Mission Guide: SFTP Agentless Connection

Your Mission: Use F-Response to collect data from a remote Non-Windows computer using SFTP Agentless Connection.

Important Note

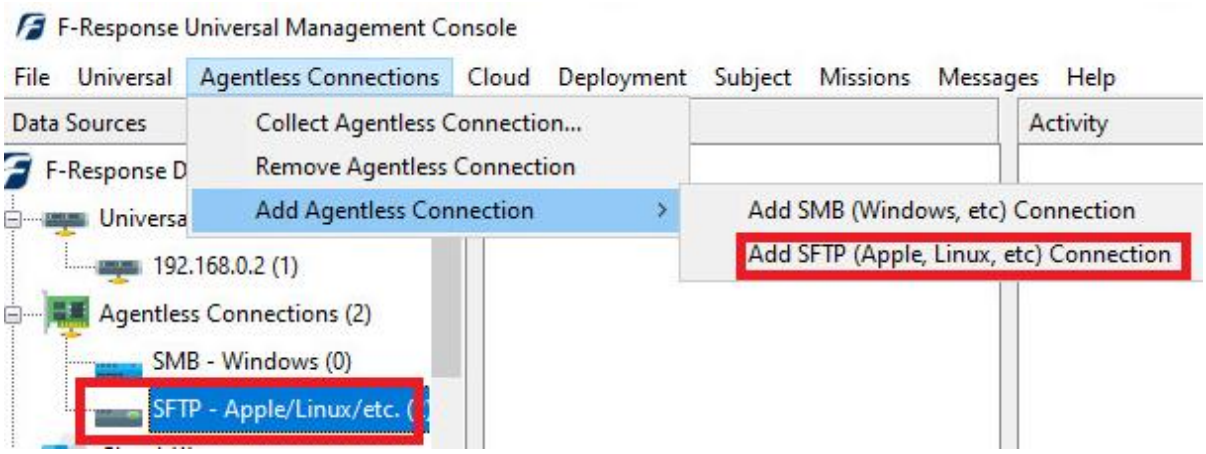
Regardless of credential levels used (Admin, Domain Admin), some system files may be locked by the OS and unavailable for collection using SFTP.

Drive mappings on remote Windows systems will not appear in the list of shares—you'll need to connect to the system where the share is hosted.

SFTP Agentless connection is a great option for collecting data from Non-Windows systems (Linux, Apple, Solaris, AIX, NAS devices, or any SFTP server that may not be accessible by other means. SFTP can be used to collect to a VHD or local directory while preserving file dates/times.

Step 1: Add the remote SFTP host

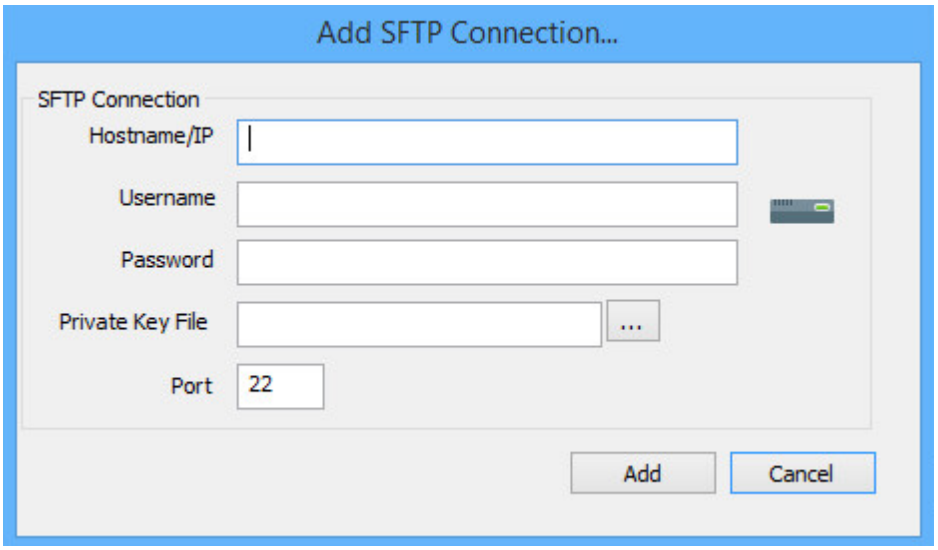
Open the F-Response Management Console and navigate to Agentless Connections->Add SFTP (Windows, etc) Connection, or double click on the appropriate icon in the Data Sources pane.



F-Response Management Console

Step 2: Enter the hostname and credentials

Next you'll need to enter the hostname or IP address of the remote system.



SFTP Connection Dialog

You will need the hostname or IP of the remote computer and sufficient credentials for access[1]. Click the **Add** button when complete and the hostname will appear in the **Items** column.

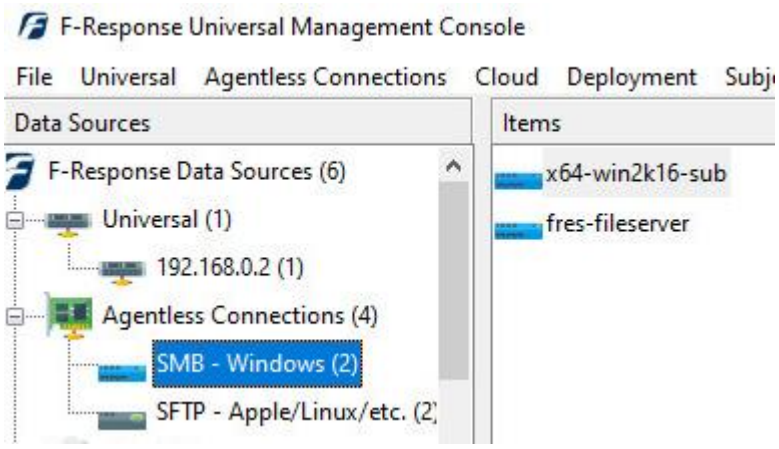
If a **Private Key File** is needed it can be added in this field, and the Port can be adjusted if the remote computer is not using the default port, TCP port 22. Click the **Add** button when complete and the hostname or IP will appear in the **Items** column.

Once you have the hostname or IP and credentials configured, click the Add button to add the host to the items column.

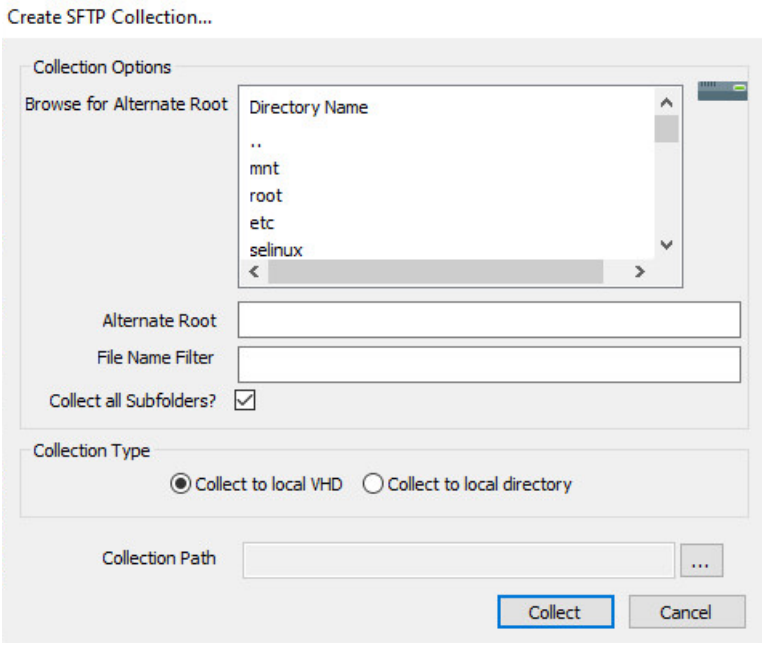
[1] Note: Regardless of credential levels used (root), some system files may be locked by the OS and unavailable for collection using SFTP.

Step 3a: Start a collection

Once the host has been added to the Items column a collection can be created. To open the **Create SFTP Collection…** window, highlight the hostname in the **Items** column and choose **Collect Agentless Collection…** from the **Agentless Connections** drop-down menu, or simply double click the hostname in the **Items** column.



Starting a new collection



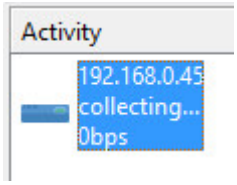
Under the **Collection Options** portion of the window, there are a few options available to adjust the scope of a collection. Browse through the **Directory Name** to locate a specific directory if needed. The directory chosen will populate the **Alternate Root** field below. The collection scope can be narrowed further by adding a **File Name** filter[2], such as "**pdf**" to collect only files with pdf in the filename.

[2] The filename filter simply compares the inputted text against the name of the file. For example, by inputting "pdf" both "this_is_not_a_pdf.txt" and "this_is_a_pdf.pdf" would be collected. To limit on file extension, simply add a period to the front. I.e. ".pdf"

You may choose to tighten the scope further by selecting or deselecting the **Collect all Subfolders?** option. Turning this off will mean only the content of the selected folder is collected, any subfolders will be ignored.

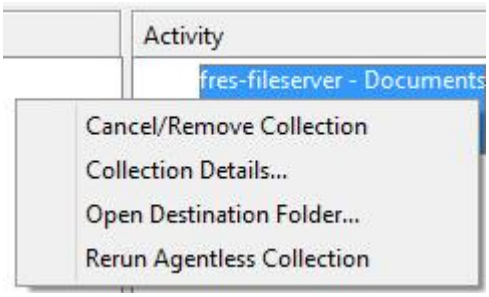
Lastly, select a **Collection Type** and choose a location to store the collected data under **Collection Path.**

Step 4: Check the Activity Pane



Active collection activity…

Completion will be noted in the activity window. You may right click on the collection for a list of options:



Collection Menu

Cancel/Remove Collection will cancel a running collection or remove a completed collection from the activity column. This action will not delete the collected data from the storage location.

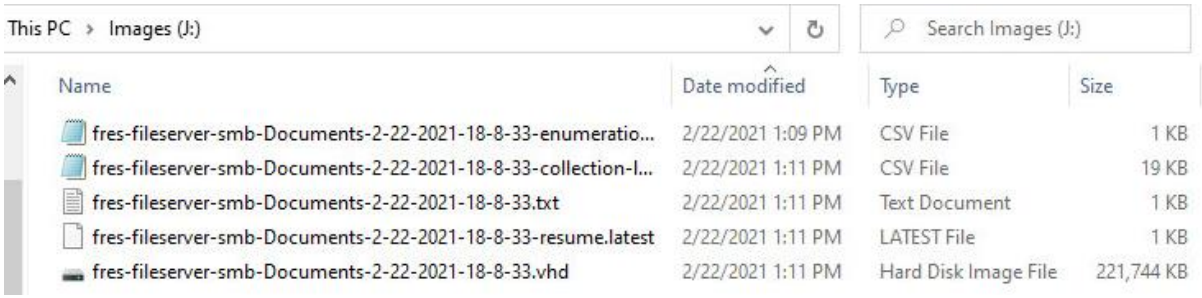
Collection Details… will provide a quick summary of the collection such as the number of files copied, current collection state, collection duration, etc.

Open Destination Folder… will open the location chosen to store the collection to review the data.

Rerun Agentless Collection If errors occurred for specific files during collection, this option will execute the collection again, focused only on the uncollected files. **This option is only available when collecting to a Local Directory.**

Step 5: Review the Completed Collection

Navigate to the destination folder at the completion of the collection to review the individual files collected, or the summary VHD, along with any log or error reports.



Collection details

Troubleshooting and FAQ

Below are some common errors you may encounter when using SFTP.

Can SFTP collections be configured to image to e01 format? No, not directly. You can collect the data to a directory then use your favorite imaging tool to collect that directory into an e01. Or collect to a VHD for an e01 alternative "forensic container".