

Contents

Installation Configuration

[Installing with Predefined Defaults](#)

[Master Encryption Key](#)

[Encryption](#)

[Users](#)

System & User Configuration

[Password](#)

[Logon](#)

[SoftHold](#)

[System Access](#)

[Encryption](#)

[Users](#)

[Saving configuration as Predefined Defaults](#)

Using Stoplock

[Everyday Use](#)

[Managing the System](#)

[Troubleshooting](#)

Information

[Contacting PCSL](#)

[De-installing Stoplock](#)

Loading Predefined Defaults

Check the 'Load Predefined Defaults' box if you have saved Predefined Defaults from a previous installation and wish to use them on installation of Stoplock.

If this box is checked then on selecting **Next** the Predefined Defaults Folder dialog box is displayed which requires you to enter the pathname and folder containing the backed-up configuration files.

Once you have selected the folder containing these files you are required to enter the password that was used to create them. On supplying the correct password and then selecting the **OK** button, the Predefined Defaults files will be copied across.

Note: The PC is returned to 'Guest' mode after using this option and exiting from the Setup Wizard. Remember to logon as a user who was current at the time of creating the Predefined Default files.

Saving Predefined Defaults

Use Predefined Defaults to save your system and user settings for use at installation time on other PCs.

Two files are created, }~sb and }~ub, containing all the System Configuration and User information. The MEK is also stored within these files and is therefore not requested at installation time. Note however that encryption configuration information specified on the Encryption window is not stored in these files with the exception of the 'SHARED' group and key (if any).

Predefined Defaults folder

Type in the folder path and name or use the **Browse** button to specify where you wish to store the Predefined Default files.

On selection of the **Save Defaults** button a dialog box will appear requesting you to enter a password of up to 8 characters. This password is case sensitive and will be used to encrypt the information stored in the created files. Duplicate this password in the **Retype password** field.

The password entered here will be requested at installation time if you decide to install using Predefined Defaults.

Note: Predefined Default files may only be used at installation time. When using Predefined Defaults, you must know the ID and password of an administrator which was current at the time when the Predefined Default files were created, in order to log on.

Master Encryption Key

The Master Encryption Key (MEK) is used for the encryption of Stoplock system files and is only ever entered at installation time.

Although you will not be asked to type in the MEK anywhere else on this PC, you should write it down and store it in a safe place. You will need to repeat the MEK when installing Stoplock on other PCs, in order to provide support for the Remote Password Change function.

The MEK is up to 16 characters long, is case sensitive, and can consist of any alphanumeric characters. You are asked to type the MEK twice to verify it.

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 required](#)

[Use Personal keys only](#)

[Use both Personal keys and a Shared key](#)

Note the following:

- The **Shared Key** and **Retype shared key** fields are grayed-out if you do not select the 'Use both Personal keys and a Shared key' option.
- If you had previously specified the 'Use both Personal keys and a Shared key' option and then select the 'Use Personal keys only' option, the user's group membership and the 'SHARED' group will automatically be removed.

No encryption required

This option is self-explanatory.

If encryption had previously been selected then use of this option will cause drive C to be de-configured (i.e. any encrypted files will be decrypted).

Use Personal keys only

Files are encrypted using a key that is specific to each user.

If you select this option then drive C is automatically configured at the end of configuration so that you can apply encryption to files. You can select the appropriate files and the personal (user) key they are encrypted under by using the File Encryption & Utilities program.

Use both Personal keys and a Shared key

Files may be encrypted under keys specific to each user and under a key which is specific to members of the 'SHARED' group. If you select this option, a group called 'SHARED' is automatically created. Group membership may be specified when adding or editing a user.

If you select this option then drive C is automatically configured at the end of configuration so that you can apply encryption to files. You can select the appropriate files and the encryption keys by using the File Encryption & Utilities program which also enables you to configure other fixed drives available on the PC.

Shared Key

Here you can specify an encryption key to be used for any files encrypted under the group 'SHARED'. Once this key is specified it may not be changed. This key must be between 1 and 8 characters in length and is case sensitive. Verify this key in the **Retype shared key** field.

Note: If you want to export encrypted files or intend to upgrade to Stoplock 95 Central Administrator in the future, then make sure all PCs are allocated the same key for the 'SHARED' group. If you install subsequent PCs with Predefined Defaults then this will automatically occur.

Users

You may define security requirements for up to 32,000 users for a single PC. Each user has a profile containing security parameters specific to that person and has as its key the user's ID.

Non-administrators do not have access to the Stoplock administration programs; they can only log on, log off, invoke SoftHold and change their passwords.

Users of type 'Guest' and 'FM' are set-up by default to make use of 'automatic guest' mode, logon, logoff and the remote password change function.

[Adding Users](#)

[Editing Users](#)

[Deleting Users](#)

Adding Users

To add a user, complete the fields on the window. Selection of the **Add User** or **OK** button adds the user to Stoplock.

[Profile](#)

[Password](#)

[Personal Encryption Key](#)

[Group Membership](#)

Profile

User ID (Name)

Type in a name for the user, as a string of between 3 and 12 alphanumeric characters (hyphens and underscore characters are also supported). The user will enter this name when they logon to Stoplock. Each user name you add to Stoplock must be unique.

User Type

Use this field to specify the basic capabilities and functions of the user. Select a value from the pull-down list:

Standard

The default setting, for non-administrators. The majority of users that you set up on the PC will use this setting.

SSA

System Security Administrator - the person responsible for setting up and maintaining Stoplock. Each PC must have at least one administrator in its user base. You may set up more than one administrator if you require.

Temporary

A temporary user has similar privileges to a standard user but has a password with a finite life, independent of the system-wide expiration. When this password expires the user obtains inactive status and can no longer log on. You can reactivate the user with a new password when necessary.

Status

This can be **Active** (the default) or **Inactive**. On adding a user, the status is always **Active** and this can only be changed when you next edit the user. Inactive users cannot log on, but can be re-activated at any time. If a user is sick or on vacation, use this field to protect their access while they are away.

Note: Setting a 'guest' user to inactive status does not prevent 'auto guest' mode being entered after automatic logon or use of logoff. What it does prevent is anyone from manually logging on using the guest user name.

Days Remaining

This tells you how many days the user has remaining before their password expires: depending on the units set on the Password window. You can only enter a value in this field for a user of type 'Temporary'.

Note: Once a user has logged on for the first time, the value that is displayed here will be the lifetime figure set on the Password window.

Force change ID on first logon

If this box is checked then the user must change his/her user ID when he/she first logs on. This option is only active when a user is first added to the system - i.e. a first logon since password change is not affected by this option. This option is not available for users of type 'FM', 'Guest' or 'Temporary'.

Do not select this option if you have files already encrypted under a user's personal key. If the user changes his/her name on their first logon then the encrypted data would no longer be readable.

User Password

New Password and Retype Password

Use these fields to enter and verify the user's password. You must do this when you add a new user although you can also set a new password for existing users.

You cannot display a current password. The password you set here expires immediately, forcing the user to change it as soon as they log on.

The minimum length of passwords are specified on the Password window of the System & User Configuration program. The maximum password length is 16.

[Password Rules](#)

Password Rules

The following rules apply for passwords:

- Passwords are case insensitive (Password, PassWord and PASSWORD are all recognized as the same string).
- The last three passwords may not be used.
- Standard users or administrators can change their passwords at any time.
- Users of type 'Guest', 'FM' or 'Temporary' cannot change their passwords.
- Passwords do not expire for users of type 'Guest' or 'FM'.
- Users can cancel out of a voluntary password change.
- Users are required to provide their old password when voluntarily changing their passwords.
- Users are forced to change their passwords once they expire. If they do not, they will attain inactive status.
- Users who reboot the PC on a forced password change (i.e. their password has expired) will be deactivated.
- Nobody, including the administrator, can display an existing password but an administrator can provide a new password to replace one which a user has forgotten.

Personal Encryption Key

Here you can specify an encryption key to be used for any files encrypted at user level (i.e. specific to the user). Each user must be allocated an encryption key regardless of whether you have specified to use encryption. Once this key has been entered it may not be changed.

This key must be between 1 and 8 characters in length and is case sensitive. Verify this key in the **Retype Key** field.

Group Membership

Check this box in order to make the user a member of the group 'SHARED'. All users that you make a member of this group will be able to access data encrypted under the shared key.

Uncheck the box if you wish to remove the user from the 'SHARED' group.

Note: The Group Membership dialog is grayed-out if you have not selected the 'Use both Personal keys and a Shared key' option on the Encryption window.

Editing Users

Use the pull-down **User ID** field to select a user name in order to update security details for an existing user. You may change the user name if necessary but make sure there is no data currently encrypted under this user's key. Once you have modified a user's profile, select the **Modify User** or **OK** button to save the changes.

The following users are already set-up on the PC and may not be deleted. Both these user types relate to a function rather than a person:

FM

Field Manager. This user may occasionally be used on a PC at a remote site, for the purposes of resetting a forgotten password - no other access to the system is allowed.

Guest

This user type allows you to make use of 'auto guest' mode, logon and logoff. SoftHold is not available when a user of type 'Guest' is logged on.

When editing users, note the following:

- Users of type 'Guest' and 'FM' are not present at installation time. Their profiles can only be edited once installation is completed.
- If the user is of type 'Guest' or 'FM', you may only change their password and status. Group membership is not available for these users.
- **Personal Encryption Key** is grayed-out for all users as once this key has been specified it cannot be changed.
- **Force change ID on First Logon** will be grayed-out if the user has already logged on to Stoplock.

Deleting Users

Use the pull-down **User ID** field to select a user name. Select the **Delete User** button in order to delete the user.

Password

A password has a limited life (configurable), a minimum length (configurable) and is defined in terms of days. Passwords are case insensitive and the last three passwords may not be used in rotation. See also [Password Rules](#)

Password Settings

- **Minimum Length**

Enter an integer that defines the minimum length of user passwords - you can use the spin buttons beside this field to increment and decrement the current value if you prefer. The default is 6, and you cannot choose a minimum value less than 4.

If users try to create passwords of less than the specified length, they will be asked to retype them. The maximum password length is 16 characters, and cannot be changed.

- **Life Time**

Every password has a finite life and its expiration is controlled by the value you set here. Enter an integer that defines password life - you can use the spin buttons beside this field to increment and decrement the current value if you prefer.

The password will expire after the specified number of days, regardless of how often it has been used. The default is 250 days. A 'change password' message is automatically displayed when 2 days remain to remind the user to change his/her password.

Password Controls

- **Force Alpha Numeric**

If you check this box then passwords must contain at least one number and one letter.

- **Must Contain at Least n Unique Characters**

If you check this box then passwords must contain at least n number of unique characters. Use the spin buttons to specify the value or type in the appropriate number. The minimum value for this field is 2 and the maximum value is 12.

Logon

Use the Logon window to specify parameters that control how users log on. The logon screen that is presented when a user logs on will display the default bitmap specified within [WLOGON.INI](#).

Logon Restrictions

Here you can control the necessary requirements for logging on.

- **Invalid logons before lockout**
Enter a number between 1 and 250 (use the spin buttons or directly type in a number); the default is 3. If a user fails to logon correctly in this number of attempts, the system will lock.
- **Lock out length in minutes**
Enter a number between 1 and 250: (use the spin buttons or directly type in a number) the default is 1. If a user fails to logon correctly in the specified number of attempts, the system will lock for this length of time, and the user will have to wait before trying again.
Lock out cannot be circumvented by rebooting the PC - the system timer restarts the lock out count if this happens.

Note: The **Invalid Logon** and **Lock-out length** Logon Restriction options also apply to password entry when clearing SoftHold.

General

- **Automatic Guest Logon**
If you check this box Stoplock does not display a logon box at boot time. Instead, the user of type 'Guest' is automatically logged on. This mode of operation is termed 'auto guest' mode.
Users can still logon to Stoplock manually by performing a normal logon.
- **Disable user account after n days of inactivity**
Enter a value within this field (use the spin buttons or directly type in a number). If a user fails to logon to Stoplock within the number of days specified here, then their account will be disabled and they will no longer be able to log on. The user account must then be reactivated by an administrator. The default value is 0 and the maximum value is 250. **If this field is left at 0 then user accounts will never be disabled.**
Note: Only users of type 'standard' are affected by the settings in this field.

SoftHold

SoftHold is a secure screen blanker and is used when the system is left unattended to prevent unauthorized use and viewing of data. In the SoftHold state the screen is blanked out and the PC will not respond until the user's password has been correctly typed on the keyboard.

An **Admin Logon** button is displayed on the SoftHold dialog box allowing an administrator to logon to Stoplock and terminate SoftHold. If the PC is rebooted whilst SoftHold is active, the SoftHold state will be re-entered when Windows 95 is loaded. Whilst in the SoftHold state, background processing will still proceed, allowing processes such as backup programs to continue whilst SoftHold is invoked.

By default SoftHold is enabled as the passive action i.e. after a period of keyboard and mouse inactivity, but you may choose to specify no action at all.

Passive Action

Use the Passive Action area to specify how the system is to behave if it is left unattended by selecting the appropriate radio button.

- **SoftHold**
All functions are inaccessible until the user has correctly supplied his/her password. The screen display will default to the option selected within **Screen Options**. On moving the mouse or pressing any key, the SoftHold dialog box will be displayed.
Only so many invalid attempts to terminate SoftHold are allowed depending on the value you set for **Invalid logons before lock out** on the Logon window.
- **None**
No action is taken - the PC will never enter a passive state.
- **Minutes before action**
Enter an integer that specifies how long an interval of inactivity will pass before SoftHold is activated. Use the spin buttons to adjust the current number, or type it in directly. The default is 5 minutes.

Screen Options

Select the appropriate radio button in order to determine the screen display when SoftHold is invoked.

- **Bitmap**
If you select this option then the screen will display the default bitmap specified within [WLOGON.INI](#).
- **Screen Saver**
If you select this option then the screen will display your Windows 95 screen saver. Obviously, a Windows 95 screen saver must be currently in use in order for this option to take affect. If a screen saver is not currently in use then the display will show no visible change at all.
This option is selected by default if Stoplock detects a Windows 95 screen saver running on installation.

IMPORTANT NOTE: If you select **Bitmap** as the screen option then you must turn your Windows 95 screen saver off to prevent it from interfering with SoftHold. If you select **Screen Saver** as the screen option, then set your Windows 95 screen saver wait time to 60 minutes.

Note also that with either of these screen options, the SoftHold dialog box will not be displayed until a key has been pressed or mouse movement has occurred.

System Access

Use the System Access window to specify users rights of access to the floppy drive and the COM/LPT ports. By default, full access is given to the floppy drive and COM/LPT ports.

Floppy Drive Access

Select the appropriate radio button in order to determine user access to the floppy drive.

- **Full Access**
No restrictions are applied to the floppy drive - it may be used as normal.
- **No Access**
All access to the floppy drive is prevented.
- **No Execute**
Users will not be able to execute programs off the floppy drive.

Note: The **No Execute** option does not prevent users from copying files to the fixed drive and then executing them: you should also configure the hard disk and run the [ANTIV script](#) provided with Stoplock. This will stop users from executing programs that they copy to the hard disk.

Device Access

Specify user rights of access to the COM/LPT ports by checking/unchecking the boxes beside the port names.

Note: Settings on the System Access window apply to all users apart from administrators. Administrators are given full access to the floppy drive and COM/LPT ports.

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.

WLOGON.INI

This file is automatically created in the SLV95 folder by the SLWIN32 program. It is used to contain values relating to the logon, SoftHold and password change processes.

LogonBackGround

This section of WLOGON.INI controls the appearance of the area surrounding the Logon and SoftHold boxes.

Specify **Bitmap=** to display a bitmap image when Logon or SoftHold is invoked. You must enter here the path to a .bmp file. The default bitmap is SLV95.bmp which is located in the SLV95 folder.

LOGON

This section of WLOGON.INI controls the appearance of the Logon, SoftHold and Change Password boxes.

LASTID= is not something you need to specify: Stoplock uses this field to hold the name of the last user who logged on.

Specify **Title=** to change the Logon, SoftHold and Password Change box title from Stoplock to Notebooks to one of your choice.

DialogPosition

You may add this section to WLOGON.INI in order to control the screen position of the Logon, SoftHold and Change Password boxes. By default these boxes appear in the center of the screen.

There is nothing to stop you dragging any of these boxes to a new screen position, but it is the settings within this file that will be used the next time the dialog box appears.

Note: If you change any of the options within WLOGON.INI, you must reboot the PC for these changes to take effect. Selecting 'Close all programs and log on as a different user' from the Windows 95 Shut-Down menu will also have the desired affect.

Everyday Use

[Stoplock Icons](#)

[Logon & Logoff](#)

[Password Change](#)

[Using SoftHold](#)

[Illegal Access](#)

Stoplock Icons



Double-click this icon to start the Stoplock File Encryption & Utilities program. This program enables you to apply file encryption to folders and files, view, export and print the audit trail, and remotely set user's passwords.

Only administrators can use this program.



Double-click this icon to start the Stoplock System and User Configuration program. This program enables you to set system and user configuration settings, specify whether you wish to use encryption and save settings to Predefined Default files for use at installation time.

Only administrators can use this program.



This icon is located on the right of the Task Bar.

Left-click this icon to invoke SoftHold.

Right-click this icon to bring up a menu from which you can Logon, Logoff (returns the system to 'Guest' mode), invoke SoftHold or Change Password. Select the appropriate option and then click either mouse button.



Double-click this icon to view any last minute changes to the product.

Logon & Logoff

Logon

Before any person can use a PC protected by Stoplock they must normally log on. This serves two main purposes:

- It allows only authorized users to use the PC
- It restricts each user to those resources to which he/she is authorized to use


Logon can take place without the user seeing the Stoplock logon screen at boot time however if Automatic Guest Logon is selected on the Logon window of the System & User Configuration program. A user of type 'Guest' is automatically logged on.

Logon would normally proceed like this:

1. The logon screen is displayed. This is a box entitled AUTHORIZED USERS ONLY that asks for a user ID (name) and password.
2. If the name and password are found to be correct, then logon proceeds.

What happens behind the scenes is that the user name is used as a key to read a user profile from the file. If no profile is found, the name is considered invalid. If there is a user profile, then logon can only proceed if the password matches and the status is Active.

Logon Box

To display the logon box, right-click the  icon (located on the Task Bar) and then select Logon from the resulting pop-up menu.

The logon box requires a user to identify him/herself by providing a User ID and Password. The R key may be used if a mistake has been made in entering an ID or password in order to clear the fields.

Selection of the **OK** button completes logon.

The logon box is usually displayed in the center of the screen, the remaining area being covered with a bitmap image. You may edit [WLOGON.INI](#) in order to change the bitmap, position of the logon box, and title text.

A User's First Logon

When a user first logs on to Stoplock, he/she is presented with the normal logon box. Pressing **OK** or the **Change password** button will cause the Change Password dialog box to appear, inviting the user to change his/her password.

If the **Force Change ID on First Logon** option had been taken when the user was first added to Stoplock, then the user must also change his/her ID (name). On pressing **OK**, the new user ID and Password will be accepted providing the criteria set on the Password window of the System & User Configuration program is met. When the user logs on to Stoplock using this ID, a password change will be required. This is because this will be the first logon with the new user ID.

Note: When an administrator changes a user's password, this resets the user's password expiration count. Therefore, the next time the user logs on, the First Logon dialog box will be displayed.

Logon Box Rules

These rules apply whenever a user enters data at the logon box:

- Passwords are never displayed: only asterisks are shown as you type.
- User Names (User ID) and Passwords are case insensitive.

Automatic Logon

Auto guest mode is the condition in which users have access to the PC without having to log on - thus the PC is protected without users being aware of it. If it is implemented it can be regarded as the default state for the PC, representing a kind of lowest common denominator in security terms.

Guest mode will be entered:

- When an automatic logon takes place
- When logon or logoff takes place

If **Automatic Guest Logon** has been specified on the Logon window of the System & User Configuration program then during boot-up automatic logon will take place. Users requiring a greater level of access to files can still logon as individuals in the usual way.

Logoff

A user has these options at the end of a session:

- He/she can execute Logon and leave the PC at the logon box, inviting a new user to logon.
- He/she can execute Logoff thus leaving the PC in 'guest' mode. Anyone can use the PC without the need to log on but they will be subject to the limitations imposed for the 'guest' user.

Password Change


Password Expiration

This password expiration message box is displayed two days before password expiration. It displays the last logon information and informs the user about his/her remaining password life.

The user may change his/her password via the **Change Password** button if he/she so wishes. Selecting the **OK** button or pressing Q will complete logon.

Note: The Password Expiration message box is not displayed if a user is of type 'Guest' or 'FM'.

Password Change

Passwords may be changed at any time via the  icon (located on the Task Bar). Right-click this icon and then select Change password from the resulting pop-up menu. The user is required to enter his/her old password in this dialog box before password change can occur.

Note: The password change dialog box is only displayed if a user voluntarily changes his/her password. An old password is not required if it is a forced password change (i.e. the password had expired).

When an administrator sets up a new user or changes a user's password within their profile, the user will be prompted to change this password at logon - this is a forced password change. If the user decides to reboot the PC at this stage then they will become deactivated (USER DEACTIVATED message is displayed) and will have to be reactivated by an administrator before they can logon again.

On supplying a new password the user is required to enter this twice to guard against mis-typing. If the passwords do not match the message 'PASSWORDS DO NOT MATCH' is displayed. The last three passwords may not be used and the password length must be equal or greater to that defined on the Password window of the System & User Configuration program. If either of these two conditions are not satisfied then the message 'PASSWORD IS ILLEGAL. PLEASE RE-ENTER' is displayed.

Note: Password change is not available for users of type 'Guest', 'FM' or 'Temporary'.

When changing a password, the **Cancel** button may or may not be available depending on the circumstances:


1. If the password had expired then the **Cancel** button is grayed-out.
2. If a voluntary password was initiated but the user changed his/her mind about doing so, then the user may select the **Cancel** button or use the D key to terminate password change, thus retaining his/her existing password.

Using SoftHold

Note that you can edit [WLOGON.INI](#) in order to change the title text of the SoftHold box, screen position and bitmap.

Invoking

SoftHold can be invoked either by:

- Clicking on the  icon (located on the Task Bar). Either left-click this icon, or right-click this icon and then select **SoftHold** from the resulting pop-up menu.
- If the passive condition specifies SoftHold, then when that condition occurs SoftHold state is entered immediately.

When SoftHold is invoked, the display may be one of the following, depending on the options taken on the SoftHold window of the System & User Configuration program:

- If the **Bitmap** option has been selected then the screen is covered by the bitmap specified within WLOGON.INI.
- If the **Screen Saver** option has been selected then the screen is covered by the chosen screen saver.
- If the **Screen Saver** option has been selected but no screen saver is currently active then the screen shows no visible change at all.

Pressing any key or moving the mouse will cause the SoftHold dialog box to be displayed in the center of the screen. The dialog box will disappear automatically after 30 seconds. Alternatively, it can be removed by selecting the *Cancel* button or pressing the **D** key. Pressing any key or moving the mouse will restore the SoftHold dialog box again.

Admin Logon button

The **Admin Logon** button displayed within the SoftHold dialog box enables an administrator to logon when SoftHold is invoked.

Note that when an administrator logs on, current applications are not shut-down. This has implications on any work that is currently visible within that application - administrators will still be able to see any open data. However, file access rights of the new user will take affect, meaning that unopened files encrypted under a user's personal key may not be read.

Terminating

Terminating the SoftHold state occurs when the user types in his/her password correctly. If the correct password is not entered an error message 'PASSWORD IS INCORRECT' will be displayed. The number of attempts permitted, and the duration of the lock-out which results by exceeding that number, are regulated in the same way as at logon.

If lock-out does occur, the 'SYSTEM TEMPORARILY LOCKED - PLEASE WAIT' message appears. The SoftHold dialog box is re-displayed on completion of lock-out. Once the password has been correctly entered, SoftHold is terminated.

SoftHold Protection

The SoftHold program is automatically protected against possible tampering. The SoftHold program, SLWIN32.EXE, should be permanently loaded. However, unless SoftHold or Logon is currently active, SLWIN32 may be shut-down by using Windows 95 CTRL-ALT-DEL function. If Stoplock fails to detect the SoftHold program at any time, it will attempt to reload SLWIN32. If this fails, the PC will become locked.

Resume Mode Support

Toshiba and Panasonic laptops support a feature known as 'resume mode'. This allows a user to power down the PC in such a way that the entire working environment is automatically restored when it is powered up again. If resume mode is entered for more than 2 minutes under Windows, SoftHold is invoked within 10 seconds of the PC being switched on again.

Full Screen DOS box

If you make use of a full screen exclusive DOS box in Windows 95, SoftHold occurs on exit from the box.

Guest Users

NOTE THAT SOFTHOLD DOES NOT OCCUR IN 'GUEST' MODE.

Guest users cannot invoke SoftHold. SoftHold options selected on the SoftHold window of the System & User Configuration program are irrelevant for a user of type 'Guest' - i.e. no passive action occurs in 'guest' mode.

Illegal Access

When a user, whether by accident or design, attempts to access an unauthorized resource, the system's response will depend on the application he/she is in. This might mean that the user receives an informative message, an obscure message, or no message at all. Very often, the application reacts as though the file, drive or other resource simply does not exist. All attempts at illegal access are logged to the audit trail.

Managing the System

[User Administration](#)

[Backups](#)

[Deletion of Encrypted Files](#)

[Changing the Master Encryption Key](#)

User Administration

Administrators

An administrator must have access to each PC in order to monitor and maintain it. It is not possible to have a PC which does not have an active administrator in its user base.

Field Managers (FM)

Field Managers are used for the sole purpose of remotely resetting a user's password. A user of type 'FM' is already set-up on the PC specifically for this purpose 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.

Standard Users

Standard users normally constitute the bulk of the user base for PCs that are shared within a department or company. All standard users must be told:

- How to log on, including what to do if they fail
- How and when to change their passwords, how long the passwords must be, how many changes they must make to passwords before they can re-use them and other password controls that may have been set
- How to handle SoftHold, if implemented
- How Stoplock will affect their access to drives, folders, and files
- How to handle any problems that may arise (such as forgotten passwords) and who to contact for help (you and your deputies)
- How to log off cleanly, leaving the system ready for another user
- Windows 95 options that are no longer accessible - Boot Menu, Safe mode

Temporary Users

A temporary user has similar privileges to a standard user but his/her password has a finite life. If one or more users will only be working on a PC for a short period, you can set them up as temporary users, with password expiration periods that will cover the period in which they are going to use the PC.

When they move on you can delete or deactivate their profiles. Otherwise, if their working period is extended or made permanent, you can extend their passwords, or create new standard profiles for them.

Guest Users

A guest user ID represents a function rather than an individual and is used during logon and logoff and automatic guest logon. A guest user is already set up on the PC and cannot be deleted.

You can also use the guest user ID if you want to have a user ID available for general use.

If you wish to perform a manual logon with the 'Guest' user name then note the password for this user is 123456. You may leave this password as it stands or edit the guest user profile and change it accordingly.

Since you can expect all kinds of people to be able to log on as the guest user you should make sure sensitive data is encrypted.

Be aware however that the guest user ID is used during bootup so be careful when encrypting particular files.

Note: You can de-activate the guest user if you don't want anyone manually logging on using the guest user name. De-activating the guest user does not affect the use of 'Auto Guest' Mode or the Logon/Logoff functions.

Deactivating Users

You can deactivate users temporarily (when users are on vacation or are off sick) and permanently (when they leave). An inactive user cannot log on to the PC, but their profile remains intact and can be activated at any time.

Backups

When backing up files using either a logical backup program or just copying, the following rules apply:

- Users (including administrators) may only backup files which are encrypted under their personal key or the shared key (if they are a member of the 'SHARED' group).
- Files copied to a 'configured drive' remain encrypted.
- Files copied to an 'open' drive are decrypted.

A physical backup takes an exact copy of your hard disk and therefore takes no notice of encryption restrictions on individual files. All files are backed up and encrypted files remain encrypted in the backup.

Predefined Defaults

Predefined Defaults can be used to backup Stoplock configuration files. These files store system configuration information, }~s, and user configuration information, }~u. Use Predefined Defaults for installing Stoplock on multiple PCs. Predefined Defaults can only be used at installation time.

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.

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.

Changing the Master Encryption Key

It is strongly recommended that you give all PCs within an organization the same Master Encryption Key (MEK). The remote password change facility cannot be used if two PCs do not share the same MEK.

Stoplock requires complete de-installation and re-installation in order to change the MEK. You cannot use any of the usual short cuts because the MEK is used to encrypt parts of stored security information in almost all of the Stoplock files, including the user base and system parameters.

When you have finished you will be back where you started, but with the required MEK.

Note: Predefined Defaults taken before the change should be discarded.

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

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.

[System Locked](#)

[Invalid Logon Attempt](#)

[Restricted Logon](#)

[User De-activated](#)

[De-installation](#)

[Password Loss](#)

[File Recovery](#)

[Virus Checkers](#)

[Installing Extended Boot Protection](#)

[EBP Error Messages](#)

System Locked

Question

The system has locked up when the wrong password was entered, and rebooting the machine does not clear it.

Answer

Leave the machine switched on but untouched for the lockout period - this is whatever value is set in 'Logon Restrictions' on the Logon window. The default is one minute.

Reason

If you reboot your PC before the system has been released the timeout count will start again at zero.

Invalid Logon Attempt

Question

When I logon, the message 'INVALID LOGON ATTEMPT' is displayed.

Answer

Logon attempts can be rejected for a variety of reasons.

Reason

Here are some of the more common reasons for rejection:

- The user name given does not match any user profile.
- The password given does not match that in the user profile.
- The user name given is that for a non-administrator, but logon has been restricted to administrators only, due to file corruption or system clock changes.

Whatever the reason, there is usually a limit to the number of invalid logon attempts tolerated before the PC locks up and waits for a period of time before inviting further attempts. The message 'SYSTEM TEMPORARILY LOCKED - PLEASE WAIT' is displayed at this point.

Restricted Logon

Question

The normal logon screen has been replaced by one entitled 'ADMINISTRATOR LOGON ONLY'.

Answer

Logon could be restricted for a variety of reasons.

Reason

Here are some of the more common reasons:

- If a Stoplock file is found to be corrupt (but not so much so that logon is blocked completely).
- If the system clock is found to have been put back such that it affects the system date.

Logon proceeds as in the normal case, except of course that an attempt by a non-administrator to log on is rejected.

User De-activated

Question

A user has been deactivated when his or her status was originally active - why ?

Answer 1

The user rebooted instead of changing his or her password when prompted. The user must be reactivated by an administrator.

Answer 2

The user is a 'Temporary' user and his/her password has expired.

Reason 1

The password had expired and was not changed at the last opportunity. Stoplock de-activates the user account in order to enforce the password policy.

Reason 2

Temporary users are automatically de-activated once their passwords expire.

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.

Password Loss

You can reset users' passwords directly on a PC at any time by changing the password in their profile. You can also change a user's password at a remote site where there is no administrator, by using the Field Administration Remote Password Change function.

Installing Extended Boot Protection

Question

When I install Extended Boot Protection (EBP) I get the error message 'An Error was detected while writing to the first sector of your hard disk'.

Answer

Check that no virus checker is running. If it is, REM it out, then re-run the Stoplock installation program. If the problem persists then check that there is no Anti-Virus option enabled in the BIOS. Again, if there is, disable it until EBP has been installed.

Reason

When you install Extended Boot Protection, it writes to the boot sector of the hard disk. Any anti-virus product will believe that the system is under attack, and act accordingly to prevent the changes from being written to the drive.

Virus Checkers

Question

I installed Extended Boot Protection and my anti-virus program asks me if I want to restore the original boot block.

Answer

DO NOT restore the original boot block!! Accept the new one.

Reason

Extended Boot Protection modifies the boot block.

EBP Error Messages

Error Screen

This screen is displayed when an error has occurred. For example:

****** ERROR ******

Stoplock Extended Boot Protection is already active.

You are running the program while EBP is active. EBP should not be active, since you should have booted from a floppy disk.

Error 0003 writing to sector <0000,00,01>

An anti-virus monitor is active either in memory or in BIOS and is preventing access to parts of the hard disk.

Installation

If Extended Boot Protection is already installed but **not** active the message displayed is:

EBP of active partition has the wrong format

This occurs because you are trying to install Extended Boot Protection where it already exists or your PC has a configuration error.

If EBP is not compatible with your PC an error message will appear informing you to contact the PCSL Help Desk for upgrade information.

Unable to determine the geometry of your hard disk

Your hard disk is accessed using a non-standard disk BIOS extension and it is not possible to determine the geometry of the disk.

PCSL recommend you continue only if you have a compatible SCSI hard disk. Contact the PCSL Help Desk for assistance.

Re-Configuration & De-installation

If either of the EBPCONF or UNPROT programs are run when Extended Boot Protection is not installed the error message displayed is:

Stoplock Extended Boot Protection is not installed on the hard disk

You are asked to enter the program password before you can use either of these programs. If the passwords match but an incorrect password was supplied then the error message displayed is:

Decrypted hard disk partition table has incorrect format. You are using an incompatible version of EBP or the wrong password

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. If you have installed Extended Boot protection you must remove it before de-installing Stoplock.
2. If you have installed the Stoplock Installation Toolkit, you must de-install it before de-installing Stoplock. De-install the Stoplock Installation Toolkit as per any other Windows 95 software (from the *Add/Remove Programs* option in Windows 95 Control Panel).
3. 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.
4. 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			

Description of Problem

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.pcsi.com>

