

# Adding a Windows Network Log

If a Windows Network machine has security activated, you require an authentication account to access it. Otherwise, if authentication is not required, you can also access a Windows Network log from the Local log type page (see [Adding a Local Log](#)).

**Note:** Windows Network logs are only available when Xpolog Center is installed on a Windows machine.

**Note:** It is highly recommended to save a user on the Xpolog Service (Windows Services -> Xpolog Center Service -> Properties -> Log On tab). Once a user is applied on the Xpolog service it is possible to add remote Windows logs using type '**local**' by providing a UNC path (`\\hostname\dir_name\`). Example: `\\qaserver\c$\Log Files\log.log`.

## To add a Windows Network log to Xpolog:

1. In **Add Data** pane click on **Local Network**. The **Source and Collection Setting** wizard opens.
  - To change a log source, near **Source Type**, click on the **Change** button.
2. In **Connection Details**, select the Windows Authentication account required to connect to the log, or click the **new** link to add an account to the system (see [Address Book](#)).

**Note:** If you do not have any Windows authentication accounts defined in Xpolog, the Add Windows Authentication account page is presented automatically.

**Recommended:** It is recommended to configure a service account (on the Xpolog Service in the Windows Services Panel) with the required permissions to read logs from remote machines in the network. Then all logs, local or any other machine in the network, can be defined as Local log type page (see [Adding a Local Log](#)).
3. In **Log Path or Directory**, type the UNC path to the log's location in the network (`\\hostname\dir_name\dir_name\LOG_NAME`)  
OR  
Type partial path to a directory in the network and then click **Browse** to open the System Files Browser of the Windows Network machine that you connected to, expand the folders to get to the desired log, and then click **Select** to display the log location in **Log Path**.
4. Optionally, append to the log path a name pattern to capture multiple files from the same log. (For pattern syntax, see [Xpolog Patterns Language](#).) The log name is displayed in the left pane in its selected location under Folders and Logs. If you put in the log path a {string} pattern, the various files of the log appear in the left pane. Otherwise, only one file appears. You can perform regular actions on this log.
5. Optionally, click on **Collection Settings** to define advanced settings for the local log – Files Attributes, Files Filters, and/or Regional Settings (see [Configuring Advanced Log Settings](#)).
6. Click **Add Log**. A progress box displays the status of the system as it scans the selected path for log. When the scan completes, the Patterns Administration Wizard screen opens.
7. Optionally, Apply patterns on the log data and save the log in Xpolog (see [Applying Patterns on the Log](#)).
8. Click **Save** – Xpolog applies an automated pattern on the incoming log. **Log Collection Settings** wizard opens.
9. Optionally, defining the basic information of the new log (see [Setting Log General Information](#)).
10. Click one of the following:
  - Save & Close** – Xpolog saves the new log and points to the logs tree. locate the log in the logs tree and enter the viewer in order to view the log.
  - Save & Add Another** – Xpolog saves the new log and points to Add Log screen so that you may another log.

## Comments:

- On a Unix machine, you can bring into Xpolog local logs that reside on the same machine or in a mounted directory to which you have direct access.
- On a Windows machine you can define zipped logs (single/multiple files) without extracting them:
  - If you have a file **archive.zip**, which contains inside a single file, it should be defined directly on that file archive.zip
  - If you have a file **archive.zip**, which contains inside multiple files (**log-name.log**, **log-name.log.1**, **log-name.log.2**, ..., **log-name.log.N**) it should be defined using the name pattern: `archive.zip?log-name.log{string}`