Stoplock
Administrator's Manual

Release 1

Revision 1.11

For information on any Stoplock product please contact us:

International Headquarters	PCSL Windsor House Spittal Street Marlow Bucks, UK SL7 3HJ Tel +44 (0)1628 890390 Fax +44 (0)1628 890116
Technical Support	Tel +44 (0)1628 890390 Fax +44 (0)1628 890116 E-mail - support@pcsl-europe.com

The Help Desk is open between the hours of 08:00 and 18:00 (GMT). You should have completed and returned to PCSL the registration card supplied with this product prior to requesting support. Support may only be provided if you have a valid maintenance agreement with PCSL. Please contact us for further details.

Internet Address	http://www.pcsl.com

Warranty Statement

The Licenser undertakes that, provided it is operated in accordance with the Licenser's instructions, the Program will perform in accordance with the Licenser's published specification and the Documentation existing at the date of delivery. The Licenser does not guarantee that the Program is free from minor errors not materially affecting such performance. The undertaking given in this Clause is in lieu of any condition or warranty express or implied by law as to the quality or fitness for any particular purpose of the Program.

This Program is subject to License conditions which are printed on the sealed envelope containing the Program disks. By opening the sealed envelope you have agreed to the conditions of the License. Alternatively this Program has been provided under a Corporate License Agreement in which case the terms of that Agreement apply.

All trademarks are recognized.
Copyright © 1998 PCSL

About this Manual

This manual is for use by administrators of Stoplock, who will be installing the product on PCs within an organization, or a department of an organization. Issues covered include installation, boot protection, use of the Stoplock Administration programs, system management, troubleshooting and de-installation.

Readers are expected to be experienced users who are familiar with Windows 95 applications, and will know most of the basic operations involved in handling windows, pull-down menus, icons, and using the mouse and pointer. Readers must be familiar with the work done on such PCs, and the sensitivity of the files they contain.

The text of this manual assumes that readers will be using mouse and pointer operations. Equivalent keyboard shortcuts are represented within the product in the normal way: by underlined letters in options, menu names, etc.

Warning boxes are used within the text to draw your attention to events that cannot be easily reversed, or that may take a long period to execute. If you are in doubt about performing any operation described here, please contact PCSL at the offices listed on the inside cover of this manual.

Conventions

To help you locate and interpret information easily, the Stoplock Administrator's Manual uses consistent visual clues and text formats.

Icon	Meaning
	Information Offers you advice/hints on using certain features
	Stop Do not proceed any further until you have read the accompanying warning
	Warning Not reading these instructions could result in damage to your system
	Enter Type in the command line text exactly as it is displayed here
	Arrow Highlights useful/important information

Text is also underlined or displayed in **BOLD** or *italics* to help highlight important information.

Contents

Chapter 1, Introduction

Stoplock 1-2
Environment 1-2
Files 1-2
The Programs 1-3
Encryption of Data 1-3
File Rights applied by Stoplock 1-4
Operational Overview 1-4

Chapter 2, Installation

Prerequisites 2-2
Documentation 2-2
Disk Drive Usage 2-2
ScanDisk 2-2
Before You Begin 2-2
Windows 95 Startup Disk 2-2
Installing Stoplock 2-3
Installation Configuration 2-4
Predefined Defaults 2-4
Master Encryption Key 2-6
Encryption 2-7
Users 2-9
Stoplock Icons 2-13
Upgrading Stoplock 2-14

Chapter 3, System & User Configuration Program

Introduction 3-2

Password 3-3
- Password Settings 3-3
- Password Controls 3-4

Logon 3-5
- Logon Restrictions 3-5
- General 3-6

SoftHold 3-7
- Passive Action 3-7
- Screen Options 3-8

System Access 3-9
- Floppy Drive Access 3-9
- Device Access 3-10

Encryption 3-11
- No Encryption 3-11
- Use Personal keys only 3-11
- Use both Personal keys & a Shared key 3-12
- Shared Key 3-12

Users 3-13
- Adding Users 3-14
- Editing Users 3-16
- Deleting Users 3-17

Predefined Defaults 3-18

Chapter 4, File Encryption & Utilities Program

Introduction 4-2
- The Resources Menu 4-3
- The Utilities Menu 4-4
- The Options Menu 4-4
- The View Menu 4-4
- The Windows Menu 4-5
- The Help Menu 4-5
- Dialog Boxes 4-5
- Selecting Items in List Boxes 4-5
- Double-Clicking Objects 4-5

Chapter 5, Configuring Drives, Folders & Files

File Manager 5-2
- Accessing File Manager 5-3
- File Manager Tool Bar 5-3
- File Manager Menu 5-4
- Options Menu 5-4
- List Control View 5-4

Configuring Drives 5-5
- Options 5-6
- Buttons 5-6

Factors Affecting Access 5-7

Protection of Files 5-7
- Windows 95 Files 5-7
- Other Files 5-7

Setting Security on a Configured Drive 5-8
- Applying Encryption to Files & Folders 5-9
- Encryption 5-10

Applying Execute Rights to Files 5-12

Chapter 6, Setting up & Using File Scripts

Introduction 6-2

Scripts 6-3
- Script Menus 6-3
- Building a Script 6-7
- Editing, Moving, Copying & Deleting Script Rules 6-11
- Modifying Script Rules 6-11
- Checking Scripts 6-11
- Running a Script 6-11
- The Result of Running a Script 6-12

ANTIV.SLS 6-13

EXECUTE.SLS 6-14

EXPORT.SLS 6-14

Chapter 7, Audit Trail & Field Administration Password Change

Audit Trail 7-2
Viewing the Audit Trail 7-2
The Auditing Menu 7-4
Copying the Audit Trail 7-6
Field Administration Password Change 7-6
Remote Password Change 7-7
Steps for the User to Follow 7-8

Chapter 8, Managing the System

Introduction 8-2
Logon 8-2
Logon Box 8-3
A Users First Logon 8-4
Logon box Rules 8-5
Automatic Logon 8-5
Invalid Logon Attempt 8-5
Restricted Logon 8-6
Windows Logoff 8-6
Passwords 8-7
Password Rules 8-7
Password Expiration Message Box 8-7
Password Change 8-8
Loss of Passwords 8-10
SoftHold 8-10
Invoking 8-11
Terminating 8-12
SoftHold Protection 8-12
Resume Mode Support 8-12
Full Screen DOS box 8-13
Guest Users 8-13

Chapter 8, Managing the System *(continued)*

User Administration 8-13
- Administrators (SSAs) 8-13
- Field Managers (FM) 8-13
- Standard Users 8-14
- Temporary Users 8-14
- Guest Users 8-14
- Auto Guest Mode 8-15
- Deactivating Users 8-15

Illegal Access 8-16

File Management 8-16
- Backups 8-16
- Predefined Defaults 8-16
- File Recovery
  - Case 1. Loss or damage to the Stoplock configuration file 8-17
  - Case 2. Loss or damage to the Stoplock user file 8-17
  - Case 3. File left encrypted with key of deleted user 8-17
  - Case 4. File left partially encrypted or decrypted 8-17
- Deletion of Encrypted files 8-18

Emergency De-installation 8-18
- Reinstallation 8-18

Handling Stoplock File Corruption 8-19

Changing the Master Encryption Key 8-20

Clock Changes 8-20

Chapter 9, De-installing Stoplock

Introduction 9-2

Before You Begin 9-2

The De-installation Process 9-3
- Starting Off 9-3
- De-installation 9-3
- Additional Considerations 9-3

Appendix A, Extended Boot Protection

For Safety A-2
Introduction A-3
Running the EBP Programs A-4
Passwords A-4
Installing EBP A-5
Program Password Entry Screen A-5
Boot Password Choice Screen A-6
Boot Password Entry Screen A-6
Select Encryption Screen A-6
Timeout Value Screen A-7
Timeout Value A-7
Encryption A-7
Boot Dialogue A-8
Reconfiguring EBP A-9
Program Password Entry Screen A-9
Re-configuration Screen A-9
De-installing EBP A-11
De-installation A-11
Program Password Entry Screen A-11
Decryption A-12
Protect Options A-12
Examples of use A-13

Appendix B, Installation Issues

Files Modified by Stoplock B-2
REGISTRY B-2
SYSTEM.INI B-2
IO.SYS B-2
MSDOS.SYS B-2
File Rights applied by Stoplock B-3
Booting Windows 95 in Safe Mode B-4

Appendix B, Installation Issues *(continued)*

NOKEY - Boot Keyboard Inhibitor B-4

Installation Script Support B-6

Extended System File Configuration B-9

Using the Exclusion List B-11

Checking the contents of the Exclusion List B-11

Installation Toolkit B-12

Appendix C, WLOGON.INI

WLOGON.INI C-2

Logon BackGround C-2

LOGON C-2

DialogPosition C-3

Appendix D, Troubleshooting

Introduction D-2

Installing Extended Boot Protection D-2

Virus Checkers D-3

System Locked D-3

Invalid Logon Attempt D-3

Restricted Logon D-4

User Deactivated D-4

De-installation D-4

EBP Error Messages D-5

Index

Access Control
Drive 3-9
factors affecting access 5-7
illegal 8-16
ANTIV.SLS 6-13
Audit Trail
copying 7-5
exporting 7-4
menu 7-4
printing 7-4
viewing 7-2
type 2-16
Automatic guest logon 3-6, 8-5, 8-15

Backups 8-16
Boot dialog A-8
Boot Protection A-2

Clock changes 8-20
Configured Drive
applying file & folder rights 5-9
setting security on 5-8, 5-10, 5-12
Configuring
drives 5-5, 5-6
logon 3-5
password 3-3
SoftHold 3-7
system access 3-3

De-activating users 8-15, D-4
De-configuring drives 3-11, 5-6, 6-9, 9-3
De-installation 9-2, D-5
emergency 8-18
Defaults
predefined 2-4, 3-18, 8-16
Device access 3-10
Drive types
No Execute 3-3
Configured 5-5
Open 5-5
Drives
configuring 5-5
de-configuring 3-11,5-6, 6-9, 9-3
fix drive 5-6
setting security 5-8
Drives *(continued)*
update drive 5-6

Emergency De-installation 8-18
Encryption 1-3, 2-7, 3-11, 5-6, 6-9
changing type 5-10
files 5-9
folder 5-9
keys 3-12, 5-11
options 5-11
Exclusion list B-11
EXECUTE.SLS 6-14
Execute rights 5-12
EXPORT.SLS 6-14
Extended Boot Protection A-2
configuring A-9
de-installing A-11
encryption A-7
error messages D-5
installing A-5, D-2
passwords A-4
protect options A-12
timeout value A-7
Extended System File Configuration B-9

Field Administration
password change 7-6
remote password change 7-7
steps for the user to follow 7-8
Field manager 3-16
File
copying 5-11
Encryption
description 1-3, 2-7, 3-11, 5-6, 6-9
deletion of encrypted files 8-18
personal key 3-16
shared key 3-16
Execute rights 5-12
Manager 5-2
list control view 5-4
menu 5-4
options menu 5-4
tool bar 5-3
Recovery 8-17
Scripts 6-2
Fix Drive 5-6

Group
encryption key 2-8, 3-12
membership 3-16
Guest user 3-16, 8-13

Illegal access 8-16
Installation 2-3
script support B-6
toolkit B-12
Invalid logon attempt D-3

Logon 8-2
admin logon 8-12
automatic guest 3-6
box 8-3
configuration 3-5
force change ID 2-11, 3-15
invalid 8-5, D-3
restrictions 3-5, 8-6
rules 8-5
user's first 8-4
Logoff 8-6

MainView Window 4-2
Master Encryption Key (MEK) 2-6
changing 8-20

NOKEY B-4

Options Menu 4-4

Passive Action
SoftHold 3-7, 8-10
Password
change 8-8
configuration 3-3
expiration 3-15, 8-7
loss of 8-10
remote password change 7-7
rules 8-7
Personal keys 2-7, 2-11, 3-11, 5-11
Predefined defaults 8-16
creation 3-18
installation with 2-4
Protection of files 5-7

Remote Password Change 7-7
Resources Menu 4-3
Restricted logon D-4

Scripts 6-3
building 6-7
menus 6-3
modifying 6-11
running 6-11
result of running 6-12
Shared key 2-8, 3-12, 5-11
SoftHold 8-10
configuring 3-7
invoking 8-11
protection against tampering 8-12
screen options 3-8
terminating 8-12
Stoplock
de-installation 9-3
environment 1-2
file corruption 8-19
file encryption & utilities program 4-2
files 1-2
files modified by B-2
file rights applied by B-3
icons 2-13
installation 2-3
operational overview 1-4
programs 1-2
system & user configuration program 3-2
upgrading 2-14
System access 3-9
System locked D-3
System Security Administrator 3-14, 8-13

Technical support ii
Temporary user 3-14
Troubleshooting D-2

Update drive 5-6
Users 2-9, 3-13
adding 2-10, 3-14
deactivating 8-15, D-4

Users *(continued)*
deleting 2-12, 3-16
editing 2-12, 3-16
encryption key 2-7, 2-11, 3-16
group membership 2-11, 3-16
password 2-11, 3-15
profile 2-10, 3-14
status 2-10, 3-14
types
corrupt 8-19
standard 2-10, 3-14, 8-14
SSA 2-10, 3-14, 8-13
Field Manager 3-16, 8-13
Guest 3-16, 8-14
Temporary 3-14, 8-14
Utilities menu 4-4

View Menu 4-4
Virus checkers D-3

Windows 95
safe mode A-3, B-4
screen saver B-3
startup disk 2-2
WLOGON.INI C-2