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

Important Note

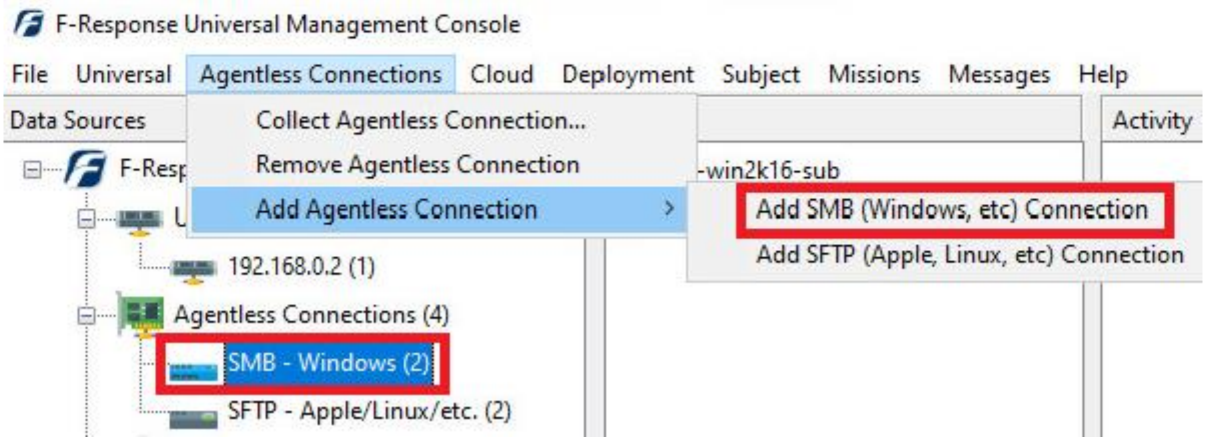
Regardless of credential levels used (Admin, Domain Admin), some system files may be locked by the OS and unavailable for collection using SMB.

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.

SMB Agentless connection is a great option for collecting data from remote shares, NAS devices, or any SMB server.

Step 1: Add the remote SMB host

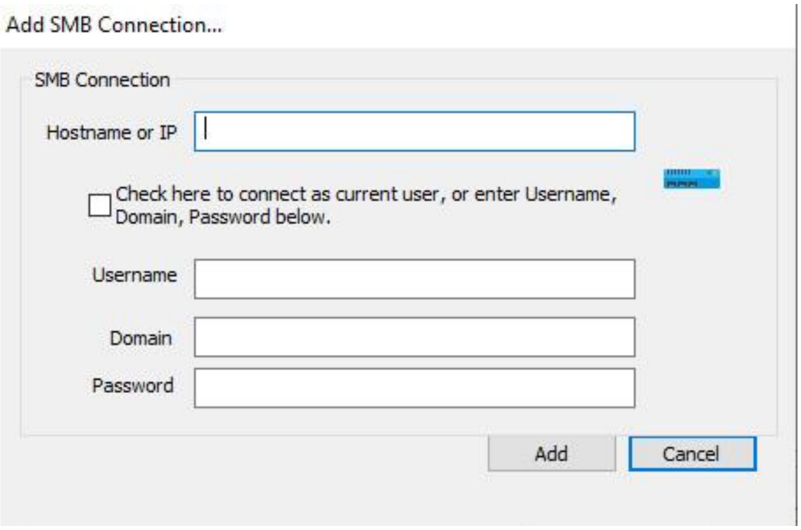
Open the F-Response Management Console and navigate to Agentless Connections->Add SMB (Windows, etc) Connection, or double click on the appropriate icon in the Data Sources pane.


F-Response Universal Management Console
File
Universal
Agentless Connections
Cloud
Deployment
Subject
Missions
Messages
Help
Data Sources
Activity
Collect Agentless Connection...
Remove Agentless Connection
Add Agentless Connection
Add SMB (Windows, etc) Connection
Add SFTP (Apple, Linux, etc) Connection
F-Resp
-win2k16-sub
192.168.0.2 (1)
Agentless Connections (4)
SMB - Windows (2)
SFTP - Apple/Linux/etc. (2)

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 Windows system.



□ Check here to connect as current user, or enter Username, Domain, Password below.

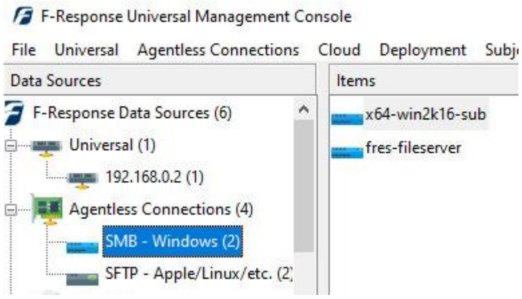
SMB Connection Dialog

You have two credential options. Either using the currently logged in user when attempting to perform the collection, or inputting a username, domain, and password value. If you use the currently logged in user, be sure to note that the software will not save your user information, and will instead execute any collection as the current management console user at the time.

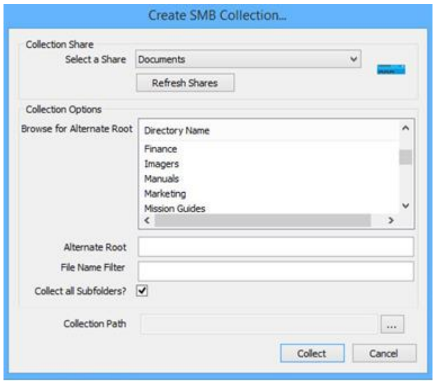
Once you have the hostname or IP and credentials configured, click the Add button to add the host to the items column.

Step 3: Start a collection

Once the host has been added to the Items column a collection can be created. To open the **Create SMB 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



Select a Share: Documents

Collect all Subfolders? ☑

First, select the share from the **Select a Share** dropdown box.

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.

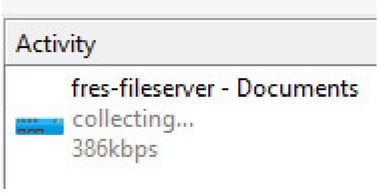
The collection scope can be narrowed further by adding a **File Name** filter[1], such as "**pdf**" to collect only files with pdf in the filename.

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, choose a location to store the collected data under **Collection Path.**

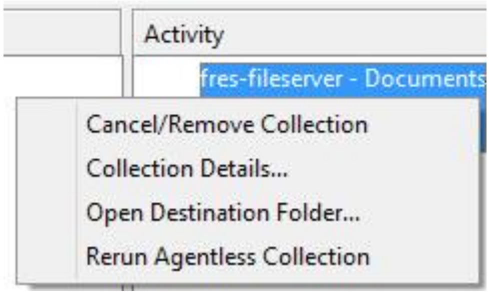
[1] The filename filter simply compares the inputted text against the name of the file. For example, by inputting "pdf" both "this_is_not_a_pdf.txt" and "this_is_a_pdf.pdf" would be collected. To limit on file extension, simply add a period to the front. I.e. ".pdf"

Step 4: Check the Activity Pane


Activity
fres-fileserver - Documents
collecting...
386kbps

Active collection activity…

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


Activity
fres-fileserver - Documents
Cancel/Remove Collection
Collection Details...
Open Destination Folder...
Rerun Agentless Collection

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.

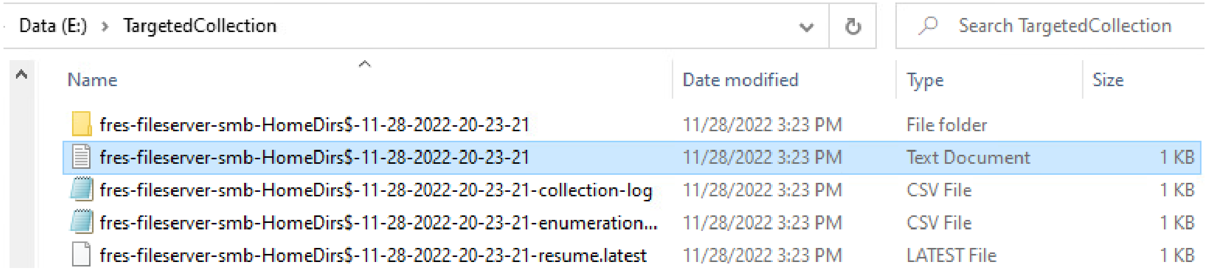
Collection Details… will provide a quick summary of the collection such as the number of files copied, current collection state, collection duration, etc.

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 along with any log or error reports.



Data (E:) > TargetedCollection

Search TargetedCollection

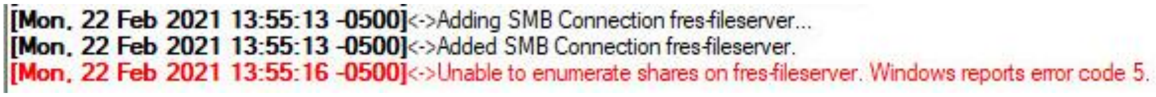
Name	Date modified	Type	Size
fres-fileserver-smb-HomeDirs$-11-28-2022-20-23-21	11/28/2022 3:23 PM	File folder	
fres-fileserver-smb-HomeDirs$-11-28-2022-20-23-21	11/28/2022 3:23 PM	Text Document	1 KB
fres-fileserver-smb-HomeDirs$-11-28-2022-20-23-21-collection-log	11/28/2022 3:23 PM	CSV File	1 KB
fres-fileserver-smb-HomeDirs$-11-28-2022-20-23-21-enumeration...	11/28/2022 3:23 PM	CSV File	1 KB
fres-fileserver-smb-HomeDirs$-11-28-2022-20-23-21-resume.latest	11/28/2022 3:23 PM	LATEST File	1 KB

Collection details

Troubleshooting

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

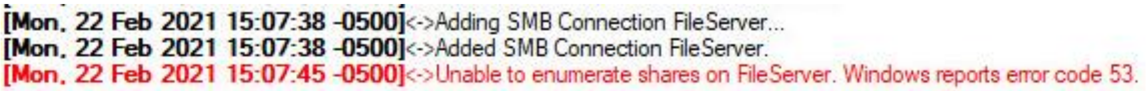
I add the host to the Items column, but when I try to open the Add SMB Connection window I receive an **error code 5**.



```
[Mon, 22 Feb 2021 13:55:13 -0500]<->Adding SMB Connection fres-fileserver...
[Mon, 22 Feb 2021 13:55:13 -0500]<->Added SMB Connection fres-fileserver.
[Mon, 22 Feb 2021 13:55:16 -0500]<->Unable to enumerate shares on fres-fileserver. Windows reports error code 5.
```

This is due to invalid credentials. There was an error or typo when the credentials were entered earlier, or the account used does not have sufficient permissions.

I add the host to the Items column, but when I try to open the Add SMB Connection window I receive an **error code 53**.



```
[Mon, 22 Feb 2021 15:07:38 -0500]<->Adding SMB Connection FileServer...
[Mon, 22 Feb 2021 15:07:38 -0500]<->Added SMB Connection FileServer.
[Mon, 22 Feb 2021 15:07:45 -0500]<->Unable to enumerate shares on FileServer. Windows reports error code 53.
```

This is due to a hostname that could not be resolved or an invalid IP address. Check to see the hostname or IP address was entered correctly.