of all downloads. Return receipts are also sent to the sender every time a file is downloaded.

Unlike FTP, Accellion's appliance-based file transfer solution is easy to manage. Account creation and maintenance is greatly simplified with Accellion. With LDAP/AD integration, users of Accellion file transfer can make use of existing network accounts and passwords. Recipients of files sent via Accellion can also voluntarily register as restricted senders and can send files back without IT intervention. With the elimination of FTP, file management is no longer IT support intensive. The Accellion secure file transfer system provides tools to automatically remove files when their availability life span has expired.

### Conclusion

FTP does not meet the requirements of today's business for compliance, security, and ease of maintenance. It is now possible to share large files quickly, securely, and effortlessly, as part of a compliant process. The use of a Secure File Transfer Appliance, offers the key advantages of auditability, traceability, security, ease of maintenance, and efficiency, and provides the preferred solution for compliant and secured *ad hoc* large file transfer. Accellion offers a proven Secure File Transfer Appliance that is deployed at leading corporations around the globe.

The most important feature, from a compliance perspective, is the fact that Accellion keeps records of all downloads.

## About Accellion

Founded in 1999, Accellion, Inc. is the premier provider of on-demand secure file transfer solutions with an extensive customer base covering industries such as advertising/media production, legal, manufacturing, healthcare, consumer goods, higher education, and more.

Accellion provides an enterprise file transfer solution that is secure, economical and easy to use for both end users and IT management. Unlike email and FTP that can no longer meet the evolving security and business requirements, Accellion enables enterprises to eliminate FTP servers, create Sarbanes Oxley compliant business processes, improve e-mail infrastructure performance, and reduce IT management footprint requirements.

The Accellion secure file transfer solution allows internal and external users to send and receive files bi-directionally on the same platform without adding administrative overhead or infrastructure burden. Accellion offers an intuitive web interface with end-to-end file security and policy-based file lifecycle management. Accellion also supports plug-in integration with Outlook and Lotus Notes email clients. For multi-site enterprises, Accellion offers clustering for multi-site load balancing, intelligent replication and failover.

Accellion is a privately held company headquartered in Palo Alto, California with offices in North America, Asia and Europe..

**[www.accellion.com](http://www.accellion.com)**

**[info@accellion.com](mailto:info@accellion.com)**

THIS DOCUMENT IS PROVIDED "AS IS." ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.