daDetective Cloud Access Utility - IT Professional Detailed View

IT Technical Overview

Audience: System Administrators, IT Security, Infrastructure Teams

Document Version: 1.0 | April 2026

Purpose

daDetective allows users to upload files from cloud storage (Google Drive, Dropbox, Amazon S3, Wasabi, Backblaze B2) directly into the daDetective platform via their browser. To accomplish this, the user's cloud storage is temporarily mounted as a local drive letter in Windows, enabling standard file selection through the browser's native upload dialog.

This document explains the two open-source utilities involved, what the setup process does at each step, and what IT teams need to know before approving deployment.

Components

rclone

Property	Detail
Description	Command-line utility for managing files on cloud storage. Often described as "rsync for cloud storage."
License	MIT (fully permissive open source)
Source Code	https://github.com/rclone/rclone — 56,000+ GitHub stars, actively

Property	Detail
	maintained
Version Included	Latest stable release at time of packaging
Binary	Single portable executable (rclone.exe), approximately 74 MB. No installation required.
Config File Location	`%APPDATA%\rclone\rclone.conf` — contains the remote name and authentication token

What rclone does in this context (two operations only):

1. **config create** — Registers the user's cloud storage credentials (OAuth token for Google/Dropbox, or access keys for S3/Wasabi/B2) in a local configuration file.
2. **mount** — Presents the cloud storage as a Windows drive letter (e.g., G: for Google Drive) using the WinFsp driver.

What rclone does NOT do:

- Does not install any Windows services
- Does not run in the background
- Does not start at login or boot
- Does not modify the Windows registry
- Does not phone home or send telemetry
- Does not copy, sync, or move files — it only mounts the remote storage as read/write

WinFsp (Windows File System Proxy)

Property	Detail
Description	A system driver that enables user-mode file systems on Windows. It is the Windows equivalent of FUSE

Property	Detail
	(Filesystem in Userspace) on Linux/macOS.
License	GPLv3 with a special exception for FLOSS. A commercial license is also available.
Source Code	https://github.com/winfsp/winfsp — 8,000+ GitHub stars, actively maintained
Installation	Standard MSI installer, installed silently via `msiexec /i ... /passive /norestart`. Installs a kernel-mode driver and a user-mode DLL. Reboot rarely required.
Compatibility	Windows 7 through Windows 11 — x86, x64, and ARM64
Adoption	Used by major software companies, cloud services providers, and financial institutions worldwide. Millions of installations.

What WinFsp does:

Provides the kernel-mode file system driver (FSD) that allows rclone to present cloud storage as a standard Windows drive letter. Without WinFsp, rclone cannot mount drives.

What WinFsp does NOT do:

- Does not access the network
- Does not transmit any data
- Does not phone home or send telemetry
- It is purely a local driver that bridges rclone's user-mode process to the Windows file system API

What the Setup Process Does (Step by Step)

The user downloads a provider-specific zip file from dadetective.com (e.g., `daDetective Google.zip`, `daDetective Dropbox.zip`, `daDetective Amazon S3.zip`, `daDetective Wasabi.zip`, or `daDetective Backblaze B2.zip`) containing four files: `rclone.exe`, the WinFsp installer (`winfsp-*.msi`), a Setup .bat file, and a Mount .bat file. They extract the zip to their Documents folder (by clicking Browse in the Extract dialog and selecting Documents), which creates a provider-specific folder (e.g., `daDetective Google`), and double-click the Setup file. Here is exactly what happens:

Step 1: WinFsp Installation

- The .bat file checks if WinFsp is already installed by looking for `%ProgramFiles%\WinFsp` or `%ProgramFiles(x86)%\WinFsp`.
- If not found, the script auto-detects any file matching the pattern `winfsp*.msi` in the extracted folder using `for %%f in ("%~dp0winfsp*.msi") do set "WINFSP_MSI=%%f"` with a `goto :winfsp_done` pattern to select the first match. It then installs WinFsp silently via `msiexec /i "%WINFSP_MSI%" /passive /norestart`, which shows only a progress bar — zero wizard clicks required. The only user interaction is the standard Windows UAC prompt ("Do you want to allow this app to make changes to your device?"). The .bat file itself does NOT require administrator privileges.
- If WinFsp is already installed, this step is skipped automatically.

Note: The WinFsp MSI triggers a standard Windows UAC prompt (“Do you want to allow this app to make changes to your device?”). This is unavoidable because WinFsp installs a kernel-mode file system driver. The user simply clicks "Yes" on the UAC prompt; no other interaction is needed since the installer runs in passive mode (progress bar only). The .bat file itself does not require administrator privileges — only the MSI installer needs UAC approval. For corporate environments where users do not have local admin rights, IT should pre-install WinFsp before distributing the setup package (see FAQ below).

Step 2: Cloud Storage Authentication

- The .bat file runs: `rclone.exe config create [remotename] [provider] [parameters]`

- **For OAuth providers (Google Drive, Dropbox):** rclone opens the user's default browser to the provider's standard OAuth consent page. The user signs in and grants permission. rclone receives an OAuth token via a temporary local HTTP listener on localhost. No credentials pass through daDetective or any third party.
- **For key-based providers (S3, Wasabi, B2):** The .bat file prompts the user to paste their access key, secret key, and region (or key ID and application key for B2). These are passed directly to `rclone config create`.
- The resulting configuration is saved to `%APPDATA%\rclone\rclone.conf`.

Step 3: Drive Mounting + Desktop Copy

- The .bat file copies the Mount .bat file to the user's Desktop using a plain `copy` command (not a shortcut). Each Mount .bat uses a provider-specific hardcoded path (e.g., `set "DADETECTIVE=%USERPROFILE%\Documents\daDetective Google"` for Google Drive, `daDetective Dropbox` for Dropbox, etc.) to locate rclone.exe, so it works correctly when run from the Desktop. It also includes a safety check at the top: `if not exist "%DADETECTIVE%\rclone.exe"` — which displays a clear error message if the provider-specific folder is not found in Documents, telling the user to extract the zip first.
- The .bat file then runs: `rclone.exe mount [remotename]: [driveletter]: --vfs-cache-mode full`
- This creates a virtual drive letter in Windows Explorer. The rclone process runs in the foreground in the command window. When the user closes the window, the drive unmounts. No background process remains.

Data Flow

All data flows directly between the user's machine and their cloud storage provider. daDetective is never in the data path for cloud storage access.

User's Browser

→

Windows File API

→

WinFsp Driver

→

rclone.exe

→

Cloud Provider API (HTTPS)

Key Points

- **daDetective never touches the cloud credentials.** OAuth tokens and access keys are stored only on the user's local machine.
- **daDetective never acts as a proxy.** File data flows directly from the cloud provider to the user's machine, then from the user's browser to daDetective via the standard upload.
- **All cloud provider connections use HTTPS (TLS encrypted).**

Network Requirements

Outbound HTTPS (port 443) to the relevant cloud provider:

Provider	Required Outbound Endpoints
Google Drive	`accounts.google.com`, `www.googleapis.com`, `oauth2.googleapis.com`
Dropbox	`www.dropbox.com`, `api.dropboxapi.com`
Amazon S3	`s3.[region].amazonaws.com`
Wasabi	`s3.[region].wasabisys.com`
Backblaze B2	`api.backblazeb2.com`

Additionally, outbound HTTPS to daDetective is required for the file upload itself.

> **Localhost Listener**
>
> rclone uses a temporary local listener on `127.0.0.1` during OAuth authentication. This does NOT require any firewall changes for inbound traffic. No inbound ports need to be opened.

Security Considerations

Credentials Storage

OAuth tokens (Google, Dropbox) and access keys (S3, Wasabi, B2) are stored in `%APPDATA%\rclone\rclone.conf` in plain text. This file is protected by standard Windows user permissions (only the logged-in user can read it).

For environments requiring additional protection, rclone supports encrypting the config file with a password. This is not enabled in the default daDetective setup for simplicity but can be configured by IT.

No Persistent Services

- rclone does not install any Windows services or scheduled tasks.

- The mount is active only while the command window is open. Closing the window unmounts the drive and terminates the process.
- Nothing runs at startup or login unless the user manually adds the Mount .bat to their startup folder.

File Access Scope

Provider Type	Scope	Restriction Options
Google Drive / Dropbox	OAuth token grants access to the user's entire drive ("drive" scope for Google, full access for Dropbox)	Token can be revoked at any time through the user's Google/Dropbox account settings
S3 / Wasabi / B2	Access scope depends on the IAM permissions attached to the access key	IT can restrict the key to read-only access on specific buckets

.bat File Contents

- The .bat files contain no obfuscated code, no encoded strings, and no network calls other than rclone commands.
- IT teams are encouraged to open the .bat files in Notepad and review them before deployment. They are plain text and fully readable.

Software Integrity

- rclone releases include SHA256 checksums on the official download page (https://rclone.org/downloads/).
- WinFsp releases are available on GitHub with checksums (https://github.com/winfsp/winfsp/releases).
- daDetective packages these unmodified binaries for convenience. IT teams can verify integrity by comparing checksums against the official releases.

Files Installed / Created

File or Location	Type	Purpose
`%USERPROFILE%\Documents\daDetective [Provider]\rclone.exe`	Portable executable	Cloud storage CLI tool
`%USERPROFILE%\Documents\daDetective [Provider]\winfsp*.msi`	MSI installer	WinFsp driver installer
`%USERPROFILE%\Documents\daDetective [Provider]\Setup [Provider].bat`	Batch file	One-time setup: installs WinFsp, authenticates cloud provider, copies Mount .bat to Desktop, mounts drive
`%USERPROFILE%\Documents\daDetective [Provider]\Mount [Provider].bat`	Batch file	Remounts cloud drive on demand. Includes a safety check for the provider-specific folder and uses a hardcoded path (e.g., `%USERPROFILE%\Documents\daDetective Google\` for Google Drive, `daDetective Dropbox\` for Dropbox, etc.)
`%USERPROFILE%\Desktop\Mount [Provider].bat`	Batch file (.bat copy)	Direct copy of the Mount .bat placed on the Desktop for convenient access (not a shortcut). Uses a provider-specific hardcoded path (e.g., `set "DADETECTIVE=%USERPROFILE%\Documents\daDetective Google"`) to locate rclone.exe. Includes a safety check (`if not exist "%DADETECTIVE%\rclone.exe"`) that displays an error if the provider-specific folder is missing.
`%APPDATA%\rclone\rclone.conf`	Config file	Cloud provider credentials and remote definitions

File or Location	Type	Purpose
`%ProgramFiles%\WinFsp\`	Installed program	WinFsp kernel driver and DLLs

Uninstallation

To completely remove all daDetective cloud storage components:

3. Delete the provider-specific folder from Documents (e.g., `%USERPROFILE%\Documents\daDetective Google`, `daDetective Dropbox`, `daDetective Amazon S3`, `daDetective Wasabi`, or `daDetective Backblaze B2`).
4. Delete the Mount .bat file from the user's Desktop.
5. Delete `%APPDATA%\rclone\rclone.conf` (removes stored credentials).
6. Uninstall WinFsp via **Windows Settings → Apps → WinFsp** (optional — only if no other applications use it).

No registry entries, startup items, or services to clean up.

Frequently Asked Questions

Can we restrict which files or folders users can access?

For S3, Wasabi, and B2: Yes. Create an IAM policy that limits the access key to specific buckets or prefixes with read-only permissions. For Google Drive and Dropbox: The OAuth scope grants access to the user's full drive. You cannot restrict it to specific folders via rclone configuration, but users only see their own files.

Does this work behind a corporate proxy?

Yes. rclone respects the standard `HTTP_PROXY` and `HTTPS_PROXY` environment variables. Set these on the user's machine if needed.

Can we deploy this via GPO or SCCM?

Yes. The zip contents can be extracted to any user-accessible folder on each machine (no admin rights required for the extraction location). WinFsp can be installed silently via: `msiexec /i winfsp*.msi /quiet /norestart`. The `rclone config create` command can be scripted with pre-provisioned credentials. Contact support@dadetective.com for enterprise deployment guidance.

Is there a Mac version?

The zip packages are Windows-only. Mac users install rclone via Homebrew and macFUSE separately. Instructions are available on request.

What happens if the user's OAuth token expires?

Google OAuth tokens auto-refresh. Dropbox tokens are long-lived. If a token becomes invalid, the user re-runs the Setup .bat file to re-authenticate. Existing configuration is overwritten with the new token.

Does rclone cache files locally?

With `--vfs-cache-mode full` (the default in the Mount .bat), rclone caches files temporarily in the user's temp directory during active use. Cached files are removed when the mount is closed. The cache location can be changed with `--cache-dir` if needed.

What if users don’t have local admin rights?

WinFsp is the only component that requires administrator approval. IT can pre-install WinFsp silently across machines using: `msiexec /i winfsp*.msi /quiet /norestart`. Once WinFsp is installed, the Setup .bat file detects it automatically and skips Step 1. Users then complete Steps 2 and 3 (cloud authentication and mounting) without any admin privileges. The rclone executable is portable and does not require installation.
