Acronis

Still using FTP to Share Files? There's a Better Way!

If your company is still using FTP, now might be a good time to take a look at a commercial-grade secure file sync and share solution as a more secure, efficient and easy-to-use FTP replacement.

Contents

Introduction

At one time or another, practically every business has used and may still be using file transfer protocol (FTP) to transfer files. With the first specification published in 1971, there are dozens of FTP servers and clients available. Although thousands of companies worldwide still use FTP today, many have criticized it for a variety of reasons including the lack of adequate security. The marketplace has introduced alternative protocols such as file transfer protocol secure (FTPS) and secure file transfer protocol (SFTP) to replace FTP for those reasons. While these offer more security, they are based on the same principles and suffer many of the same weaknesses. In some cases they are also more complicated to set up and use.

Regardless of the security issues, companies use FTP to transfer files for use within applications, including their website, and for sharing of files with internal or external constituents. This solution brief discusses the benefits of replacing FTP with Acronis Access Advanced to ensure:

- The reliable transfer and sharing of files and documents to internal and external constituents
- End-to-end security and privacy of files and documents
- Ease of use and ease of IT management
- Improvements in employee productivity

If your company is still using FTP, now might be a good time to take a look at a commercial-grade secure file sync and share solution as a more secure, more efficient, and easier-to-use FTP replacement.

Why Companies Use FTP

Like many organizations, you are still using FTP today because:

- You have been using it for many years and it works, so “if it ain’t broke, don’t fix it.”
- Your system administrators know how to manage FTP servers, accounts, and security. Or: No one in your company knows anything about how FTP works, nor where the FTP server is located.
- It’s perceived as inexpensive to buy and operate — even free.
- If you stop using FTP, you might “break” something.
- It’s too much work to rip and replace.

5 Weaknesses of FTP

Although FTP can be relatively inexpensive and fairly easy to set up and use, it is technology from the 1970s and 1980s and not without risk when it comes to handling sensitive documents and data. Here are five reasons why you should seriously consider an alternative to FTP:

1. FTP is not secure: With the risk of corporate data breaches happening more and more every day, companies are concerned with data security. Plain FTP offers no native encryption of data in transit or at rest, potentially leaving confidential information exposed. Sending user names and passwords via FTP leaves them in the clear — unencrypted. You can access FTP servers with any of the hundreds of FTP clients available, making it virtually impossible to secure and control both ends.
2. FTP is not end-user friendly: To send files to a new contact, a new FTP account needs to be set up. Users do not normally have access to the FTP server administration and managing FTP is far from user friendly, so they need to rely on the help of an IT Administrator to create new accounts, retrieve forgotten passwords, and remove accounts for those who no longer require access. This can result in your organization leaving user accounts active for too long a period of time, and in users sharing accounts in order to avoid waiting for IT. Both of these are violations of security best practices.
3. FTP requires manual management: FTP does not normally allow users or administrators to set policies to automatically expire or purge files. Every file ever sent to, or from, an FTP server remains on the server until an IT administrator deletes it. Manual management of these files is a low-value, high cost, labor-intensive chore for IT, and another needless security vulnerability.
4. FTP lacks adequate auditing tools: FTP provides companies with limited capabilities to track file transfers: who sent what, to whom, and when. In the wake of an attack on the FTP server, or the use of FTP to leak sensitive information, companies struggle to track, diagnose, report, or conduct forensics on the security breach. Without the ability to provide an audit trail, FTP makes it difficult for companies to take the necessary steps to prevent subsequent breaches, and to achieve regulatory compliance.
5. FTP is unreliable: When sending a file via an FTP server, the sender has no way to verify whether the recipient successfully received or downloaded the file. If an error occurs during the transfer, the system does not notify the sender. Without external verification (e.g., via email, text, scripts, or voice call), it is difficult to know if a FTP file transfer is successful.

5 Strengths of Acronis Access Advanced

Acronis Access Advanced provides secure mobile access to files and documents, breaking down barriers between people, information, privacy, and security. Powered by the Acronis AnyData Engine, Acronis Access Advanced is an easy, complete and secure file access, sync and share solution. Users can access their files and content anywhere, across any of their devices, and securely share files and collaborate with others. Acronis Access Advanced was created from the ground up to meet the productivity, security and management requirements the modern mobile workforce, especially in industries with compliance concerns.

Let's compare how Acronis Access Advanced addresses the five weaknesses of FTP.

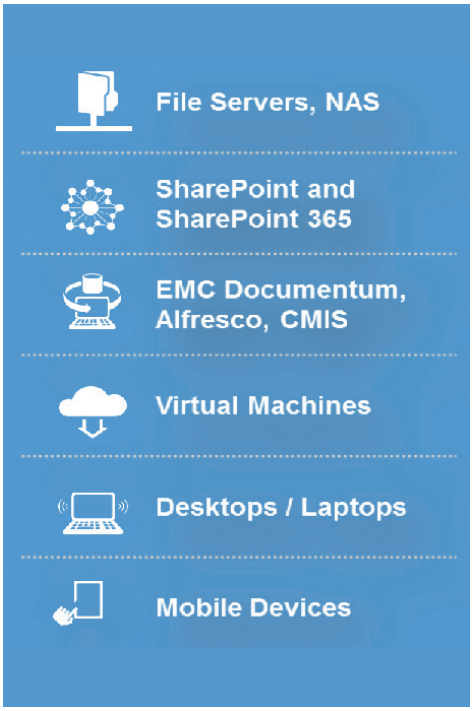
1. Acronis Access Advanced secures user content with end-to-end protection including **encryption in-transit and on-device, secure in-app editing, secure web preview of documents, IT control of authorized users for sharing, and a simple and secure way to confirm guest identity before sharing documents.**
2. Acronis Access Advanced is easy to use: Employees can easily and safely create new documents and edit content that resides on **on-premise file servers, Network-Attached-Storage (NAS), SharePoint®, servers and content management systems — including Alfresco, EMC Documentum, and generic content management interoperability services (CMIS) data — whether working from a smartphone, tablet, laptop or PC.** It also offers **an intuitive, natural, and consistent user experience;** employees require virtually no training to use it.
3. Acronis Access Advanced is easy to manage: IT administrators can control data, users, and devices with an advanced **Policy Engine and Active Directory®** support that simplifies user management and onboarding. IT can define policies on **50+ administrator-configurable features** including file types, size, and properties. Acronis Access Advanced easily **integrates with mobile device management (MDM) solutions**; a Setup Wizard makes it simple to install.
4. Acronis Access Advanced provides **audit capabilities**: **it logs all access**, **sync, and sharing activities and filters information by various elements** — all capabilities required to meet compliance standards and improve monitoring and oversight of user activities.
5. Acronis Access Advanced is reliable: Users can immediately **view any content uploaded** to Acronis Access Advanced and are **notified when content is available.**

Additional Key Features

In addition to the features discussed above, Acronis Access Advanced also:

- Provides full support for Bring Your Own Device (BYOD), enabling mobile users to access their work from their own smartphones, tablets, laptops and desktops, including from Web browsers.
- Offers built-in Microsoft® Office document editing and PDF annotation.
- Scales to any number of users and servers.
- Supports file sync and sharing across multiple devices.
- Supports both physical and virtual environments.
- Integrates with Microsoft Intune mobile application management (MAM) to prevent corporate data from leaking into personal apps and file stores.

With Acronis Access Advanced, your employees have immediate access to files to better drive your business and respond to customer needs.



Acronis Access Advanced Key Features

BOOST EMPLOYEE PRODUCTIVITY AND GAIN A COMPETITIVE EDGE THROUGH ANYPLACE, ANYTIME ACCESS AND COLLABORATION FROM ANY DEVICE.

Use Case – Investment Bank

At a large investment management firm, an external system regularly uploads a variety of important documents, such as stock quotes, banking reports, financial statements, fund updates, and other time-sensitive information. The bank has a service level agreement (SLA) with many of its customers to deliver these files within 10 minutes of the bank receiving them from the external system.

With FTP, the bank is having difficulty getting these documents to all of its customers as required by their SLAs. When customers have slow connections or the transfer takes longer than 15 seconds, the transfer suffers a timeout error and IT must manually restart the transfer. In the meantime, all subsequent documents in the queue are forced to wait, as each document must be sent in chronological order. If three or four destination servers are slow, then the last documents in line are not getting to customers in accordance with their SLAs.

After moving from FTP to Acronis Access Advanced, the investment firm now sets up unique folders for each customer which only that customer can access. Only that customer can access their folder. When the system transfers the documents to the investment bank, the documents are copied directly into all appropriate customer folders via Acronis Access Advanced.

ACRONIS ACCESS ADVANCED AUTOMATICALLY NOTIFIES THE BANK'S CUSTOMERS WHEN THE DOCUMENTS ARRIVE IN THE FOLDER.

And unlike FTP, Acronis Access Advanced provides end-to-end control of data, users, storage, server software, and client applications.

Use Case – Healthcare

The healthcare industry is finally embracing the electronic medical record, making it challenging to move large documents such as x-rays, CAT scans, MRIs, even videos of surgical procedures. Not only is the size of these files a challenge, but the security and privacy required as per HIPAA regulations must ensure that unauthorized individuals CANNOT access the documents.

With FTP, a user can connect and log in to an FTP-based server with any FTP client — regardless of the brand or precedence. Once an unauthorized user is on the server, anything can happen including a breach.

With Acronis Access Advanced, one large medical center can easily transfer the largest of files to external providers and payers. Internal users set up folders for specific individuals who require patient records. Documents can be manually or automatically uploaded to the appropriate folder. Once uploaded, Acronis Access Advanced automatically notifies the recipient provider or insurer via email, and only that individual can access, view, or download the records.

THE PATIENT RECORD IS SECURE FROM END TO END. ACRONIS ACCESS ADVANCED ALSO PROVIDES AN AUDIT TRAIL TO ENSURE AND PROVE PATIENT PRIVACY AS REQUIRED BY HIPAA.

Summary

FTP can be slow, unpredictable, unreliable, and unsecure. Even though it has worked for your organization for many years, it is time to reconsider how more up-to-date technologies can help you share critical documents — in accordance with SLAs and compliance regulations — and with end-to-end security in mind.

	Acronis Access Advanced	FTP
Security	End-to-end control and security including: • Encryption in-transit and on-device • Managed remote wipe in case of lost device • Secure in-app editing • Secure web preview of documents • IT control of authorized users for sharing • Secure guest identity confirmation before sharing documents	Plain FTP offers: • No encryption of data in transit or at rest, potentially leaving confidential information exposed • No remote wipe • No control over content that is stored on-device Any user can connect and log in to a FTP-based server with any FTP client. Some vendors claim "advanced security" with newer or adjunct products, but details are always vague.
Ease of Use	Employees can easily and safely create new documents and edit content that resides on on-premises file servers, NAS, and SharePoint®, and content management systems.	Users need IT to set up new accounts for users and sharing, retrieve forgotten passwords, and remove accounts for those who no longer require access. This can result in leaving user accounts active for too long a period of time, or in users sharing accounts so as to avoid waiting for IT. Both of these are violations of security best practices.
IT Management	IT can: • Control data, users, and devices with an advanced Policy Engine and Active Directory® support that simplifies user management and onboarding, data access, sharing and operations. • Define policies on 50+ administrator-configurable features including file types, size, and properties. Acronis Access Advanced easily integrates with mobile device management (MDM) policies. A Setup Wizard makes it simple to install.	FTP does not normally allow users or administrators to set policies to automatically expire or purge files. Every file ever sent to, or from, an FTP server remains on the server until an IT administrator deletes it. Manual management of these files is a low-value, labor-intensive chore for IT and opens up a security vulnerability.

	Acronis Access Advanced	FTP
Audit Capabilities	Acronis Access Advanced provides: • Audit capabilities; logs all access, sync, and sharing activities and filters information by various elements — all capabilities required to meet compliance standards and improve monitoring and oversight of user activities • Automatic email notification of events, access, sharing and content change	FTP provides companies with limited capabilities to track file transfers. Companies struggle to track, diagnose, report, or conduct forensics on a security breach. Without the ability to provide an audit trail, FTP makes it difficult for companies to take the necessary steps to prevent subsequent breaches and to achieve regulatory compliance.
Reliability	• In case of errors, the internal user knows right away. • Authorized users can immediately view any content uploaded to Acronis Access Advanced and receive notifications when content is available.	When sending a file via an FTP server, the sender has no way to verify whether the recipient successfully received or downloaded the file. If an error occurs during the transfer, the system does not automatically notify the sender. Without external verification (e.g., via email, text, or voice call), it is difficult to know if a FTP file transfer is successful.

About Acronis

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile.

Founded in 2003, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products have been named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com**.
Follow Acronis on Twitter: **http://twitter.com/acronis**.