Adding a Windows Events Log

Adding a Windows Events log (format evt/evtx) is similar to importing a local log, except that you are also required to enter a host name and set the type of events (Application/Security/System/Custom/*.evt).

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

To add a Windows Events log to XpoLog:

1. In **Connection Details**, select the Windows authentication account required to connect to the remote log, or click the **new** link to add an account to the system.
   Note: If you do not have any Windows Events account, the Add Windows Events account page is presented automatically.
2. In **SelectHost** dialog box, leave the default localhost for local host OR type the IP address/name of the host OR select the relevant IP address/host name from the list.
3. Select the type of log event(s) to bring into XpoLog:
   Do one of the following:
   a. Add Log File(s) by selection:
      Application – Mark the **Application** checkbox.
      Security – Mark the **Security** checkbox.
      System – Select the **System** checkbox.

      Note: the option 'Collect *.EVTX File Directly From File System' may be used for faster data collection however requires permissions to the remote machines.

   b. Add a Log File manually:
      Locate the **Add File** dialog box and add a direct path to the ***.evt/*.evtx** file, and select its type: **Application**, **System** or **Security**.
      In case the file is local, the path should be **\WIN_INSTALL_DIR\Windows\System32\winevt\Logs\<LOG>.evtx/.evt**
      ELSE, if the log is remote, type the UNC path to the log's location in the network (**\\HOST_NAME\WIN_INSTALL_DIR$\Windows\System32\winevt\Logs\<LOG>.evtx/.evt**)
4. Optionally, click on **Collection Settings** to define advanced settings for the Windows Events log(s) – Data Filter, and/or Regional Settings (see Configuring Advanced Log Settings).
5. Click **Done**. A progress box displays the status of the system as it scans the selected path for log. When the scan completes, then in case only ONE log was chosen, the Patterns Administration Wizard screen opens.
   Otherwise, if more than one log was chosen, then action item 6 will be skipped and **Log Collection Settings** wizard opens.
6. Optionally, Apply patterns on the log data and save the log in XpoLog (see Applying Patterns on the Log).
7. Click **Save** – XpoLog applies an automated pattern on the incoming log. **Log Collection Settings** wizard opens.
8. Optionally, defining the basic information of the new log (see Setting Log General Information).
9. 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.