

10 Reasons Why FTP is No Longer the Right Tool for the Job

It's hard to believe the original file transfer protocol (FTP) was created back in 1971, and has been moving files for more than 40 years. The version of the protocol in use in most organizations today has not seen significant changes or improvements in 25 years — which is surprising when you consider how file transfer requirements have broadened and evolved during that time. It's not hard to understand why FTP has been and still is so widely deployed — it enables easy file exchange between just about any device and system. But when it comes to today's complex information exchange requirements, FTP is missing key elements enterprises can't afford to be without.

Here are ten reasons FTP is no longer the right tool for the job:

1. FTP has no encryption capabilities.

Encryption is the safest method available today for securing data, and FTP does not have the ability to encrypt or decrypt data.

2. FTP does not protect user names and passwords.

Attackers can easily locate user names and passwords when FTP sessions are initiated.

3. FTP does not have integrity checking.

When files sent via FTP arrive at their destination, there is no assurance that they arrive intact.

4. FTP has no checkpoint restart feature.

When FTP transfers fail, they cannot be resumed from the point of failure, but must start from the beginning. With the growth in file size and overall data volumes, this limitation greatly increases transfer times (not to mention the accompanying frustration for senders and receivers of those files).

5. FTP doesn't offer non-repudiation.

Using just FTP, there is no ability to prove that files have been sent.

6. FTP can't compress data.

With today's file sizes, data compression is a necessity. FTP requires scripting to compress files, adding even more complexity and work for IT, and yet another potential failure point.

7. FTP makes you wait.

FTP cannot push or pull files unless the client is available, which means transfers can be delayed without notification.

8. FTP does not provide visibility.

When you can't see what's happening with your file transfers, you can't be in control of your business. FTP does not have monitoring capabilities.

9. FTP is hard to manage.

It offers no consolidated view, automation or governance capabilities.

10. FTP is not "free."

Despite the perception that FTP is a "free" tool, in actuality achieving and maintaining security using FTP requires complex scripting, constant maintenance, and even other applications for added layers of security — all of which can be costly to your organization.

Axway Can Help

Axway enables organizations to reliably transfer critical business files internally and across their partner and customer communities, all while securing data and keeping up with evolving compliance and regulatory demands. Axway MFT solutions provide the visibility, governance and community management today's companies require to gain control and reduce TCO.

For More Information, visit www.axway.com

Copyright © Axway 2012. All rights reserved.

