

Leverage Zero Trust File SharingSM in FileCloud Using Zip Files

What is Zero Trust?

Zero Trust operates on a principle of continuous identity verification and least privilege access. Users only have access to the data they absolutely need. Using the Zip folder mechanism, end users can securely share files inside and outside the organization's perimeter ("perimeter-less security").

Why Zero Trust?

The U.S. Department of Defense has recently released their Zero Trust Strategy and Roadmap for FY 2027. This roadmap establishes a Zero Trust framework to improve the U.S. government's security posture. The private sector will likely adapt this framework to roll out their own Zero Trust strategies, in the wake of evolving cyberattacks.



How Does Zero Trust Help Me?

As a user, I need to be able to package and share business-sensitive files with my colleagues and clients. The solution needs to be convenient and easy for me and my team, while also ensuring that my data is secure inside and outside the organization.

FileCloud already offers many features critical to a Zero Trust framework, including:



Identify Authentication



Endpoint Security



Malware Prevention



Activity Monitoring



Security Incident Response



AES Encryption

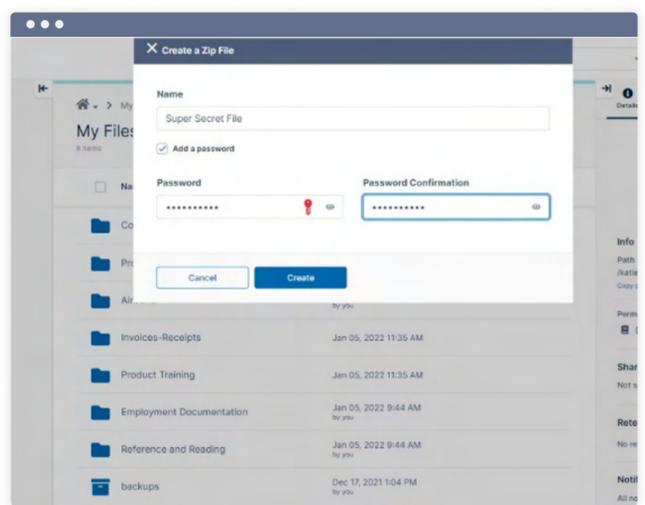
With Zero Trust folders, FileCloud admins and users can implement another level of hyper-security and control over highly sensitive or confidential data.

Zero Trust File SharingSM

Enable Zero Trust File SharingSM and storage with password-protected Zip files in FileCloud.

The decryption key is not stored within FileCloud, so your data remains secure even in the event of an attack or breach.

Once entered by a user, passwords are stored in the browser UI for the duration of the session by default. Admins can control this setting via FileCloud policy.



Hyper-Secure Control

Zip files are not scanned by FileCloud. Zero Trust files (Zip files with password-protection) are secured in FileCloud with 256-bit AES encryption.



Create & Share

Create, view, edit, download, and share Zip files in FileCloud Managed (local) storage. Share permissions can be set to read-only (view, download) or read-write (view, download, upload, delete).



Supported File Types & Limits

- Images (jpg, png), files (pdf, txt, docx), presentations (pptx) and spreadsheets (xlsx)
- All standard Zip compression formats and encryption formats (excluding TarGZ, 7-Zip archives, and RAR archives)
- Upload Zip files up to 4GB to FileCloud and create Zip files up to 100 MB.



Content Management with Zero Trust

Only users with the Zip file password can access data in Zero Trust storage. As a result, certain content management operations are not available, including activity logs, DLP, workflows, retention policies, metadata, content indexing, search, and file versioning.

How to Use Zero Trust Storage

1. Login to FileCloud and click "Add Files and Folders"
2. Select "New Zip File."
3. Name the Zip file and create a password.

How to Manage Content in Zero Trust Storage

1. In FileCloud, click the Zip file or the "Enter" icon.
2. Enter the password.
3. Upload new content or delete existing content.*

**Users with read-only access will only be able to view and download content.*