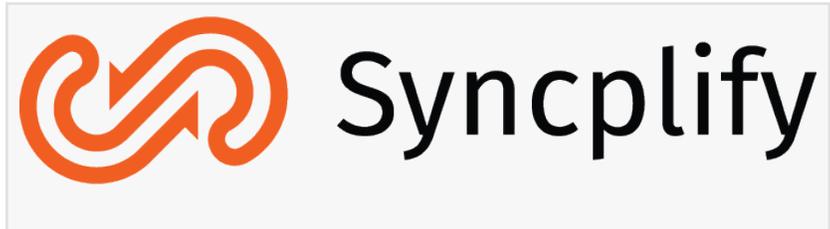# Syncplify Introduces Cryptographically Signed Log Files for Complete Audit Integrity

Syncplify Server! now features tamper-proof audit trails with cryptographic verification, raising the bar for SFTP compliance and forensic accountability.

CUPERTINO, CA, UNITED STATES, March 24, 2026 /EINPresswire.com/ -- Syncplify, the leading provider of secure file transfer solutions, announced today that Syncplify Server! will include cryptographically signed log files with full audit trace capabilities. This feature ensures the integrity and authenticity of every recorded action, making it impossible to alter, delete, or reorder audit records without detection.

Audit logs are the backbone of compliance investigations and incident response. With Syncplify Server!'s new cryptographically signed logs, every file transfer, user access attempt, permission change, and configuration modification is sealed with a cryptographic signature that proves no tampering has occurred. The signature chain links each log entry to the previous one, meaning that even a single altered character will break the verification chain and expose the tampering immediately.

"In a zero-trust world, audit trails should be verifiable, not assumed trustworthy," said Fjodr Soyevskji, CTO at Syncplify. "We built cryptographic signing into Syncplify Server! so that log files are not just records, but tamper-evident proof. In the event of a security incident or compliance audit, administrators can mathematically verify whether their logs have been manipulated by anyone, including privileged users."

The feature addresses a critical gap in file transfer security. While most SFTP servers generate logs, those logs remain vulnerable to manipulation by administrators with high-level access. Syncplify's approach binds each log entry to its cryptographic hash chain, creating an auditable record that can be verified independently and presented as evidence in compliance audits, forensic investigations, or legal proceedings. Administrators gain built-in verification tools that prove log integrity without question, while support for key rotation and long-term log retention ensures logs remain secure and accessible for years to come.

The innovation reflects Syncplify's ongoing commitment to practical security. Just as Syncplify remained unaffected by the Heartbleed vulnerability in 2014 and the Terrapin exploit in 2023,

this development demonstrates the company's focus on addressing real-world security challenges before they become industry-wide problems.

Cryptographically signed logs are available in Syncplify Server! 7.0.14 and are included as a standard feature with all new installations and renewals.

About Syncplify

Syncplify provides a comprehensive suite of secure file transfer solutions designed to safeguard sensitive data during transfers. Syncplify offers a robust selection of features, including military-grade encryption, granular access controls, and unwavering compliance support. For more information, please visit www.syncplify.com.

Helga Kessler
Syncplify Inc.
info@syncplify.com
Visit us on social media:
LinkedIn
YouTube