SFTP Drive V2

- Website
- Support

Version 2.0 [Build 7447]

Welcome to SFTP Drive, a powerful solution for accessing remote resources as if they were local drives, eliminating the need to download and upload files you need to access and work with. Once installed, you can create a new drive, enter your server information, and click the "Start" button to start browsing the file system from your favorite file management utility or the command line. Choose from three authentication types: Password, Key-based, or both. A wide variety of key-based authentication options are supported including full support for all standard file formats (PPK, PEM, etc), Pageant, and any physical Security Key which supports PKCS11 (for instance Yubikey).

SFTP Drive is completely free for personal non-commercial use. SFTP Drive may only be re-distributed with an agreement from /n software. Contact us to receive a quote.

Features:

- Work with a remote file system as if it were a local disk drive.
- Support for multiple drive configurations.
- Run as a Windows service or a desktop application.
- Upload and download files via your favorite file manager, such as Windows Explorer.
- Supports all common directory and file operations such as move, copy, and rename.
- Support for all common authentication types including password, key-based, and multi-factor.

You will always find SFTP Drive and any updates to the product at our web site - www.nsoftware.com. You may download trial versions of our product for a free 30 day evaluation period.

Please direct all your technical questions to support@nsoftware.com. You will speed up a response to your question if you provide an accurate description of your problem, the results you expected and the results you received when using our product. For all other inquiries, please direct your questions to sales@nsoftware.com.

Running SFTP Drive

SFTP Drive can be started directly from the application's main window, via command line, or configured to run as a Windows service.

The application will mount each of the enabled drives when the *Start* button is pressed. After the drives are successfully mounted, processes may interact with the files on the mounted drive just like any other drive on the system. Drives may be managed from the *Drives* tab (see Drive Management for more information).

Application

The first step in mounting a remote server with SFTP Drive is to create a new drive. Click the *New...* button in the Drives tab and configure the drive to add it to the drive list (See Drive Configuration for more information).

In the top left of the application window click the *Start* button to mount the enabled drives. Alternatively, right click the System Tray icon and select *Start*.

Once running, the options to *Stop* or *Restart* the application are enabled. Unmount all drives by clicking the *Stop* button. The buttons in the main application window or the context menu in the System Tray may be used to manage the application.

Starting as a Windows Service

The application may also be configured to run as a Windows service. When configured to run as a Windows service no user interaction is required to start the application.

To enable running as a Windows service navigate to the *Service* tab of the application and check the *Run as a Windows Service* checkbox. Click *Save Changes* to save the changes.

When enabled, the Windows service will be configured with a startup type of automatic. The user interface does not need to remain open when running as a Windows service.

Command Line Parameters

The application may also be controlled via the command line. The command line values allow management of the application from unattended configurations such as scripts. The following command line parameters are available:

/start	Starts the application and connects all enabled drives
/start uimin	Starts the application minimized and connects all enabled drives
/stop	Disconnects all drives and then exits the application
/servicestart	Starts the SFTP Drive service
/servicestop	Stops the SFTP Drive service
/isolated	Launches SFTP Drive in Isolated Mode
/registerservice	Registers the SFTP Drive service with Windows
/unregisterservice	Unregisters the SFTP Drive service with Windows

Drive Management

The *Start* and *Stop* buttons provide the basic functionality of SFTP Drive. Enabled drives are mounted when *Start* is pressed and all drives are unmounted when *Stop* is pressed. *Start* and *Stop* buttons can also be found in the system tray. The *Restart* button unmounts and subsequently mounts the enabled drives.

Press the *Exit* button to unmount any connected drives and stop the application. When running as a Windows Service, the *Exit* button will exit the graphical application and leave the service running. The service can be stopped from the application interface by clicking the *Stop* button or stopped manually in the Windows Service Manager.

The *Drives* tab is the control center for the application. Once a drive is configured it is added to the drive list. Select a drive from the drive list and click the control buttons on the right panel to change it or open it. Alternatively, right-click a particular drive and manage it from the context menu.

Working with Drives

- The *Enable* button designates a drive to be mounted when the *Start* button is pressed or the service is started.

- The *Edit...* button opens the Drive Configuration window.
- The *Delete* button permanently removes the drive from the drive list.
- The *Open* button opens an instance of Windows Explorer at the drive's mount point.

Configuration details about each drive are included in drive list. Click on the column headers to sort the drives by the respective category.

Drive Configuration

The drive configuration window is used to configure new drives and edit existing drives. It can be accessed by clicking the *New...* button in the Drives tab or clicking the *Edit...* button when a drive is selected in the drive list. Drive-specific configuration for example, the connection settings, the drive name, the drive selection settings, and the startup behavior are specified in this window (additional configuration can be specified in the Advanced tab).

Please be aware that configuration changes will not take effect until you click the *Save Changes* button in the SFTP Drive toolbar, which will save the settings to the Windows registry.

Adding a Drive

- To add a drive, click the *New...* button on the Drives tab of the main window.
- Enter a name for the drive in the *Drive name* field, and if needed, choose the desired drive letter. This will be the drive letter where the remote file system will be mounted.
- Enter your server's address and port in the *Remote host* and *Remote port* fields.
- Enter your username in the *Username:* field.
- Use the *Authentication Type* drop-down menu to choose the type of authentication and provide the corresponding credentials (see Authentication for more information).
- The *Remote Folder* section provides additional options to use when connecting to the remote file system.
    - *Root folder on server* specifies which folder on the SFTP server should be treated as the root of the local drive when mounted.
    - *Read-only mode* tells the application whether to mount the drive in read-only mode.
    - *Open Remote Folder On Connect* specifies which folder to open in Explorer when the drive is mounted (if any). If set, each time the drive is connected an Explorer window will open at the specified path. Uncheck this box to disable this functionality.
- The *Test SSH Connection* button will verify the connection to the SFTP server can be successfully established. When configuration is complete press *OK* to complete the drive configuration.

After clicking *OK* the drive will be added to the drive list . Use the Advanced Settings to set additional configuration settings at the drive level and at the global level.

Authentication

Select the SSH authentication protocol by choosing an option from the *Authentication Type* dropdown in the Drive Configuration window. This setting can also be managed in the registry (see the *AuthType* value in the Advanced Settings for more information). When a particular method is selected the corresponding credentials can be specified in the configuration window.

Once you have entered your credentials click *Test SSH Connection* and if authentication is successful, the *Host Key Fingerprint* field will be populated with a SHA-256 fingerprint of the server's public key.

Supported Authentication Methods

- *Password*
- *Public Key*
- *Keyboard-Interactive*
- *Multi-factor*
- *Public Key (Pageant)*
- *Public Key (Security key)*

Password Authentication

Selecting this authentication method instructs SFTP Drive to attempt to authenticate to the server using a username and password combination. If authentication fails, SFTP Drive will automatically fall back to Keyboard-Interactive mode.

Public Key Authentication

Selecting this option instructs SFTP Drive to attempt to authenticate to the server via the standard public key authentication mechanism supported by the SSH protocol. The user must set the location and format of the private key as well as a username to be able to authenticate.

Keyboard-Interactive Authentication

Selecting this authentication method instructs SFTP Drive to authenticate in a challenge-response cycle, displaying a response dialog for each prompt. Password prompts are automatically processed using the value entered in the password field in the Edit Drive dialog.

Multi-factor Authentication

Multi-factor authentication enables multiple forms of authentication. Typically servers will require a combination of password and public key authentication. Additional factors of authentication are also supported by specifying the appropriate credentials.

Public Key (Pageant)

Selecting this authentication method instructs SFTP Drive to communicate with PuTTY's ssh-agent "Pageant" over shared memory and perform public key authentication.

Note: Ensure SFTP Drive and Pageant are running with the same level of permission use this method of authentication.

Public Key (Security Key)

Selecting this authentication method instructs SFTP Drive to interact with a physical security key which will be used to authenticate to the server via the standard public key authentication mechanism. The user must load the PKCS #11 library that will allow SFTP Drive to interact with the security key.

Advanced

The *Advanced* tab of the drive settings dialog provides access additional settings which are not commonly used.

Allow all users access to the drive

This option controls whether drives are visible to other users on the system. When checked (default), drives are accessible by all users on the system. When unchecked, the drive is only accessible by the account under which SFTP Drive is running. Note: this setting should not be disabled when running as a Windows Service. When running as a Windows Service with sharing disabled only the identity of the Windows Service itself will be able to access the drive (typically the Network Service identity). For more information see Shared Drives.

Handle case-sensitive filenames

This option controls whether SFTP Drive should treat file requests as case-sensitive (treating uppercase and lowercase letters as being different). This is only applicable if your server's filesystem is case-sensitive. To use this setting you must disable case-insensitivity in Windows by creating a value in the *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel* registry key. The value should be called *obcaseinsensitive* (DWORD) with a value of 0. Most Windows applications are not prepared to handle filenames in a case-sensitive manner so using case-insensitive apps may result in unexpected behavior. This setting only helps with unix-related apps.

Additional Configuration

The *Settings* tab of the defines application-wide settings. Settings such as log settings, reconnection logic, etc. are controlled here.

Advanced settings are available through the Windows Registry which allow setting infrequently used values.

Settings

The *Settings* tab is used to configure application-wide settings. Please note that configuration changes will not take effect until you click the *Save Changes* button in the SFTP Drive toolbar. Options specific to Drives are configured via the Drives tab.

Logging Options

These options can be used to configure SFTP Drive's logging features.

- *Write Log to a File* checkbox defines whether logs are written to a file. By default logs are not written to a file and are only available in the *Service* tab.
- *Log Mode* defines the verbosity of the logs generated by the application. The following Log Mode values are supported:
  - *Off* - Nothing will be logged.
  - *Error* - Only errors in SFTP Drive's operation will be logged.
  - *Warning* - Additional warning information will be logged.
  - *Info* - General information about the status of the connection will be logged.
  - *Verbose* - Logs additional information about the connection and individual SSH/SFTP packets being sent and received.
  - *Debug* - Logs detailed debug information, including the contents of the SSH/SFTP packets.
- Log Rotation is available when logging to a file. The logs may be rotated after a specified number of days, and the application can also be configured to automatically delete log files older than a specified number of days. When a log is rotated the existing log file will be renamed to include the last date for which the log applies. For instance *sftpdrive.log* may be renamed to *sftpdrive-2020-07-15.log*. The date portion of the rotated log name is in the format *yyyy-MM-dd*.

Connection Settings

The settings in this section allow granular control over the SSH connection settings. In most cases the settings specified here should not be adjusted. The default settings enable automatic reconnection in the case where the connection is dropped. The connection is also kept alive by sending a keep-alive packet at regular intervals during periods of inactivity.

The *Use Compression* setting enables compression to be used on the SSH connection if the server supports it.

Proxy Settings

If a proxy is required to be used when connecting to the SFTP server the proxy connection details may be specified here. The application supports the following type of proxies:

- Tunnel (most common)
- SOCKS4
- SOCKS5

Specify the *Proxy Type*, *Address*, *Port*, and if applicable the *Username* and *Password*.

Advanced Settings

Advanced options for SFTP Drive are stored in the Windows registry in *HKEY_LOCAL_MACHINE\SOFTWARE\nsoftware\SFTPDrive\2*. This registry key holds settings that are available for SFTP Drive globally. Sub-keys at this path hold settings for individual drives, and trusted SSH host keys.

The following keys hold configuration information:

Registry Key	Applicable Settings
HKEY_LOCAL_MACHINE\SOFTWARE\nsoftware\SFTPDrive\2	Global settings for the application.
HKEY_LOCAL_MACHINE\SOFTWARE\nsoftware\SFTPDrive\2\Drives	Drives hold drive specific settings.
HKEY_LOCAL_MACHINE\SOFTWARE\nsoftware\SFTPDrive\2\TrustedSSHHostKeys	Trusted SSH Host Keys stores trusted host keys.

The following values can be configured within the root *HKEY_LOCAL_MACHINE\SOFTWARE\nsoftware\SFTPDrive\2* registry key:

Name	Type	Description
DeleteLogDays	DWORD	Specifies the number of days that log files will remain before being deleted. Only applies if *RotateLogDays* is greater than 0. If set to 0, old logs will not be deleted.
KeepAliveInterval	DWORD	Determines how often a keep alive packet is sent to the server, in seconds. If set to 0, no keep alive packets will be sent.
LogFile	String	Contains the path to the log file.
LocalHost	String	Specifies the local IP address of the network interface to use when connecting. This settings is typically only useful in machines with multiple network interfaces.
LogMode	DWORD	Determines the level of logging: • 0 - Off. Nothing will be logged. • 1 - Error. Only errors in SFTP Drive's operation will be logged. • 2 - Warning. Additional warning information will be logged. • 3 - Info. General information about the status of the connection will be logged. • 4 - Verbose. Logs additional information about the connection and individual SSH/SFTP packets being sent and received. • 5 - Debug. Logs detailed debug information, including the contents of the SSH/SFTP packets.

LogPackets	DWORD	Determines whether or not the contents of SFTP Packets will be written to the log. Note that the additional output from this mode will slow operation considerably, so it is recommended that it only be enabled when necessary to diagnose an issue. • 0 - SFTP packet contents will not be logged (default) • 1 - SFTP packet contents will be written to the log.
LogPort	DWORD	The SysLog port that will be used to communicate between the service and the UI when SFTP Drive is running as a service.
LogToFile	DWORD	Determines whether or not the log will be written to a file. The file itself is specified by *LogFile*. • 0 - The log will only be written to the Log window on the Service tab. (default) • 1 - The log will also be saved to a file.
MaskSensitive	DWORD	Determines whether or not passwords will be masked in the log. • 0 - Passwords will be visible in the log. • 1 - Passwords will be replaced with '*' characters in the log. (default)
MaxLogLines	DWORD	Determines the maximum number of lines that will be stored in the Log window in the Service tab.
MountTimeout	DWORD	Determines how long (in seconds) SFTP Drive will wait for Windows to mount a drive without reporting an error. The default is 20 seconds when this value is not present in the registry.
PasswordEncryptionMethod	String	Determines how passwords are encrypted for storage. The default value is *Auto*. Possible values are: • *Auto* (default) - Microsoft DPAPI is used to encrypt passwords. When running the application as a user (not as a Windows service) the password are encrypted and can only be decrypted by the current user. When running as a Windows service the passwords are encrypted for the machine and can be decrypted by any user on the machine. When running as a Windows service the user application and the service run under different accounts and must both be able to decrypt the values stored in the registry. Additional values are reserved for future use.
PromptForRegPermissions	DWORD	Determines if SFTP Drive will ask for registry permissions if it does not have them when it tries to write to the registry. • 0 - SFTP Drive will not ask for registry permissions, instead bringing up a UAC dialog for one-time access. • 1 - SFTP Drive will ask to be granted registry permissions. If granted, UAC access will not be required in the future. (default)
ProxyChecked	DWORD	Specifies whether or not the proxy settings are enabled.
ProxyHost	String	Specifies the host that SFTP Drive will use to connect to the proxy.
ProxyPassword	String	Specifies the password that SFTP Drive will use to connect to the proxy.
ProxyPort	DWORD	Specifies the port that SFTP Drive will use to connect to the proxy.
ProxyType	DWORD	Specifies the type of proxy that SFTP Drive will connect to. • 0 - None (default) • 1 - Tunnel • 2 - SOCKS4

- 3 - SOCKS5

ProxyUsername	String	Specifies the username that SFTP Drive will use to connect to the proxy.
ReconnectAttempts	DWORD	Specifies the number of times SFTP Drive will attempt to reconnect if the connection to the server is lost.
ReconnectInterval	DWORD	Specifies the time (in seconds) between attempting another reconnection to the server. Default is 5 seconds.
RotateLogDays	DWORD	Specifies how many days SFTP Drive will use a log file before rotating to a new log file. If set to 0, the log file will never rotate.
RunAsService	DWORD	Determines whether or not SFTP Drive will run as a service.
ShowDotFiles	DWORD	Determines whether files that start with a dot or period (.) are displayed.
Timeout	DWORD	Determines how many seconds SFTP Drive will wait for a response from the server before ending the connection.
UseCache	DWORD	Specifies whether or not SFTP Drive will use caching for file metadata and contents. Disabling will slow performance, and will cause SFTP Drive to re-download a file every time it is requested by Windows. • 0 - No cache • 1 - Use caching (default)
UseCompression	DWORD	Determines whether or not the SSH connection will use zlib compression. • 0 - No compression (default) • 1 - Use zlib compression

Drives

The following values can be configured independently for each drive, at *HKEY_LOCAL_MACHINE\SOFTWARE\nsoftware\SFTPDrive\2\Drives\{Drive Name}*:

Name	Type	Description
AuthType	DWORD	Determines the type of authentication used to connect to the server: • 0 - Password • 1 - Public key • 2 - Keyboard-interactive • 3 - Password + public key
CertStore	String	The name of the certificate store for the client certificate
CertStoreType	DWORD	The type of certificate store for this certificate • 0 - User • 1 - Machine • 2 - PFX File • 3 - PFX Blob • 4 - JKS File • 5 - JKS File • 6 - PEM Key File

- 7 - PEM Key File
- 8 - Public Key File
- 9 - Public Key File
- 10 - SSH Public Key Blob
- 11 - P7B File
- 12 - P7B Blob
- 13 - SSH Public Key File
- 14 - PPK File
- 15 - PPK Blob
- 16 - XML File
- 17 - XML Blob
- 18 - JWK File
- 19 - JWK Blob
- 20 - Security Key

CertStorePassword	String	If the certificate store is of a type that requires a password, this registry setting is used to specify that password in order to open the certificate store.
CertSubject	String	The subject of the certificate used for client authentication. The certificate subject is a comma separated list of distinguished name properties and values. For instance "CN=www.server.com, OU=test, C=US, E=support@nsoftware.com".
DriveLetter	String	Contains the drive letter where the drive will be mounted (e.g. "Z:").
DriveName	String	Contains the name that will be displayed for the drive.
DriveType	DWORD	Determines the type of drive that will be mounted: • 0 - Network Drive (default) • 1 - Local Disk • 2 - Removable Disk
Enabled	DWORD	Determines whether or not the drive will be mounted when SFTP Drive is started. • 0 - Disabled • 1 - Enabled
Host	String	Contains the remote host that SFTP Drive will connect to.
Index	DWORD	The position of the drive in the list of drives.
OpenRemoteFolder	DWORD	Determines whether or not SFTP Drive will automatically open a folder after mounting the drive. • 0 - Disabled • 1 - Enabled
OpenSpecifiedFolder	String	Contains the folder that SFTP Drive will open if OpenRemoteFolder is enabled.
Password	String	Contains the password for the SFTP server.
Port	DWORD	Contains the port on the remote host that SFTP Drive will connect to.
QueryAvailableSpace	DWORD	Whether to query the remote server for available space when connecting. Possible values are:

		• 0 - Disabled • 1 - Enabled (default)
ReadOnly	DWORD	Determines whether or not SFTP Drive will mount the drive in read-only mode. • 0 - Disabled (default) • 1 - Enabled
RemoteRoot	String	Contains the folder on the server that SFTP Drive will use as the root of the mounted drive.
RemoteRootType	DWORD	Determines how the drive decides what folder to use as the root of the drive. • 0 - Server Root (/) • 1 - User's home folder (/home) • 2 - Specified folder (use RemoteRoot)
SecurityKeyAccount	String	An opaque token holding information about the certificate selected from the security key. This value is created by the application and should not be set manually.
SecurityKeyName	String	A friendly name of the chosen key. This is populated after selecting a key. For instance "PIV AUTH pubkey"
SecurityKeyPIN	String	The encrypted PIN of the security key.
SecurityKeyPKCS11LibPath	String	The path to the library which implements the PKCS11 interface. This may be provided by the security key vendor, or may be an alternative implementation like OpenSC. For instance "C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll"
SecurityKeySavePIN	DWORD	Whether to save the PIN. If saved, the PIN is encrypted.
Shared	DWORD	Determines whether or not other users can access the mounted drive. • 0 - Private • 1 - Shared (default)
SignedSSHCert	String	The CA signed client public key used when authenticating. When authenticating via public key authentication this setting may be set to the CA signed client's public key. This is useful when the server has been configured to trust client keys signed by a particular CA. For instance: *SignedSSHCert=ssh-rsa-cert-v01@openssh.com AAAAB3NzaC1yc2EAAAADAQABAAAB...")* The algorithm such as *ssh-rsa-cert-v01@openssh.com* in the above string is used as part of the authentication process. To use a different algorithm simply change this value. For instance all of the following are acceptable with the same signed public key: • *ssh-rsa-cert-v01@openssh.com AAAAB3NzaC1yc2EAAAADAQABAAAB...* • *rsa-sha2-256-cert-v01@openssh.com AAAAB3NzaC1yc2EAAAADAQABAAAB...* • *rsa-sha2-512-cert-v01@openssh.com AAAAB3NzaC1yc2EAAAADAQABAAAB...*
UseIPv6	String	If "False", the drive will use IPv4 to connect. If "True", the drive will use IPv6.
Username	String	Contains the username for the SFTP server.

Trusted SSH Host Keys

The product maintains a list of trusted SSH host keys. When connecting to a new SSH host a prompt is displayed to the user asking whether to accept or reject the host key. If the host key is accepted the key and IP address of the host are stored in the list here.

Any time a connection is made to an SSH host the server's host key is checked against the list of trusted keys defined in this section.

The host keys are stored under *HKEY_LOCAL_MACHINE\SOFTWARE\nsoftware\SFTPDrive\2\TrustedSSHHostKeys*. Entries at this location will hold a string value for each host in the format *[host]:[port]*, and the value being the fingerprint of the server.

Shared Drives

SFTP Drive allows drives to be shared among all local users or only available to the current user. This is controlled by the "Allow all users access to the drive" setting found in the Advanced tab of the Drive Configuration window. It is also controlled by the *Shared* registry setting for a particular drive (see Drives for more information). When this setting is enabled, the drive is accessible to all local users on the machine. When disabled, the drive is only accessible by the account under which SFTP Drive is running.

When "Allow all users access to the drive" is turned on SFTP Drive creates a virtual drive accessible to all user sessions. The application maintains one "live" connection to the server per drive and all file system operations that occur produce SFTP commands over the connection. Any user that interacts with the drive inherits the credentials of the SFTP connection to work with files on the drive. Settings for the application and drives can be specified in a subkey of the *HKEY_LOCAL_MACHINE* hive to indicate the settings apply system-wide to any user interacting with the drive.

On the other hand, when "Allow all users access to the drive" is turned off the drive is only accessible in the current user session. Attempting to access the drive from another user session will cause Windows to throw a "Cannot find drive." error message. While default-shared behavior allows you to share a drive among all local users easily, it may be advantageous to have granular control over file access on the mounted drive (see Isolated Mode for more information).

Isolated Mode

SFTP Drive can be launched with a command line flag to indicate all settings should be completely separate for each local user account. The */isolated* flag controls this behavior (see Running SFTP Drive for usage examples). When this flag is specified the current user will appear to be interacting with a fresh installation of SFTP Drive. The user's list of drives and application settings will persist across logons.

This flag will tell SFTP Drive to read application configuration and drive configuration from the *HKEY_CURRENT_USER* hive instead of the *HKEY_LOCAL_MACHINE* hive. When this flag is specified and a new instance is created, it is called an "isolated instance" or "HKCU instance". When a new instance is created without this flag it is called a "global instance" or "HKLM instance".

The default values of configuration settings are the same regardless of whether you are running an HKCU or HKLM instance. For example, drives are shared among all local users by default. It is a common pitfall to think an isolated instance will only create drives that are private - but that is not the case. To create a private drive in isolated mode turn off the "Allow all users access to the drive" setting as discussed in Shared Drives. Below is a table to illustrate the interaction between shared drives and isolated mode.

Launch mode	Shared setting	Description
Isolated	Enabled	Configuration is per-user and drives are accessible to everyone.
Isolated	Disabled	Configuration is per-user and drives are only accessible in the current user's session.
Normal	Enabled	Configuration is system-wide and drives are accessible to everyone.
Normal	Disabled	Configuration is system-wide but drives are only accessible in the current user's session.

Isolated mode is useful in environments where each user needs to mount a drive with their own credentials. Drives can be configured and started manually by each end-user or via an automated logon script. This allows many isolated instances to be running at the same time but *only one global instance can ever be running at a time*. One important note: running as a Windows Service is not possible in an isolated instance.

Troubleshooting

If you are having problems with SFTP Drive, our support team is here to help. Visit https://www.nsoftware.com/support/submit.aspx to submit a ticket. Please be as detailed as possible about your issue. It is also helpful if you generate and send a log file to support@nsoftware.com.

How to Generate a Log File

1. Navigate to the *Settings* tab.
2. Enable *Write Log to a File* and specify a local file.
3. Increase the *Log Mode*.
4. Click the *Save Changes* button.
5. Reproduce the issue.
6. Click the *Stop* button.

Note that the length of time it takes for any operation is increased when *Debug* logging in enabled. Additional logging of SSH packet communication is available through the *LogPackets* configuration setting in the Advanced Settings. The amount of data logged with these options enabled is substantial. We recommend enabling these settings for debugging purposes only.

Common Issues

Below you will find a list of common issues reported by our customers that you may find useful in troubleshooting a problem.

SFTP Drive fails to connect to a TLS-enabled FTP server

The drives mounted by SFTP Drive V2 work exclusively with SFTP servers. TLS-enabled FTP servers are not currently supported by the application.

SSH connection failed: Connection failed: No connection could be made because the target machine actively refused it.

A connection refused error indicates a TCP-reset flag was received when the connection was initiated. This can mean no process is listening on the specified port, the port is being blocked by a firewall, or the IP address is incorrect.

SSH connection failed: Timeout.

A timeout error is thrown when the remote host does not respond after the specified amount of time in the Settings tab. It could indicate a firewall, antivirus, or proxy is dropping the connection.

SSH connection failed: Could not bind to LocalAddress.

A bind error indicates the application was not able to bind to the default networking interface. This can happen if the machine has multiple networking interfaces. To resolve the issue, set the LocalHost value of the Advanced Settings to the IP address of your default network interface.

SFTP Drive V2 - Version 2.0 [Build 7447]