Chapter Seven

Audit Trail & Field Administration Password Change

- **Viewing the Audit Trail**
- **The Auditing Menu**
- **Copying the Audit Trail**

- **Field Administration Password Change**
- **Steps for the User to follow**

Audit Trail

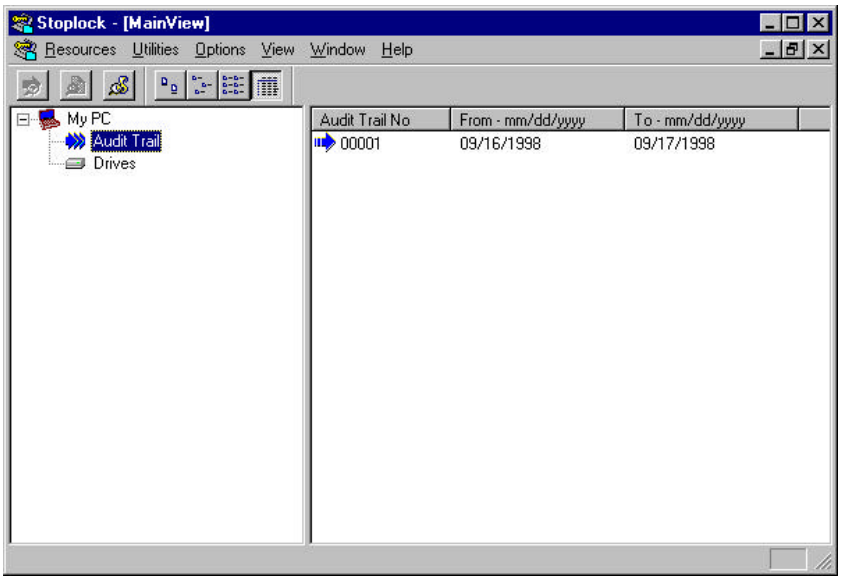
The audit trail is the main tool available to you for monitoring the use of a PC. The audit trail is a single recycled file - the oldest records in the file are overwritten with new ones when the file becomes full (500 records). The audit trail is held locally in the SLV95 directory.

The following events are logged to the audit trail:

- Logon
- Invalid Logon
- Logoff
- System Locked
- Password change
- Illegal Access events

Viewing the Audit Trail

To view the PC's audit trail, select the *Audit Trail* feature on the left of the MainView window.

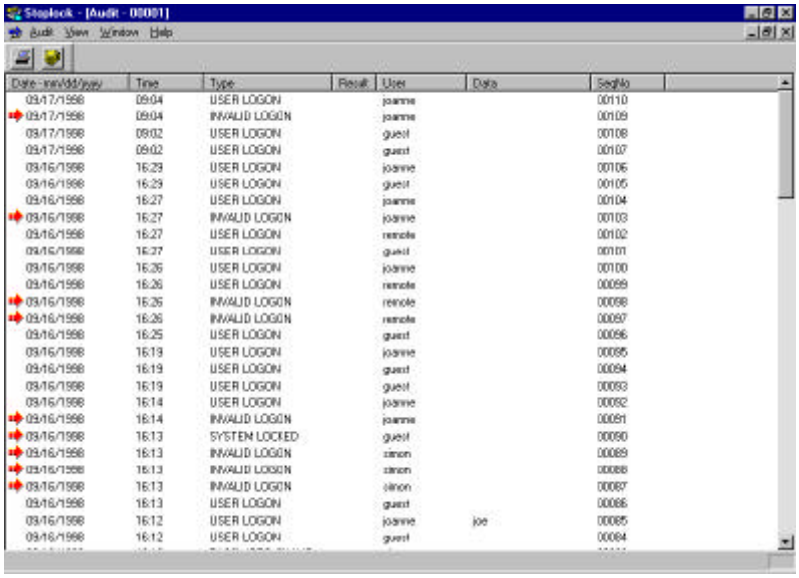


To view the contents of the audit trail, select the *Audit Trail No (00001)* in the right view and then do one of the following:

- Click on the  icon.
- Select Audit View from the Resources, Audit Trail pull-down menu.
- Right-click the mouse button, then select Audit from the resulting pop-up menu.
- Double-click the Audit Trail No.

The contents of the audit trail are shown in this format:

The seven columns on this window show the values of the seven fields in each audit trail record. *Date* and *Time* are self explanatory; the other fields are described below:



-  This icon highlights an illegal event.
- ***Type*** describes the logged event.
- ***Result*** is only relevant to file-access events. It shows GRANTED or DENIED, depending on the legality of the access.

- ***User*** shows the ID of the user responsible for the logged event.
- ***Data*** shows the name of the object affected by the event. This will either be a user, the 'SHARED' group, or a filename.
- ***SeqNo*** is just a record counter.

Note: Windows 95 opens and reads a file in order to execute it, so these auditing parameters will be displayed instead of EXECUTE. Also, when you delete a file using Windows 95 Explorer, the file is renamed to the Recycle Bin. Thus, RENAME appears in the audit trail instead of DELETE.

The Auditing Menu

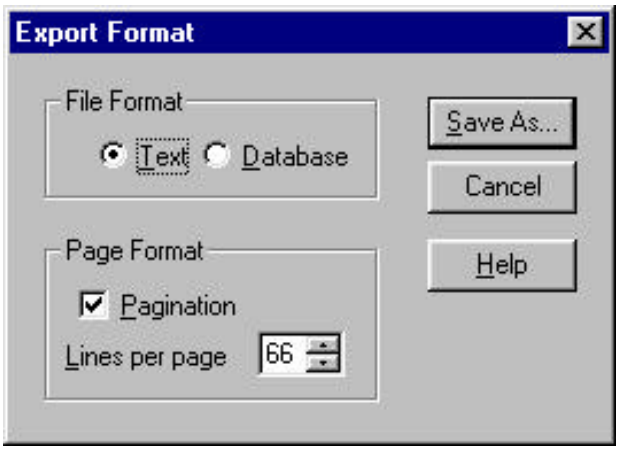
The Audit pull-down menu offers the following options, which are also available as icons in the toolbar:

Print

Use this option to print the audit trail. Selecting this option calls up a standard Windows 95 printer-selection window where you can choose the printer, port, and number of copies. Since the trail is unpaginated, the print range is always All. Other defaults are taken from your Windows 95 setup.

Export

Use this option to create an editable file containing the records in the audit trail. Selecting this option calls up the Export Format window:



File Format

Select the appropriate radio button to save the audit trail as **Text** (*.TXT) or **Database** (*.DB) format.

Database records are of fixed format, with fields corresponding to the columns on the window: Date, Time, Type, Result, User, Data, and SeqNo. Each field is of fixed length, padded with spaces on the right, and enclosed in double quotes.

At least one trailing space is always included before the terminating quotes. Fields are separated by commas.

For example:

"10/06/96 ","08:25 ","USER CHANGED ", ...

Page Format

This area is only available if you have selected **Text** as the file format. Here you can set the page length if you keep the Pagination box checked.

Select the *Save As* button to save the audit trail.

Copying the Audit Trail

This section covers the copying of the audit trail for non-administrators only - administrators may copy the audit trail as per any other file.

Non-administrators cannot view or delete the audit trail but may copy it to a removable or network drive in order to provide remote viewing by an administrator. Because Stoplock prevents the audit trail from being overwritten, it must be saved as a new filename. As Windows 95 does not support the copying and renaming of a file in one process, this must occur using the copy command at the MS-DOS prompt. For example:

copy }~a00001 filename

Once the user has sent you their audit trail you should then rename it back to }~axxxxx (where x represents a number) in order to view it.

Field Administration Password Change

The field administration password change function enables standard users or administrators to reset their forgotten passwords via a remote challenge/response function. You cannot reset ‘Temporary’ or ‘Guest’ user passwords with this function.

A remote password change can only be done with the help of a administrator who is logged on to another PC with the same Master Encryption Key (MEK). The challenge and response strings are generated from the user's identifier, using the MEK as a base: this is why both PCs must use the same MEK.

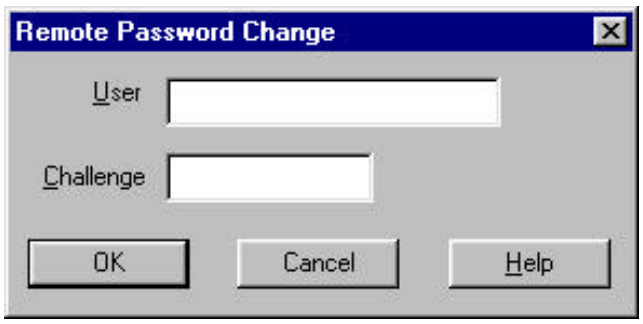
A user of type ‘FM’ (Field Manager) is already set-up on the PC in order to use this function and cannot be deleted. The ID of this user is ‘remote’ and the password is **123456**. You may leave this password as it stands or edit the FM user profile and change it accordingly.

When a user logs on as type ‘FM’ a controlled logon session is initiated - the user can only use this function to change his/her password, all other access to the system is prevented. On successful password change the user is presented with a normal logon box, enabling him/her to logon with his/her own user name and the new password.

You will need to talk the user through the procedure by phone and it is your responsibility to check the validity of the user.

Remote Password Change

Select Field Administration Password Change from the Utilities menu in order to display the following dialog box:



- ***User***
  In this field type the ID of the user whose password is to be changed. This should be the same as the name the remote user typed into the FIELD ADMINISTRATION: PASSWORD CHANGE box and is case insensitive.
- ***Challenge***
  Type the character string that appears on the remote user's screen - this is also case insensitive.

On pressing *OK* a password **Response** code will now appear instead of the challenge box. Give this response code to the user to enable him/her to change his/her password.

Note: If the user who had forgotten his/her password had also been deactivated, then following a successful password change, the user will automatically attain active status.

Steps for the User to Follow

1. Logon with the user name and password of the user who has been set up as type 'FM'.
2. Once the 'Field Manager' ID and password have been accepted, a dialog box will appear. Enter your own user name in the ***User ID*** field (the one you have forgotten the password of) and then press the **Q** key.
3. A **Challenge code** is displayed on the screen with a Response box. Give the challenge code to your administrator.
4. Your administrator will supply you with a Response Code. Enter the **Response Code** in the ***Response*** field.
5. A Password change box now appears for your own password to be reset - change the password.
6. Logon with your normal user ID and the new password.
7. You will then be prompted to change this password again to a new one.

Note: If the Response Code is not accepted for some reason (could be due to mis-typing or both machines not sharing the same MEK), the ***User ID*** field will be displayed again.