How to Use Section Tool to Backup the MassLynx Audit Log

Section Tool is used to backup the MassLynx security audit log (mlevt file) in case of disaster.

The mlevt file is a 'live' file that is locked when being actively written to, which makes it difficult to backup using standard 3rd party backup software. However, the mlevt file can be backed-up using Section Tool. Another advantage of Section Tool is that it allows a big log to be backed up into several smaller files or sections which are small enough to be backed up to conventional media.

The SectionTool.exe is a standalone executable installed with MassLynx. It is located at C:\Windows\SysWOW64. The tool is executed from the command prompt. MassLynx must be installed in order to use Section Tool.

Note 1: To use section tool on a standalone system (i.e. one logging to the local log rather than logging to a remote logserver), the PC must be connected to the network. However, the PC does not need to be on a domain.

A. Backing up the log using Section Tool

1. On the PC that hosts the active mlevt file, log on to the desktop as the local administrator and start a command prompt.

2. Change the working directory to the folder location of Section Tool.exe. Enter:
cd C:\Windows\Syswow64

3. Enter: *sectiontool -d \\computer name\c$\folder\basename*

The folder location in the above path is the destination folder for the newly-created backup. You do not need to specify the folder location of existing mlevt file – only the name of the PC (which in the following example is ukw-ukmgekm).
e.g.

```
C:\>cd c:\windows\syswow64
c:\Windows\SysWOW64>sectiontool -d \\ukw-ukmgekm\c$\log_997\logbackup1
```

In this case, correct execution should result with a return to the C:\> prompt, and creation of a backup file called logbackup100001 in the folder log_997 on PC 'ukw-ukmgekm'.

When larger files are backed up, they are divided into chunks and numbered incrementally, e.g. logbackup10002, logbackup10003 etc. By default the segment size is 10 MB, this can be changed using the –m flag, using a range between 1 MB – 100 MB.

e.g.

C:\>sectiontool –d \\mm2737\c$\waters\auditlog\mlevtbckup -m 20 (equates to 20Mb segment size)

Note 2: the folder name must not have a space in it.

Note 3: If the name of the backup file is not changed, any existing file will be overwritten.

Note 4: the backup destination can be on another PC on the network. To write the backup file to a remote PC, you need to be logged in to Windows locally as a domain user.

e.g.

C:\>sectiontool -d \\NameOfRemotePC\C$\AuditlogBackup\mlevtbackup.

B. Recovering a backed-up log (mlevt file) after a disaster

To restore the backed-up file(s), copy the file(s) to a new or restored PC which does not have MassLynx installed.

If there are multiple files, use the copy command at the command prompt to re-combine them into one file using the /b (binary flag), followed by the path to the required mlevt file destination, i.e. the folder where you want the log to be located. Section tool is not needed.

If there is one file, you just need to copy the file to the required folder on the new PC and manually re-name the file 'mlevt'.

Once the log has been recovered, MassLynx security can be installed. When you install MassLynx, you specify the folder location of the backed-up log file (step 3 below).

Steps for Re-Combining Several Backed-up Files

1. At the command prompt, set the working directory to the folder location of the backup file(s).

   Cd C:\ nameoffolder

2. Use the copy command to generate a new mlevt file using the backed-up file(s):

E.g.

C:\Backup>copy /b mlevtbckup00001+mlevtbckup 00002 C:\Waters\MSAuditLog\mlevt

where \Waters\MSAuditLog\mlevt is the folder where you want to create the restored mlevt file.

Note: the destination folder name must not have any spaces in it.

e.g.

```
C:\Documents and Settings\DARNLEYP.TU-DOMAIN1>cd\

C:\>cd c:\AuditBackup

C:\AuditBackup>copy /b mlevtbckup00001 c:\Waters\AuditLog\mlevt
        1 file(s) copied.

C:\AuditBackup>
```

3. Install MassLynx security, specifying the appropriate folder location for the audit log. The restored mlevt file will become a system file when the new checksums are generated.

Note 5: the Windows desktop logon must have sufficient access to the registry to set the location of the log file during the installation of MassLynx. You need permission to read and write in HKEY_LOCAL_MACHINE. If the desktop logon has insufficient permission, the following error is displayed:

“Error setting log file location: Code 1”

Note 6: When you start LogLynx, you will find the following event has been written to the log:

'The event file had the wrong security attributes at startup'

When the log service starts up, it always checks the properties of the mlevt log file, for protection against tampering of the audit trail. It checks the file attributes, the file owner and the access control list.
After restoring a log file that was backed up using section tool, the newly created log file does not have the correct attributes. As a result, the above ‘security attributes’ event is generated in LogLynx.

Recommendation: after recovering a log file that was backed up using Section Tool, users are advised to record the backup in their external log file. Such a record can be used to explain the ‘security attributes’ event in LogLynx.