

If it is necessary to use network resources as source / target of the files to be handled by the Common sFTP connector, in order to get the connector to work correctly, the following must be considered:

- The use of mapped network drives as source / target of the files **is not recommended**, because it requires much more complex actions. Network drives defined by a user in a Windows session (desktop) are local to the context of use. System services, such as the Common sFTP connector, run in their own security context, and therefore user-defined network drives are not available for them. It is possible to define drives, but it requires much more complex mechanisms than usual, and ensuring that the service's security context will have sufficient privileges to interact with the network share. Next, what is not recommended, we show a sequence of steps to enable units in the context of a service:

1. Starting with Windows Vista, Microsoft implemented the User Account Control feature, or just UAC. This feature is designed to improve the OS security. A side effect of this feature is that mapped network drives are inaccessible to programs running as administrator, i.e. if you start the app elevated, it won't see your mapped drives. This can be a major inconvenience especially if you run apps as admin regularly.

Check out this Microsoft documentation:

<https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/mapped-drives-not-available-from-elevated-command>

The Common sFTP connector Wizard is executed with admin privileges to be able to modify the configuration file and to perform post-install operations on the service in Windows.

If it is necessary, to enable access to mapped network drives from elevated apps, you need to merge **EnableLinkedConnections.reg** file into Windows Registry.

After this operation, you must restart the OS.

2. For this hack you will need **SysInternalsSuite**.
<https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>
3. Open an elevated **cmd.exe** prompt (Run as administrator).
4. Elevate again to root using "**PSEXec.exe**": Navigate to the folder containing **SysInternalsSuite** and execute the following command:

```
> psexec -i -s cmd.exe
```

you are now inside of a prompt that is "**nt authority\system**" and you can prove this by typing "**whoami**". The "**-i**" is needed because drive mappings need to interact with the user.

5. Create the persistent mapped drive as the SYSTEM account with the following command:

```
> net use z: \\servername\sharedfolder /persistent:yes
```

The newly created mapped drive will now appear for all users of this system but they will see it displayed as "Disconnected Network Drive (Z:)". It may claim to be disconnected but it will work for everyone.

WARNING: You can only remove this mapping the same way you created it, from the SYSTEM account. If you need to remove it, follow steps 3 and 4 but change the command on step 5 to:

```
> net use z: /delete
```

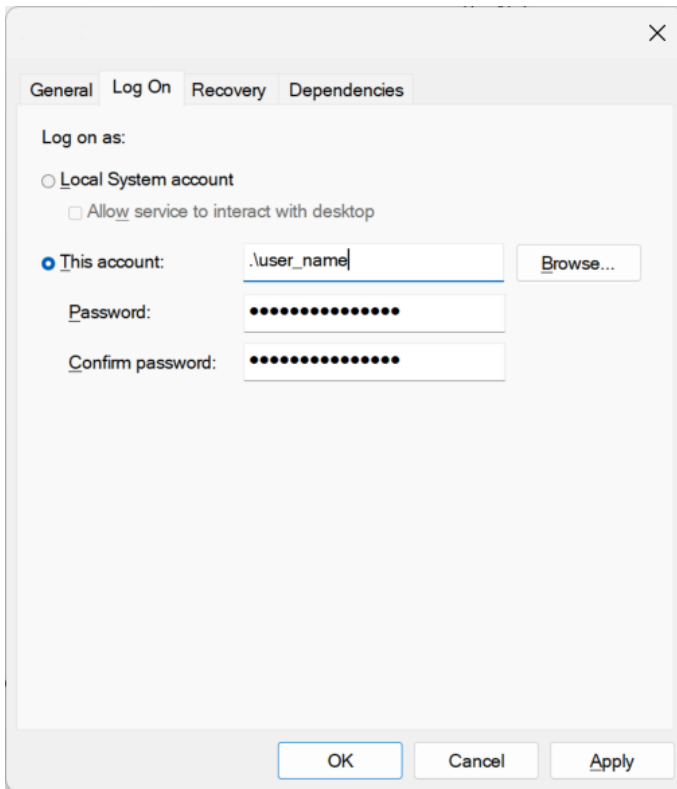
- Instead of mapped network drives, **we suggest using UNC** (Universal Naming Convention) paths to refer to network resources (shared folders). This is achieved by specifying the resource in the format:

\\servername\sharedfolder

The service / connector must be running in a security context with sufficient privileges on the shared network resource. In other words, the user under which the service logs in must have the necessary access to be able to execute the actions that are defined on the remote folder.

- The service (connector), in addition to running with a user who has privileges over remote resources, must have sufficient local privileges to modify files in Program Files (connector installation folder) and to add / to modify values in the Windows Registry.

Specifying a different user for the service logon is possible by accessing its properties in the Windows Services Manager, right-clicking and choosing the Properties option. Then configure as shown in the following image:



- The network resources must be properly shared with sufficient permissions so that the session or security context under which the Common sFTP connector is executed can perform the operations specified in the configuration of each one of the agencies, that is, to read in all cases and to write / modify / delete when archiving the processed files is configured.