

# Contents

[Introduction](#)

[Resources Menu](#)

[Utilities Menu](#)

[Options Menu](#)

[View Menu](#)

[Configuring Drives, Folders & Files](#)

[File Scripts](#)

[Audit Trail](#)

[Field Administration Password Change](#)

## Information

[Contacting PCSL](#)

[Troubleshooting](#)

[Deletion of Encrypted Files](#)

## **De-installing Stoplock**

## Introduction

The File Encryption & Utilities program enables you to apply encryption to folders and files, manage the audit trail and remotely change a user's password. When you start this program, the MainView window is displayed. The following menus are available from the MainView window:

[Resources Menu](#)

[Utilities Menu](#)

[Options Menu](#)

[View Menu](#)

## Resources Menu

This menu offers the same options as the icons in the toolbar: **Audit Trail**, **File Manager** and **Scripts**, plus an **Exit** option for leaving Stoplock.



### **Audit Trail/Audit View**

Use the Audit View option on the Audit Trail sub-menu to display the contents of the audit trail. This option is dimmed if the Audit Trail no. in the right view is not currently selected.



### **File Manager**

Use the File Manager option to start the File Manager within Stoplock. File Manager enables you to apply encryption to folders and files.



### **Scripts**

Use the Scripts option to start the Script Manager within Stoplock. Scripts enable you to define encryption rules that can be applied to files and folders on your PC.

## **Utilities Menu**

### **Field Administration Password Change**

This facility enables you to remotely change a user's forgotten password.

## **Options Menu**

### **Set Bitmap**

Selecting this option will bring up a standard Windows 95 browse dialog, from which you can select a .BMP file to be displayed on the left-hand side of data-entry windows.

### **Use Default Bitmap**

This option is selected by default in order to display the Stoplock bitmap on the left-hand side of data-entry windows.

## **View Menu**

### **Toolbars**

Enable you to hide and show the various toolbars that are displayed on different windows within the system. By default all boxes are checked except for the Styles box.

### **Status Bar**

Enables you to hide and show the status bar at the foot of the window. This bar shows messages from the system, and also indicates whether the keyboard's number, capitals, and scroll locks are on or off.

**Note:** Unless you have an overriding reason for hiding them, you will normally find it easier to use the system with the toolbars and the status bar displayed.

## Configuring Drives, Folders & Files


The File Manager program in Stoplock allows you to encrypt files on a fixed drive, making them available only to specified individuals and/or to members of the 'SHARED' group.

**Note:** The setting up of encryption can be made less tiresome by using [file scripts](#)

If you click the **Drives** feature on the left of the MainView window, all the fixed drives accessible from your PC will be listed on the right. The entries in the **State** column show the ways in which the drives have been configured by Stoplock; if you selected encryption at installation time, drive C: is shown as 'Configured', otherwise, it is shown as 'Open'. Subsequent fixed drives are shown as 'Open'.

### Accessing File Manager

To access File Manager, highlight a drive letter and then do one of the following:

- Click the  icon.
- Select Drive View from the Resources, Drives sub-menu.
- Double-click on the drive letter.
- Right-click the mouse button then select File Manager from the resulting pop-up menu.

[File Manager Toolbar](#)

[File Manager Menu](#)

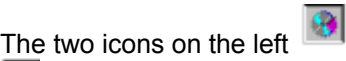
[File Manager Options Menu](#)


[List Control View](#)


### [Configuring Drives](#)

## File Manager Toolbar

### Icons

The two icons on the left 

 correspond to the Configure drive and Security options on the File Manager menu.

The  icon moves you up one folder level in the display. **Note this icon is grayed-out if the current display is the root folder.**

### Files

Use this field to specify a file pattern to filter the files shown on the window, using wild cards as necessary.



## **File Manager Menu**

The following options are offered on the File Manager pull-down menu:

### **Configure Drive**

This option allows you to set up security information for a drive.

### **Security**

This option is only available if the drive has been configured. It allows you to apply encryption to folders and files.

## **File Manager Options Menu**

### **Select All Files**

This option automatically selects every file in the file name list – excluding sub-folders. You can subsequently de-select single or multiple entries in the usual way.

### **Check Access Control Lists**

Check this option if you want access control lists to be checked for consistency whenever this program reads a folder. If any errors are found, you are informed and asked if you want them to be fixed.

## List Control View

### FileName

This displays a list of the files on the drive.


### Encrypt

This displays the type of key (if any) the file has been encrypted under. If a file is encrypted under a user key or the shared key then the name of the user or the 'SHARED' group is shown.

This column also displays whether a file has 'Reserved' status.

## Configuring Drives

By configuring a drive, you tell Stoplock how to react to drive access. You cannot expand a drive to show its folders and files until you have 'configured' it. This will have occurred at installation time if you selected encryption or if you specified encryption during system configuration. Note that only the first fixed drive (drive C) will be configured by either of these methods. Subsequent drives that you wish to apply encryption to can be configured as follows:

- Click the  icon **or**
- Select Configure Drive from the File Manager menu

You are shown the [Configure Drive window](#)

[Factors Affecting Access](#)

[Protection of Files](#)

[Setting Security on a Configured Drive](#)

# Configure Drive window

## Options

The drive type options available are:

- **Configured**  
This option enables you to apply encryption to folders and files. An access control list (ACL) is added to each folder on a configured drive which contains the encryption key type. You must configure a drive if you wish to apply encryption.
- **Open**  
Selection of this option de-configures the drive. Any files that are encrypted will be decrypted.

## Buttons

- **Update Drive**  
Select this button to apply a particular drive type option.
- **Fix Drive**  
This button only applies if you select the **Configured** option.  
Select this button to check and correct all the ACLs on the selected drive. You should use this rather than the **Update Drive** button if you have had to reinstall Stoplock while leaving a drive configured.

## Factors Affecting Access

There are two separate factors affecting the access a user has to a file. In order of priority they are:

### 1. System Files

These are Stoplock files which have pre-defined access rights that are automatically set by Stoplock and affect non-administrators. Administrators however, also have READ ONLY Rights to CHKDSK. These files cannot be encrypted.

<b>File Affected</b>	<b>Rights Assigned</b>
FDISK	NO Rights
CHKDSK	READ ONLY Rights
CONFIG.SYS	READ ONLY Rights
SLV96.VXD	NO Rights
SL5D.SYS	READ ONLY Rights
SL5L.SYS	READ ONLY Rights
IO.SYS	NO Rights
MSDOS.SYS	NO Rights

**Note:** The file rights applied by Stoplock may be modified via an [exclusion list text file](#).

### 2. Encryption

If a file is encrypted under a key which the user is not party to then the user has no access to the file. This also applies to administrators. An administrator however could remove this encryption via Stoplock's File Manager program if desired.

## Protection of Files

### Windows 95 Files

By default, Windows 95 is loaded in Stoplock 'guest' mode and it is important that the 'guest' user has the necessary access rights to allow the Windows 95 operating system to load. The files for the Windows 95 operating system are stored in the Windows 95 folder which on a standard Windows 95 installation will be C:\WINDOWS.

**DO NOT encrypt files in this folder and it's sub-folders.**

### Other Files

It is important that files which are used by the Stoplock administration programs are not encrypted under keys which are not available to the administrator.

### Extended System File Configuration

An [exclusion list text file](#) is provided with Stoplock. This text file (excl.txt) is based on the default settings used within Stoplock and may be modified accordingly to suit your environment.

By modifying the existing text file or by creating a new text file, you can build a list of reserved files/folders which will remain unencrypted or have certain access rights set against them by default.

## Exclusion List Text File

This text file (excl.txt) is based on the default settings used within Stoplock and may be modified accordingly to suit your environment.

By modifying the existing text file or by creating a new text file, you can build a list of reserved files/folders which will remain unencrypted or have certain access rights set against them by default.

**YOU SHOULD CREATE THE EXCLUSION LIST BEFORE RUNNING A FILE SCRIPT. Be aware that if you specify no encryption within the exclusion list against files/folders that already contain encrypted data then these files will not get decrypted by Stoplock.**

### Example Exclusion List Text File

An example exclusion list text file is shown as follows. Explanations are shown in italics:

**[Extensions]**

**EXE,-eNOENCRYPTION**

*No encryption will be applied to files of type .EXE*

**[Files]**

**CONFIG.SYS,-aR**

*Only read rights are available for CONFIG.SYS*

**[Paths]**

**C:\WINDOWS95,-eNOENCRYPTION,-dSUBFOLDERS**

*No encryption will be applied to files in the Windows95 folder and any of its sub-folders.*

**Note:** The **[Paths]** section should come before the **[Files]** section in order for the exclusion list text file to be properly compiled.

This exclusion list text file may be edited using a text editor and configured as follows:

**[Extensions]**

- Here you may specify file extensions e.g. .EXE

**[Files]**

- Here you can specify filenames e.g. C:\CONFIG.SYS  
(Note that pathnames must be provided)  
Wildcards (\*) may be used in filenames.

**[Paths]**

- Here you can specify pathnames e.g. C:\WINDOWS95\  
( Note that folder paths must be terminated by a \ )

The following switches may be used:

<b>-a</b>	Used to specify file access rights (RWECD) R=Read, W=Write, E=Execute, C=Create (only applies to folders), D=Delete
<b>-aS</b>	Used to specify search rights
<b>-eNOENCRYPTION</b>	Used to specify no encryption of files/folders
<b>-eNOFILEENCRYPTION</b>	Used to specify no encryption - files only
<b>-eNOFOLDERENCRYPTION</b>	Used to specify no encryption - folders only
<b>-DSUBFOLDERS</b>	Used to specify sub-folders

### NOTE THE FOLLOWING:

- Any files you apply access rights to are treated as reserved files by Stoplock. These files will not get encrypted and encryption cannot be applied using Stoplock's File Manager.



- Any files/folders that have NOENCRYPTION, NOFILEENCRYPTION or NOFOLDERENCRYPTION specified against them cannot have encryption applied to them using Stoplock's File Manager (the Encryption window is not available).

## **Using the Exclusion List**

**Make sure that every variable is separated by a comma (,) and paths are terminated by a backslash (\) before compiling the exclusion list for use by Stoplock.**

**Make sure the [Paths] section comes before the [Files] section in the exclusion list text file.**

The following actions need to occur before the modified/newly created exclusion list text file is used by Stoplock:

- Save the text file - you may specify any filename e.g. myfile.txt
- At the command line type:  
C:\PATHNAME\EXCLLIST -w c:\pathname\filename.txt  
where PATHNAME is the path to the executable and text file and filename.txt is the name of the exclusion list text file. This will create a }~E file in the SLV95 folder which is then used by Stoplock.
- Reboot the PC in order for Stoplock to read the new }~E file.

## **Checking the contents of the Exclusion List**

If you want to read the }~E file to examine its contents, type the following at the command line:

**EXCLLIST -r c:\pathname\filename.txt**

where pathname is the path to the executable and filename.txt is the name of the file you want to store the contents of the }~E file to.


## Setting Security on a Configured Drive

If you select the **Configured** option on the Configure Drive window, and then the **Update Drive** button, the system will prompt you to confirm, and then create access control lists (ACLs) in all the folders on the drive. When this has finished, select the **Close** button to clear the window. All the folders and files in the root folder will then be displayed. If you double-click on a folder name, the files and sub-folders in that folder will be listed on the right.

### Applying Encryption to Files & Folders

To set encryption on one or more files or folders, select them from either the left (only available for folders) or the right display lists. **Note: You cannot mix files and folders in the same selection.** Once folders/files have been selected, you can then apply encryption via the [Security window](#)

To view the Security window do one of the following:

- Click the  in the tool bar.
- Select Security from the File Manager pull-down menu.
- Right-click the mouse button, then select Security from the resulting pop-up menu.

### Encryption on Folders

If encryption is being set against a folder then encryption does not take place immediately: instead, files created in the folder will take on the encryption attribute specified. You must double-click on the folder name and select **all files** in order to apply encryption to existing files. Alternatively, you can check the 'This folder, files and subfolders' box on the Security window to apply encryption to all files and sub-folders within the selected folder.

### Changing the EncryptionType

If you choose encryption for a file that is already encrypted, it is decrypted before being encrypted with the new key.

### Copying/Moving Files

Files copied or moved to a folder will inherit the encryption status of the folder. This may cause files to be encrypted, decrypted or both.

### File Encryption

A file can become encrypted in one of two ways:

- A file is created in a folder on a drive which has type 'Configured', and encryption is specified for the folder.
- You can use Stoplock's File Manager program to encrypt or change the encryption key of any file on a configured drive.

**Note: System files and files with the extensions CCC, COM, EXE, OVL, DLL, and SYS cannot be encrypted.**

### Applying Execute Rights to Files

To set execute rights for one or more executables, select the file(s) from the right display list. Right-click the mouse button, then select Security from the resulting pop-up menu. The [Security window](#) is displayed.

## Security window

### Encryption

Encryption protects data by a controlled scrambling which renders the contents of a file meaningless except when it is decrypted using the same algorithm and key that was used for encryption.

Select the appropriate radio button corresponding to the desired level of encryption required:

- **No encryption**  
This option is self-explanatory. If you specify this for files that are already encrypted they are decrypted.
- **Personal key**  
Files are encrypted using a key that is specific to the user. A list of users is shown in the **Users** box and you must select one to use.
- **Shared key**  
Files are encrypted, using a key that is specific to the 'SHARED' group. Users must be a member of this group in order to access files encrypted under this key.

### Encryption Options

#### **This folder, files and subfolders**

Check this box in order to apply encryption to all files and sub-folders within the selected folder. If this box is left unchecked, only newly created files will be affected by the chosen encryption option. This option is not available if the root folder has been selected in order to prevent you from encrypting files in the WINDOWS folder.

**Note: The Encryption Options section is not available when creating File Script rules.**

Drives are automatically updated with security settings once the **OK** button is pressed.

## Security window (Execute Rights)

This window is only available when you are applying security to one or more executables (.COM, .EXE, .OVL, .DLL etc.).

Check the execute box in order to grant or deny execute rights to files.

**Note:** The Execute window is meant to be used in conjunction with the ANTIV.SLS script in order to grant execute rights to newly created files. Although it can be used to deny execute rights to any existing files, it is not intended for this purpose. Confusion could certainly result if this option is used for any other purpose as you can only display a files execute status on viewing this window. Remember to virus check the file before granting execute permission via this window.

## File Scripts

A script is a collection of rules, simple or complex, that can be applied to one or more folders or files, defining file encryption.

Use scripts to avoid having to manually set encryption using Stoplock's File Manager, which allows manual definition of file encryption attributes. This process may introduce a significant "manual" overhead in large systems. Stoplock supports functionality referred to as scripts which allows the batch processing of file encryption.

Once you have created a script you can save it and subsequently copy, modify or run it. This means that you can create scripts on one PC and run them on other PCs, thus saving valuable time and effort when installing and configuring Stoplock or other software on a number of PCs.



Use the Scripts option from the Resources Menu to start the Script Manager within Stoplock.

The column on the left will show your default drive. You can choose a different fixed drive by selecting it from the pull-down field on the toolbar, and expand it to show its folders by double-clicking it.

### [Script Menus](#)

### [Building a Script](#)

### [Script Rules - Editing, Moving, Copying & Deleting](#)

### [Script Rules - Modifying](#)

### [Checking Scripts](#)

### [Running a Script](#)

### [The Result of Running a Script](#)

The following scripts are supplied with Stoplock:

- [ANTIV.SLS](#) - protects your hard disk against viral infection.
- [EXECUTE.SLS](#) - to be used in conjunction with the ANTIV script to grant execute rights to all files.
- [EXPORT.SLS](#) - allows files to be securely moved between PCs by remaining encrypted.

## Script Menus

[File menu](#)

[Edit menu](#)

[Security menu](#)

[Run menu](#)

[Drive Field](#)

## Configure Drive window (scripts)

### Configure Options

- **Configure**  
This option enables you to apply encryption to folders and files. An access control list ({}~t) is added to each folder on a configured drive which contains the encryption key type. You must configure a drive if you wish to apply encryption. You can only run a script on a drive which has been configured.
- **Fix**  
Select this option to check and correct all the ACLs on the selected drive. You should use this option if you have had to reinstall Stoplock while leaving a drive configured.
- **Open**  
Select this option to de-configure the drive. Any files that are encrypted will be decrypted.

## File menu

This menu offers you standard options for creating, editing, and saving files containing scripts. The icons shown can be used as shortcuts to the relevant options.



### **New**

Use this option to create a new script after creating or editing one. When you select it, the scripts window returns to its initial format.



### **Open**

Use this option to open an existing script. When you select it you will see a standard window for locating and selecting a script.

Find and select the script you want to work with in the usual way, then edit it, or run it.

**Note: You may also use this window to delete a script - highlight a script name and then press the delete key.**



### **Save**

Use this option to save a new or edited script.

### **Save as**

Use this option to save a script to a new file.

### **Exit**

Use this option to leave Stoplock.



## Edit menu

This menu allows you to define the contents of the script in the right half of the window. The icons shown can be used as shortcuts to the relevant options.

### **Add Drive**

This is the only option available when you first create a script: use it to specify the drive containing the folders that will be the target of the script.

You can only specify one drive as the target of a script: the other options described below are only available once you have done so and started building the script.

### **Configure Drive**

This option gives you the opportunity to re-configure the drive as 'Configured' or 'Open' and also allows you to **Fix** the drive.

The other options on the Edit menu are summarized below; they are all for use when you create or edit rules in a script.

### **Create Folder**

Use this option to create a folder. When you run the script, the folder specified here will automatically be created by Stoplock and rules will be applied to this folder as defined in the script. You must specify the full pathname when creating a folder.

### **Insert Before**

Use this option to add an entry to a script before the currently selected script entry.

### **Insert After**

Use this option to add an entry to a script after the currently selected script entry.

## Delete

Use this option to remove a selected script entry. This option only applies to whole folder entries.

## Copy

Use this option to copy a selected script entry to the end of a script, where you can edit the rules as necessary. This option only applies to whole folder entries.

### **Move Up**

Use this option to move a script entry one place towards the beginning of the script. This option only applies to whole folder entries.

### **Move Down**

Use this option to move a script entry one place towards the end of the script. This option only applies to whole folder entries.

**Note:** Many of the create/edit rules options are also available from a pull-down menu which is activated by clicking the right mouse button on a **folder** rule. If you expand the folder and click on a subsequent rule, the only option available is Edit which allows you to modify that rule.

## Security menu



### **Security**

Use this option when building scripts to specify encryption for specific target files and folders.

## Create Folder

Enter a folder and pathname in the **folder** field. When you run the script, the folder specified here will automatically be created by Stoplock and rules will be applied to this folder as defined in the script. You must specify the full pathname when creating a folder.

## Run menu




### **Run Script**


Select this option when you want to apply the script to the drive that it specifies.

## **Drive Field**

This pull-down field is located on the far left of the toolbar. Use it to select a drive that you want to build a script for.

## Building a Script

To start a new script click the  icon or select Add Drive from the Edit menu. The currently selected drive is then shown in the right half of the window. You may then specify target folders, files and sub-folders, and the security rules that will apply to them when you run the script. To do so proceed as follows:

1. Expand the folder display on the left by clicking the  boxes as necessary, until you can see all the sub-folders that you want to cover in the script.


**The only function of this display is for viewing purposes only, so you can see what folders exist on your PC.**

2. Select the name of the first folder that you want to set rules for. You can only specify one folder at a time, but you can later specify that rules should apply to all sub-folders of a chosen folder. Once you have defined rules for one folder, you can copy them to another folder if desired.

3. Select the Inset After option from the Edit menu. You will see the [Profile window](#)

4. Select the Encryption tab. You will see the [Encryption window](#)

**Note: When you apply a script that includes file encryption, any existing encryption specification of the affected files or folders will be replaced: this may cause to files to be encrypted, decrypted or both.**

5. Select the **OK** button to save what you have done and remove the window. The appearance of the Scripts window will not have changed. However you can now expand the display on the right by clicking the  boxes to view the script.

6. Select the next folder that you want to set rules for, and repeat the process above.

## Profile window

Here you may specify files/folders to be affected by the script.

### Folder

The **Folder** field shows the currently selected folder and the type of files (i.e. \*.\* meaning **all** files) this script will be applied to. You may edit this field as necessary.

### Folder Options

Select the appropriate radio button:

- **Folder [New file rights]**  
The rules in the script will only affect newly created files in folders.
- **Folder and files**  
The rules in the script will affect the selected folder(s) and their contents. Both existing files and newly created files are affected - the result is a combination of the **Folder [New file rights]** and **Files Only** radio buttons.
- **Files Only**  
The rules in the script will affect only existing files in the selected folder(s) - newly created files will not be affected by this rule.
- **This folder and sub folders**  
Check this box if you want any of the above folder options to be applied to all sub-folders of the selected folder(s).

## Script Rules - Editing, Moving, Copying & Deleting

The Move Up/Down and Insert Before/After options and icons apply to whole folder entries only. Use them to re-position rules within the script.

If you click anywhere in the entry for a folder and then select the Delete option from the Edit menu, the whole folder entry is deleted.


If you click anywhere in a folder entry and then select the Copy option from the Edit menu, the whole folder entry is copied to the end of the script - you can use Move Up to reposition it if necessary.

You can Edit the folder specification on the **Profile** script-rules window for the new copy to specify a new folder, and also make any rule changes that apply to the new folder.



## Script Rules - Modifying

Once you have included a folder in the script, you can add and change its rules by any of the following methods:

- Clicking the  icon.
- Double-clicking on a rule - this takes you directly to the tab whose window was used to set that rule.
- Selecting the Security option from the Security menu.


This displays the script-rules windows for that folder again, and you can change the entries as necessary.

## Checking Scripts

When you have finished building a script, expand it in full and check it. Make sure that folders are specified in the correct order - when you run the script, rules will be applied to folders in the order they are defined, so be careful not to override one entry with a later one. Save the script once you are satisfied with it.

## Running a Script

To run a script, open it from the File menu if it is not already displayed, then either:

- Click the  icon
- select Run Script from the Run menu

### **WARNING!**

You are not prompted to confirm that you want to run the script; it will run immediately. Even if you have only specified a small number of folders in the script, Stoplock will check the entire contents of the specified drive: this may take a considerable time for large capacity drives.

**Note:** Scripts may also be run from the Windows 95 command line by typing the following text at the command line prompt:

```
SLV95 /S SCRIPT.SLS
```

where SCRIPT.SLS is the pathname and filename of the script to be run.

Scripts executed from the command line may be run by both administrators and non-administrators.

[The Result of Running a Script](#)

## **The Result of Running a Script**

Once a script has been run, you can use Stoplock's File Manager to check the effects of the script on the selected folders.

The way that the script is applied to the folder will depend on the way you set up its profile. If you chose to apply the script to existing files, the security values shown for files in the folder should reflect those set in the script.

## **ANTIV Script**

This script is supplied with Stoplock to help protect your hard disk against viral infection. Run a virus checker before running this script to ensure your disk is virus free.

### **Rules applied by this script**

The first rule affects all folders and sub-folders but does not affect any existing files. Any new files created or copied to the hard disk will not be allowed to execute.

The other rules affect all the existing files in folders and sub-folders. These rules allow all existing executables to run and prevents them from being modified or deleted (this stops viruses from writing directly to the executables).

**Note that this script is provided to help prevent virus infection. PCSL recommends that you still continue to regularly use a virus checker program to ensure your PC is virus free.**

### **New Files**

Any new file(s) added to the PC once the script has run should be checked for viruses. Execute permission can then be granted to these file(s) using Stoplock's File Manager or by using the [Execute script](#) supplied.

## **Execute Script**

EXECUTE.SLS - This script is to be used in conjunction with the ANTIV.SLS script. It grants execute permission to all files on the drive thus allowing files that have been copied to the hard disk after the ANTIV.SLS script has run to be executed. You may use Stoplock's File Manager instead to achieve the same result but running this script is more convenient if you need to grant execute permission to multiple executables.

## Export Script

This script is provided in order to allow files to be moved between PCs while remaining encrypted. Normally, if you were sending an encrypted file via a modem it would be decrypted when read into memory, travel unencrypted, and arrive at its destination unencrypted.

This script sets up two folders which are explained as follows:

- **Export**  
Files are encrypted using the shared key when written to an Export folder but not decrypted when read.
- **Import**  
Files are decrypted using the shared key when read from an Import folder but not encrypted when written.

A file copied from an 'Export' folder to an 'Import' folder will travel in encrypted form, whereas it would normally be decrypted when read and encrypted when written. Clearly, these folders need to be used in pairs and should not be used for any other purpose.

**If you wish to share encrypted data with other PCs then you must specify the same key for the 'SHARED' group on each PC. Users who wish to share encrypted data must be made a member of the 'SHARED' group.**

**Note:** The Encrypt rights column in the list control view informs you as to whether a folder is of type Import (I) or of type Export (E).

## 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](#)

[Printing the Audit Trail](#)


[Exporting the Audit Trail](#)

[Copying the Audit Trail](#)




## 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 seven columns displayed on the auditing 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.

## Printing the Audit Trail



### Print

Use this option to print the audit trail or select Print from the Audit pull-down menu. 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.

## Exporting the Audit Trail



### **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](#)

## 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 an 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. By default, there is a user of type 'FM' (Field Manager) set-up on each PC in order to use this function.

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 Remote Password change dialog box.

[Remote Password Change dialog box](#)

[Steps for the User to follow](#)

## Remote Password Change 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** supplied by your administrator 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 mistyping or both machines not sharing the same MEK), the User ID field will be displayed again**



## Contacting PCSL

### International Headquarters

PCSL  
Windsor House  
Spittal Street  
Marlow  
Bucks, UK SL7 3HJ

**Tel** +44 (0)1628 890390

**Fax** +44 (0)1628 890116

**Web** <http://www.pcsl.com>

**E-Mail** [info@pcsl-europe.com](mailto:info@pcsl-europe.com)

## Troubleshooting

This section answers to commonly asked support questions. In the majority of cases no additional software is needed, and a full explanation of the reason behind the problem can be found by referring to the on-line help. A brief explanation of the problem is given here.

If a problem persists, or is not mentioned below, then telephone or fax your local support office.

### [Contacting PCSL](#)

Should you wish to contact PCSL outside office hours, then please fax the support desk. Please print out and fill in the details on the form provided.

### [Technical Support Fax Sheet](#)

In certain situations you may need to fax a copy of the PC's CONFIG.SYS, AUTOEXEC.BAT, SYSTEM.INI and WIN.INI files and possibly sections of the Registry plus any network configuration/batch files. Please ensure that you have access to these.

### [File Recovery](#)

### [De-installation](#)

## **File Recovery**

### **Loss or damage to the Stoplock configuration file**

The recommended solution is to reinstall Stoplock. System and user information can be restored using Predefined Defaults. If these are not available however, remember to enter the same MEK as was used previously. If the drive was left 'configured' you must run **Fix Drive** in order for Stoplock to re-read the access control lists. If Predefined Defaults have been used then remember to reboot the PC and log on using a user name from your backed-up configuration.

### **Loss or damage to the Stoplock user file**

This case may not be so severe, depending on the exact nature of the damage. It may be that only a non-administrator's profile has been damaged, in which case it can be deleted and recreated.

### **File left encrypted with key of deleted user**

This should not occur, unless you are forced to delete a user due to a corrupt profile because you are always warned of the possible danger of deleting a user. Provided you know what the key was, you can recreate the user, specifying the appropriate key. The file should then be accessible again.

### **File left partially encrypted or decrypted**

If there is a sudden failure of the PC – software, hardware or power failure – during encryption or decryption of a file, it may be left in an unusable state. Provided this is noticed before any further encryption or decryption takes place the file can be recovered as soon as the PC is operational again.

During encryption and decryption a copy of a file is held in the SLV95 folder under the name AE, so all you have to do is to copy this file over the unusable file (having established beyond any doubt which file is affected). The result will be as though the encryption or decryption had never begun.

## De-installation

When Stoplock de-installs, it automatically sets all drives to type 'Open'. By setting a drive to type 'Open', all files are automatically decrypted. However, if the key of any file encrypted under a user has been lost because the user has been deleted, then decryption cannot take place and Stoplock will refuse to change the drive type.

Because nobody has access to such a file, it cannot be deleted, so you might think you are stuck with a configured drive. The solution is to temporarily add a user with the same name as the one which had been deleted - the Encrypt column in Stoplock's File Manager will display the user name the file is currently encrypted under.

This will give you access to the file so that you can delete it, after which you should have no problem in successfully de-installing Stoplock.

## **Deletion of Encrypted Files**

When you delete a file, Windows 95 moves this file to the Recycle Bin. If no encryption is set against the Recycle Bin then any encrypted file which is deleted will be stored decrypted. You should either regularly empty the Recycle Bin or specify encryption against the Recycle Bin using an appropriate key.

## De-installing Stoplock

**As Stoplock was installed using the InstallShield Wizard this program is also used to de-install Stoplock.**

The procedure here removes everything related to Stoplock: programs, the audit trail, user information and system configuration information. All system files altered by the installation program are modified to remove all the changes made by Stoplock. The Stoplock folder and icons are also removed.

You can only remove Stoplock if you have logged on as an administrator.

**NOTE: You do not need to remove Stoplock in order to upgrade to a new release.**

### Before You Begin

Check the following points before running the de-installation program:

1. The entire SLV95 folder is deleted by de-installation, so if you have saved additional data there you should save it to another folder. Check that any file scripts and Predefined Defaults that you want to keep are not stored in this folder.
2. Close all applications that are currently active.

### The De-installation Process

1. Select the *Add/Remove Programs* icon in Windows 95 Control Panel.
2. Select Stoplock from the list of programs displayed.
3. Click on the *Add/Remove* button.
4. Click the *Yes* button to confirm de-installation.

De-installation will now proceed. Stoplock will inform you that it is removing all of its components.

On de-installation, Stoplock automatically de-configures all fixed drives (the drive is returned to type 'Open'). All encrypted files are decrypted and the access control lists are deleted.

Your PC will then be rebooted in order to remove the Stoplock kernel from memory.

**THIS COMPLETES THE DE-INSTALLATION OF STOPLOCK.**

# Technical Support Fax Sheet

---

## Stoplock

---

Company Name	
Contact Name	
Telephone No.	
Fax No.	
E Mail	

Product Version			
Priority of Call	Urgent <input type="checkbox"/>	Moderate <input type="checkbox"/>	General Enquiry <input type="checkbox"/>
Make of PC			

<b>Description of Problem</b>         
---

**For PCSL Use Only**

---

Support Ref No.	
Assigned	
Date Closed	



PCSL, Windsor House, Spittal Street, Marlow, Bucks, UK, SL7 3HJ  
 Tel: +44 (0)1628 890390 Fax +44 (0)1628 481342 Web : <http://www.pcsl.com>

---

